



Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (Loi sur l'e-ID, LeID)

Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull'Id-e, LIdE)

Stellungnahmen zum Vernehmlassungsverfahren

Prises de position suite à la procédure de consultation

Pareri della procedura di consultazione

KTN	Kantone / Cantons / Cantoni
P	In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell'Assemblea federale
VSGB	Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna
VW	Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national / associazioni mantello nazionali dell'economia
IK	Interessierte Kreise gemäss der Liste der Vernehmlassungsadressaten / Milieux intéressés selon la liste des destinataires consultés / Ambienti interessati secondo l'elenco dei destinatari della consultazione
WK	Weitere Kreise / Autres milieux / Altri ambienti

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon 062 835 12 40, Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

A-Post Plus
Bundesamt für Justiz
Bundesrain 20
3003 Bern

19. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassung

Sehr geehrte Damen und Herren

Die Kantonsregierungen wurden mit Schreiben vom 29. Juni 2022 zur Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) eingeladen. Der Regierungsrat des Kantons Aargau bedankt sich für diese Gelegenheit und nimmt wie folgt Stellung:

1. Grundsätzliche Beurteilung

Der Regierungsrat des Kantons Aargau unterstützt die Vorlage zum neuen E-ID-Gesetz. Er begrüsst die rasche Erarbeitung einer neuen Vorlage, die unter dem umfassenden Einbezug kantonaler wie privater Akteure erfolgt ist. Aus Sicht des Kantons Aargau ist die Schaffung einer einheitlichen staatlichen E-ID für die Schweiz unumgänglich, um zukunftsfähig zu bleiben und die Digitalisierung auch auf Ebene der öffentlichen Verwaltung voranzutreiben.

Der Regierungsrat des Kantons Aargau ist der Ansicht, dass den Vorbehalten, die im März 2021 zur Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste geführt haben, mit dem vorliegenden Entwurf in angemessener und nachvollziehbarer Weise Rechnung getragen wird. Ausdrücklich begrüsst werden insbesondere die folgenden Punkte:

- Im Gegensatz zur in der Volksabstimmung gescheiterten Vorlage sieht der neue Entwurf eine Ausstellung der E-ID durch eine staatliche Stelle vor. Auch die nötige Infrastruktur wird durch den Bund zur Verfügung gestellt.
- Die Grundsätze von Datensparsamkeit, dezentraler Datenspeicherung und "privacy by design" entsprechen wichtigen Anliegen der Bevölkerung. Die Schweiz orientiert sich damit auch an den Vorgaben der geplanten europäischen Gesetzgebung (elektronische IDentifizierungs-, Authentifizierungs- und Vertrauensdienste [eIDAS]-Verordnung).
- Die Vorlage berücksichtigt die Entwicklungen auf europäischer Ebene und ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um die Anerkennung der schweizerischen E-ID im Ausland beziehungsweise die Anerkennung ausländischer elektronischer Identitäten in der Schweiz zu erleichtern.
- Die Möglichkeit, die Vertrauensstruktur für das Ausstellen weiterer elektronischer Nachweise zu nutzen, und die kostenlose Ausstellung der E-ID für Privatpersonen ermöglichen eine schnellere Verbreitung und Akzeptanz der Infrastruktur.

Benutzerfreundlichkeit

Entscheidend für die künftige Verbreitung der E-ID und der Vertrauensinfrastruktur wird die Benutzerfreundlichkeit der entsprechenden Applikationen sein. Sie muss für alle Beteiligten möglichst unkompliziert und niederschwellig zugänglich und anwendbar sein. Unter anderem an diesem Punkt sind in der Vergangenheit Vorhaben wie die qualifizierte elektronische Signatur gescheitert. Der Benutzerfreundlichkeit wird somit bei der Ausarbeitung der bundesrätlichen Verordnung besondere Beachtung zu schenken sein.

Koordination mit Vollzugsträgern

Die Umsetzung des BGEID und insbesondere seiner Art. 8–9 verlangt nach umfassenden Massnahmen auf Ebene der Kantone und Gemeinden. Im erläuternden Bericht fehlen jedoch Ausführungen zur Notwendigkeit, die Umsetzung mit den Vollzugsträgern koordiniert zu planen. Auch werden keine Angaben gemacht zum Zeitbedarf für die Umsetzung in den Kantonen und Gemeinden (gemäss Art. 8 Vernehmlassungsverordnung [VIV]) sowie zum geplanten Zeitpunkt des Inkrafttretens. Der Regierungsrat des Kantons Aargau erwartet in der Botschaft des Bundesrats entsprechende Ausführungen. Eine koordinierte Umsetzung gemäss dem Arbeitspapier von Bund und Kantonen vom 28. Oktober 2015 ist an die Hand zu nehmen.

Haftung und Qualitätsstandards

Die E-ID wird zur Identifizierung in kantonalen elektronischen Diensten zur Anwendung kommen und kantonale Lösungen ersetzen. In der Vernehmlassungsvorlage und im erläuternden Bericht fehlen jedoch Ausführungen zum Umgang mit Haftungsansprüchen, sollten Fehler im System des Bundes zu Lücken in den kantonalen Anwendungen führen. Entsprechende Angaben mit Bezug zu anerkannten Qualitätsstandards (Standard eCH-0170) sind in der Botschaft zu ergänzen.

Vollmacht und gesetzliche Vertretung

Weder im Entwurf noch im erläuternden Bericht sind Hinweise zu finden auf die Abläufe in Zusammenhang mit Vollmachten und der gesetzlichen Vertretung. Gemäss Art. 4 und Art. 5 BGEID ist zur Ausstellung einer E-ID für Minderjährige bis 14 Jahre und Personen unter umfassender Beistandschaft das Einverständnis der gesetzlichen Vertretung nötig. Diese Altersgrenze ist nochmals zu überdenken, eine Harmonisierung mit Art. 5 Abs. 1 des Ausweisgesetzes (AwG) wäre wünschenswert. Es fehlen auch Aussagen zu späteren Vertretungs- und Delegationsmöglichkeiten in der Nutzung der E-ID oder in der Anwendung anderer Nachweise. Im Interesse einer einheitlichen Vollzugspraxis ist eine entsprechende Klärung in der Botschaft wichtig. Die Nutzung durch Minderjährige soll ohne allzu starke Einschränkungen möglich sein. Zugleich muss es den Eltern möglich sein, die Verwendung der E-ID durch ihre Kinder möglichst einfach einzustellen und zu kontrollieren. Die Verwendung der E-ID hat dagegen keinen Einfluss auf die rechtlichen Vorschriften der Handlungsfähigkeit, weshalb zur Vertretung im Rechtsverkehr keine neuen Vorschriften nötig sind.

2. Bemerkungen zu einzelnen Artikeln des BGEID

Art. 1

Gemäss Art. 1 Abs. 1 Bst. a wird im BGEID die Ausstellung einer E-ID an natürliche Personen geregelt. Der erläuternde Bericht (Seite 8 zu Art. 3) weist darauf hin, dass juristische Personen nicht Inhaber einer E-ID sein können. Die elektronischen Dienste der kantonalen Verwaltungen sollen aber auch juristischen Personen zur Verfügung stehen. Für eine einheitliche und flächendeckende Lösung wäre die Ausstellung eines vergleichbaren Elektronischen Ausweises gemäss Art. 12 ff. an juristische Personen durch den Bund deshalb zu begrüssen. Es ist zu prüfen, wie die Einbindung der juristischen Personen erfolgen soll, wobei auch die Zeichnungsberechtigung zu zweien und Wechsel der

Zeichnungsberechtigten zu berücksichtigen sind. Auch ist zu prüfen, ob die Regelung anderer elektronischer Ausweise nicht beim Zweck in Art. 1 Abs. 2 Erwähnung finden sollten.

Art. 2 (Form und Inhalt)

Es ist auszuführen, warum auf die Aufnahme des Heimatorts als Personenidentifizierungsmerkmal verzichtet wurde.

Art. 3 (Persönliche Voraussetzungen)

Art. 3 BGEID sieht vor, dass nur Personen mit geregelter Aufenthalt in der Schweiz eine E-ID beantragen können. Der Kreis der Personen, die mit kantonalen Verwaltungen interagieren, ist aber weiter gefasst. Zu denken ist unter anderem an Personen, die ohne geregelten Aufenthalt in der Schweiz wohnhaft sind ("Sans-Papiers") oder an Zweitwohnungsbesitzer. Es ist zumindest die Möglichkeit zu prüfen, für solche Fälle eine spezifische E-ID auszustellen. Da die Identität der betroffenen Personen nicht in jedem Fall eindeutig festzustellen sein wird, dürfte der Einsatzbereich einer solchen E-ID entsprechend beschränkt sein.

Gemäss dem erläuternden Bericht (Seite 9 zu Art. 3) sollen gesetzliche Einschränkungen in der Anwendung der E-ID möglich sein für Personen, deren Identität nicht verlässlich festgestellt werden konnte. Nicht deutlich wird aus dem Bericht, ob in solchen Fällen auf der E-ID ein entsprechender Vermerk angebracht wird. Ohne Vermerk kann keine Einschränkung der Verwendung gemacht werden. Ein kategorischer Ausschluss von Personen abhängig von ihrem Aufenthaltsstatus hätte keinen sachlichen Grund und wäre daher diskriminierend.

Es ist zu prüfen, ob die Information über die Verlässlichkeit in die Daten unter Art. 2 Abs. 3 aufgenommen werden kann oder ob dies Persönlichkeitsrechte verletzen würde. Andernfalls ist auf eine Einschränkung der Verwendung, wie der erläuternde Bericht sie vorsieht, zu verzichten.

Art. 5 (Widerruf)

Art. 5 Bst. d Ziff. 2 BGEID legt fest, dass die E-ID widerrufen wird, wenn das Bundesamt für Polizei (fedpol) über eine Änderung der Personenidentifizierungsdaten der Inhaberin oder des Inhabers informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen müssen sich dann nicht noch einmal um die Ausstellung einer neuen E-ID bemühen und profitieren so von den erleichterten Abläufen, die durch die Digitalisierung ermöglicht werden. Auch für eine Neuausstellung nach einem Widerruf gemäss Art. 5 Bst. a (etwa nach einem Verlust) ist ein vereinfachtes Verfahren zu prüfen.

Darüber hinaus ist zu regeln, dass ein Entzug der E-ID bei begründetem Verdacht auf Missbrauch (Art. 5 Bst. c) den Betroffenen begründet mitgeteilt und auf Verlangen als anfechtbare Verfügung eröffnet wird. Weil die E-ID für die Inhaberinnen und Inhaber im Alltag eine grosse Bedeutung erlangen kann, sollte das BGEID zudem klarstellen, dass gegen einen allfälligen Widerruf ein wirksamer Rechtsschutz besteht.

Art. 8 (Anlaufstellen der Kantone)

Die Bestimmung sieht eine zusätzliche Aufgabe für die Kantone vor. Der erläuternde Bericht zur Vernehmlassungsvorlage geht davon aus, dass die benötigten Strukturen in den Kantonen bereits vorhanden sind. Dies ist jedoch nicht notwendigerweise der Fall. Der Bundesrat plant, die Investitionskosten des Bundes über finanzielle Beiträge der Digitalen Verwaltung Schweiz (DVS) zu finanzieren (Ziff. 5.1 erläuternder Bericht). Es ist somit zu prüfen, ob auf diesem Weg auch die entstehenden Kosten auf Seiten der Kantone finanziert werden können.

In den Erläuterungen zu dieser Bestimmung wird von einem Second-Level-Support der Anlaufstellen durch den Bund gesprochen (Seite 11 erläuternder Bericht). Es fehlt allerdings eine normative Verankerung dieser Aufgabe.

Art. 9 (Pflicht zur Akzeptanz der E-ID)

Art. 9 E-BGEID sieht vor, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Der Begriff der "öffentlichen Aufgabe" wird im erläuternden Bericht mit "Verwaltungsaufgaben" gleichgesetzt, was dem Begriff von Art. 178 Abs. 3 BV entspricht. Es empfiehlt sich, im BGEID ebenfalls von "Verwaltungsaufgaben" zu sprechen, oder, falls der Begriff der "öffentlichen Aufgabe" weiter gefasst werden soll, die Botschaft in diesem Punkt zu präzisieren. Es ist zu bedenken, dass unter anderem im Gesundheitswesen eine Vielzahl von privaten Akteuren öffentliche Aufgaben ausführen, so zum Beispiel Krankenversicherer, Betreiber von Krebsregistern und Transplantationsregistern oder Anbieter des Elektronischen Patientendossiers (EPD). Die Pflicht zur Akzeptanz der zukünftigen E-ID bei all diesen Akteuren ist durchaus sinnvoll, wird aber Investitionen und Vorbereitungsarbeiten zur Folge haben, die den Betroffenen möglichst rasch klar kommuniziert werden müssen. Es ist somit wichtig, dass bei allen Beteiligten von Anfang an Klarheit herrscht über den Geltungsbereich von Art. 9 BGEID.

Art. 10 (Vorweisen einer E-ID)

Art. 10 BGEID legt fest, dass eine Identifizierung in der physischen Welt weiterhin auch ohne eine E-ID durch das Vorweisen eines Ausweisdokuments möglich sein muss. Die Bestimmung verhindert aber nicht, dass der Zugang zu Dienstleistungen, die ausschliesslich elektronisch verfügbar sind, künftig eine E-ID voraussetzen kann. Die Freiwilligkeit zum Bezug einer E-ID wird damit unter Umständen eingeschränkt. Die leichtere Abwicklung einer elektronischen Identifizierung birgt zudem das Risiko, dass eine solche künftig von öffentlichen wie privaten Akteuren auch für den Zugang zu Dienstleistungen verlangt wird, für die das Vorweisen eines Personalausweises bisher nicht nötig war.

In der Umsetzung ist somit darauf zu achten, dass durch den Einsatz der E-ID der Zugang zu öffentlichen Dienstleistungen nicht in unzumutbarer Weise eingeschränkt wird. Problematisch wäre beispielsweise, wenn der Zugriff auf in der Volksschule verwendete Online-Lehrmittel künftig nur mit einer E-ID möglich wäre. Dies würde nicht nur Schülerinnen und Schüler ausschliessen, deren Eltern keine E-ID beantragen möchten, sondern auch solche ohne geregelten Aufenthalt in der Schweiz, die gemäss Art. 19 BV dennoch ein Recht auf Grundschulunterricht haben.

Ferner ist zu prüfen, Art. 10 BGEID einfacher und verständlicher zu formulieren.

Art. 16 (Vorweisen von elektronischen Nachweisen)

Art. 16 Abs. 1 bestimmt, dass die Inhaberin beziehungsweise der Inhaber einer E-ID selber darüber bestimmt, welche Informationen an die betreffende Verifikatorin übermittelt werden. In der Praxis werden dennoch oft die Verifikatorinnen darüber bestimmen, da die Person ansonsten vom Angebot keinen Gebrauch machen kann. Private Verifikatorinnen unterliegen dabei nicht der Kontrolle durch einen Datenschutzbeauftragten, womit erhebliches Missbrauchspotenzial besteht. Vielfach unterlaufen heute marktmächtige Anbieter den Datenschutz, indem sie Personen von Käufen ausschliessen, wenn sie nicht allen Datenverarbeitungen zustimmen, während sie die vom Datenschutz verlangte "Opt-Out-Wahl" (Widerspruchsmodell) maximal erschweren. Es soll nicht dazu kommen, dass die Inhaberin oder der Inhaber durch ständig notwendige komplizierte Zustimmungserklärungen zermüht allem zustimmt. Das schadet dem Vertrauen in die E-ID. In der zu erarbeitenden Botschaft sind deshalb Ausführungen zu machen, wie die Beschränkung der Datenbearbeitung auf das Minimum bei privaten Verifikatorinnen sichergestellt werden soll.

Art. 17 (Basisregister)

Es erschliesst sich nicht, auf was "daraufhin" in Art. 17 Abs. 2 lit. b Ziff. 1 Bezug nimmt.

Art. 21 (System für Sicherungskopien)

Gemäss Art. 21 BGEID kann der Bundesrat vorsehen, dass der Bund ein System für Sicherungskopien elektronischer Nachweise zur Verfügung stellt. Ein solches Sicherungssystem ist eine unabdingbare Voraussetzung für ein benutzerfreundliches E-ID-System und einen wirkungsvollen technischen Support. Die Kann-Formulierung in Art. 21 BGEID ist durch eine Muss-Formulierung zu ersetzen.

Der Tod einer Person ist gemäss Art. 5 lit. d Ziff. 3 ein gesetzlicher Grund für den Widerruf einer E-ID, jedoch keiner für die Vernichtung von Sicherheitskopien – diese können von den Angehörigen gemäss Art. 21 Abs. 3 nicht mehr vernichtet werden. Es ist zu prüfen, ob neben den abschliessend formulierten Gründen des Art. 21 Abs. 3 weitere Gründe in Verbindung mit dem Widerruf nach Art. 5 hinzuzufügen sind. Allenfalls würde eine Verknüpfung der Widerrufsgründe der Originale mit den Vernichtungsgründen der Sicherheitskopien Sinn ergeben.

Art. 25 (Technische Entwicklung)

Die Funktionsweise von Absatz 2 dieser Bestimmung ist unklar: Wer entscheidet darüber, ob ein Anwendungsfall von Absatz 2 vorliegt? Entscheidet dies der Bundesrat bereits mit dem Erlass der Verordnung?

Zudem ist der Zusammenhang zwischen Abs. 1 und Abs. 2 von Art. 25 im Text deutlicher hervorzuheben:

"² Sofern Bestimmungen gemäss Abs. 1 zur Bearbeitung besonders schützenswerter Personendaten führen [...]."

Art. 26 (Gebühren)

Art. 26 BGEID sieht vor, dass von Ausstellerinnen und Verifikatorinnen elektronischer Nachweise Gebühren erhoben werden. Dies betrifft auch Stellen, die öffentliche Aufgaben erfüllen, obwohl diese gemäss Art. 9 BGEID zur Akzeptanz der E-ID verpflichtet sind. Gleichzeitig möchte der Bundesrat die E-ID durch Beiträge aus der Digitalen Verwaltung Schweiz finanzieren, die von den Kantonen mitfinanziert wird. Gemäss Art. 3 Abs. 2 AllgGebV verzichtet die Bundesverwaltung auf die Erhebung von Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Dies soll auch vorliegend entsprechend gehandhabt und Verrechnungen zwischen den Gemeinwesen auf ein Minimum beschränkt werden.

Der Bundesrat soll darüber hinaus mit der Kompetenz ausgestattet werden, die Gebühren für weitere Akteure ganz oder teilweise zu erlassen, soweit diese öffentliche Aufgaben erfüllen. Unter anderem besteht im Gesundheitsbereich ein grosses Interesse an einer breiten Nutzung der E-ID, um die Aufbereitung von Gesundheitsdaten zu erleichtern. Die Kosten für die betroffenen Stellen sind somit möglichst tief zu halten.

Die Vorlage und der erläuternde Bericht äussern sich nicht beziehungsweise nur sehr vage über die Höhe der zu erhebenden Gebühren. Diese sollen auf Verordnungsstufe festgelegt werden. Eine explizite Kostenfolgeschätzung für die Nutzer aufgrund der Gebühren sollte in die Botschaft aufgenommen werden, da die Kosten einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben dürften.

Art. 28 (Ausführungsbestimmungen)

Zahlreiche technische Aspekte zur Umsetzung der E-ID werden auf Verordnungsstufe geregelt. Aufgrund der unterschiedlichen bestehenden Lösungen in den einzelnen Kantonen, aber auch in den einzelnen Sektoren ist es unabdingbar, dass die zuständigen Akteure eng in die Erarbeitung der Vollzugsregelungen miteinbezogen werden. Es ist eine der Voraussetzungen einer breiten Akzeptanz der E-ID, dass diese unkompliziert in bestehende Anwendungen integriert werden kann.

Art. 29 (Änderung anderer Erlasse)

Gemäss dem erläuternden Bericht (Ziff. 3.1) wurde die Verwendung der E-ID in spezifischen Bereichen und damit die Änderung anderer Erlasse im Entwurf nur exemplarisch geregelt. Es ist unabdingbar, die Gesetzgebung des Bundes im weiteren Verfahren systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder eine qualifizierte elektronische Signatur verlangt werden. Dies betrifft insbesondere auch die Verfahrensgesetzgebung des Bundes. Die entsprechenden Bestimmungen sind durchgehend anzupassen.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Freundliche Grüsse

Im Namen des Regierungsrats

Alex Hürzeler
Landammann

Joana Filippi
Staatsschreiberin

Kopie

- rechtsinformatik@bj.admin.ch



Regierungsrat, 9102 Herisau

Eidg. Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 30. September 2022 / ssc

Eidg. Vernehmlassung; Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 werden die Kantonsregierungen vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) eingeladen, sich zum Entwurf für ein neues Gesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz; BGEID) bis zum 20. Oktober 2022 vernehmen zu lassen.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Grundsätzlich wird die Vorlage und insbesondere die vorgeschlagene Umsetzung einer Lösung für die E-ID nach den Grundsätzen des Schutzes der Privatsphäre durch Technik ("privacy by design"), der Datensparsamkeit und der dezentralen Datenspeicherung, vom Regierungsrat begrüsst. Damit dürfte die Akzeptanz in der Bevölkerung grösser sein als dies beim Bundesgesetz über elektronische Identifizierungsdienste, welches am 7. März 2021 vom Volk abgelehnt wurde, der Fall war. Ausdrücklich befürwortet wird zudem, dass die Infrastruktur für elektronische Nachweise auch für bereits bestehende kantonale Lösungen genutzt werden kann (Art. 12 des Vorentwurfs).

Nach Ansicht des Regierungsrates soll der Bund verpflichtet werden, bereits im Einsatz stehende kantonale eID für seine Verwaltungsprozesse anzuerkennen. Der Vorentwurf des BGEID ist dahingehend entsprechend zu ergänzen.

Nachfolgend wird zu einzelnen Artikeln Stellung genommen, bei welchen nach Erachten des Regierungsrates ein Anpassungs- oder Klärungsbedarf besteht:

Es erscheint unklar, weshalb die AHV-Nummer nicht unter den Personenidentifizierungsdaten in Art. 2 Abs. 2 aufgeführt wird, gilt doch die AHV-Nummer ebenfalls als Personenidentifikator. Eine explizite Erwähnung würde auch ermöglichen, dass die AHV-Nummer in Anwendungsfällen, wo diese notwendig ist, zur Personenidentifizierung genutzt werden kann.

Art. 5 Abs. 1 Bst. b sieht vor, dass das fedpol die E-ID unverzüglich widerruft, wenn die gesetzliche Vertretung von Minderjährigen bis zum vollendeten vierzehnten Lebensjahr oder von Personen unter umfassender Beistandschaft dies verlangt. Obschon die Bestimmung offensichtlich im Zusammenhang mit Art. 4 Abs. 2 steht, sollte geprüft werden, ob das Antragsrecht auf Widerruf auch gesetzlichen Vertretern von Minderjährigen bis zu deren Volljährigkeit zustehen soll. Dies würde Art. 19 ZGB entsprechen, gemäss dem urteilsfähige handlungsunfähige Personen nur mit Zustimmung ihres gesetzlichen Vertreters Verpflichtungen eingehen oder Rechte aufgeben können.

Weiter sollte geprüft werden, welche rechtlichen Folgen ein Verlust der elektronischen Briefftasche bzw. des Gerätes mit der E-ID hat.

Beim Art. 9 wird nicht erwähnt, was gelten soll, wenn ein Erlass eine andere Identifizierung oder eine elektronische Signatur vorschreibt (vgl. z.B. Art. 21a des Verwaltungsverfahrensgesetzes [SR 172.021]). Eine elektronische Signatur dient nach Art. 2 Abs. 1 Bst. b Ziff. 2 des Bundesgesetzes über die elektronische Signatur (SR 943.03) ebenfalls der Identifizierung. Es stellt sich deshalb die Frage, ob eine Behörde die E-ID anstelle der elektronischen Signatur zu akzeptieren hat, wenn eine elektronische Signatur vorgeschrieben ist. Zudem wird in den Erläuterungen zu Art. 9 ausgeführt, dass die Pflicht zur Akzeptanz der E-ID nur für Identifizierungsprozesse gilt, bei "denen ein persönliches Erscheinen die Vorlage eines Identifizierungsdokuments erforderlich sind" und nicht die bestehenden kantonalen und kommunalen Login-Lösungen betreffen. Diese Voraussetzungen bzw. Vorbehalte kommen jedoch in der Formulierung von Art. 9 nicht zum Ausdruck. Ausserdem trifft die Aussage in den Erläuterungen, wonach die Fragen im Zusammenhang mit der Verwendung der E-ID im Vorentwurf nicht geregelt seien, auf Art. 9 gerade nicht zu. Die Notwendigkeit und die Formulierung von Art. 9 sollten daher genauer geprüft werden. Auch soll eine Präzisierung der Erläuterungen erfolgen.

Bei Art. 13 kann auf die Ausführungen zu Art. 5 verwiesen werden. So sollte es auch bei anderen elektronischen Nachweisen für gesetzliche Vertreter von Minderjährigen bis zu deren Volljährigkeit möglich sein, einen Widerruf zu beantragen. Falls dennoch für den Widerruf auf die Altersgrenze von 14 Jahren abgestellt wird, dann müsste dies auch für die Ausstellung gelten. Im Gegensatz zu Art. 4 Abs. 2 wird diese Bedingung aber in Art. 12 nicht erwähnt. Ausserdem müsste auch hier geprüft werden, ob ein Widerruf erfolgen soll, wenn der technische Träger (Art. 14) des elektronischen Nachweises verloren geht.

Der Sinn und Zweck von Art. 15 Abs. 2 erscheinen unklar. Gemäss den Erläuterungen geht es hier um Sicherungskopien nach Art. 21. In diesem Fall erscheint jedoch dieser Absatz nebst Art. 21 nicht notwendig bzw. in der vorliegenden Form eher irreführend, da in Art. 21 nicht die Formulierung "Übertragung von elektronischen Nachweisen" verwendet wird. Besser wäre zum Beispiel, in Art. 15 einen Vorbehalt zu Art. 21 aufzunehmen. Ansonsten müssten zumindest die Ausführungen in den Erläuterungen zu Art. 15 Abs. 2 präzisiert werden.



Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Bundesamt für Justiz BJ
Rolf Rauschenbach
Bundesrain 20
3003 Bern

Per E-Mail an: rechtsinformatik@bj.admin.ch

Liestal, 18. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassungsantwort

Sehr geehrte Damen und Herren

Mit dem Schreiben vom 29. Juni 2022 laden Sie uns ein, im Rahmen des Vernehmlassungsverfahrens zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise unsere Stellungnahme abzugeben.

Der Regierungsrat des Kantons Basel-Landschaft schliesst sich vollumfänglich der Stellungnahme der Konferenz der Kantonsregierungen vom 23. September 2022 an. In Ergänzung dazu bitten wir Sie, die folgenden Punkte zu berücksichtigen:

Art. 1 Abs. 1 Bst. A VE BGEID

Der jetzige Gesetzesentwurf sieht nur den Identitätsnachweis von natürlichen Personen vor. Der Prozess zur Verknüpfung einer E-ID einer natürlichen Person mit der einer juristischen Person sollte jedoch normiert werden, beispielsweise indem in Art. 2 Abs. 3 diejenigen Daten ergänzt werden, die für die Identifikation einer juristischen Person notwendig sind.

Art. 2 Abs. 3 Bst. a VE BGEID

Mit Blick auf die Zielsetzungen der Revision des AHVG soll die AHVN systematisch verwendet werden für die Verhinderung von kostenintensiven Verwaltungsfehlern sowie mehr Effizienz dank automatisiertem Datenaustausch zwischen den Behörden, Vermeidung von Verwechslungen (Botschaft zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (Systematische Verwendung der AHV-Nummer durch Behörden; BBl 2019 7359, S. 7376). Entsprechend bestehen weniger Vorbehalte, wenn es die Identifikation zwischen Behörden und Privaten (und nicht zwischen Privaten untereinander) sowie die darauffolgende Verwendung beim elektronischen Behördenzugang betrifft, sofern es sich um öffentliche Organe handelt, die unter Art. 153c Abs. 1 AHVG fallen (und bei denen kein spezialgesetzliches Verbot der Verwendung der AHVN besteht).

Die AHVN-Nummer sollte wie vorgesehen als Teil der E-ID geführt werden können. Das Gesetz sollte jedoch – z.B. in Art. 16 VE-BGEID – ausdrücklich festhalten, dass die AHV-Nummer mit Hilfe

von technischen Massnahmen nur jenen Verifikatorinnen zugänglich gemacht werden darf, für welche grundsätzlich die rechtlichen Grundlagen für die systematische Verwendung gemäss AHVG gegeben sind. Private Verifikatorinnen sollten somit keinen Zugang erhalten.

Art. 5 Abs. Bst. d und e VE-BGEID

Der Prozess zum Widerruf im Falle des Todes einer E-ID-Inhaberin ist im Detail zu prüfen, da die E-ID im Kanton zukünftig für die Abwicklung von digitalen Geschäften und damit auch für den Abruf von elektronischen Dokumenten verwendet werden soll. Es stellt sich beispielsweise die Frage, wie Rechnungen einer verstorbenen Person nach Widerruf der E-ID für die Erben noch abrufbar bleiben, um allfälligen Zahlungsverpflichtungen nachkommen zu können.

Art. 6 VE-BGEID

Wir befürworten, dass die Gültigkeit der elektronischen Identität identisch mit der Gültigkeit des physischen Ausweisdokuments ist. Es sollte jedoch eine Übergangsregelung für die elektronische Identität vorgesehen werden, um die Gültigkeit der elektronischen Identität bis zur Erneuerung der physischen Ausweisdokumente sicherzustellen. Zudem ist der Prozess zur Erneuerung einer elektronischen Identität nach Ablauf ihrer Gültigkeit klar zu regeln.

Art. 8 VE-BGEID

Die für die Kantone anfallende Kosten für die genannte Unterstützungsstelle sind zu quantifizieren. Auch wenn von «geringen» Kosten auszugehen ist, können bei diesem hohen Kostenrahmen «geringe» Kosten bereits ausserhalb der Kompetenz des Regierungsrates liegen.

Art. 16 Abs. 3 VE-BGEID

Gemäss Entwurf soll die Betreiberin des Systems «möglichst» keine Rückschlüsse über die Verwendung und die Beteiligten der elektronischen Nachweise ziehen können. Der Grundrichtung dieser Bestimmung ist zuzustimmen, da über die Verwendung der E-ID besonders schützenswerte Personendaten oder sogar eigentliche Profile entstehen können. Die Erläuterungen schweigen sich jedoch über die Gründe aus, weshalb darauf verzichtet wurde, die Bestimmung so zu formulieren, dass gar keine Möglichkeit der Rückschlüsse entstehen darf. Sollten rechtliche oder technische Gründe bestehen, die (ausnahmsweise) eine solche Datenspur notwendig machen, sollten sie in den Erläuterungen erwähnt werden. Gibt es keine solche Gründe, wird die Streichung des Wortes «möglichst» beantragt.

Art. 21 VE-BGEID

Der Umstand, dass der Schutz der elektronischen Nachweise gemäss Art. 14 des Entwurfs vollständig in die Verantwortung der Inhaberin resp. des Inhabers gestellt wird, ist bedenklich. Denn die Erfahrungen im Bereich Cybercrime zeigen auf, dass dies ein vergleichsweise illusorischer Ansatz ist. Die einzelnen IT-User sind im Regelfall nicht in der Lage, ihre persönlichen Daten gegen eine gezielt ausgeführte Cyberattacke hinreichend zu schützen. Erforderlich wäre also grundsätzlich einen besseren Schutz der E-ID durch die ausgebende Stelle bzw. durch den Bund selbst, wobei die Zugriffe in ähnlicher Weise zu schützen sind, wie bei E-Banking-Systemen üblich. Die Datensätze wären somit beim Bund zu verwahren und lediglich im Bedarfsfall mittels verschiedener Schlüssel temporär abrufbar. Wenn das nicht möglich ist, muss zwingend Wert auf das in Art.

21 vorgesehene System für Sicherheitskopien gelegt werden. Dieses wäre bei Fehlen der geforderten Schutzmassnahmen eine zwar nach wie vor suboptimale, jedoch einigermaßen sinnhaltige Sicherungsmöglichkeit für sensible Datensätze. Wir beantragen deshalb die Streichung des Wortes «kann» in Art. 21 Abs. 1, erster Satz und eine zwingende Formulierung, wonach der Bundesrat ein solches System in jedem Fall vorzusehen hat.

Positiv möchten wir erwähnen, dass der Bund einen Ökosystem-Ansatz verfolgt, der schrittweise auch zur Ausstellung anderer elektronischer Nachweise wie Strafregisterauszüge, Führerausweise etc. genutzt werden kann. Dies ermöglicht das stringente Verfolgen des once-only Ansatzes, indem mit einem Identitätsprofil zahlreiche Behördengänge niederschwellig abgeschlossen werden können. Dies ist zentral für das Gelingen des Vorhabens. Weiter begrüssen wir, dass die Vorlage die Grundsätze der Datensparsamkeit berücksichtigt und somit dem Datenschutz Rechnung trägt.

Abschliessend möchten wir anregen, dass die beabsichtigten Verordnungsbestimmungen möglichst zeitnah den Kantonen vorgelegt werden. Denn erst auf dieser Basis kann der technische und personelle Aufwand in den Kantonen vollständig abgeschätzt werden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse



Kathrin Schweizer
Regierungspräsidentin



Elisabeth Heer Dietrich
Landschreiberin



Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
Fax: +41 61 267 85 72
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Als Word- und als pdf-Dokument an:

Email: rechtsinformatik@bj.admin.ch

Basel, 18. Oktober 2022

P220955

Regierungsratsbeschluss vom 18. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassung

Stellungnahme des Kanton Basel-Stadt

Sehr geehrter Herr Rauschenbach, sehr geehrte Damen und Herren

Der Bundesrat hat am 29. Juni 2022 das EJPD beauftragt, ein Vernehmlassungsverfahren zum Entwurf über das E-ID-Gesetz durchzuführen. Wir danken Ihnen für die Gelegenheit zur Stellungnahme.

Die Konferenz für Kantonsregierungen (KdK) hat zum Vorentwurf des E-ID-Gesetzes nach Anhörung der Kantone eine konsolidierte Stellungnahme zusammengetragen und anlässlich der Plenarversammlung vom 23. September 2022 verabschiedet.

Der Regierungsrat schliesst sich der Stellungnahme der KdK an, mit nachfolgendem Einbringen:

Zu Art. 2,3 oder 4 E-ID-Gesetz:

Die E-ID muss online und ohne physische Präsenz erlangt werden können.

Kurzbegründung: Die E-ID dient inskünftig der elektronischen Identifikation im digitalen Behördenverkehr und mit Privaten. Es wäre widersprüchlich und nicht zeitgemäss für ebendiesen digitalen Geschäftsverkehr ein persönliches Erscheinen auf einem Amt zu verlangen. Dieses Anliegen ist auch für die Ausbreitung des elektronischen Patientendossiers zentral.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Barbara Schüpbach-Guggenbühl, Staatsschreiberin; Tel. 061 267 85 60, gerne zur Verfügung.

Regierungsrat des Kantons Basel-Stadt

Freundliche Grüsse

Im Namen des Regierungsrates des Kantons Basel-Stadt

A stylized handwritten signature in blue ink, consisting of a large 'B' and 'J' intertwined.

Beat Jans
Regierungspräsident

A handwritten signature in blue ink, appearing to read 'B. Schüpbach-Guggenbühl'.

Barbara Schüpbach-Guggenbühl
Staatsschreiberin



Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Per E-Mail als PDF- und Word-Dokument an:
rechtsinformatik@bj.admin.ch

RRB Nr.: 1057/2022
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

19. Oktober 2022

**Vernehmlassung des Bundes: Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).
Stellungnahme des Kantons Bern**

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Regierungsrat dankt Ihnen für die Gelegenheit zur Stellungnahme zum titelerwähnten Gesetzesvorentwurf.

1. Grundsätzliches

Der Kanton Bern unterstützt den Vorentwurf des BGEID. Eine sichere, hoch verfügbare und allgemein akzeptierte E-ID ist eine unabdingbare Voraussetzung für die Digitalisierung der Geschäftsprozesse der Verwaltung und der Wirtschaft.

Der Regierungsrat dankt Ihnen und der Bundesverwaltung für die rasche Erarbeitung des Vorentwurfs und für den vorbildlichen, partizipativen Einbezug der Stakeholder aus Verwaltung, Wirtschaft und Gesellschaft in den Konzeptionsprozess. Unserer Meinung nach enthält der nun vorliegende Vorentwurf wesentliche Verbesserungen gegenüber dem in der Volksabstimmung abgelehnten Gesetz:

- Er sieht eine **rein staatliche E-ID-Infrastruktur** vor. Damit begegnet er der Kritik an der im ersten BGEID vorgesehenen teilweisen Auslagerung der E-ID an die Privatwirtschaft, welche dem Referendum zugrunde lag.
- Er basiert auf dem zukunftsweisenden Ansatz der **«self-sovereign identity» (SSI)**, die es den Inhaberinnen und Inhabern erlaubt, nur die Daten bekanntzugeben, die für den jeweiligen Geschäftsfall erforderlich sind. Dies entspricht dem Gebot der Datensparsamkeit und der «privacy by design» sowie der geplanten europäischen Gesetzgebung.

- Er erlaubt staatlichen und privaten Stellen, **eigene Nachweise** auszustellen (wie Führerausweise oder Arztrezepte) und diese über die E-ID zu vermitteln. Damit entsteht ein Ökosystem digitaler Nachweise, das den Nutzen der E-ID weit über die eigentliche Identifikation hinaus ausweitet.

Damit die E-ID ein Erfolg wird, sollte bei der Umsetzung u.E. unbedingt Folgendes beachtet werden:

- **Die E-ID muss einfach** und sicher sein. Frühere Vorhaben wie die SuisselD scheiterten daran, dass sie zu teuer, zu kompliziert oder zu bürokratisch waren. Die E-ID muss für alle Stakeholder – die Benutzenden, die Überprüfenden und die Ausstellerinnen von Nachweisen – möglichst niederschwellig zugänglich sein. Gleichzeitig sind die Integrität der E-ID und das daran geknüpfte Vertrauen aller Beteiligten als zentrale Pfeiler des Erfolgs durch geeignete Massnahmen zu schützen.
- **Der Support muss sichergestellt sein.** Der SSI-Ansatz ist für die Bevölkerung, die Wirtschaft und die Verwaltung neu. Er und die E-ID müssen allen Stakeholdern mit einer professionellen Marketing- und Sensibilisierungskampagne vermittelt werden. Und alle Stakeholder müssen bei der Anwendung der E-ID von einer gut ausgebauten, zentralen Supportorganisation des Bundes unterstützt werden (s. auch unseren Antrag zu Art. 8 unten).

Zum von Ihnen unterbreiteten Vorentwurf verweist der Regierungsrat grundsätzlich auf die beiliegende Stellungnahme der Konferenz der Kantonsregierungen (KdK). Dieser schliesst er sich ausdrücklich an, ausser soweit nachstehend Abweichungen und Ergänzungen angebracht werden.

2. Anträge

2.1 Antrag zu Artikel 2 (Form und Inhalt)

Es ist sicherzustellen, dass das Ablaufdatum der E-ID keine Auswirkungen auf die Gültigkeit digitaler Ausweise bzw. Nachweise hat, die auf der Basis der E-ID ausgestellt wurden (Art. 12 f. BGEID).

2.1.1 Begründung

Einige der Nachweise, die auf der Basis der E-ID ausgestellt werden sollen, wie etwa Führerausweise, sind unbefristet gültig. Eine Erneuerung der E-ID darf daher keinen bedeutenden Mehraufwand zur Erneuerung der auf der E-ID basierenden Ausweise verursachen.

Mittelfristig wäre es im Übrigen zielführend, die Personenidentifizierungsdaten von ISA, ZEMIS und weiteren Umsystemen wie denen des Informationssystems (IVZ) des ASTRA zu harmonisieren.

2.2 Antrag zu Artikel 2 Absatz 2 Buchstabe g (Gesichtsbild)

Die zwingende Notwendigkeit der Erfassung eines Gesichtsbilds in der E-ID ist in der Botschaft zu begründen, oder es ist auf die Erfassung eines Gesichtsbilds zu verzichten.

2.2.1 Begründung

In Artikel 4 Absatz 4 VE-BGEID und den zugehörigen Erläuterungen wird der Bedarf nach einem biometrischen Gesichtsbild nur für den Ausstellungsprozess begründet. Demgegenüber wird der Bedarf nach einem biometrischen Gesichtsbild in der E-ID selbst weder in den Erläuterungen zu Artikel 2 Absatz 2 Buchstabe g – der auf die Informationssysteme nach dem Ausweisgesetz (AwG) und dem Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) verweist, die beide biometrische Gesichtsbilder enthalten können (vgl. Art. 11 i. V. m. Art. 2^{bis} AwG und Art. 1 i. V. m. Art. 4 Abs. 1 Bst. a^{bis} BGIAA) – noch anderswo erklärt. Es bleibt deshalb nicht nachvollziehbar, weshalb auf einer ID für den Einsatz in der digitalen Welt ein biometrisches Gesichtsbild enthalten sein soll.

2.3 Antrag zu Artikel 15 (Übertragbarkeit von elektronischen Nachweisen) und Artikel 28 (Ausführungsbestimmungen)

Artikel 15 und 28 sind so anzupassen, dass sichergestellt wird, dass Nachweise, die auf der Basis der E-ID ausgestellt werden (Art. 12 f.), wie etwa der eFahrzeugausweis, mit anderen Personen geteilt werden können.

2.3.1 Begründung

Die Strassenverkehrsämter planen den Fahrzeugausweis künftig als digitalen Ausweis abzugeben. Der Fahrzeugausweis verbleibt bei der Halterin oder dem Halter eines Fahrzeuges. Sie oder er hat jedoch die Möglichkeit, den Fahrzeugausweis einer anderen Person für eine bestimmte Zeit «auszuleihen». Es muss deshalb die Möglichkeit bestehen, einen digitalen Ausweis zeitbefristet oder unbegrenzt «teilen» zu können. Wir bitten Sie daher zu prüfen, wie dies im Rahmen des BGEID umgesetzt werden kann, etwa dadurch, dass in Artikel 15 Absatz 2 auf den Vorbehalt «die nicht auf eine natürliche Person ausgestellt sind» verzichtet wird.

2.4 Antrag zu Artikel 16 Absatz 3 (Datenspuren bei der Verwendung elektronischer Nachweise)

In Artikel 16 Absatz 3 VE-BGEID ist das Wort «möglichst» zu streichen. Wenn aus technischen oder rechtlichen Gründen nicht darauf verzichtet werden kann, ist in der Botschaft klar darzulegen, warum eine Ausgestaltung eines Systems, das keine Rückschlüsse über die Verwendung der E-ID oder anderer elektronischer Nachweise zulässt, nicht möglich ist.

2.4.1 Begründung

Die Prüfung der E-ID oder anderer elektronischer Nachweise durch die Verifikatorin im System zur Bestätigung von Identifikatoren in Artikel 18 VE-BGEID darf keine Personendaten hinterlassen. Es darf nicht ersichtlich sein, wann, wo und für was eine Nutzerin oder ein Nutzer der E-ID oder eines anderen elektronischen Nachweises die E-ID oder den elektronischen Nachweis eingesetzt hat. Artikel 16 Absatz 3 VE-BGEID hält fest, dass die Betreiberin der Systeme keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise hat und «möglichst» keine Rückschlüsse auf deren Verwendung und die Beteiligten ziehen kann. Es ist nicht klar, warum die Systeme nicht so gestaltet werden müssen bzw. können, dass *gar* keine Rückschlüsse gezogen werden können.

2.5 Antrag zu Artikel 17 Absatz 3 (Verifizierung der Identität von privaten Ausstellerinnen und Verifikatorinnen)

Artikel 17 Absatz 3 VE-BGEID ist so zu ändern, dass die Ausstellerinnen und Verifikatorinnen ihre Daten nicht in das Basisregister eintragen können, ohne dass die Ausstellerinnen und Verifikatorinnen sicher identifiziert werden.

2.5.1 Begründung

Die Öffnung des Systems zur Bestätigung von Identifikatoren für die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bedingt begleitende Massnahmen. Insbesondere ist eine Verifizierung der Identität der privaten Ausstellerinnen und Verifikatorinnen vorzusehen. In den Erläuterungen wird das Risiko ausgewiesen, dass Ausstellerinnen oder Verifikatorinnen mit vorgetäuschter Identität elektronische Beweismittel ausstellen könnten. Weil jedoch ein Zulassungsverfahren ressourcenintensiv wäre und zu einem teuren und unnötigen Flaschenhals führen würde, soll auf eine Verifikation verzichtet werden. Artikel 22 VE-BGEID sieht vor, dass der Bund öffentlich über Fälle von begründetem Verdacht auf Missbrauch der Vertrauensinfrastruktur informiert. Die Erläuterungen nennen dies als risikomindernde Massnahme. Ein nachträglicher Kommunikationsweg ausserhalb der Systeme der VE-BGEID erscheint jedoch ungenügend, dem benannten Risiko zu begegnen. Die hohen Kosten des Zulassungsprozesses dürfen zudem kein Argument sein, die Risiken des Missbrauchs der Vertrauensinfrastruktur zu erhöhen. Von einer Vertrauensinfrastruktur kann zudem nur gesprochen werden, wenn die Risiken des Missbrauchs mit allen möglichen Mitteln reduziert werden.

Ohne einen Verifizierungsprozess bei der Öffnung für Private kann namentlich das folgende in den Erläuterungen ausgewiesene Ziel nicht erreicht werden: «Der Bund stellt sicher, dass alle interessierten Behörden und Private Zugang zum Mechanismus zur Bestätigung des Identifikators haben. Über diesen Zugang können sie sicherstellen, dass es sich bei ihrem Gegenüber in der virtuellen Welt tatsächlich um die Organisation, Einheit oder die Person handelt, für die sie sich ausgibt. So kann die Authentizität der an einem Geschäftsprozess Beteiligten überprüft werden». Diese Authentizität muss beiderseits sichergestellt sein.

2.6 Antrag zu Artikel 25 (Technische Entwicklung)

Artikel 25 Absatz 1 VE-BGEID ist wie folgt anzupassen: «Der Bundesrat kann ~~vorsehen~~ sieht vor, dass die in diesem Gesetz vorgesehene Infrastruktur um zusätzliche Elemente erweitert wird, sofern dies angesichts der technischen Entwicklung erforderlich ist, um die Ziele dieses Gesetzes zu erreichen. Er bezieht dazu die Kantone und Vertretungen der Privatwirtschaft mit ein.»

2.6.1 Begründung

Dass die Entwicklung der Technik, der digitalen Wirtschaft und Gesellschaft sowie der Cybersicherheitslage laufend nach Anpassungen an der Infrastruktur der E-ID oder ihre Erweiterung verlangen wird, ist sicher. Die laufende Weiterentwicklung des Systems E-ID auf rechtlicher und technischer Ebene ist daher als Aufgabe des Bundes und nicht nur als Kann-Bestimmung zu formulieren. Weil die E-ID auch für die Kantone und die Wirtschaft als Basis eines Ökosystems digitaler Nachweise dienen soll, sind sie als wichtige Stakeholder in den Prozess der Erhebung und Umsetzung neuer Anforderungen mit einzubeziehen.

2.7 Antrag zu Artikel 26 (Gebühren)

Artikel 26 VE-BGEID ist wie folgt mit einem Absatz 3 zu ergänzen: «Die Gebühren sind angemessen auszugestalten und frühzeitig bekanntzugeben.»

2.7.1 Begründung

Im Kontext der Führerausweise wäre eine Gebühr in der Grössenordnung der Gestehungskosten heutiger physischer Ausweise wünschenswert. Ansonsten müssten die Kantone die Kosten durch höhere Gebühren für diese Produkte auf die Nutzenden abwälzen. Dies könnte zur Ablehnung von Digitalisierungsvorhaben führen.

Die im erläuternden Bericht erwähnten Betriebskosten (jährlich CHF 15 – 20 Mio.), welche durch Gebühren bezahlt werden müssen, sind im Verhältnis zu den Projektkosten von ca. 25 – 30 Millionen Franken aus der Sicht des Regierungsrates zu hoch. Es darf nicht sein, dass der Bund die E-ID «gratis» zur Verfügung stellt und die Kantone, Gemeinden und Private mit den Gebühren für ihre digitalen Ausweise die hohen Betriebskosten bezahlen, welche dann an die Nutzenden überwältigt werden müssen. Dies könnte zur Folge haben, dass digitale Ausweise von Kantonen und Dritten nicht über die Basisinfrastruktur und das dazugehörige «Bundeswallet» verteilt werden, sondern dass sich alternative Kanäle etablieren.

3. Weiteres

Zu einzelnen Punkten der Vorlage haben wir folgende Bemerkungen:

- **Artikel 3 (Persönliche Voraussetzungen):**

- Den Antrag in Ziffer 2.2 der Stellungnahme der KdK, wonach für weitere Personen mit Aufenthalt in der Schweiz eine spezielle E-ID vorzusehen ist, halten wir kaum für umsetzbar. Die KdK kommt selbst zum Schluss, die Identität der betroffenen Personen dürfte nicht in jedem Fall eindeutig festzustellen sein, so dass der Einsatzbereich einer solchen E-ID entsprechend beschränkt sein dürfte. Es fragt sich unter diesen Umständen, welchen Zweck eine solche E-ID überhaupt haben könnte. Laut dem erläuternden Bericht zu Artikel 3 Buchstabe b kann selbst bei bestimmten Ausweiskategorien (z.B. Ausweise N, F, S und Ci) nicht davon ausgegangen werden, dass die Identität der betreffenden Personen verlässlich festgestellt werden kann mit der Folge, dass für diese der Zugang zu gewissen Diensten eingeschränkt werden kann. Der Zweck der E-ID besteht ja gerade in der sicheren Identifizierung einer Person (Art. 1 Abs. 2 Bst. a E-BGEID).
- In den Erläuterungen zu Artikel 3 steht, dass mit der Kann-Formulierung von Absatz 1 sichergestellt werde, dass die antragstellenden Personen nicht verpflichtet sind, eine E-ID zu beziehen oder zu verwenden. Der Einleitungssatz von Artikel 3 ist jedoch nicht als Kann-Formulierung ausgestaltet. Der Regierungsrat bittet Sie, dies zu überprüfen.

- **Artikel 5 (Widerruf):** Ergänzend zum Antrag der KdK, wonach bei der Änderung von Personendaten automatisch eine neue E-ID ausgestellt werden soll, ist zu bemerken, dass dabei darauf zu achten ist, dass bestehende Nachweise und Berechtigungen, die auf der bisherigen E-ID basieren, bei der Neuausstellung der E-ID nicht ihre Gültigkeit verlieren. Das gilt auch für den Fall, dass eine E-ID abläuft und deswegen neu ausgestellt wird.

- **Artikel 8 (Anlaufstellen der Kantone):** Ergänzend zu der in der Stellungnahme der KdK vertretenen Haltung, wonach der Aufbau einer Supportinfrastruktur Sache des Bundes ist, ist zu bemerken, dass der Aufwand für die Kantone deshalb besonders gross wäre, weil die Anlaufstellen nicht nur Unterstützung bei der Ausstellung der E-ID leisten müssten, sondern auch bei deren Einsatz. Die Abgrenzung zwischen den Supportaufgaben des Bundes (für die E-ID als solche) und den Supportaufgaben weiterer Behörden, die Nachweise gestützt auf die E-ID ausstellen (für die von ihnen ausgestellten Nachweise wie eLernfahrausweis, eFührerausweis, ePersonalausweis, eWohnsitzbestätigung, eStrafregistrauszug, usw.) muss klar erfolgen und kommuniziert werden. In der Einführungsphase ist eine diesbezügliche Koordination durch den Bund notwendig, der z.B. als Support der ersten Ebene auftreten und nachweisspezifische Anliegen den zuständigen Fachbehörden weiterleiten könnte, ebenso wie eine direkte Absprache zwischen den betroffenen Organisationen.
- **Artikel 9 (Pflicht zur Akzeptanz der E-ID):** Sprachlich und inhaltlich nicht verständlich ist u.E. die Aussage auf Seite 11 des erläuternden Berichts zu Artikel 9, wonach die Pflicht zum Akzeptieren der E-ID nur «für Identifizierungsprozesse [gilt], bei denen ein persönliches Erscheinen die Vorlage eines Identitätsdokuments erforderlich sind» *[sic]*. Bei der Vorlage eines physischen Ausweises findet u.E. gerade keine elektronische Identifizierung statt und findet Artikel 9 daher nicht Anwendung. Irreführend ist u.E. auch die Aussage, die Pflicht zum Akzeptieren der E-ID betreffe «nicht die bestehenden kantonalen und kommunalen Login-Lösungen». Vielmehr werden diese Lösungen gemäss dem klaren Wortlaut von Artikel 9 (und den zutreffenden Aussagen in Ziffer 5.2 des erläuternden Berichts) so anzupassen sein, dass sie die E-ID akzeptieren. Der Regierungsrat bittet Sie, die Erläuterungen in der Botschaft entsprechend anzupassen.
- **Artikel 10 (Vorweisen einer E-ID):** Die Regelung erscheint unklar. Was für Fälle hat man im Auge, in denen eine Person persönlich bei der Behörde vor Ort erscheint, die Identifizierung aber mittels E-ID erfolgt? Nach dem erläuternden Bericht zu Artikel 1 Absatz 2 Buchstabe a kann die E-ID auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden. Dies kann zur Annahme verleiten, die E-ID könne die physische Identitätskarte (ID) ersetzen, was jedoch kaum beabsichtigt sein wird. Der erläuternde Bericht zu Artikel 10 geht davon aus, dass das Vorweisen der E-ID anstelle der ID möglich, aber nicht verpflichtend ist. Wir bitten Sie, diesen Themenbereich klarer zu regeln. Zumindest sollte die Botschaft Ausführungen dazu enthalten, welche Bedeutung die E-ID ausserhalb des digitalen Verkehrs haben soll.
- **Artikel 12 (Ausstellung anderer elektronischer Nachweise):** Laut dem erläuternden Bericht zu Absatz 1 können Behörden und Private die Vertrauensinfrastruktur des Bundes nutzen, um elektronische Nachweise auszustellen. Die Arten von elektronischen Nachweisen, die ausgestellt werden können, sind gemäss dem erläuternden Bericht nicht beschränkt; die Vertrauensinfrastruktur solle verschiedenen Akteuren zur Verfügung stehen und ihnen ermöglichen, elektronische Nachweise unterschiedlichster Art auszustellen. Indessen wird im erläuternden Bericht nicht erklärt, welche Beispiele es gibt für elektronische Nachweise, die von Privaten ausgestellt werden und die Vertrauensinfrastruktur des BGEID benutzen. Die Botschaft sollte sich dazu äussern, welche Arten von Nachweisen von Behörden (z.B. der digitale Führerausweis, s. oben) und Privaten ins Auge gefasst werden.
- **Artikel 15 (Übertragbarkeit von elektronischen Nachweisen):** In Artikel 15 Absatz 2 wird geregelt, der Bundesrat könne die Übertragung von elektronischen Nachweisen, die nicht auf natürliche Personen ausgestellt sind, zulassen. Die Regelung von Artikel 15 ist auch unter Einbezug der Erläuterungen unklar. Die Erläuterungen zu Artikel 15 Absatz 2 nehmen Bezug auf das System für Sicherungskopien nach Artikel 21. Der Zusammenhang zwischen

diesen Sicherungskopien und Artikel 15 Absatz 2 ist indessen nicht klar. Nach dem Dafürhalten des Regierungsrates muss es bei Artikel 15 Absatz 2 um die Übertragung von elektronischen Nachweisen *auf das System für Sicherungskopien* gehen. In den Erläuterungen zu Artikel 3 Buchstabe a wird ausgeführt, dass juristische Personen nicht Inhaberinnen einer E-ID sein können und mittels der einheitlichen Unternehmens-Identifikationsnummer UID identifiziert werden. Es fragt sich, was der Gesetzgeber unter «elektronischen Nachweisen, die nicht auf eine natürliche Person ausgestellt sind» versteht. Wir erachten es als unerlässlich, dass in der Vernehmlassung eine Klärung von Artikel 15 Absatz 2 beantragt wird.

- **Artikel 17 und 18 (Vertrauensinfrastruktur):** Der erläuternde Bericht zur Vertrauensinfrastruktur (Vorbemerkungen und Art. 17 – 18) ist auch unter Zuhilfenahme der Grafik schwer verständlich. Insbesondere ist unklar, wie das Zusammenspiel zwischen Verifikatorinnen und Identifikatorinnen ist und wie dies praktisch funktioniert. Der Regierungsrat bittet Sie, dies in der Botschaft verständlicher darzustellen.
- **Artikel 19 (Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen):** Im erläuternden Bericht wird dazu ausgeführt: «Die Verwendung von elektronischen Brieftaschen, die von privaten Akteuren ausgestellt werden, ist im Gesetz nicht geregelt. Neben der staatlichen elektronischen Brieftasche können die Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden». Daraus ist zu schliessen, dass auch Private «elektronische Brieftaschen» schaffen können. Darin können nicht nur die privaten elektronischen Nachweise nach Artikel 12, sondern auch die staatliche E-ID gespeichert werden. Nicht klar ist indessen, ob umgekehrt in der staatlichen «elektronischen Brieftasche» auch die privaten elektronischen Nachweise gespeichert werden können. Dazu sollte die Botschaft Stellung nehmen.
- **Artikel 21 (System für Sicherungskopien):** Die Sicherheitskopien sollen der Wiederherstellung der E-ID beim Verlust oder Wechsel des Smartphones dienen. Dem Bericht zufolge können nur die Inhaberinnen und Inhaber auf die Sicherheitskopien zugreifen. Die Botschaft oder das Gesetz sollten darauf eingehen, wie sich die Inhaberinnen und Inhaber als solche ausweisen sollen, um die E-ID wiederherstellen zu können, wenn sie ihr Smartphone und damit die E-ID verloren haben.
- **Weitere Anpassungen des Bundesrechts:** Das in der Stellungnahme der KdK (Rz. 30) geäußerte Anliegen, die Gesetzgebung des Bundes systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder eine qualifizierte elektronische Signatur verlangt werden, ist mit dem Anliegen zu ergänzen, die entsprechenden Bestimmungen so anzupassen, dass auch die E-ID genügt. Im erläuternden Bericht zu Artikel 9 E-BGEID (3. Abschnitt) steht, der Vorentwurf trage insbesondere dem elektronischen Patientendossier sowie dem Bereich Schuldbetreibung und Konkurs Rechnung. Das Sozialversicherungsrecht und andere für die Massenverwaltung wichtige Bereiche des Bundesverwaltungsrechts werden jedoch nicht adressiert. Der Regierungsrat bittet Sie, diesen Bereichen besondere Aufmerksamkeit zu schenken.
- **Pilotprojekt digitaler Führerausweis:** Die asa (Vereinigung der Strassenverkehrsämter) und das ASTRA können mit dem Teilprojekt T1 (digitaler Führerausweis, mDL) ein Pilotprojekt im Rahmen des Vorhabens E-ID realisieren. Die Zusammenarbeit mit der Projektleitung E-ID verläuft sehr gut und zielführend. Der Kanton Bern bedankt sich, dass er zusammen mit dem ASTRA und der asa an diesem wegweisenden Digitalisierungsprojekt aktiv mitarbeiten und die Interessen der digitalen Ausweise im Strassenverkehr einbringen darf. Zudem wird die auch von der E-ID genutzte Basisinfrastruktur die zeitnahe Einführung digitaler Ausweise der Verkehrszulassung schweizweit ermöglichen. Dies ist angesichts der hohen

Anzahl ausgestellter Ausweise pro Jahr wichtig (Lernfahrausweis: 300'000; Führerausweis: 6.5 Mio.; Ausweis 95 / Chauffeurzulassung; Fahrzeugausweis: 6 Mio.; Schiffsführerausweis: 300'000; Schiffsausweis: 100'000).

Der Regierungsrat dankt Ihnen für die Berücksichtigung seiner Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrates



Christine Häslar
Regierungspräsidentin



Christoph Auer
Staatsschreiber

Verteiler

- Finanzdirektion
- Staatskanzlei
- Gremien der digitalen Verwaltung und der ICT (via Finanzdirektion)

Beilage

- Stellungnahme der Konferenz der Kantonsregierungen vom 23. September 2022



ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil
Rue des Chanoines 17, 1701 Fribourg

d'Etat

PAR COURRIEL

Département fédéral de justice et police
A l'attention de Mme Karin Keller-Sutter
Conseillère fédérale
Chef du département fédéral de justice et police
3003 Berne

Courriel : rechtsinformatik@bj.admin.ch

Fribourg, le 4 octobre 2022

2022-1019

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID) - Procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du canton de Fribourg vous remercie de lui avoir soumis l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (LeID).

Le canton de Fribourg, en tant que membre fondateur de l'association iGovPortal.ch, est particulièrement concerné par l'avant-projet de loi, notamment dans le cadre de la cyberadministration. Dans notre prise de position, il nous paraît important de relever les facteurs clé de succès de mise en œuvre que nous avons pu observer jusqu'ici à savoir la simplicité d'utilisation, l'implication du secteur privé et les moyens de preuve électroniques.

Le projet de loi positionne la Confédération comme autorité de délivrance d'une identité électronique étatique (e-ID) pour la population en possession d'un document d'identité émis par une autorité officielle. Nous saluons cette initiative visant et l'uniformisation sur le plan national de ce service de base à la population. Le Conseil d'Etat constate que l'avant-projet tient compte de la compatibilité de l'identité électronique avec les projets européens ce qui est important étant donné qu'uniquement les citoyennes et citoyens auront accès à une e-ID.

L'avant-projet appelle toutefois les remarques suivantes :

1. e-ID

Identité (e-ID): la création d'une identité électronique fédérale utilisable par les citoyens sur les mêmes bases que leurs papiers d'identité physiques, est perçue de manière positive et permettra à terme de favoriser la digitalisation de l'administration publique et donc la vie des citoyens et résidents étrangers suisses.

Nous saluons le fait d'attribuer des e-ID uniquement à des personnes physiques (art. 1). Le Conseil d'Etat ne souhaite pas d'attribution à des personnes morales.

L'attribution d'une e-ID est garantie par l'article 3 de l'avant-projet pour les citoyens suisses ou les citoyens étrangers au bénéfice d'une autorisation ou permis de séjour en Suisse. Cette disposition ne traite toutefois pas de la question des personnes étrangères qui font appel à des prestations étatiques suisses, notamment les contribuables étrangers de biens immobiliers.

Si l'article 27 de l'avant-projet permet au Conseil fédéral de conclure des conventions internationales pour faciliter la reconnaissance juridique des e-ID suisses à l'étranger ainsi que la reconnaissance des e-ID étrangères en Suisse, force est de constater que cette démarche s'inscrit dans le temps et qu'elle dépend d'une série de facteurs politiques non compressibles.

Dans les deux cas, celui de l'e-ID nationale et des autres moyens internationaux, il appert que les processus de renouvellement de l'identité numérique relèvent d'un réel défi. A notre sens, il est primordial que la Confédération place l'utilisateur au centre des réflexions pour avoir un taux d'adhésion élevé, y compris pour les personnes en situations de handicap (eInclusion).

2. Infrastructure électronique de confiance

Moyen d'authentification (login) incluant l'identification (e-ID et autres systèmes internationaux): L'article 12 de l'avant-projet permet l'usage de systèmes d'identification parallèle à l'e-ID, mais la coordination internationale prendra du temps et risque de mettre certains de nos utilisateurs sur la touche. Actuellement, le moyen d'authentification utilisé intégrant ces identités permet à tous les destinataires de prestations de se connecter au guichet virtuel et de faire évoluer les niveaux d'identification selon les besoins de réassurance des métiers. Avec la nouvelle solution, uniquement les personnes détenant un document d'identité tel que décrit dans le paragraphe précédent pourraient y être intégrées. Cela veut dire concrètement qu'au lieu d'un système de login nous devrions en intégrer plusieurs ce qui complexifie l'intégration en regard de la solution actuelle. Actuellement, le système privé permet d'adresser sur la même solution d'authentification et d'identification tant la population suisse que les étrangers qui travaillent ou ont des relations dans notre canton. Il est donc nécessaire que cela reste possible à l'avenir.

Le Conseil d'Etat souhaite que la solution finale reste simple et compréhensible pour la population afin que son adoption soit la plus grande et rapide possible.

Lors de ses visites dans les pays qui sont en avance en matière de cyberadministration, le Conseil d'Etat a pu constater que l'implication du secteur privé était un facteur clé de succès. La population fera plus volontiers le pas si la solution permet son utilisation dans son eBanking, dans le cadre de la santé et les différents éléments numériques du quotidien.

3. Moyens de preuves numériques

Nous soutenons la volonté de la Confédération, qui en plus de l'e-ID, exprime la volonté d'initier un projet d'émission et d'utilisation d'autres moyens de preuve électroniques (art. 12 à 16). La création d'un portefeuille électronique (wallet) avec des documents officiels (permis de conduire, attestations, etc.) Nous saluons l'idée de partager l'infrastructure électronique à tous les types de preuves numériques émises par des entités publiques, mais à terme également privées. A ce titre, nous disposons de plusieurs solutions permettant de vérifier l'authenticité du document et l'identité de l'émetteur. Nous souhaiterions être associés en tant que partenaire dans le développement de la solution dès la phase pilote. Toutefois, nous émettons certaines réserves en ce qui concerne l'identification des émetteurs. Ne serait-il pas judicieux de porter une réflexion plus approfondie sur les modes de signature, notamment la signature électronique qualifiée ou le cachet réglementé ?

L'avant-projet ne traite effectivement qu'une partie du problème, et la SCSE n'est modifiée que pour introduire la possibilité d'une présentation « numérique » par l'entremise de l'e-ID mais non pas pour éventuellement remplacer les différents types de cachet et signatures.

4. Mesures concrètes devant être prises par les cantons et les communes

L'obligation imposée aux cantons et aux communes d'accepter l'e-ID ainsi que l'infrastructure électronique aura pour conséquences l'adaptation du système d'information des cantons et des communes. Ces conséquences seront lourdes au niveau financier, comme organisationnel, d'autant plus que pour les raisons précitées, des systèmes d'identification privés devront coexister, un certain temps du moins, avec l'e-ID.

Les mesures organisationnelles et techniques nécessaires à la mise en œuvre au niveau cantonal de l'avant-projet nécessitera que les actes d'exécution de la LeID soient connus. Il est dès lors nécessaire de partager le plus en amont possible ces actes d'exécution afin de permettre aux communes et cantons d'anticiper la nécessité d'intégrer dans leur budget les conséquences de la mise en place de ces mesures techniques et organisationnelles majeures. A ce stade, il sera difficile de chiffrer les nouveaux besoins mais la diffusion d'informations ainsi que l'inclusion des cantons aux travaux législatifs et techniques en la matière s'avèrent nécessaires.

Vous trouverez également des remarques article par article dans l'annexe jointe.

En vous remerciant de nous avoir consultés, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Olivier Curty, Président



Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Annexe

—

Mentionnée

Copie

—

à la Direction des finances, pour elle et le Service de l'informatique et des télécommunications ;
à la Direction de la sécurité, de la justice et du sport ;
à la Chancellerie d'Etat.

ANNEXE

Commentaires par article

Art. 3 Conditions personnelles

Le projet de loi permet d'établir une identité numérique s'appuyant sur un permis délivré par l'autorité suisse compétente. Nous saluons cette proposition pragmatique. Cependant, les cas d'usage de cette identité pourraient s'étendre au-delà des personnes disposant d'un tel permis. Il s'agit par exemple de propriétaires de résidences secondaires ou de touristes à qui des prestations numériques spécifiques sont également destinées. Le Conseil d'Etat souhaite donc qu'un concept visant à lier les moyens d'identification à différents types d'identité, dont celle délivrée par la Confédération (mais pas uniquement), soit élaboré par les groupes de travail en charge de la mise en œuvre, notamment l'Administration numérique Suisse.

Le rapport explicatif précise que l'e-ID sera disponible pour les frontaliers. Ce point est salué par le canton de Fribourg qui compte également des frontaliers travaillant dans des entreprises fribourgeoises. Il est important que ces personnes physiques puissent continuer à utiliser les prestations du guichet virtuel fribourgeois. Une mise en place rapide de l'interopérabilité du système Suisse avec les systèmes d'identités mondiaux éviterait aux frontaliers de demander une e-ID suisse. Dans l'intervalle, le projet de loi définitif devra absolument garder la possibilité de délivrer des e-ID à des frontaliers.

Art. 4 Émission

Le canton de Fribourg constate que 96% de ses utilisateurs peuvent effectuer des transactions sur le guichet virtuel en conformité du cadre légal. La solution actuelle simple et conviviale a prouvé sa large adoption. A cet effet, nous souhaitons absolument pouvoir préserver les utilisateurs existants y compris ceux qui possèdent un login non vérifié pour accéder au guichet virtuel. Nous attendons donc de la Confédération un plan de mise en œuvre, notamment avec La Poste Suisse, pour assurer une procédure facilitée qui permette une adoption de la nouvelle eID sans perdre la flexibilité actuelle au niveau des niveaux de confiance mis en œuvre dans le cadre des solutions actuelles.

Art. 8 Points de contact cantonaux

Le canton de Fribourg est favorable à la mise en place de points de contact régionaux pour accompagner les utilisateurs dans l'obtention de leur e-ID. Les collaborateurs travaillant dans ces bureaux auront les compétences nécessaires pour guider les citoyens dans le processus d'acquisition ou de renouvellement d'une e-ID.

Pour un accompagnement plus large dans l'utilisation de l'e-ID ou dans un support plus général à la cyberadministration, nous n'envisageons pas d'engager des collaborateurs spécialisés. Nous pensons que le développement d'un écosystème avec des acteurs tiers, comme les offices postaux, est une piste à poursuivre. Nous interprétons la désignation de « services », dans l'article 8, de manière large et permettant d'associer des partenaires externes à l'administration publique pour effectuer ces tâches d'accompagnement. La Confédération devrait avoir un rôle clé dans la mise en place de ces points de contact pour définir de bonnes pratiques et une cohérence au niveau national.

Art. 9 Obligation d'accepter l'e-ID

Nous saluons l'obligation d'accepter l'e-ID pour les autorités et les services accomplissant des tâches publiques. Il serait souhaitable que les entités paraétatiques ou privées s'acquittant de tâches publiques ou bénéficiant de financement étatique soient soumises à la même obligation d'acceptation de l'e-ID, comme moyen d'identification.

Article 12 : Émission

La possibilité donnée à quiconque d'émettre des moyens de preuve électroniques à l'aide de l'infrastructure de confiance amène une grande souplesse pour des cas d'utilisation particuliers. Cependant, nous demandons que le chiffrage des émoluments prélevés pour de telles utilisations soit communiqué lorsque les projets-pilotes auront abouti et que le message du Conseil fédéral sera transmis au Parlement. Ces émoluments devront être raisonnables afin d'inciter le plus grand nombre d'organisations possible à en faire usage.

Article 17 alinéa 3 : Registre de base

Le fait que les émetteurs et les vérificateurs inscrivent leurs données dans le registre de base peut conduire à un risque d'usurpation d'identité. Nous demandons que la Confédération s'assure qu'une attention particulière soit apportée à la sécurisation des processus d'inscription.

Art. 26 Émoluments

La mise en place d'un système de copie de sécurité (art. 21) est une approche qui semble pertinente et nécessaire. Néanmoins, nous ne sommes pas favorables au fait de lier des émoluments à l'utilisation de ce système de copie de sécurité. Si les citoyens doivent payer pour l'utilisation du système de copie de sécurité, cela risque de créer une barrière importante, alors que cette sécurisation est un réel avantage pour faciliter la récupération en cas de perte et diminuer les cas de support.

Art. 27 Conventions internationales

Il est très important de garantir une interopérabilité et une reconnaissance des systèmes d'identification électronique européens et mondiaux. Pour certaines prestations, le guichet virtuel du canton de Fribourg est actuellement disponible pour des personnes et entreprises étrangères et devra continuer à l'être.

Art. 28 Dispositions d'exécution

Au sens de cet article, de nombreux aspects, notamment techniques, sont réglés par voie d'ordonnance. Compte tenu de la diversité des solutions existant dans les cantons et les différents domaines, tels que la cyberadministration et la santé numérique, il est indispensable que l'ensemble des acteurs concernés soient étroitement associés à l'élaboration des dispositions d'exécution. Il est en effet impératif que l'e-ID s'intègre parfaitement avec les différents services numériques existants ou projetés, en particulier dans les domaines précités.



Genève, le 19 octobre 2022

Le Conseil d'Etat

4442-2022

Département fédéral de justice et police
Mme Karin Keller-Sutter
Conseillère fédérale
Palais fédéral ouest
Bundesgasse 3
3003 Berne

Concerne : consultation sur l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID)

Madame la Conseillère fédérale,

Votre courrier du 29 juin 2022 relatif à l'objet cité en titre nous est bien parvenu et a retenu toute notre attention.

Nous vous remercions de nous avoir consultés. L'identité électronique nationale est une brique centrale et essentielle à la transition numérique de notre pays. Nous nous réjouissons à ce titre de l'avancée décisive que cet avant-projet de loi constitue.

Nous relevons que cet avant-projet de loi fédérale tient compte du refus par le peuple, le 7 mars 2021, de la loi sur les services d'identification électronique. En particulier, l'avant-projet donne un rôle central à l'Etat, celui d'émetteur d'une identité électronique (e-ID) et pose un ensemble de principes importants, tels la protection des données dès la conception, la minimisation des données ou encore un enregistrement décentralisé. L'avant-projet prévoit également une infrastructure de confiance mise à disposition par la Confédération, permettant une utilisation large de moyens de preuve électroniques par les secteurs publics et privés. De plus, il pose des principes tels la neutralité technologique, l'attention au progrès technique ou encore la collaboration internationale, en particulier avec l'Europe.

Notre Conseil se réjouit de ces orientations générales de l'avant-projet de loi fédérale. Il souligne également le travail de mobilisation des acteurs publics, privés et de la société civile dans l'élaboration de projets pilotes en parallèle du travail législatif, démarche exemplaire pour un sujet de politique numérique, ainsi que la vitesse de mise en place d'un nouveau projet législatif. Il exprime le souhait de voir ce mode ouvert et collaboratif se maintenir dans les suites du travail sur l'e-ID (notamment l'élaboration de l'ordonnance), ainsi que sur d'autres projets de politique numérique suisse.

Pour répondre à la consultation, notre Conseil souhaite formuler quatre réserves majeures :

Notre Conseil souhaite qu'un concept soit proposé pour permettre à toutes les personnes susceptibles d'interagir avec les administrations publiques d'accéder à une e-ID. Il peut donc s'agir de personnes ne disposant pas d'un document d'identité suisse ou d'un permis (autorisation pour étrangers), par exemple certains collaborateurs d'organisations internationales et leur famille, certains retraités vivant à l'étranger, des personnes vivant en Suisse sans disposer d'un permis de séjour (sans papiers), ou encore des propriétaires de résidences secondaires. Ces publics peuvent, par exemple, être amenés à utiliser un dossier électronique du patient répondant à la loi fédérale sur le dossier électronique du patient LDEP. Une identité spécifique pourrait être créée pour de tels cas, selon un concept à définir, sans quoi notre canton sera sans doute amené à maintenir un moyen d'identification électronique permettant l'accès aux prestations publiques cantonales, en alternative à l'e-ID nationale, pour les publics n'ayant pas accès à cette dernière.

Notre Conseil se réjouit de la préoccupation de veiller à l'inclusion numérique et à accompagner la population dans l'utilisation des e-ID. Il tient à relever qu'il s'agit d'une nouvelle tâche pour les cantons et qu'il s'agira donc de veiller à développer un mécanisme de financement de cette tâche, par exemple par l'Administration numérique suisse (ANS), *a minima* pour la mise en place de ces points de contact cantonaux. En complément, un support sous le format d'un service desk global fourni dans les quatre langues nationales devrait être assuré par la Confédération. Nous relevons également qu'il s'agira de prévoir un support dans l'utilisation des moyens de preuve électroniques.

Notre Conseil propose de renoncer aux émoluments (art. 26) pour les cantons et les communes liés à leur inscription dans le registre de base et dans le système de confirmation des identifiants au titre d'émetteurs et de vérificateurs. En effet, les autorités sont tenues d'accepter l'e-ID (art. 9). L'art. 3, al. 2, OGEmol précise que l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes pour autant qu'ils lui accordent la réciprocité. Cette disposition devrait s'appliquer dans le contexte de cette loi également, notamment pour inciter les cantons et les communes à émettre des moyens de preuve électroniques à l'aide de l'infrastructure de confiance. De même, il s'agit d'exonérer de tout ou partie des émoluments d'autres acteurs prestataires de services publics, par exemple dans le domaine de la santé afin de favoriser l'adoption de ce système.

Si notre Conseil se réjouit de voir l'intention d'une convergence des bases légales concernant l'identité électronique, il tient à rappeler ses investissements dans la mise à disposition d'une identité électronique répondant aux exigences élevées de la loi sur le dossier électronique du patient (LDEP) et de ses ordonnances. Un effort important a été investi dans l'enrôlement de la population, notamment en faisant certifier plusieurs lieux d'enregistrement ainsi qu'en mettant en place la possibilité de s'inscrire intégralement en ligne, avec une vérification de l'identité par vidéo. Il souhaite que le nouveau système mis en place tienne compte du travail effectué et, dans la mesure du possible, ne nécessite pas de repartir de zéro au niveau de l'enrôlement.

En complément, nous vous faisons parvenir en annexe des remarques portant sur des articles spécifiques. Pour toute précision concernant cette annexe, vous pouvez vous adresser à M. Alexander Barclay, délégué au numérique du canton de Genève (alexander.barclay@etat.ge.ch).

Nous vous remercions de nous avoir consultés et vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancellerie :

A stylized, handwritten signature in black ink, consisting of several loops and a long vertical stroke.

Michèle Righetti

Le président :

A stylized, handwritten signature in black ink, featuring a large, sweeping loop at the top and several smaller loops below.

Mauro Poggia

Annexe mentionnée

Copie à : rechtsinformatik@bj.admin.ch

Annexe : Commentaires concernant l'avant-projet de loi fédérale et le rapport explicatif

Remarques générales

- Il serait utile d'ajouter un article de définitions, permettant de préciser ce qu'est un moyen de preuve électronique, un registre, un vérificateur, un identificateur.
- Si le rapport explicatif indique le caractère volontaire de l'identité numérique, cela n'est pas précisé dans le texte de la loi. Il pourrait être utile de le faire, par exemple à l'article 4.
- De façon générale (et notamment concernant les articles 8 et 9), il s'agira de préciser la planification et la date d'entrée en vigueur afin de permettre aux administrations cantonales et communales de se préparer de façon coordonnée et cohérente.
- Le rapport explicatif ne comprend aucune indication concernant les actions en responsabilité en cas de défauts du système mis en place par la Confédération susceptibles d'entraîner des lacunes dans les applications cantonales. Il convient de préciser ce point en se référant à des normes de qualité reconnues.

Remarques par article

Art. 1, al. 1, let. a

Nous proposons de préciser "au moyen d'identification électronique émis par l'État à l'intention de personnes physiques (identité électronique, e-ID)". Cela permet l'accord "une e-ID" à l'art. 2, al. a.

Art. 1, al. 1, let a

La présentation du but prévu à la lettre a prête à confusion, dès lors que deux buts distincts sont ici mélangés, soit la réglementation du moyen d'identification électronique émis par l'Etat (cf. Section 2 E-ID) et la réglementation applicable aux autres moyens de preuve électroniques proposés par des tiers privés (cf. Section 3 Autres moyens de preuves électroniques). Ces deux buts auraient dû faire l'objet d'une lettre chacun, l'article 1, lettres a à c, devenant l'article 1, lettres a à d.

Art. 1, al. 2, let. b

Nous proposons de préciser "la protection des données dès la conception et par défaut" (en lien avec la nouvelle loi fédérale sur la protection des données nLPD), ainsi que de remplacer "la sécurité des données" par "la sécurité de l'information et la sécurité opérationnelle des données", terminologie plus précise.

Art. 3

Concernant les conditions personnelles, le canton de Genève souhaite que le dispositif permette l'accès à une e-ID pour des publics amenés à utiliser des services publics numériques (p.ex. plateforme de démarches administratives en ligne, dossier électronique du patient, etc.). Les conditions personnelles actuelles excluent, à notre lecture, notamment les sans-papiers, certains cas liés de personnel d'organisations internationales et leur famille, ou des retraités résidant à l'étranger. Alternativement, le canton maintiendra son moyen d'identification électronique pour lui permettre de fournir des prestations publiques répondant aux bases légales cantonales.

Art. 4, al 2

En lien avec l'alinéa 1, est-ce que cela implique que les mineurs de moins de 14 ans doivent faire eux-mêmes la demande et donc que le représentant légal ou la représentante légale ne peut le faire pour eux ? De plus, il serait utile de mener une réflexion sur les cas d'usage

d'une e-ID pour les mineurs entre 14 et 18 ans ne nécessitant pas le consentement de leur représentant légal.

Art. 4, al. 3, let. a

Cette disposition indique que fedpol émet l'e-ID si l'identité du demandeur est vérifiée. Cette disposition ne précise toutefois pas qui vérifie et comment. Il est juste mentionné, à l'alinéa 4, que la photographie du demandeur peut être prélevée. A notre sens, l'article 4, alinéa 3, lettre a devrait être complété, à tout le moins par un renvoi aux dispositions pertinentes de la loi.

Art. 4, al. 4

Cette disposition indique que fedpol peut prélever des données biométriques pendant la procédure d'émission et les comparer avec des photographies dans ISA ou SYMIC. S'agissant de données sensibles selon la nLPD, cette disposition devrait être précisée. Que veut dire prélever ? Est-ce que ces « prélèvements » sont conservés ? Si oui, où, par qui et pendant combien de temps ?

Art. 4 et 5

Le projet mis en consultation ne prévoit pas de procuration et de représentation légale. Il s'agirait de préciser ce point.

Art. 5, al. 1, let. d, ch. 2

Il est prévu que fedpol révoque immédiatement une e-ID si les données d'identification personnelles ont été modifiées. Il s'agit d'envisager alors l'établissement automatique d'une nouvelle e-ID, simplifiant ainsi la vie de la population.

Art. 5, let. c

En cas de révocation d'une e-ID suite à un soupçon fondé d'utilisation abusive de l'e-ID, il s'agit de motiver et communiquer cette décision en l'indiquant comme susceptible de recours. Il s'agit par ailleurs de préciser dans la LeID qu'il existe une protection juridique efficace en cas de révocation.

Art. 6

Il y a un enjeu important en lien avec renouvellement de l'e-ID (ou plus largement de son cycle de vie), car aucune technologie ne dure aussi longtemps que les documents physiques d'identité. Si la solution ne traite pas correctement cette question du renouvellement on peut donc s'attendre à des ruptures de service pour cause d'expiration de l'identité numérique, qui conduiront à des mécontentements et finalement à des renoncements.

Art. 7

En lien avec l'art. 22 et les explications du rapport à ce sujet ("Il ne faut toutefois assumer que les titulaires qui n'ont peut-être pas pris connaissance des informations ainsi publiées violent automatiquement leur devoir de diligence au sens de l'article 7, al. 1."). Nous trouvons cette phrase un peu ambiguë par rapport aux conséquences pour les titulaires d'une e-ID. Il faudrait être plus au clair sur les conséquences et sur une éventuelle obligation pour le titulaire de consulter ces informations. A notre sens, la responsabilité ne devrait pas peser sur les épaules des titulaires.

Art. 9

Cet article s'applique à toute autorité ou tout service qui accomplit une tâche publique. Le terme "service accomplissant des tâches publiques" prête à confusion. La question se pose de savoir si cette disposition ne s'applique qu'aux autorités et à leurs administrations centralisée et décentralisée ou si cet article s'applique également aux entités privées délégataires d'une tâche publique. Par ailleurs, nous trouvons un peu étrange de régler

l'émission de ces e-ID mais de renvoyer à plus tard toutes les questions relatives à l'utilisation de ces e-ID.

Art. 10

Cette disposition énonce que les particuliers qui se présentent en personne doivent avoir la possibilité de s'identifier avec un moyen autre qu'une e-ID. Cette disposition ne s'applique pas en l'état pour l'accès à des prestations numériques, relativisant son caractère facultatif. Exiger, par exemple, l'utilisation d'une e-ID pour accéder à du matériel pédagogique en ligne utilisé à l'école obligatoire, reviendrait de fait à rendre l'utilisation de l'e-ID obligatoire, ou d'exclure une part des parents et élèves (voir également remarque sur le public ayant accès à une e-ID).

Art. 10

La fin de la disposition "pour autant que les exigences, notamment en matière de sécurité du processus, puissent également être remplies de cette manière" n'est pas suffisamment claire, dans la mesure où la personne s'identifierait avec un document d'identité valable. L'exemption est une notion sujette à interprétation qui peut vider de son sens la règle. Et, par ailleurs, l'interprétation littérale de l'article 10 semble être en contradiction avec le rapport, qui indique : "Ainsi, lorsqu'il est possible d'identifier une personne au moyen d'un document d'identité dans le cadre d'un processus requérant sa présence, la présentation de l'e-ID (ou des parties de celle-ci) ne peut être offerte qu'à titre optionnel".

Art. 11, al. 5

Nous proposons de préciser "... après la date de fin de validité".

Art. 12

Il serait plus cohérent et lisible d'écrire "moyens électroniques de preuve" dans l'ensemble de l'avant-projet de loi, afin d'éviter les ambiguïtés. À plus forte raison que dans l'article 12, alinéa 2, on ne peut se baser sur le pluriel pour déterminer quel est le nom qualifié par l'adjectif "électronique".

Art. 15, al. 1

Il est prévu que les moyens de preuve électroniques ne peuvent pas être transmis à un autre titulaire. Il y a toutefois des cas où cette transmission pourrait faire sens, à l'image du cercle familial ou pour les proches aidants.

Art. 16

Si l'intention est de permettre au titulaire de déterminer quelles informations sont transmises aux vérifications, il conviendrait de prévoir la possibilité d'un contrôle des vérificateurs privés par le préposé ou la préposée à la protection des données afin de prévenir le potentiel d'abus.

Art. 16, al. 3

Qui est l'exploitant des systèmes ? Il serait judicieux de se référer à l'exploitant de l'article 24, s'il s'agit bien de cet exploitant étatique unique. Par ailleurs, il semble incompréhensible que cet exploitant puisse, le cas échéant, tirer des conclusions sur l'utilisation des moyens de preuve. Les termes "dans toute la mesure du possible" devraient être supprimés.

Art. 18

Nous proposons la modification suivante : "~~Le Conseil fédéral peut prévoir que la~~ La Confédération confirme aussi les identifiants et les clés cryptographiques des émetteurs et vérificateurs privés." Il semble indispensable que les émetteurs et vérificateurs privés soient confirmés.

Art. 21, al. 3

Nous proposons d'ajouter une let. c "si l'e-ID est révoquée, ou que sa date de validité soit expirée depuis 5 ans", par analogie avec l'article 11, alinéa 5.

Art. 22

Nous estimons que la notion d'abus dans cette disposition est trop vague et qu'il convient de la préciser. Par ailleurs, nous nous demandons pourquoi le rapport indique (p. 16) : "L'exclusion des émetteurs du registre de base n'étant pas techniquement possible, l'avant-projet prévoit cette mesure afin de combattre les abus éventuels". Pourquoi ne pourrait-on pas les exclure ?

Art. 24

La notion de "prestataire de service" donne à penser qu'il s'agit d'un mandataire ou d'un sous-traitant malgré l'ajout de "au sein de l'administration fédérale". Cette formulation nous paraît pouvoir prêter à confusion, alors que c'est ici que se joue un enjeu majeur de la loi. A notre sens, la volonté populaire, qui a refusé la votation de mars 2021, signifiait de garder cette mission à l'interne de l'administration fédérale centrale, voire éventuellement à un établissement public dédié exclusivement à cette tâche, et non pas de la confier à une société anonyme, fût-elle de droit public.

Art. 26, al. 1

S'agit-il d'un émolument unique ou périodique ?

Remarques concernant les autres actes

- Afin d'assurer l'utilisation de l'e-ID dans les autres domaines pertinents, il s'agira de procéder à un examen systématique des dispositions fédérales contenant l'obligation de présenter un document d'identité physique ou exigeant une signature électronique qualifiée.

Regierungsrat
Rathaus
8750 Glarus

per E-Mail
rechtsinformatik@bj.admin.ch

Glarus, 4. Oktober 2022
Unsere Ref: 2022-1314

Vernehmlassung i. S. Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Hochgeachtete Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Eidgenössische Justiz- und Polizeidepartement gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und lassen uns gerne wie folgt vernehmen:

1. Grundsätzliches

1.1. Allgemeine Einschätzung

Der Regierungsrat des Kantons Glarus unterstützt die Vorlage zum neuen E-ID-Gesetz. Er begrüsst die rasche Erarbeitung einer neuen Vorlage, die unter dem umfassenden Einbezug kantonaler wie privater Akteure erfolgt ist. Aus Sicht des Regierungsrates ist die Schaffung einer einheitlichen staatlichen E-ID für die Schweiz unumgänglich, um zukunftsfähig zu bleiben und die Digitalisierung auch auf Ebene der öffentlichen Verwaltung voranzutreiben.

Der Regierungsrat ist der Ansicht, dass den Vorbehalten, die im März 2021 zur Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste geführt haben, mit dem vorliegenden Entwurf in angemessener und nachvollziehbarer Weise Rechnung getragen wird. Ausdrücklich begrüsst werden insbesondere die folgenden Punkte:

- Im Gegensatz zur in der Volksabstimmung gescheiterten Vorlage sieht der neue Entwurf eine Ausstellung der E-ID durch eine staatliche Stelle vor. Auch die nötige Infrastruktur wird durch den Bund zur Verfügung gestellt.
- Die Grundsätze von Datensparsamkeit, dezentraler Datenspeicherung und «privacy by design» entsprechen wichtigen Anliegen der Bevölkerung. Die Schweiz orientiert sich damit auch an den Vorgaben der geplanten europäischen Gesetzgebung (eIDAS-Verordnung).
- Die Vorlage berücksichtigt die Entwicklungen auf europäischer Ebene und ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um Anerkennung der schweizerischen E-ID im Ausland bzw. die Anerkennung ausländischer elektronischer Identitäten in der Schweiz zu erleichtern.

- Die Möglichkeit, die Vertrauensstruktur für das Ausstellen weiterer elektronischer Nachweise zu nutzen, und die kostenlose Ausstellung der E-ID für Privatpersonen ermöglichen eine schnellere Verbreitung und Akzeptanz der Infrastruktur.

1.2. Begriffsdefinitionen

Das BGEID verwendet eine Vielzahl von technischen Begriffen wie «elektronischer Nachweis», «Verifikatorin», «Basisregister», «Vertrauensregister» oder «Identifikator». Diese sind im allgemeinen Sprachgebrauch nicht geläufig und bedürfen daher einer genaueren Definition. Die entsprechenden Begriffe werden zwar teilweise im Rahmen einzelner Artikel (z. B. «Verifikatorin» in Art. 16) oder im Rahmen des erläuternden Berichts definiert. Die Verständlichkeit des Gesetzes und die Systematik würden indes profitieren, wenn eine neue Bestimmung (z. B. als Art. 2) aufgenommen würde, welche die relevanten Definitionen für das gesamte Gesetz vornimmt. Zu achten ist dabei auch auf eine klare Unterscheidung zwischen «elektronischen Nachweisen» (als Oberbegriff, der die E-ID und andere elektronische Nachweise umfasst) und «anderen elektronischen Nachweisen».

1.3. Sicherheit und Benutzerfreundlichkeit

Mitentscheidend für die künftige Verbreitung der E-ID und der Vertrauensinfrastruktur wird die Benutzerfreundlichkeit der entsprechenden Applikationen sein. Sie müssen für alle Beteiligten möglichst unkompliziert und niederschwellig zugänglich und anwendbar sein. Unter anderem an diesem Punkt sind in der Vergangenheit Vorhaben wie die qualifizierte elektronische Signatur gescheitert. Gleichzeitig darf Benutzerfreundlichkeit nicht auf Kosten von Sicherheit und Datenschutz gehen. Hierbei ist den Schutzziele der Authentizität und der Verbindlichkeit besonderes Gewicht beizumessen. Sind diese nicht gewährleistet, entstehen hohe Risiken, nicht nur für die betroffenen Personen, sondern auch für die öffentlichen Organe und die Privaten, die auf die Bestätigung der Identität des Gegenübers angewiesen sind. Spätestens bei Bekanntwerden vom Missbrauchsfällen hätten Sicherheitslücken zudem einen Vertrauensverlust zur Folge, mit den entsprechenden Konsequenzen für die Verbreitung der E-ID und die Nutzung der Vertrauensinfrastruktur. Den Aspekten der Benutzerfreundlichkeit und der Sicherheit wird somit bei der Ausarbeitung der bundesrätlichen Verordnung besondere Beachtung zu schenken sein. Die Infrastruktur muss laufend den technischen Veränderungen angepasst werden können.

1.4. Koordination mit Vollzugsträgern

Die Umsetzung des BGEID und insbesondere seiner Artikel 8 und 9 verlangt nach umfassenden Massnahmen auf Ebene der Kantone und Gemeinden. Im erläuternden Bericht fehlen jedoch Ausführungen zur Notwendigkeit, die Umsetzung mit den Vollzugsträgern koordiniert zu planen. Auch werden keine Angaben gemacht zum Zeitbedarf für die Umsetzung in den Kantonen und Gemeinden (gemäss Art. 8 VIV) sowie zum geplanten Zeitpunkt des Inkrafttretens. Die Kantonsregierungen erwarten in der Botschaft des Bundesrates entsprechende Ausführungen. Eine koordinierte Umsetzung gemäss dem Arbeitspapier von Bund und Kantonen vom 28. Oktober 2015 ist an die Hand zu nehmen.

Der Regierungsrat erinnert daran, dass die Digitalisierung der Verwaltung auf Kantons- und Gemeindeebene bereits in vollem Gange ist. Es wurden bereits und werden in den nächsten Jahren weitere grosse Investitionen vorgenommen. Für die Kantone ist es deshalb von entscheidender Bedeutung, dass die Identifizierung über die E-ID sich technisch problemlos in ihre bestehenden Anwendungen integrieren lässt. Der erläuternde Bericht (Kap. 5.2., S. 20-21) geht pauschal davon aus, dass Kantone und Gemeinden von der E-ID und der Vertrauensinfrastruktur profitieren werden, was ihre (nicht weiter bezifferten) Aufwände in jedem Fall rechtfertigen werde. Diese Ausführungen genügen nicht. Es ist eine detailliertere Kostenfolgebabschätzung vorzunehmen, und der Berücksichtigung der Anschlussfähigkeit bestehender Lösungen ist bei der Ausarbeitung der technischen Details vorrangige Beachtung zu schenken.

1.5. Haftung und Qualitätsstandards

Die E-ID wird zur Identifizierung in kantonalen elektronischen Diensten zur Anwendung kommen und kantonale Lösungen ergänzen. Im erläuternden Bericht fehlen jedoch Ausführungen zum Umgang mit Haftungsansprüchen, sollten Fehler im System des Bundes zu Lücken in den kantonalen Anwendungen führen. Entsprechende Angaben mit Bezug zu anerkannten Qualitätsstandards (Standard eCH-0170) sind im Hinblick auf nachfolgende Ausführungsbestimmungen in der Botschaft zu ergänzen.

1.6. Vollmacht und gesetzliche Vertretung

Weder im Entwurf noch im erläuternden Bericht sind Hinweise zu finden auf die Abläufe in Zusammenhang mit Vollmachten und der gesetzlichen Vertretung. Gemäss Artikel 4 und 5 BGEID ist zur Ausstellung einer E-ID für Minderjährige bis 14 Jahre und Personen unter umfassender Beistandschaft das Einverständnis der gesetzlichen Vertretung nötig. Es fehlen aber Aussagen zu späteren Vertretungs- und Delegationsmöglichkeiten in der Nutzung der E-ID oder in der Anwendung anderer Nachweise. Im Interesse einer einheitlichen Vollzugspraxis ist eine entsprechende Klärung in der Botschaft wichtig.

2. Bemerkungen zu einzelnen Artikeln des BGEID

Artikel 1

Artikel 7 des neuen Datenschutzgesetzes (nDSG) postuliert neben dem Grundsatz des «Datenschutz durch Technik» («privacy by design») jenen der «datenschutzfreundlichen Voreinstellungen» («privacy by default»). Letzterer ist in Artikel 1 Absatz 2 Buchstabe b zusätzlich aufzuführen, um diesem zentralen Aspekt Betonung zu verleihen und eine Harmonisierung mit dem nDSG sicherzustellen.

Artikel 3; Persönliche Voraussetzungen

Artikel 3 E-BGEID sieht vor, dass nur Personen mit geregelter Aufenthalt in der Schweiz eine E-ID beantragen können. Der Kreis der Personen, die mit kantonalen Verwaltungen interagieren, ist aber weiter gefasst. Zu denken ist unter anderem an Personen, die ohne geregelten Aufenthalt in der Schweiz wohnhaft sind («Sans-Papiers») oder an Zweitwohnungsbesitzer. Es ist zumindest die Möglichkeit zu prüfen, für solche Fälle eine spezifische E-ID auszustellen. Die Gesetzesvorlage ist entsprechend so zu ergänzen, dass der Bundesrat ermächtigt wird, für weitere Personen mit Aufenthalt in der Schweiz eine spezielle E-ID mit eingeschränktem Einsatzbereich vorzusehen.

Gemäss dem erläuternden Bericht (S. 9 zu Art. 3) sollen Anbieterinnen die Möglichkeit haben, die Nutzung ihrer Dienste für die Inhaberinnen und Inhaber gewisser Ausweiskategorien zu beschränken. Der Bericht weist darauf hin, dass bei Ausweisen der Kategorien N, F, S und Ci nicht davon ausgegangen werden könne, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. Es ist festzuhalten, dass die Verlässlichkeit der Identifizierung einer Person nicht aus der Kategorie ihres Ausweises ersichtlich ist (nicht jede asylsuchende Person kann keine Identitätsdokumente vorweisen, während über eine Härtefallbewilligung auch Personen, deren Identität nicht abschliessend geklärt ist, unter Umständen einen Ausweis B erhalten können). Sollen Einschränkungen spezifisch aufgrund der Verlässlichkeit der Identitätsdokumente möglich sein, so ist dies im Gesetz auszuführen und eine entsprechende Angabe ist unter die Daten gemäss Artikel 2 Absatz 3 BGEID aufzunehmen. Ein blosser Verzicht auf eine gesetzliche Regelung, ohne dass die entsprechende Angabe in der E-ID erfasst wird, geht am Ziel vorbei.

In Artikel 3 Buchstabe a wird konkret das Ausweisgesetz (AwG) genannt. Es ist nicht nachvollziehbar, weshalb in Artikel 3 Buchstabe b bloss allgemein auf die Ausländergesetzgebung verwiesen und nicht die konkreten Gesetze (Ausländer- und Integrationsgesetz und

Asylgesetz) genannt werden. Für Aussenstehende ist mit der heutigen Formulierung nicht ersichtlich, welche gesetzlichen Bestimmungen angewendet werden.

Artikel 4; Ausstellung

Der Ausstellungsprozess und damit verbunden die Frage, wie die Identifizierung der antragsstellenden Personen durchgeführt wird, sind für die Sicherheit und damit auch für die künftige Akzeptanz der E-ID zentral. Eine Regelung des Ausstellungsprozesses muss deshalb ins Gesetz aufgenommen werden. Dabei dürfen Sicherheitsüberlegungen nicht hinter Kosten- und Effizienzfragen zurückstehen. Artikel 6 Absatz 5 nDSG statuiert die Pflicht des Datenbearbeiters oder der Datenbearbeiterin, sich über die Richtigkeit der Personendaten zu vergewissern. Die Angemessenheit der Massnahmen muss sich dabei auch nach dem – im Falle der E-ID erheblichen – Risiko für die Grundrechte der betroffenen Person richten.

Der Entwurf sieht gemäss Artikel 4 Absatz 2 vor, dass ab dem 15. Altersjahr die E-ID eigenständig beantragt werden kann. Nach Artikel 5 Absatz 1 AwG brauchen Minderjährige dagegen zum Bezug eines (physischen) Ausweises die Einwilligung Ihres gesetzlichen Vertreters. Die Begründung des erläuternden Berichtes zu diesem Unterschied überzeugt nicht. Im Vordergrund sollten Sicherheitsüberlegungen stehen und nicht die Frage, welche Ausweisarten von Jugendlichen mehrheitlich genutzt werden. Die Altersgrenze zum selbständigen Bezug einer E-ID ist somit jener zum Bezug eines physischen Ausweises anzugleichen.

Artikel 5; Widerruf

Artikel 5 Buchstabe d Ziffer 2 legt fest, dass die E-ID widerrufen wird, wenn das fedpol über eine Änderung der Personenidentifizierungsdaten des Inhabers oder der Inhaberin informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen müssen sich dann nicht noch einmal um die Ausstellung einer neuen E-ID bemühen und profitieren so von den erleichterten Abläufen, die durch die Digitalisierung ermöglicht werden.

Artikel 6; Gültigkeitsdauer

Neben der Gültigkeitsdauer ist im Entwurf auch die Frage der Verlängerung nicht geregelt. Es wird nicht klar, ob nach Ablauf des physischen Ausweisdokuments – sofern die Gültigkeit der E-ID an diese geknüpft wird – erneut eine E-ID beantragt werden muss oder ob dies bei Verlängerung des Ausweises automatisch geschieht. Dies ist spätestens in der Verordnung ebenfalls zu klären.

Artikel 7; Sorgfaltspflicht

Artikel 7 E-BGEID sieht eine Sorgfaltspflicht für Inhaberinnen und Inhaber einer E-ID vor. Nicht konkret geregelt sind dabei die Verpflichtungen bei Verlust des E-ID-Trägers, dies im Gegensatz zu Artikel 8 AwG, das eine Meldepflicht bei Verlust eines (physischen) Ausweises vorsieht. Zur Konkretisierung der Sorgfaltspflichten ist dieser Fall auch im BGEID auszuführen.

Artikel 8; Anlaufstellen der Kantone

Die Bestimmung sieht eine zusätzliche Aufgabe für die Kantone vor. Der erläuternde Bericht zur Vernehmlassungsvorlage geht davon aus, dass die benötigten Strukturen in den Kantonen bereits vorhanden sind. Dies ist jedoch nicht notwendigerweise der Fall.

Als Vollzugsträger steht hier der Bund in der Verantwortung. Wer eine Informatiklösung anbietet und betreibt, hat auch den nötigen Support sicherzustellen, soweit die eigene Anwendung betroffen ist. Die Kantone sehen sich da als zuständig, wo es darum geht, Unterstützung beim Einsatz der E-ID für kantonale E-Government-Angebote zu leisten. Für Schwierigkeiten bei der Beantragung der E-ID oder bei der Nutzung der Vertrauensinfrastruktur muss

dagegen der Bund eine Ansprechstelle schaffen. Eine solche ist im erläuternden Bericht zwar erwähnt, sie fehlt jedoch im Gesetzesentwurf ebenso wie der Second Level Support, den der Bund gemäss dem Bericht für die Kantone wahrnehmen soll.

Unter Bezugnahme auf die Ausführungen im erläuternden Bericht ist zudem darauf hinzuweisen, dass Personen, die bereit sind, eine E-ID zu nutzen, üblicherweise auch in der Lage sind, einen Support per Telefon oder E-Mail in Anspruch zu nehmen. Es müssen dafür nicht zwingend physische Anlaufstellen geschaffen werden.

Artikel 9; Pflicht zur Akzeptanz der E-ID

Artikel 9 E-BGEID sieht vor, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Der Begriff der «öffentlichen Aufgabe» wird im erläuternden Bericht mit «Verwaltungsaufgaben» gleichgesetzt, was dem Begriff von Artikel 178 Absatz 3 BV entspricht. Es empfiehlt sich, im BGEID ebenfalls von «Verwaltungsaufgaben» zu sprechen, oder, falls der Begriff der «öffentlichen Aufgabe» weiter gefasst werden soll, die Botschaft in diesem Punkt zu präzisieren. Es ist zu bedenken, dass unter anderem im Gesundheitswesen eine Vielzahl von privaten Akteuren öffentliche Aufgaben ausführen, so zum Beispiel Krankenversicherer, Betreiber von Krebsregistern und Transplantationsregistern oder Anbieter des EPD. Die Pflicht zur Akzeptanz der zukünftigen E-ID bei all diesen Akteuren ist durchaus sinnvoll, wird aber Investitionen und Vorbereitungsarbeiten zur Folge haben, die den Betroffenen möglichst rasch klar kommuniziert werden müssen. Es ist somit wichtig, dass bei allen Beteiligten von Anfang an Klarheit herrscht über den Geltungsbereich von Artikel 9 BGEID.

Die Umsetzung von Artikel 9 E-BGEID bedingt eine Integration der E-ID in bestehende IT-Anwendungen von Kantonen und Gemeinden. Diesen ist dafür eine ausreichende Übergangsfrist einzuräumen.

Artikel 13; Widerruf

Analog zur Regelung bei der E-ID (Art. 5 Bst. d Ziff. 3) sollten auch andere elektronische Nachweise unverzüglich durch die Ausstellerinnen widerrufen werden, wenn die Inhaberin oder der Inhaber verstorben ist.

Artikel 15; Übertragbarkeit von elektronischen Nachweisen

Die Hinweise zu Artikel 15 Absatz 2 E-BGEID im erläuternden Bericht (S. 13) lassen sich nur schwer mit der Bestimmung im Entwurf selber vereinbaren. Während sich Artikel 15 Absatz 2 mit der Übertragbarkeit von Nachweisen befasst, nimmt der erläuternde Bericht Bezug auf ein System für Sicherungskopien. Sollte mit der Bestimmung tatsächlich nur die Übertragbarkeit in ein System für Sicherungskopien gemeint sein, ist dies entsprechend zu formulieren.

Artikel 16; Vorweisen von elektronischen Nachweisen

Artikel 16 Absatz 1 bestimmt, dass die Inhaberin bzw. der Inhaber einer E-ID selber darüber bestimmt, welche Informationen an die betreffende Verifikatorin übermittelt werden. In der Praxis werden dennoch oft die Verifikatorinnen darüber bestimmen, da die Person ansonsten vom Angebot keinen Gebrauch machen kann. In der zu erarbeitenden Botschaft sind deshalb Ausführungen zu machen, wie die Beschränkung der Datenbearbeitung auf das Minimum bei privaten Verifikatorinnen sichergestellt werden soll und wie trotz der dezentralen Struktur des Systems eine wirksame Kontrolle möglich ist.

Artikel 17; Basisregister

Wie der erläuternde Bericht (S. 14) ausführt, birgt die Tatsache, dass Ausstellerinnen ohne weitere Überprüfung ihre Daten selber ins Basisregister gemäss Artikel 17 Absatz 3 E-BGEID eintragen können, das Risiko, dass diese unter falscher Identität elektronische Beweismittel ausstellen können. Es liegt auf der Hand, dass dies für die betroffenen Personen unter Umständen weitreichende Folgen haben kann. Die Abfederung dieses Risikos durch Veröffentlichung bei begründetem Verdacht gemäss Artikel 22 EBGEID ist nicht ausreichend, da sie bereits eine Verletzung der Persönlichkeitsrechte von betroffenen Personen voraussetzt. Auch können durch blosses Öffentlichmachen erfahrungsgemäss nicht alle Nutzenden rechtzeitig erreicht werden. Ein Eintrag ins Vertrauensregister nach Artikel 18 E-BGEID muss entsprechend auch für private Anbieter zwingend sein. Andernfalls können Missbräuche nicht verhindert werden.

Artikel 20; Anwendung zur Prüfung von elektronischen Nachweisen

Aus dem Wortlaut von Artikel 20 E-BGEID wird nicht klar, dass es dabei um eine Prüfung von elektronischen Nachweisen bei persönlichem Erscheinen und nicht um einen Online-Vorgang geht. Dies muss deutlicher ausgeführt werden. In jedem Fall ist bei der technischen Umsetzung – mithilfe einer Anwendung nach Artikel 20 oder ohne – sicherzustellen, dass eine zuverlässige Überprüfung der Gültigkeit von elektronischen Nachweisen für die Verifikatorinnen ohne weiteres möglich ist.

Zudem beantragen wir anstelle einer Kann-Bestimmung, dass der Bund zwingend eine Anwendung zur Verfügung stellt, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können. Andernfalls müssten die Kantone allenfalls eigene Anwendung schaffen, was aus systemischer Sicht nicht effizient ist.

Artikel 21; System für Sicherungskopien

Analog zu Artikel 20 sollte der Bund auch zwingend ein System zur Verfügung stellen, dem die Inhaberinnen und Inhaber Sicherungskopien ihrer elektronischen Nachweise zur Aufbewahrung übergeben können (keine Kann-Bestimmung). Damit kann die Akzeptanz elektronischer Nachweise letztlich positiv beeinflusst werden.

In Absatz 3 ist zudem eine Regelung aufzunehmen, wie mit Sicherungskopien von Inhaberinnen und Inhabern umgegangen wird, die verstorben sind.

Artikel 25; Technische Entwicklung

Die Funktionsweise von Absatz 2 dieser Bestimmung ist unklar: Wer entscheidet darüber, ob ein Anwendungsfall von Absatz 2 vorliegt? Entscheidet dies der Bundesrat bereits mit dem Erlass der Verordnung? Zudem ist der Zusammenhang zwischen Absatz 1 und Absatz 2 von Artikel 25 im Text deutlicher hervorzuheben und es sollte der Vollständigkeit halber der Fall des fakultativen Referendums miterfasst werden:

«² Sofern Bestimmungen, die gestützt auf Abs. 1 erlassen werden, einer weiteren Grundlage in einem Gesetz bedürfen, treten diese Bestimmungen ausser Kraft:

a) [...]

b) mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung oder die Stimmberechtigten; oder [...]»

Artikel 26; Gebühren

Artikel 26 BGEID sieht vor, dass von Ausstellerinnen und Verifikatorinnen elektronischer Nachweise Gebühren erhoben werden. Dies betrifft auch Stellen, die öffentliche Aufgaben erfüllen, obwohl diese gemäss Artikel 9 BGEID zur Akzeptanz der E-ID verpflichtet sind. Gleichzeitig möchte der Bundesrat die E-ID durch Beiträge aus der Digitalen Verwaltung

Schweiz finanzieren, die von den Kantonen mitfinanziert wird. Gemäss Artikel 3 Absatz 2 AllgGebV verzichtet die Bundesverwaltung auf die Erhebung von Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Dies soll auch vorliegend entsprechend gehandhabt und Verrechnungen zwischen den Gemeinwesen auf ein Minimum beschränkt werden.

Der Bundesrat soll darüber hinaus mit der Kompetenz ausgestattet werden, die Gebühren für weitere Akteure ganz oder teilweise zu erlassen, soweit diese öffentliche Aufgaben erfüllen. Unter anderem besteht im Gesundheitsbereich ein grosses Interesse an einer breiten Nutzung der E-ID, um die Aufbereitung von Gesundheitsdaten zu erleichtern. Die Kosten für die betroffenen Stellen sind somit möglichst tief zu halten.

Die Vorlage und der erläuternde Bericht äussern sich nicht bzw. nur sehr vage über die Höhe der zu erhebenden Gebühren. Diese sollen auf Verordnungsstufe festgelegt werden. Die Kosten dürften jedoch einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben. Eine explizite Kostenfolgeschätzung für die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise aufgrund der Gebühren sollte deshalb in die Botschaft aufgenommen werden.

Artikel 28; Ausführungsbestimmungen

Zahlreiche technische Aspekte zur Umsetzung der E-ID werden auf Verordnungsstufe geregelt. Aufgrund der unterschiedlichen bestehenden Lösungen in den einzelnen Kantonen, aber auch in den einzelnen Sektoren ist es unabdingbar, dass die zuständigen Akteure eng in die Erarbeitung der Vollzugsregelungen miteinbezogen werden. Es ist eine der Voraussetzungen einer breiten Akzeptanz der E-ID, dass diese unkompliziert in bestehende Anwendungen integriert werden kann.

Artikel 29; Änderung anderer Erlasse

Gemäss dem erläuternden Bericht (Ziff. 3.1) wurde die Verwendung der E-ID in spezifischen Bereichen und damit die Änderung anderer Erlasse im Entwurf nur exemplarisch geregelt. Es ist unabdingbar, die Gesetzgebung des Bundes im weiteren Verfahren systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder eine qualifizierte elektronische Signatur verlangt werden. Dies betrifft insbesondere auch die Verfahrensgesetzgebung des Bundes. Die entsprechenden Bestimmungen sind durchgehend anzupassen.

Genehmigen Sie, hochgeachtete Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Für den Regierungsrat

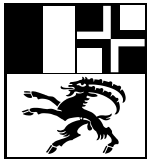


Benjamin Mühlemann
Landammann



Hansjörg Dürst
Ratsschreiber

E-Mail an (PDF- und Word-Version):
- rechtsinformatik@bj.admin.ch



Sitzung vom

17. Oktober 2022

Mitgeteilt den

17. Oktober 2022

Protokoll Nr.

804/2022

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per E-Mail (PDF- und Word-Version) zustellen an: rechtsinformatik@bj.admin.ch

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 erhalten die Kantone Gelegenheit, sich zu erwähn-
tem Geschäft zu äussern. Dafür danken wir Ihnen bestens.

Die uns zugesandte Dokumentation haben wir geprüft. Die Regierung begrüsst
grundsätzlich den Vorentwurf des Bundesgesetzes über den elektronischen Identi-
tätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

I. Allgemeine Bemerkungen

1. Grundsätzliches

Vor dem Hintergrund des in der Volksabstimmung im Jahr 2021 abgelehnten Bun-
desgesetzes über elektronische Identifizierungsdienste wurden die Bedenken der
Bevölkerung aufgenommen. Mit dem neuen Vernehmlassungsentwurf wird nun ein
Konzept verfolgt, welches die Herausgabe elektronischer Identitäten nicht mehr

durch Private, sondern alleine durch den Staat vorsieht. Die Ausgestaltung der Vorlage nimmt die Forderungen der nach der Volksabstimmung eingereichten Motionen auf und stellt die Grundsätze "privacy by design", Datensparsamkeit und dezentrale Datenspeicherung ins Zentrum, wodurch dem Schutz der Persönlichkeit Rechnung getragen werden kann. Ebenfalls zu begrüßen ist, dass nach den gleichen Grundsätzen die Grundlagen für ein Ökosystem weiterer elektronischer Nachweise geschaffen werden sollen, um eine umfassende Digitalisierung zu ermöglichen.

Hinsichtlich der technischen Ausgestaltung bleibt das Gesetz berechtigterweise unbestimmt, so dass die laufenden technischen Entwicklungen vor dem Hintergrund der datenschutzrechtlichen Vorgaben (Art. 1 Abs. 2 lit. b BGEID) übernommen werden können, ohne die rechtlichen Grundlagen anpassen zu müssen. Naturgemäss leidet darunter die Präzision der Bestimmungen. Dieser Mangel ist jedoch gegenüber der Flexibilität von untergeordneter Bedeutung.

2. Begriffsdefinitionen

Das BGEID verwendet eine Vielzahl von technischen Begriffen wie "elektronischer Nachweis", "Verifikatorin", "Basisregister", "Vertrauensregister" oder "Identifikator". Diese sind im allgemeinen Sprachgebrauch nicht geläufig und bedürfen daher einer genaueren Definition. Die entsprechenden Begriffe werden zwar teilweise im Rahmen einzelner Artikel (z.B. "Verifikatorin" in Art. 16 BGEID) oder im Rahmen des erläuternden Berichts (nachfolgend: EB) definiert. Die Verständlichkeit des Gesetzes und die Systematik würden indes profitieren, wenn eine neue Bestimmung (z.B. als Art. 2 BGEID) aufgenommen würde, welche die relevanten Definitionen für das gesamte Gesetz vornimmt. Zu achten ist dabei auch auf eine klare Unterscheidung zwischen "elektronischen Nachweisen" (als Oberbegriff, der die E-ID und andere elektronische Nachweise umfasst) und "anderen elektronischen Nachweisen".

3. Sicherheit und Benutzerfreundlichkeit

Mitentscheidend für die künftige Verbreitung der E-ID und der Vertrauensinfrastruktur wird die Benutzerfreundlichkeit der entsprechenden Applikationen sein. Sie müssen für alle Beteiligten möglichst unkompliziert und niederschwellig zugänglich und anwendbar sein. Unter anderem an diesem Punkt sind in der Vergangenheit Vorhaben

wie die qualifizierte elektronische Signatur gescheitert. Gleichzeitig darf Benutzerfreundlichkeit nicht auf Kosten von Sicherheit und Datenschutz gehen. Hierbei ist den Schutzzielen der Authentizität und der Verbindlichkeit besonderes Gewicht beizumessen. Sind diese nicht gewährleistet, entstehen hohe Risiken, nicht nur für die betroffenen Personen, sondern auch für die öffentlichen Organe und die Privaten, die auf die Bestätigung der Identität des Gegenübers angewiesen sind. Spätestens bei Bekanntwerden vom Missbrauchsfall hätten Sicherheitslücken zudem einen Vertrauensverlust zur Folge, mit den entsprechenden Konsequenzen für die Verbreitung der E-ID und die Nutzung der Vertrauensinfrastruktur. Den Aspekten der Benutzerfreundlichkeit und der Sicherheit wird somit bei der Ausarbeitung der bundesrätlichen Verordnung besondere Beachtung zu schenken sein. Die Infrastruktur muss laufend den technischen Veränderungen angepasst werden können.

4. Koordination mit Vollzugsträgern

Die Umsetzung des BGEID und insbesondere seiner Art. 8 und Art. 9 verlangt nach umfassenden Massnahmen auf Ebene der Kantone und Gemeinden. Im EB fehlen jedoch Ausführungen zur Notwendigkeit, die Umsetzung mit den Vollzugsträgern koordiniert zu planen. Auch werden keine Angaben gemacht zum Zeitbedarf für die Umsetzung in den Kantonen und Gemeinden (gemäss Art. 8 der Vernehmlassungsverordnung, VIV; SR 172.061.1) sowie zum geplanten Zeitpunkt des Inkrafttretens. Wir erwarten in der Botschaft des Bundesrates entsprechende Ausführungen. Eine koordinierte Umsetzung gemäss dem Arbeitspapier von Bund und Kantonen vom 28. Oktober 2015 ist an die Hand zu nehmen.

Wir erinnern daran, dass die Digitalisierung der Verwaltung auf Kantons- und Gemeindeebene bereits in vollem Gange ist. Es wurden bereits und werden in den nächsten Jahren weitere grosse Investitionen vorgenommen. Für die Kantone ist es deshalb von entscheidender Bedeutung, dass die Identifizierung über die E-ID sich technisch problemlos in ihre bestehenden Anwendungen integrieren lässt. Der EB (Kap. 5.2., S. 20-21) geht pauschal davon aus, dass Kantone und Gemeinden von der E-ID und der Vertrauensinfrastruktur profitieren werden, was ihre (nicht weiter bezifferten) Aufwände in jedem Fall rechtfertigen werde. Diese Ausführungen genügen

nicht. Es ist eine detailliertere Kostenfolgeabschätzung vorzunehmen, und der Berücksichtigung der Anschlussfähigkeit bestehender Lösungen ist bei der Ausarbeitung der technischen Details vorrangige Beachtung zu schenken.

5. Haftung und Qualitätsstandards

Die E-ID wird zur Identifizierung in kantonalen elektronischen Diensten zur Anwendung kommen und kantonale Lösungen ergänzen. Im EB fehlen jedoch Ausführungen zum Umgang mit Haftungsansprüchen, sollten Fehler im E-ID-System zu Lücken in den kantonalen Anwendungen führen. Entsprechende Angaben mit Bezug zu anerkannten Qualitätsstandards (Standard eCH-0170) sind im Hinblick auf nachfolgende Ausführungsbestimmungen in der Botschaft zu ergänzen.

6. Vollmacht und gesetzliche Vertretung

Weder im Entwurf noch im EB sind Hinweise zu finden auf die Abläufe in Zusammenhang mit Vollmachten und der gesetzlichen Vertretung. Gemäss Art. 4 und Art. 5 BGEID ist zur Ausstellung einer E-ID für Minderjährige bis 14 Jahre und Personen unter umfassender Beistandschaft das Einverständnis der gesetzlichen Vertretung nötig. Es fehlen aber Aussagen zu späteren Vertretungs- und Delegationsmöglichkeiten in der Nutzung der E-ID oder in der Anwendung anderer Nachweise. Im Interesse einer einheitlichen Vollzugspraxis ist eine entsprechende Klärung in der Botschaft wichtig.

7. Fehlende Ausführungen zur Funktionsweise des elektronischen Identitätsnachweises

Die technologieneutrale Ausgestaltung des Gesetzesentwurfs ist aufgrund der laufenden technischen Entwicklungen grundsätzlich zu begrüßen, da nur auf diese Weise die Flexibilität und Zukunftsorientiertheit des Gesetzes sichergestellt werden kann. Kritisch ist jedoch anzumerken, dass auch im Rahmen des EB Aussagen zur vorgesehenen Ausgestaltung der Lösung weitgehend fehlen. Es werden zwar verschiedene Schlagworte wie "Self Sovereign Identity" im Rahmen des EB genannt, ohne jedoch auszuführen, wie eine entsprechende Lösung ausgestaltet sein könnte. Dies macht es für Personen, welche die Debatte und insbesondere die informelle öffentliche Konsultation bisher nicht verfolgt haben schwierig, sich eine abschliessende Meinung zum Erlass zu bilden. Es wird daher angeregt, dass zumindest im Rahmen

der Botschaft etwas konkreter auf die Ausgestaltung der möglichen Lösung eingegangen werden soll.

8. E-ID mit und ohne Identitätsnachweis

Die vom Volk am 7. März 2021 deutlich abgelehnte Vorlage hatte den Titel "Bundesgesetz über elektronische Identifizierungsdienste". Diese sprachliche Verschiebung weg von "Identifizierung" neu hin zu "Identitäts(-nachweis) stiftet Verwirrung. So benötigt die ausländische Wohnbevölkerung bloss einen gültigen Ausweis nach Ausländer- und Integrationsgesetz (AIG; SR 142.20) vorzuweisen, um eine E-ID ausgestellt zu erhalten. In seiner physischen Form gilt ein solcher Ausländerausweis nun aber einerseits nie als Identitätsausweis. Andererseits kann bei bestimmten Ausweiskategorien nicht davon ausgegangen werden, dass vorgängig die Identität der betreffenden Personen verlässlich festgestellt werden konnte (so N, F, S und Ci). Mit anderen Worten kann bei der Grundlage, die zur Ausstellung einer E-ID führt, unterschieden werden in:

- E-ID mit Identitätsnachweis
- E-ID ohne Identitätsnachweis

Der Gesetzgeber möchte darauf verzichten, den beiden in ihrer Fundiertheit und Aussagekraft doch unterschiedlichen E-ID-Konstellationen unterschiedliche rechtliche Wirkungen beizumessen. So wird in Art. 9 BGEID festgehalten, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Des Weiteren liest man in den Erläuterungen: *"Dies ist angezeigt, weil die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet wird und damit vergleichbar ist mit Identitätskarte oder Pass in der physischen Welt, die auch bei jeder Identifizierung von allen Behörden akzeptiert werden."* Klar ist, dass die E-ID in ihrer Wirkung nicht über diejenige des Ausländerausweises gehen darf. Dies soll so auch im Gesetz festgehalten sein. Um Missverständnissen vorzubeugen, erscheint es zudem sinnvoll, dass der Gesetzgeber terminologisch sehr deutlich zwischen einem Identifikationsmittel und dem Identitätsnachweis unterscheidet. Mit dem Ausländerausweis kann sich die betroffene Person als diejenige identifizieren, der in der Schweiz ein Aufenthaltsrecht unter den im Ausweis genannten Daten (Namen, Geburtsdatum etc.) bewilligt worden ist. Ob diese Daten auch der tatsächlichen Identität entsprechen, ist hiervon klar zu trennen. Insofern kann es nach dem Gesagten

nicht genügen, im EB zu Art. 3 BGEID die Problematik aufzuzeigen ("fehlender Identitätsnachweis"), daran aber keine Konsequenzen zu knüpfen. Hier gilt es dringend, anzusetzen und zu differenzieren.

9. Sprachliche Form des Vorentwurfs

Im Vorentwurf sind noch einige Formulierungen enthalten, welche noch nicht einheitlich gendergerecht scheinen. Art. 5 BGEID verwendet beispielsweise die männliche und die weibliche Form, Art. 13 Abs. 1 BGEID nur die weibliche Form, Art. 13 Abs. 2 BGEID wieder beide, Art. 17 Abs. 1 BGEID nur die weibliche. Dies ist zu korrigieren.

II. Bemerkungen zu den einzelnen Bestimmungen des BGEID

Art. 1 BGEID: (Marginalie fehlt)

Es wird ausdrücklich begrüsst, dass auf den Schutz der Persönlichkeit und die technischen Möglichkeiten hingewiesen wird. Indessen bezweckt das Gesetz lediglich die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten. Dabei sind die in Art. 1 Abs. 2 lit. b - d BGEID aufgeführten Aspekte zu berücksichtigen. Sie bilden nicht Zweck des Gesetzes, sondern Massnahmen für die Zweckerfüllung. Es wird deshalb beantragt, einen neuen Art. 1 Abs. 3 einzufügen, der Art. 1 Abs. 2 lit. b - d BGEID beinhaltet.

Gemäss Art. 1 Abs. 1 Bst. a wird im BGEID die Ausstellung einer E-ID an natürliche Personen geregelt. Der EB (S. 8 zu Art. 3 BGEID) weist darauf hin, dass juristische Personen nicht Inhaber einer E-ID sein können. Wir unterstützen diesbezüglich den Standpunkt des Bundes. Die E-ID für juristische Personen würde dem Identity & Access Management-Konzept des Kantons Graubünden widersprechen. Eine juristische Person wird immer von einer oder mehreren natürlichen Person(en) vertreten. Ein Einbezug von juristischen Personen wird deshalb abgelehnt.

Art. 2 BGEID: Form und Inhalt

Weder aus der Formulierung noch aus den Erläuterungen wird die in Art. 2 BGEID aufgeführte Aufzählung von Attributen plausibel. Unter dem Titel "Personenidentifizierungsdaten" (Art. 2 Abs. 2 BGEID) werden Daten aufgeführt, die eine Person iden-

tifizieren sollen. Die AHV-Nummer, welche für sich alleine eine Person individualisiert, wird jedoch unter dem Titel "Folgende Daten" (Art. 2 Abs. 3 BGEID) festgehalten. Die E-ID enthält gemäss Gesetz alle Daten gemäss Art. 2 Abs. 2 und 3 BGEID. Aus dem Gesetz geht nicht hervor, welche Daten gegen aussen erkennbar sind. Es darf sein, dass für jedermann die AHV-Nummer erkennbar ist. In Art. 16 Abs. 1 BGEID wird wohl festgehalten, die Inhaberin des elektronischen Nachweises bestimme, welche Bestandteile des Nachweises an Behörden oder Private, die elektronische Nachweise überprüfen, übermittelt werden. Diese Vorgehensweise entspricht nicht der gelebten Wirklichkeit. Obwohl im EB auf den Grundsatz der Beschränkung der Datenbearbeitung auf das strikte Minimum verwiesen wird, läuft es in der Praxis darauf hinaus, dass sämtliche Daten der E-ID bekannt gegeben werden müssen, wenn eine Dienstleistung bezogen werden will, zumal die Verifikatorin bestimmt, welche Daten für den Bezug von Leistungen erforderlich sind.

In Art. 2 Abs. 1 BGEID ist definiert, welche Personenidentifizierungsdaten eine E-ID zwingend enthalten muss. Sowohl in Anwendung des Datenschutzrechtes als auch der allgemeinen verwaltungsrechtlichen Normen ist immer dem Prinzip der Verhältnismässigkeit nachzuleben. Die Verwendung der meisten dieser Personenidentifizierungsdaten ist im Zusammenhang mit der Identifizierungsfunktion der E-ID durchaus nachvollziehbar (etwa amtlicher Name und Vorname, Geburtstag oder Geschlecht). In diesem Zusammenhang nicht einleuchtend erscheint die Verwendung des Geburtsorts. Die Erforderlichkeit des Geburtsorts als Personenidentifizierungsdatum wird auch im EB nicht weiter begründet. Es sind im nicht-digitalen Rechtsverkehr kaum Fälle ersichtlich, in denen zu Identifizierungszwecken der Geburtsort einer Person benötigt wird. An die Identifizierung im digitalen Raum sollen, wie sich aus dem EB ergibt, nicht höhere Anforderungen gestellt werden als an die Identifizierung im nicht-digitalen Raum. Daher ist auf die Verwendung des Geburtsorts als Personenidentifizierungsdatum zu verzichten.

Gemäss Art. 2 Abs. 2 BGEID enthält die E-ID zudem unter anderem die AHV-Nummer. Diese AHV-Nummer wurde ursprünglich nur für die Anwendung in den Sozialversicherungen geschaffen. Seit dem 1. Januar 2022 dürfen Behörden von Bund, Kantonen und Gemeinden im Rahmen ihrer gesetzlichen Aufgaben die

AHV-Nummer systematisch verwenden. Die Verwendung der AHV-Nummer als Personenidentifizierungsdatum ist jedoch verschiedentlich kritisiert und auf ihren Nutzen hinterfragt worden. So wurde insbesondere auch im Rahmen der Botschaft zum ursprünglichen BGEID aufgrund der Rückmeldungen aus dem Vernehmlassungsverfahren von einer Verwendung der AHV-Nummer als Personenidentifizierungsdatum weitgehend abgesehen. Diese solle nur vom fedpol zur Identifizierung von Personen systematisch verwendet werden können (vgl. BBl 2018 3936). Mit der Aufnahme der AHV-Nummer in Art. 2 Abs. 3 BGEID kann diese nun wieder flächendeckend zur Identifizierung im Rahmen der Verwendung einer E-ID verwendet werden. Warum die neue Gesetzesvorlage, welche einen grossen Wert auf den Aspekt der Datensparsamkeit legt, in diesem Bereich über die vorherige Vorlage ohne Erforderlichkeit und weitere Erläuterung hinausgeht, ist nicht nachvollziehbar. Wir beantragen, auf die Nennung der AHV-Nummer in Art. 2 Abs. 3 lit. a BGEID zu verzichten oder deren Verwendung so zu beschränken, dass sie nur vom fedpol im Rahmen der Identifizierung verwendet werden kann.

Gemäss Art. 2 Abs. 2 lit. g Ziff. 1 BGEID enthält die E-ID ein Gesichtsbild gestützt auf Art. 11 Ausweisgesetz (AwG; SR 143.1). Massgebend ist aber vielmehr Art. 2 AwG. Danach enthält jeder Ausweis eine Fotografie, nicht jedoch zwingend einen Datenchip mit einem Gesichtsbild. Aus dem EB geht nicht hervor, ob der Begriff Fotografie und Gesichtsbild identisch ist. Hier besteht Erklärungsbedarf. Die gesetzliche Grundlage für den Inhalt des Informationssystem ZEMIS findet sich in Art. 4 des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA; SR 142.51). Gemäss Art. 4 Abs. 1 lit. a^{bis} BGIAA werden im System biometrische Daten, unter anderem Gesichtsbilder gespeichert. Hier ist eine Präzisierung angebracht, zumal sich die Begriffe Fotografie und Gesichtsbild gemäss BGIAA und AwG deutlich unterscheiden.

Art. 3 BGEID: Persönliche Voraussetzungen

Die Bestimmung sieht vor, dass nur Personen mit geregelter Aufenthalt in der Schweiz eine E-ID beantragen können. Der Kreis der Personen, die einen entsprechenden Identitätsnachweis in der Schweiz z.B. im Verkehr mit Behörden aber auch im Privatrechtsverkehr benutzen können, ist aber weiter gefasst. Hierbei ist etwa an Personen zu denken, welche ohne geregelten Aufenthalt in der Schweiz wohnhaft

sind ("Sans-Papiers") oder an Zweitwohnungsbesitzer. Es rechtfertigt sich nicht, diese Personengruppen per se von der Nutzung entsprechender elektronischer Identitätsnachweise auszuschliessen. Dies zumal auch bei Personengruppen mit einem gültigen Ausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl, bei welchen die Identität nicht eindeutig festgestellt werden kann, eine eingeschränkte Nutzung der E-ID vorgesehen werden kann (vgl. S. 9 EB). Es ist zu prüfen, ob diese Möglichkeit auch auf Personengruppen ohne Ausweis ausgeweitet werden kann.

Gemäss dem EB (S. 9 zu Art. 3 BGEID) sollen gesetzliche Einschränkungen in der Anwendung der E-ID möglich sein für Personen, deren Identität nicht verlässlich festgestellt werden konnte. Die Einschränkung für Personen ohne geregelten Aufenthalt in der Schweiz soll nicht über einen weiteren "Vermerk", sondern über die bereits definierten Vertrauensstufen gem. eCH-1070 gelöst werden. Der Kanton Graubünden sieht vor, dass jede natürliche Person die Möglichkeit hat, eine elektronische Identität zu erstellen. Je nach Identifizierung der Person (z.B. persönliches Vorsprechen), erhält diese eine entsprechende Vertrauensstufe (siehe eCH-0170). Dies ermöglicht auch bspw. ausländischen Personen die Nutzung von elektronischen Dienstleistungen des Kantons. Wichtig ist, dass diese Vertrauensstufe in der E-ID hinterlegt ist. Die Vertrauensstufe soll durch einen entsprechenden Identifizierungsprozess jederzeit erhöht werden können, ohne dass eine neue E-ID ausgestellt werden muss.

Im Weiteren fehlt in Art. 3 Abs. 1 BGEID die gemäss dem EB vorgesehene Kann-Bestimmung, *"mit der (...) sichergestellt (wird), dass die antragstellenden Personen nicht verpflichtet sind, eine E-ID zu beziehen oder zu verwenden"*. Es ist richtig und nachvollziehbar, dass keine Verpflichtung zur Nutzung einer E-ID bestehen soll, auch wenn man die persönlichen Voraussetzungen für deren Ausstellung erfüllt. Sofern man zum Schluss kommt, dass dies mit der gegebenen Formulierung nicht der Fall ist, so ist Art. 3 BGEID explizit als Kann-Bestimmung zu formulieren.

Art. 4 BGEID: Ausstellung

Der Ausstellungsprozess und damit verbunden die Frage, wie die Identifizierung der antragsstellenden Personen durchgeführt wird, sind für die Sicherheit und damit auch

für die künftige Akzeptanz der E-ID zentral. Eine Regelung des Ausstellungsprozesses muss deshalb ins Gesetz aufgenommen werden. Dabei dürfen Sicherheitsüberlegungen nicht hinter Kosten- und Effizienzfragen zurückstehen. Art. 6 Abs. 5 des revidierten Bundesgesetzes über den Datenschutz (nDSG; SR 235.1) statuiert die Pflicht des Datenbearbeiters oder der Datenbearbeiterin, sich über die Richtigkeit der Personendaten zu vergewissern. Die Angemessenheit der Massnahmen muss sich dabei auch nach dem – im Falle der E-ID erheblichen – Risiko für die Grundrechte der betroffenen Person richten.

Der Vorentwurf sieht in Art. 4 Abs. 2 BGEID u.a. vor, dass Minderjährige bis zum vollendeten vierzehnten Lebensjahr die Einwilligung ihrer gesetzlichen Vertretung benötigen. Im Gegensatz dazu wird für den Bezug eines physischen Schweizer Identitätsausweises Volljährigkeit vorausgesetzt. Diese Unterscheidung ist schwierig nachvollziehbar. Somit könnte eine Person ab dem vierzehnten Lebensjahr ohne die Zustimmung der gesetzlichen Vertretung eine E-ID beziehen. Auch die Begründung im EB, wonach die Jugendlichen für die Erledigung ihrer alltäglichen Aufgaben und Aktivitäten hauptsächlich das Internet verwenden und demzufolge eine unterschiedliche Handhabung gerechtfertigt sei, vermag nicht zu überzeugen. Im Vordergrund sollten Sicherheitsüberlegungen stehen und nicht die Frage, welche Ausweisarten von Jugendlichen mehrheitlich genutzt werden. In Analogie zum physischen Ausweis sollte das massgebende Alter für den eigenmächtigen Bezug einer elektronischen ID ebenfalls auf achtzehn Jahre erhöht werden, alternativ zumindest bis zum achtzehnten Altersjahr die Zustimmung der gesetzlichen Vertretung erfordern.

Im Rahmen einer Ausweisbeantragung sollte es ferner (ohne Zwang) möglich sein, direkt im Ausweiszentrum eine E-ID zu beantragen. Ein in der Folge nachgelagerter Antrag beim fedpol würde einen (vermeidbaren) administrativen Leerlauf darstellen.

Art. 5 BGEID: Widerruf

Art. 5 Bst. d Ziff. 2 BGEID legt fest, dass die E-ID widerrufen wird, wenn das fedpol über eine Änderung der Personenidentifizierungsdaten des Inhabers oder der Inhaberin informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen müssen sich

dann nicht noch einmal um die Ausstellung einer neuen E-ID bemühen und profitieren so von den erleichterten Abläufen, die durch die Digitalisierung ermöglicht werden.

Art. 5 BGEID regelt die Voraussetzungen, gemäss denen die E-ID bei begründetem Verdacht auf Missbrauch den Betroffenen entzogen werden kann (Art. 5 Bst. c BGEID). Sofern die E-ID die gewünschte und vorgesehene grosse Bedeutung im Alltag erlangt, kann eine entsprechende Sperrung für die Inhaberin oder den Inhaber im Alltag einschränkende Auswirkungen haben. Dies kann auch durch die Pflicht zur Akzeptanz eines Ausweisdokuments anstelle der E-ID nicht gänzlich ausgeschlossen werden. Daher muss gegen einen allfälligen Widerruf zwingend ein wirksamer Rechtsschutz bestehen und es ist sicherzustellen, dass der Entzug den Betroffenen mitzuteilen und auf Verlangen als anfechtbare Verfügung zu eröffnen ist.

Antrag (neuer Art. 5 Abs. 2 BGEID)

"Der Widerruf der E-ID gemäss Art. 5 Abs. 1 lit. c ist der Inhaberin oder dem Inhaber mitzuteilen und auf Verlangen innert 30 Tagen nach der Mitteilung als anfechtbare Verfügung zu eröffnen."

Art. 6 BGEID: Gültigkeitsdauer

Gemäss EB bleibt nach Ablauf der Gültigkeit die E-ID auf dem Gerät des Inhabers / der Inhaberin bestehen. Es müssen in diesem Zusammenhang zwei Aspekte beachtet werden. Art. 32 Abs. 2 lit. c nDSG gibt einer betroffenen Person das Recht, dass Personendaten gelöscht werden. Kann dieses Recht gestützt auf die Ausführungen im EB durchgesetzt werden? Unseres Erachtens müsste die Löschung der abgelaufenen E-ID automatisch erfolgen. Darüber hinaus wird dem Missbrauch von abgelaufenen E-ID Vorschub geleistet, da in vielen Fällen dem Ausstellungs- und Ablaufdatum wenig Gewicht beigemessen wird. Auch aus diesem Blickwinkel betrachtet, drängt sich eine Löschung der Daten auf dem Gerät des Inhabers / der Inhaberin auf, selbst wenn dies mit technischen Schwierigkeiten verbunden ist.

Neben der Gültigkeitsdauer ist im Entwurf auch die Frage der Verlängerung nicht geregelt. Es wird nicht klar, ob nach Ablauf des physischen Ausweisdokuments – sofern die Gültigkeit der E-ID an diese geknüpft wird – erneut eine E-ID beantragt werden

muss oder ob dies bei Verlängerung des Ausweises automatisch geschieht. Dies ist spätestens in der Verordnung ebenfalls zu klären.

Art. 7 BGEID: Sorgfaltspflicht

Art. 7 BGEID sieht eine Sorgfaltspflicht für Inhaberinnen und Inhaber einer E-ID vor. Nicht konkret geregelt sind dabei die Verpflichtungen bei Verlust des E-ID-Trägers / der E-ID Trägerin, dies im Gegensatz zu Art. 8 AwG, das eine Meldepflicht bei Verlust eines (physischen) Ausweises vorsieht. Zur Konkretisierung der Sorgfaltspflichten ist dieser Fall auch im BGEID auszuführen. Die Inhaberin oder der Inhaber einer E-ID muss jeden Verdacht auf Missbrauch ihrer oder seiner E-ID dem fedpol melden. Dies sollte aus praktischen Gründen auch über die kantonale Anlaufstelle möglich sein (analog z.B. beim Verlust der Identitätskarte).

Art. 8 BGEID: Anlaufstellen der Kantone

Die Bestimmung sieht eine zusätzliche Aufgabe für die Kantone vor. Der EB geht davon aus, dass die benötigten Strukturen in den Kantonen bereits vorhanden sind. Dies ist jedoch nicht notwendigerweise der Fall. Als Vollzugsträger steht hier der Bund in der Verantwortung. Wer eine Informatiklösung anbietet und betreibt, hat auch den nötigen Support sicherzustellen, soweit die eigene Anwendung betroffen ist. Die Kantone sehen sich da als zuständig, wo es darum geht, Unterstützung beim Einsatz der E-ID für kantonale E-Government-Angebote zu leisten. Für Schwierigkeiten bei der Beantragung der E-ID oder bei der Nutzung der Vertrauensinfrastruktur muss dagegen der Bund eine Ansprechstelle schaffen. Eine solche ist im EB zwar erwähnt, sie fehlt jedoch im Gesetzesentwurf ebenso wie der Second Level Support, den der Bund gemäss dem EB für die Kantone wahrnehmen soll. Unter Bezugnahme auf die Ausführungen im EB ist zudem darauf hinzuweisen, dass Personen, die bereit sind, eine E-ID zu nutzen, üblicherweise auch in der Lage sind, einen Support per Telefon oder E-Mail in Anspruch zu nehmen. Es müssen dafür nicht zwingend physische Anlaufstellen geschaffen werden.

Art. 9 BGEID: Pflicht zur Akzeptanz der E-ID

Gemäss Art. 9 BGEID müssen Behörden und andere Stellen, die eine öffentliche Aufgabe erfüllen, die staatliche E-ID akzeptieren, wenn sie eine elektronische Identifizierung vornehmen. Aus dem EB wird klar, dass diese Verpflichtung sich lediglich auf

Identifizierungsprozesse beschränkt, bei denen ein persönliches Erscheinen und die Vorlage eines Identitätsdokuments erforderlich sind. In diesen Fällen muss es der betroffenen Person offenstehen, sich gegenüber der Behörde mit einer E-ID auszuweisen. Gemäss der Formulierung im EB nicht vorgesehen ist, dass alle kantonalen und kommunalen Online-Dienstleistungen, welche auf einer Login-Lösungen basieren, zwingend auch die Verwendung einer E-ID anbieten müssen. Dies erachten wir im Ergebnis als richtig, ergibt sich jedoch nicht aus dem Wortlaut des Gesetzes. Aus Klarheitsgründen sei das Gesetz daher entsprechend anzupassen.

Der Begriff der "öffentlichen Aufgabe" wird im EB mit "Verwaltungsaufgaben" gleichgesetzt, was dem Begriff von Art. 178 Abs. 3 der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101) entspricht. Es empfiehlt sich, im BGEID ebenfalls von "Verwaltungsaufgaben" zu sprechen, oder, falls der Begriff der "öffentlichen Aufgabe" weiter gefasst werden soll, die Botschaft in diesem Punkt zu präzisieren. Es ist zu bedenken, dass unter anderem im Gesundheitswesen eine Vielzahl von privaten Akteuren öffentliche Aufgaben ausführen, so zum Beispiel Krankenversicherer, Betreiber von Krebsregistern und Transplantationsregistern oder Anbieter des EPD. Die Pflicht zur Akzeptanz der zukünftigen E-ID bei all diesen Akteuren ist durchaus sinnvoll, wird aber Investitionen und Vorbereitungsarbeiten zur Folge haben, die den Betroffenen möglichst rasch klar kommuniziert werden müssen. Es ist somit wichtig, dass bei allen Beteiligten von Anfang an Klarheit herrscht über den Geltungsbereich von Art. 9 BGEID.

Die Umsetzung von Art. 9 BGEID bedingt eine Integration der E-ID in bestehende IT-Anwendungen von Kantonen und Gemeinden. Diesen ist dafür eine ausreichende Übergangsfrist einzuräumen.

Art. 10 BGEID: Vorweisen einer E-ID

Art. 10 BGEID legt fest, dass eine Identifizierung in der physischen Welt weiterhin auch ohne eine E-ID durch das Vorweisen eines Ausweisdokuments möglich sein muss. Die Bestimmung verhindert aber nicht, dass der Zugang zu Dienstleistungen, die ausschliesslich elektronisch verfügbar sind, künftig eine E-ID voraussetzen kann. Die Freiwilligkeit zum Bezug einer E-ID wird damit unter Umständen eingeschränkt. Die leichtere Abwicklung einer elektronischen Identifizierung birgt zudem das Risiko,

dass eine solche künftig von öffentlichen wie privaten Akteuren auch für den Zugang zu Dienstleistungen verlangt wird, für die das Vorweisen eines Personalausweises bisher nicht nötig war. In der Umsetzung ist somit darauf zu achten, dass durch den Einsatz der E-ID der Zugang zu öffentlichen Dienstleistungen nicht in unzumutbarer Weise eingeschränkt wird. Problematisch wäre beispielsweise, wenn der Zugriff auf in der Volksschule verwendete Online-Lehrmittel künftig nur mit einer E-ID möglich wäre. Dies würde nicht nur Schülerinnen und Schüler ausschliessen, deren Eltern keine E-ID beantragen möchten, sondern auch solche ohne geregelten Aufenthalt in der Schweiz, die gemäss Art. 19 BV dennoch ein Recht auf Grundschulunterricht haben.

Art. 11 BGEID: Informationssystem zur Ausstellung und zum Widerruf der E-ID

Gemäss Art. 11 BGEID betreibt das fedpol ein Informationssystem zur Ausstellung und zum Widerruf der E-ID. In der Bestimmung werden die beinhalteten Daten und die Schnittstellen zu anderen Informationssystemen geregelt. Gemäss Art. 11 Abs. 5 BGEID regelt der Bundesrat die Aufbewahrungsfristen, wobei diese für längstens bis fünf Jahre nach dem Ablauf oder Widerruf einer E-ID aufbewahrt werden können.

Nach dem weiteren oben Ausgeführten sind Datenbearbeitungen aus Verhältnismässigkeitsgründen auf das erforderliche Mass zu beschränken. Dies gilt neben der Art der bearbeiteten Daten auch in zeitlicher Hinsicht. Es trifft zu, dass auch nach dem Ablauf oder Widerruf ein Interesse an der Einsicht in diese Daten bestehen kann, etwa um Missbräuche nachträglich aufzudecken. Jedoch gilt es zu beachten, dass das Interesse hieran im Laufe der Zeit abnimmt. Zudem ist ein entsprechendes Ereignis umso schwerer zu beweisen, je länger es zurückliegt. Die vorgesehene Aufbewahrungsdauer erscheint zu lange und ist auf zwei Jahre zu begrenzen.

3. Abschnitt: Andere elektronische Nachweise

Der Bund stellt Behörden oder Privaten die Vertrauensinfrastruktur zur Verfügung. Gemäss Art. 17 BGEID besteht ein öffentlich zugängliches Register (Basisregister). Daneben wird offenbar ein Vertrauensregister geführt. Im Gesetz finden sich dazu keine Angaben. Es ist also nicht klar, was Inhalt des einen und des anderen Registers bildet und wie sich diese beiden Register zueinander verhalten. Ganz grundsätzlich erschliessen sich die Ausführungen im EB zu dieser Thematik einem aussenstehenden Dritten kaum.

Art. 15 BGEID: Übertragbarkeit von elektronischen Nachweisen

Art. 15 BGEID regelt die Übertragbarkeit von elektronischen Nachweisen. Hierbei wird festgelegt, dass Nachweise nicht einer Drittperson übertragen werden dürfen. Dies ist zu begrüßen. Kritisch betrachtet wird indes die Formulierung von Art. 15 Abs. 2 BGEID, gemäss welcher dem Bundesrat die Kompetenz übertragen wird, die Übertragung von elektronischen Nachweisen, die nicht auf eine natürliche Person ausgestellt sind, zuzulassen.

Diese Formulierung suggeriert, dass z.B. auch juristische Personen entsprechende elektronische Nachweise nutzen können. Dies erscheint nicht ausgeschlossen steht jedoch im Gegensatz zur E-ID, welche gemäss den persönlichen Voraussetzungen nur durch natürliche Personen genutzt werden kann (vgl. Art. 3 Bst. a BGEID). Sofern die elektronischen Nachweise (ausser der E-ID) juristischen Personen offenstehen soll, so ist fraglich, ob der entsprechende Verweis zur Regelung auf Verordnungsstufe ausreicht. Gemäss dem EB ist Art. 15 Abs. 2 BGEID indes in erster Linie dahingehend zu verstehen, dass es ermöglicht werden soll, ihre Nachweise etwa beim Wechsel des technischen Trägers (z.B. Smartphone) auf ein neues Gerät übertragen zu können. Der Verlust oder der Wechsel des technischen Trägers ist in der Praxis ein häufiges Szenario. Es wird daher richtigerweise eine Möglichkeit vorgesehen, um die elektronischen Nachweise in diesen Fällen möglichst umstandslos wiederherstellen zu können. Der Gesetzgeber entschliesst sich hierzu ein System für Sicherungskopien bereitzustellen, welches in Art. 21 BGEID geregelt wird. Wenn der entsprechende Absatz nur die Möglichkeit abdecken soll, die eigenen elektronischen Nachweise auf diese Weise wiederherzustellen, so ist er zu weit gefasst und ist anzupassen.

Antrag (Anpassung Art. 15 Abs. 2 BGEID):

"Elektronische Nachweise können mithilfe des Systems für Sicherungskopien auf ein neues Trägermedium übertragen werden. Der Bundesrat regelt die Übertragung."

Art. 16 BGEID: Vorweisen von elektronischen Nachweisen

Gemäss Art. 16 Abs. 1 BGEID bestimmt die Inhaberin oder der Inhaber darüber, welche Bestandteile des Nachweises oder davon abgeleitete Informationen an die Verifikatorin übermittelt werden. Diese begrüssenswerte Regelung wird bereits im EB

dadurch eingeschränkt, dass die Verifikatorin festlegt, welche Daten für den Zugang zu ihren Diensten erforderlich sind. Es liegt hier bei im Interesse der Verifikatorinnen so viele Daten wie möglich zu akquirieren. Dies steht in einem Spannungsverhältnis zum datenschutzrechtlichen Verhältnismässigkeitsgrundsatz. Es ist insofern problematisch, als dass keine Kontrolle darüber stattfindet, welche Daten die Verifikatorinnen von den Inhaberinnen und Inhabern eines Nachweises verlangen dürfen. In Anbetracht dessen, dass sich die Inhaberin resp. der Inhaber kaum gegen die unzulässige Erhebung von persönlichen Daten wehren kann, ist es angebracht, Vorkehrungen für die Verifikatorin zu treffen. Eine entsprechende Kontrolle der Daten, welche maximal verlangt werden dürfen, könnte z.B. im Zusammenhang mit der Aufnahme in das Basisregister erfolgen.

5. Abschnitt: Vertrauensinfrastruktur

Vergleiche obige Ausführungen zum 3. Abschnitt.

Art. 17 BGEID: Basisregister

Wie der EB (S. 14) ausführt, birgt die Tatsache, dass Ausstellerinnen ohne weitere Überprüfung ihre Daten selber ins Basisregister gemäss Art. 17 Abs. 3 BGEID eintragen können, das Risiko, dass diese unter falscher Identität elektronische Beweismittel ausstellen können. Es liegt auf der Hand, dass dies für die betroffenen Personen unter Umständen weitreichende Folgen haben kann. Die Abfederung dieses Risikos durch Veröffentlichung bei begründetem Verdacht gemäss Art. 22 BGEID ist nicht ausreichend, da sie bereits eine Verletzung der Persönlichkeitsrechte von betroffenen Personen voraussetzt. Auch können durch blosses Öffentlichmachen erfahrungsgemäss nicht alle Nutzenden rechtzeitig erreicht werden. Ein Eintrag ins Vertrauensregister nach Art. 18 BGEID muss entsprechend auch für private Anbieter resp. private Anbieterinnen zwingend sein. Andernfalls können Missbräuche nicht verhindert werden.

Art. 20 BGEID: Anwendung zur Prüfung von elektronischen Nachweisen

Der Bundesrat kann gemäss dieser Bestimmung vorsehen, dass der Bund eine Anwendung zur Verfügung stellt, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden kann. Dies ist nicht nur vorzusehen, sondern unbedingt umzusetzen. Die Kann-Bestimmung ist entsprechend anzupassen. Nur so stösst die E-ID in

der Gesellschaft auf Akzeptanz. Es muss ein Nutzen vorliegen und die Handhabung muss einfach sein - auch bei der prüfenden Stelle.

Art. 21 BGEID: System für Sicherungskopien

Es ist zu begrüßen, dass der Bund dem Inhaber resp. der Inhaberin eine Möglichkeit zur Aufbewahrung bereitstellt. Da auch eine Cloud-Lösung möglich sein soll, ist auf die Sicherheitsaspekte einer Cloud-Lösung hinzuweisen. Gemäss Art. 21 Abs. 2 BGEID werden die Sicherheitskopien vor Zugriffen durch andere Personen geschützt. Der Schutz muss auch den Bund mitumfassen, da in der Briefftasche auch elektronische Nachweise Dritter aufbewahrt werden. Zumindest in der Botschaft ist auf diesen Aspekt hinzuweisen. Eine treffendere Formulierung im Gesetz ist anzustreben, z.B.: *"Die Sicherheitskopien werden vor unberechtigtem Zugriff geschützt"*.

Art. 25 BGEID: Technische Entwicklung

Die Funktionsweise von Abs. 2 dieser Bestimmung ist unklar: Wer entscheidet darüber, ob ein Anwendungsfall von Abs. 2 vorliegt? Entscheidet dies der Bundesrat bereits mit dem Erlass der Verordnung? Zudem ist der Zusammenhang zwischen Abs. 1 und Abs. 2 von Art. 25 BGEID im Text deutlicher hervorzuheben, und es sollte der Vollständigkeit halber der Fall des fakultativen Referendums miterfasst werden:

"2 Sofern Bestimmungen, die gestützt auf Abs. 1 erlassen werden, einer weiteren Grundlage in einem Gesetz bedürfen, treten diese Bestimmungen ausser Kraft:

a) [...]

b) mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung oder die Stimmberechtigten; oder [...]"

Art. 26 BGEID: (Marginalie fehlt)

Art. 26 BGEID sieht vor, dass von Ausstellerinnen und Verifikatorinnen elektronischer Nachweise Gebühren erhoben werden. Dies betrifft auch Stellen, die öffentliche Aufgaben erfüllen, obwohl diese gemäss Art. 9 BGEID zur Akzeptanz der E-ID verpflichtet sind. Gleichzeitig möchte der Bundesrat die E-ID durch Beiträge aus der Agenda Digitale Verwaltung Schweiz finanzieren, die von den Kantonen mitfinanziert wird. Gemäss Art. 3 Abs. 2 der Allgemeinen Gebührenverordnung (AllgGebV; SR

172.041.1) verzichtet die Bundesverwaltung auf die Erhebung von Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Dies soll auch vorliegend entsprechend gehandhabt und Verrechnungen zwischen den Gemeinwesen auf ein Minimum beschränkt werden.

Der Bundesrat soll darüber hinaus mit der Kompetenz ausgestattet werden, die Gebühren für weitere Akteure ganz oder teilweise zu erlassen, soweit sie öffentliche Aufgaben erfüllen. Unter anderem besteht im Gesundheitsbereich ein grosses Interesse an einer breiten Nutzung der E-ID, um die Aufbereitung von Gesundheitsdaten zu erleichtern. Die Kosten für die betroffenen Stellen sind somit möglichst tief zu halten.

Die Vorlage und der EB äussern sich nicht bzw. nur sehr vage über die Höhe der zu erhebenden Gebühren. Diese sollen auf Verordnungsstufe festgelegt werden. Eine explizite Kostenfolgeschätzung für die Nutzer aufgrund der Gebühren sollte in die Botschaft aufgenommen werden, da die Kosten einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben dürften. Eine explizite Kostenfolgeschätzung für die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise aufgrund der Gebühren sollte deshalb in die Botschaft aufgenommen werden.

Art. 28 BGEID: Ausführungsbestimmungen

Zahlreiche technische Aspekte zur Umsetzung der E-ID werden auf Verordnungsstufe geregelt. Aufgrund der unterschiedlichen bestehenden Lösungen in den einzelnen Kantonen, aber auch in den einzelnen Sektoren ist es unabdingbar, dass die zuständigen Akteure eng in die Erarbeitung der Vollzugsregelungen miteinbezogen werden. Es ist eine der Voraussetzungen einer breiten Akzeptanz der E-ID, dass diese unkompliziert in bestehende Anwendungen integriert werden kann.

Art. 29 BGEID: Änderung anderer Erlasse

Gemäss dem EB (Ziff. 3.1) wurde die Verwendung der E-ID in spezifischen Bereichen und damit die Änderung anderer Erlasse im Entwurf nur exemplarisch geregelt. Es ist unabdingbar, die Gesetzgebung des Bundes im weiteren Verfahren systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder

eine qualifizierte elektronische Signatur verlangt werden. Dies betrifft insbesondere auch die Verfahrensgesetzgebung des Bundes. Die entsprechenden Bestimmungen sind durchgehend anzupassen.



Namens der Regierung

Der Präsident:

A handwritten signature in black ink, appearing to read "M. Caduff".

Marcus Caduff

Der Kanzleidirektor:

A handwritten signature in black ink, appearing to read "D. Spadin".

Daniel Spadin

Hôtel du Gouvernement – 2, rue de l'Hôpital, 2800 Delémont

Département fédéral de justice et police
Palais fédéral Ouest
CH-3003 Berne

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont

t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Adressé par courriel à rechtsinformatik@bj.admin.ch

Delémont, le 27 septembre 2022

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID) : procédure de consultation

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Par la présente, le Gouvernement de la République et Canton du Jura vous remercie de le consulter sur l'objet cité en titre et vous transmet sa réponse après une analyse détaillée de la législation proposée.

Avant tout chose, il salue l'élaboration rapide de ce nouveau projet de loi suite au rejet du précédent par le peuple, en mars 2021.

Le canton du Jura, membre fondateur de l'association iGovPortal.ch, est très attentif au présent avant-projet de loi. En effet, le développement de la cyberadministration est inscrit dans sa stratégie depuis plusieurs législatures. Des échanges ont ainsi eu lieu entre nos services et ceux de la Confédération, notamment pour comprendre les enjeux et les impacts de cette nouvelle loi sur l'e-ID. Nous remercions le Département fédéral de justice et police pour sa disponibilité et pour l'organisation des sessions de présentation.

Nous nous positionnons en premier lieu sur trois points particuliers qu'il nous semble important de considérer pour la future mise en application de la loi, à savoir l'expérience utilisateur, l'utilisation de l'e-ID dans le secteur privé et les moyens de preuve électroniques. Ces positionnements seront à prendre en compte dans la mise en œuvre du projet, car le canton du Jura ne demande pas d'adaptations formelles de la proposition de loi sur ces trois sujets.

Nous reviendrons ensuite sur des éléments plus précis en faisant référence aux articles de l'avant-projet de loi.

Expérience utilisateur

Notre expérience acquise depuis de nombreuses années avec les systèmes SuisselD et SwissID nous permet d'attirer l'attention sur l'importance d'établir une vraie stratégie autour de l'expérience utilisateur, ici en l'occurrence l'expérience des citoyens dans l'utilisation future de la nouvelle e-ID. Cette démarche doit permettre de soigner le processus d'acquisition de l'e-ID, son utilisation ainsi que son renouvellement, facteurs essentiels du succès du projet. Nous avons pleinement conscience que conjuguer sécurité, protection des données et facilité d'utilisation pour les citoyens est un réel défi. Néanmoins, il nous paraît primordial que les services de la Confédération puissent placer l'utilisateur au centre des réflexions et des analyses pour que le futur système puisse obtenir un taux d'adhésion élevé.

Le même soin sur l'ergonomie et la facilité d'utilisation devra également être apporté sur le système des moyens de preuve électroniques (art. 15) et le système des copies de sécurité (art.21).

Utilisation de l'e-ID dans le secteur privé

L'avant-projet de loi définit le caractère contraignant de l'acceptation de l'e-ID dans tous les services numériques accomplissant des tâches publiques (art. 9), ce que nous saluons. Nous comprenons que l'avant-projet décrive uniquement l'utilisation de l'e-ID dans le secteur public. Néanmoins, nous souhaitons attirer l'attention sur l'importance d'établir une stratégie de collaboration et d'utilisation dans les secteurs privés. Parmi les facteurs clés de succès de la cyberadministration dans les pays qui font figure de modèles dans ce domaine, à l'instar des pays nordiques, celui de l'utilisation de l'e-ID dans le privé est régulièrement mis en avant. Le citoyen fera plus volontiers l'acquisition de l'e-ID s'il y trouve un intérêt dans une utilisation régulière comme par exemple pour prouver son identité dans son système d'eBanking, d'assurance et de titre de transport, pour ne citer que ces exemples. Il nous semble très important d'avoir une stratégie globale d'utilisation de la future e-ID et de développer des partenariats pour que son utilisation soit faite à large échelle et ceci d'autant plus que le choix d'architecture SSI pour la nouvelle e-ID garantit la protection des données des citoyens.

Nous saluons également l'approche d'attribuer uniquement des e-ID à des personnes physiques (art. 1). Nous ne souhaitons pas d'attribution d'e-ID à des personnes morales. En effet, dans la stratégie de développement de la cyberadministration jurassienne, nous délivrons des prestations à des personnes physiques, mais également à des personnes morales. Néanmoins, nous gérons uniquement les identités de personnes physiques rattachées dans notre guichet virtuel à des entités de type personnes morales. Nous souhaitons poursuivre dans cette voie et, par conséquent, nous soutenons le projet de la Confédération de délivrer uniquement des identités de personnes physiques.

Moyens de preuve électroniques

Nous soutenons la volonté de la Confédération de ne pas uniquement se concentrer sur l'e-ID, mais également d'initier un projet d'émission et d'utilisation d'autres moyens de preuve électroniques (art. 12 à 16). La création d'un portefeuille électronique (wallet) avec des documents officiels (extraits, attestations, permis, etc.) fait pleinement partie de la stratégie du canton du Jura. Notre canton a

acquis une expérience certaine dans la mise en place des extraits de poursuite sécurisés au travers de la Blockchain KSI (projet soutenu en 2020 par eGovernment Suisse). A ce titre, nous avons la volonté d'orienter ce portefeuille électronique dans la même direction que la Confédération et par conséquent, il nous paraît indispensable que notre canton soit impliqué en tant que partenaire dans le développement de la solution et durant les phases pilotes.

Prise de position par article :

Art. 3 Conditions personnelles

Le rapport explicatif précise que l'e-ID sera disponible pour les frontaliers. Ce point est salué par le canton du Jura et doit absolument être préservé. Nous avons en effet de nombreux frontaliers travaillant dans des entreprises jurassiennes et il est important que ces personnes physiques puissent réaliser les transactions numériques de leur employeur au travers du guichet virtuel du canton du Jura. Une mise en place rapide de l'interopérabilité du système Suisse avec le système d'identités européennes éviterait aux frontaliers de demander une e-ID suisse. Mais dans l'intervalle, le projet de loi définitif devra absolument garder la possibilité de délivrer des e-ID à des frontaliers.

Art. 4 Émission

En septembre 2022, 36'000 utilisateurs jurassiens possèdent une SwissID pour s'identifier et s'authentifier sur le guichet virtuel cantonal, ce qui représente plus de 75% des contribuables. Parmi ces 36'000 utilisateurs, 11'200 sont détenteurs d'une identité vérifiée. Au niveau suisse, cela représente plus de 3.5 millions d'utilisateurs SwissID, dont 650'000 avec une identité vérifiée. De ce fait, le présent projet doit prendre en considération cette situation.

Il serait dès lors paradoxal que les cantons qui ont consentis d'importants efforts en matière de cyberadministration depuis de nombreuses années, comme pour le canton du Jura, soient pénalisés et perdent l'adhésion de leurs utilisateurs, en raison d'un processus complexe d'acquisition d'une e-ID Suisse qui imposerait de recommencer les démarches depuis le début.

Le canton du Jura veut absolument pouvoir préserver les 11'200 utilisateurs possédant une identité vérifiée et faciliter les démarches d'acquisition pour les personnes ayant déjà une identité électronique non vérifiée pour accéder au guichet virtuel cantonal. Nous attendons donc de la Confédération un plan de mise en œuvre, notamment avec La Poste Suisse, pour assurer une procédure facilitée d'obtention de l'e-ID fédérale.

Art. 8 Points de contact cantonaux

Le canton du Jura est favorable à la mise en place de points de contact régionaux pour accompagner les utilisateurs dans l'obtention de leur e-ID. Les collaborateurs travaillant dans ces bureaux auront les compétences nécessaires pour guider les citoyens dans le processus d'acquisition ou de renouvellement d'une e-ID.

Pour un accompagnement plus large dans l'utilisation de l'e-ID ou dans un support plus général à la cyberadministration, nous n'envisageons pas d'engager des collaborateurs spécialisés. Nous pensons que le développement d'un écosystème avec des acteurs tiers, comme les offices postaux,

est une piste à poursuivre. Nous interprétons la désignation de « services », dans l'article 8, de manière large et permettant d'associer des partenaires externes à l'administration publique pour effectuer ces tâches d'accompagnement. La Confédération devrait avoir un rôle clé dans la mise en place de ces points de contact pour définir de bonnes pratiques et une cohérence au niveau national.

Art. 9 Obligation d'accepter l'e-ID

Nous saluons l'obligation d'accepter l'e-ID pour les autorités et les services accomplissant des tâches publiques. Il serait souhaitable que les entités paraétatiques ou privées s'acquittant de tâches publiques ou bénéficiant de financement étatique soient soumises à la même obligation d'acceptation de l'e-ID, comme moyen d'identification.

Art. 26 Émoluments

La mise en place d'un système de copie de sécurité (art. 21) est une approche qui semble pertinente et nécessaire. Néanmoins, nous ne sommes pas favorables au fait de lier des émoluments à l'utilisation de ce système de copie de sécurité. Si les citoyens doivent payer pour l'utilisation du système de copie de sécurité, cela risque de créer une barrière importante, alors que cette sécurisation est un réel avantage pour faciliter la récupération en cas de perte et diminuer les cas de support.

Art. 27 Conventions internationales

Il est très important de garantir une interopérabilité et une reconnaissance des systèmes d'identification électronique européens. Pour certaines prestations, le guichet virtuel du canton du Jura devrait pouvoir être accessible par des entreprises étrangères.

Art. 28 Dispositions d'exécution

Au sens de cet article, de nombreux aspects, notamment techniques, sont réglés par voie d'ordonnance. Compte tenu de la diversité des solutions existant dans les cantons et les différents domaines, tels que la cyberadministration et la santé numérique, il est indispensable que l'ensemble des acteurs concernés soient étroitement associés à l'élaboration des dispositions d'exécution. Il est en effet impératif que l'e-ID s'intègre parfaitement avec les différents services numériques existants ou projetés, en particulier dans les domaines précités. Le canton du Jura est à disposition pour participer de manière active à ces réflexions.

Le Gouvernement jurassien vous remercie de l'avoir consulté sur l'objet cité en titre et vous présente, Mesdames, Messieurs, l'expression de sa très haute considération.

AU NOM DU GOUVERNEMENT DE LA
RÉPUBLIQUE ET CANTON DU JURA


David Eray
Président




Jean-Baptiste Maître
Chancelier d'État



Finanzdepartement

Bahnhofstrasse 19
6002 Luzern
Telefon 041 228 55 47
info.fd@lu.ch
www.lu.ch

Öffnungszeiten:
Montag - Freitag
08:00 - 11:45 und 13:30 - 17:00

Eidg. Justiz- und Polizeidepartement
per E-Mail an (Word- und PDF-Datei):
rechtsinformatik@bj.admin.ch

Luzern, 18. Oktober 2022

Protokoll-Nr.: 1191

Vernehmlassung «Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)»

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 haben Sie die Kantonsregierungen in eingangs erwähnter Angelegenheit zur Stellungnahme eingeladen.

Im Namen und Auftrag des Regierungsrates teile ich Ihnen mit, dass sich der Kanton Luzern der gemeinsamen Stellungnahme der Konferenz der Kantonsregierungen (KdK) vom 23. September 2022 anschliesst und die Stossrichtung des Vorentwurfs unterstützt.

Der Kanton Luzern begrüsst es, dass die neue Vorlage rasch und unter Einbezug staatlicher und privater Akteure erarbeitet wurde. Eine einheitliche, staatliche Lösung ist unumgänglich, um die Digitalisierung auch in der öffentlichen Verwaltung voranzubringen. Aus Sicht des Kantons Luzern werden die Benutzerfreundlichkeit der künftigen Anwendung und die Achtung des Datenschutzes bei den Nutzerinnen und Nutzern massgeblich sein. Diesen Anforderungen ist deshalb besondere Beachtung zu schenken.

Schliesslich weise ich darauf hin, dass die Digitalisierung der Verwaltung auf Kantons- und Gemeindeebene bereits in vollem Gange ist. Es wurden und werden grosse Investitionen getätigt. Für den Kanton Luzern ist es deshalb von entscheidender Bedeutung, dass sich die geplante E-ID technisch problemlos in bestehende Anwendungen integrieren lässt.

Ich danke für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse


Reto Wyss
Regierungsrat

Beilage:

- Stellungnahme der Konferenz der Kantonsregierungen (KdK) vom 23. September 2022



LE CONSEIL D'ÉTAT

DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Par courrier électronique :

Département fédéral de justice et police
Palais fédéral ouest
3003 Berne

Avant-projet de loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques

Madame la conseillère fédérale,

Votre correspondance du 29 juin 2022 relative à l'objet susmentionné nous est bien parvenue et a retenu notre meilleure attention. Conformément à votre demande et après avoir pris connaissance de l'avant-projet LeID, nous pouvons vous confirmer que le Gouvernement neuchâtelois soutient le projet de nouvelle loi sur l'identité électronique.

L'avant-projet proposé tient compte de manière appropriée des réserves qui ont conduit au rejet de la loi fédérale sur les services d'identification électronique en mars 2021. Le nouveau projet prévoit que l'émission de l'e-ID relève d'une instance publique et que l'infrastructure nécessaire sera fournie par la Confédération. L'utilisation d'une infrastructure de confiance pour émettre d'autres moyens de preuve électronique et la gratuité de l'e-ID pour les particuliers contribueront à l'adhésion de la population. Le canton de Neuchâtel poursuit sa stratégie digitale sur la base de son Guichet sécurisé unique et il est déterminant que la future e-ID puisse s'intégrer dans les applications sans difficulté. Si le canton et les communes neuchâteloises auront recours à l'infrastructure de confiance proposée, il conviendra d'évaluer de manière détaillée les coûts engendrés par la mise en production de l'e-ID et la planification du déploiement.

Cet avant-projet soumis à consultation a fait l'objet de prises de position de la part de la Conférence des gouvernements cantonaux (CdC) le 28 septembre 2022, et de la part de la Conférence latine des directeurs et directrices du numérique (CLDN) le 11 octobre 2022. Le Conseil d'État neuchâtelois rejoint les positions et les remarques formulées par ces conférences, auxquelles il a participé.

En vous remerciant de nous avoir donné la possibilité de prendre position sur cet objet, nous vous prions d'agréer, Madame la conseillère fédérale, l'expression de notre haute considération.

Neuchâtel, le 19 octobre 2022

Au nom du Conseil d'État :

Le président,
L. KURTH

La chancelière,
S. DESPLAND



NE



KANTON
NIDWALDEN

LANDAMMANN UND
REGIERUNGSRAT

Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL

Eidg. Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 18. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID). Stellungnahme

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 29. Juni 2022 eröffnete das Eidgenössische Justiz- und Polizeidepartement EJPD bei den Kantonen das Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Wir danken Ihnen für diese Möglichkeit und lassen uns wie folgt vernehmen.

1 Vorbemerkung

Der Regierungsrat Nidwalden ist der Ansicht, dass den Vorbehalten, die im März 2021 zur Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste geführt haben, mit dem vorliegenden Entwurf in angemessener und nachvollziehbarer Weise Rechnung getragen wird.

Die rasche Erarbeitung einer neuen Vorlage, die unter dem umfassenden Einbezug kantonaler wie privater Akteure erfolgt ist, wird ausdrücklich begrüsst. Die Schaffung einer einheitlichen staatlichen E-ID für die Schweiz ist unumgänglich, um zukunftsfähig zu bleiben und die Digitalisierung auch auf Ebene der öffentlichen Verwaltung voranzutreiben.

2 Beurteilung der Vorlage

Die Vorlage wird befürwortet. Insbesondere werden die folgenden Punkte begrüsst:

- Im Gegensatz zur in der Volksabstimmung gescheiterten Vorlage sieht der neue Entwurf eine Ausstellung der E-ID durch eine staatliche Stelle vor. Auch die nötige Infrastruktur wird durch den Bund zur Verfügung gestellt.
- Die Grundsätze von Datensparsamkeit, dezentraler Datenspeicherung und "privacy by design" entsprechen wichtigen Anliegen der Bevölkerung. Die Schweiz orientiert sich damit auch an den Vorgaben der europäischen Gesetzgebung (insbesondere der geplanten Revision der eIDAS-Verordnung).

- Die Vorlage berücksichtigt die Entwicklungen auf europäischer Ebene und ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um die Anerkennung der schweizerischen E-ID im Ausland bzw. die Anerkennung ausländischer elektronischer Identitätsnachweise in der Schweiz zu erleichtern.
- Die Möglichkeit, die Vertrauensstruktur für das Ausstellen weiterer elektronischer Nachweise zu nutzen, und die kostenlose Ausstellung der E-ID für Privatpersonen ermöglichen eine schnellere Verbreitung und Akzeptanz der Infrastruktur.

Bezüglich der detaillierten Ausführungen wird vollumfänglich auf die Stellungnahme der Konferenz der Kantonsregierung vom 23. September 2022 verwiesen.

Ergänzend weisen wir aber darauf hin, dass die Verankerung der Sorgfaltspflichten bei der Inhaberin oder beim Inhaber der E-ID nach Art. 7 mit Massnahmen begleitet werden muss, welche die Inhaberinnen und Inhaber der E-ID bei der Wahrnehmung der Sorgfaltspflichten unterstützen. Die in Art. 8 verankerte Pflicht der Kantone, Anlaufstellen zur Unterstützung bei der Ausstellung und dem Einsatz der E-ID einzurichten, erachten wir aufgrund der Nähe der kantonalen Behörden zu den Bürgerinnen und Bürgern als sinnvoll. Zusätzlich regen wir aber an, Massnahmen zur Wahrnehmung der Sorgfaltspflichten übersichtlich und gut zugänglich in der Applikation mit der E-ID darzustellen.

3 Antrag

Der Regierungsrat Nidwalden unterstützt die Vernehmlassung der Konferenz der Kantonsregierungen vom 23. September 2022 vollumfänglich und dankt für die Berücksichtigung der vorgebrachten ergänzenden Anliegen.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Joe Christen
Landammann



A. Eberli
lic. iur. Armin Eberli
Landschreiber

Geht an:

- rechtsinformatik@bj.admin.ch



CH-6061 Sarnen, Postfach, Staatskanzlei

A-Post

Bundesamt für Justiz
3003 Bern

Mail an: rechtsinformatik@bj.admin.ch

Referenz/Aktenzeichen: 2022-0416
Unser Zeichen: ue

Sarnen, 18. Oktober 2022

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz; BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für Ihre Einladung zur Stellungnahme im Rahmen des Vernehmlassungsverfahrens zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

1. Allgemeine Einschätzung

Der Kanton Obwalden unterstützt die Vorlage zum neuen E-ID-Gesetz. Er begrüsst die rasche Erarbeitung einer neuen Vorlage, die unter dem umfassenden Einbezug kantonaler wie privater Akteure erfolgt ist. Die Schaffung einer einheitlichen staatlichen E-ID für die Schweiz ist unumgänglich, um zukunftsfähig zu bleiben und die Digitalisierung auch auf Ebene der öffentlichen Verwaltung voranzutreiben.

Der Kanton Obwalden ist der Ansicht, dass den Vorbehalten, die im März 2021 zur Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste geführt haben, mit dem vorliegenden Entwurf in angemessener und nachvollziehbarer Weise Rechnung getragen wird. Ausdrücklich begrüsst werden insbesondere die folgenden Punkte:

- Im Gegensatz zur in der Volksabstimmung gescheiterten Vorlage sieht der neue Entwurf eine Ausstellung der E-ID durch eine staatliche Stelle vor. Auch die nötige Infrastruktur wird durch den Bund zur Verfügung gestellt.
- Die Grundsätze von Datensparsamkeit, dezentraler Datenspeicherung und „privacy by design“ entsprechen wichtigen Anliegen der Bevölkerung. Die Schweiz orientiert sich damit

auch an den Vorgaben der europäischen Gesetzgebung (insbesondere der geplanten Revision der eIDAS-Verordnung).

- Die Vorlage berücksichtigt die Entwicklungen auf europäischer Ebene und ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um die Anerkennung der schweizerischen E-ID im Ausland bzw. die Anerkennung ausländischer elektronischer Identitätsnachweise in der Schweiz zu erleichtern.
- Die Möglichkeit, die Vertrauensstruktur für das Ausstellen weiterer elektronischer Nachweise zu nutzen und die kostenlose Ausstellung der E-ID für Privatpersonen ermöglichen eine schnellere Verbreitung und Akzeptanz der Infrastruktur.

2. Begriffsdefinitionen

Das BGEID verwendet eine Vielzahl von technischen Begriffen wie „elektronischer Nachweis“, „Verifikatorin“, „Basisregister“, „Vertrauensregister“ oder „Identifikator“. Diese sind im allgemeinen Sprachgebrauch nicht geläufig und bedürfen daher einer genaueren Definition. Die entsprechenden Begriffe werden zwar teilweise im Rahmen einzelner Artikel (z.B. „Verifikatorin“ in Art. 16) oder im Rahmen des erläuternden Berichts definiert. Die Verständlichkeit des Gesetzes und die Systematik würden indes profitieren, wenn – analog anderer Bundesgesetze – eine Bestimmung (z.B. als Art. 2) aufgenommen würde, welche die relevanten Definitionen für das gesamte Gesetz vornimmt. Zu achten ist dabei auch auf eine klare Unterscheidung zwischen „elektronischen Nachweisen“ (als Oberbegriff, der die E-ID und andere elektronische Nachweise umfasst) und „anderen elektronischen Nachweisen“.

3. Sicherheit und Benutzerfreundlichkeit

Mitentscheidend für die künftige Verbreitung der E-ID und der Vertrauensinfrastruktur wird die Benutzerfreundlichkeit der entsprechenden Applikationen sein. Sie müssen für alle Beteiligten möglichst unkompliziert und niederschwellig zugänglich und anwendbar sein. Unter anderem an diesem Punkt sind in der Vergangenheit Vorhaben wie die qualifizierte elektronische Signatur gescheitert. Gleichzeitig darf Benutzerfreundlichkeit nicht auf Kosten von Sicherheit und Datenschutz gehen. Hierbei ist den Schutzziele der Authentizität und der Verbindlichkeit besonderes Gewicht beizumessen. Sind diese nicht gewährleistet, entstehen hohe Risiken, nicht nur für die betroffenen Personen, sondern auch für die öffentlichen Organe und die Privaten, die auf die Bestätigung der Identität des Gegenübers angewiesen sind. Spätestens bei Bekanntwerden vom Missbrauchsfällen hätten Sicherheitslücken zudem einen Vertrauensverlust zur Folge, mit den entsprechenden Konsequenzen für die Verbreitung der E-ID und die Nutzung der Vertrauensinfrastruktur. Den Aspekten der Benutzerfreundlichkeit und der Sicherheit wird somit bei der Ausarbeitung der bundesrätlichen Verordnung besondere Beachtung zu schenken sein. Die Infrastruktur muss laufend den technischen Veränderungen angepasst werden können.

4. Koordination mit Vollzugsträgern

Die Umsetzung des BGEID und insbesondere seiner Art. 8 und Art. 9 verlangt nach umfassenden Massnahmen auf Ebene der Kantone und Gemeinden. Im erläuternden Bericht fehlen jedoch Ausführungen zur Notwendigkeit, die Umsetzung mit den Vollzugsträgern koordiniert zu planen. Auch werden keine Angaben gemacht zum Zeitbedarf für die Umsetzung in den Kantonen und Gemeinden (gemäss Art. 8 VIV) sowie zum geplanten Zeitpunkt des Inkrafttretens. Der Kanton Obwalden erwartet in der Botschaft des Bundesrates entsprechende Ausführungen. Eine koordinierte Umsetzung gemäss dem Arbeitspapier von Bund und Kantonen vom 28. Oktober 2015 ist an die Hand zu nehmen. Der Kanton Obwalden erinnert daran, dass die Digitalisierung der Verwaltung auf Kantons- und Gemeindeebene bereits in vollem Gange ist. Es wurden bereits und werden in den nächsten Jahren weitere grosse Investitionen vorgenommen. Für die Kantone ist es deshalb von entscheidender Bedeutung, dass sich die Identifizierung über die E-ID technisch problemlos in ihre bestehenden Anwendungen integrieren lässt. Der erläuternde Bericht (Kap. 5.2., S. 20-21) geht pauschal davon aus, dass Kantone und Gemeinden von der E-ID und der Vertrauensinfrastruktur profitieren werden, was ihre (nicht weiter bezifferten) Aufwände in jedem Fall rechtfertigen werde. Diese Ausführungen genügen nicht. Es ist eine detailliertere Kostenfolgeabschätzung vorzunehmen, und der Berücksichtigung der Anschlussfähigkeit bestehender Lösungen ist bei der Ausarbeitung der technischen Details vorrangige Beachtung zu schenken.

5. Haftung und Qualitätsstandards

Die E-ID wird zur Identifizierung in kantonalen elektronischen Diensten zur Anwendung kommen und kantonale Lösungen ergänzen. Im erläuternden Bericht fehlen jedoch Ausführungen zum Umgang mit Haftungsansprüchen, sollten Fehler im E-ID-System zu Lücken in den kantonalen Anwendungen führen. Entsprechende Angaben mit Bezug zu anerkannten Qualitätsstandards (Standard eCH-0170) sind im Hinblick auf nachfolgende Ausführungsbestimmungen in der Botschaft zu ergänzen.

6. Vollmacht und gesetzliche Vertretung

Weder im Entwurf noch im erläuternden Bericht sind Hinweise zu finden auf die Abläufe in Zusammenhang mit Vollmachten und der gesetzlichen Vertretung. Gemäss Art. 4 und Art. 5 BGEID ist zur Ausstellung einer E-ID für Minderjährige bis 14 Jahre und Personen unter umfassender Beistandschaft das Einverständnis der gesetzlichen Vertretung nötig. Es fehlen aber Aussagen zu späteren Vertretungs- und Delegationsmöglichkeiten in der Nutzung der E-ID oder in der Anwendung anderer Nachweise. Im Interesse einer einheitlichen Vollzugspraxis ist eine entsprechende Klärung in der Botschaft wichtig.

7. Bemerkungen zu einzelnen Artikeln des BGEID

Art. 1

Art. 7 des neuen Datenschutzgesetzes (nDSG) postuliert neben dem Grundsatz des „Datenschutz durch Technik“ („privacy by design“) jenen der „datenschutzfreundlichen Voreinstellungen“ („privacy by default“). Letzterer ist in Art. 1 Abs. 2 Bst. b zusätzlich aufzuführen, um diesem zentralen Aspekt Betonung zu verleihen und eine Harmonisierung mit dem nDSG sicherzustellen.

Art. 3 (Persönliche Voraussetzungen)

Art. 3 BGEID sieht vor, dass nur Personen mit geregelter Aufenthalt in der Schweiz eine E-ID beantragen können. Der Kreis der Personen, die mit öffentlichen Verwaltungen interagieren, ist aber weiter gefasst. Zu denken ist unter anderem an Personen, die ohne geregelten Aufenthalt in der Schweiz wohnhaft sind, oder an Zweitwohnungsbesitzer. Es ist zumindest die Möglichkeit zu prüfen, für solche Fälle eine spezifische E-ID auszustellen. Die Gesetzesvorlage ist entsprechend so zu ergänzen, dass der Bundesrat ermächtigt wird, für weitere Personen mit Aufenthalt in der Schweiz eine spezielle E-ID mit eingeschränktem Einsatzbereich vorzusehen.

Gemäss dem erläuternden Bericht (S. 9 zu Art. 3) sollen Anbieterinnen die Möglichkeit haben, die Nutzung ihrer Dienste für die Inhaberinnen und Inhaber gewisser Ausweiskategorien zu beschränken. Der Bericht weist darauf hin, dass bei Ausweisen der Kategorien N, F, S und Ci nicht davon ausgegangen werden könne, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. Es ist festzuhalten, dass die Verlässlichkeit der Identifizierung einer Person nicht aus der Kategorie ihres Ausweises ersichtlich ist (nicht jede asylsuchende Person kann keine Identitätsdokumente vorweisen, während über eine Härtefallbewilligung auch Personen, deren Identität nicht abschliessend geklärt ist, unter Umständen einen Ausweis B erhalten können). Sollen Einschränkungen spezifisch aufgrund der Verlässlichkeit der Identitätsdokumente möglich sein, so ist dies im Gesetz auszuführen und eine entsprechende Angabe ist unter die Daten gemäss Art. 2 Abs. 3 BGEID aufzunehmen. Ein blosser Verzicht auf eine gesetzliche Regelung, ohne dass die entsprechende Angabe in der E-ID erfasst wird, geht am Ziel vorbei.

In Art. 3 Bst. a wird konkret das Ausweisgesetz (AwG) genannt. Es ist nicht nachvollziehbar, weshalb in Art. 3 Bst. b bloss allgemein auf die Ausländergesetzgebung verwiesen und nicht die konkreten Gesetze (Ausländer- und Integrationsgesetz und Asylgesetz) genannt werden. Für Aussenstehende ist mit der heutigen Formulierung nicht ersichtlich, welche gesetzlichen Bestimmungen angewendet werden.

Art. 4 (Ausstellung)

Der Ausstellungsprozess und damit verbunden die Frage, wie die Identifizierung der antragsstellenden Personen durchgeführt wird, sind für die Sicherheit und damit auch für die künftige Akzeptanz der E-ID zentral. Eine Regelung des Ausstellungsprozesses muss deshalb ins Gesetz aufgenommen werden. Dabei dürfen Sicherheitsüberlegungen nicht hinter Kosten- und Effizienzfragen zurückstehen. Art. 6 Abs. 5 nDSG statuiert die Pflicht des Datenbearbeiters oder der Datenbearbeiterin, sich über die Richtigkeit der Personendaten zu vergewissern. Die Angemessenheit der Massnahmen muss sich dabei auch nach dem – im Falle der E-ID erheblichen – Risiko für die Grundrechte der betroffenen Person richten.

Der Entwurf sieht gemäss Art. 4 Abs. 2 vor, dass ab dem 15. Altersjahr die E-ID eigenständig beantragt werden kann. Nach Art. 5 Abs. 1 AwG brauchen Minderjährige dagegen zum Bezug eines (physischen) Ausweises die Einwilligung ihres gesetzlichen Vertreters. Die Begründung des erläuternden Berichtes zu diesem Unterschied überzeugt nicht. Im Vordergrund sollten Sicherheitsüberlegungen stehen und nicht die Frage, welche Ausweisarten von Jugendlichen mehrheitlich genutzt werden. Die Altersgrenze zum selbständigen Bezug einer E-ID ist somit jener zum Bezug eines physischen Ausweises anzugleichen.

Art. 5 (Widerruf)

Art. 5 Bst. d Ziff. 2 legt fest, dass die E-ID widerrufen wird, wenn das Bundesamt für Polizei über eine Änderung der Personenidentifizierungsdaten des Inhabers oder der Inhaberin informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen müssen sich dann nicht noch einmal um die Ausstellung einer neuen E-ID bemühen und profitieren so von den erleichterten Abläufen, die durch die Digitalisierung ermöglicht werden.

Art. 6 (Gültigkeitsdauer)

Neben der Gültigkeitsdauer ist im Entwurf auch die Frage der Verlängerung nicht geregelt. Es wird nicht klar, ob nach Ablauf des physischen Ausweisdokuments – sofern die Gültigkeit der E-ID an diese geknüpft wird – erneut eine E-ID beantragt werden muss oder ob dies bei Verlängerung des Ausweises automatisch geschieht. Dies ist spätestens in der Verordnung ebenfalls zu klären.

Art. 7 (Sorgfaltspflicht)

Art. 7 BGEID sieht eine Sorgfaltspflicht für Inhaberinnen und Inhaber einer E-ID vor. Nicht konkret geregelt sind dabei die Verpflichtungen bei Verlust des E-ID-Trägers, dies im Gegensatz zu Art. 8 AwG, das eine Meldepflicht bei Verlust eines (physischen) Ausweises vorsieht. Zur Konkretisierung der Sorgfaltspflichten ist dieser Fall auch im BGEID auszuführen.

Art. 8 (Anlaufstellen der Kantone)

Die Bestimmung sieht eine zusätzliche Aufgabe für die Kantone vor. Der erläuternde Bericht (S. 10 zu Art. 8) geht davon aus, dass die benötigten Strukturen in den Kantonen bereits vorhanden sind. Dies ist jedoch nicht notwendigerweise der Fall.

Als Vollzugsträger steht hier der Bund in der Verantwortung. Wer eine Informatiklösung anbietet und betreibt, hat auch den nötigen Support sicherzustellen, soweit die eigene Anwendung betroffen ist. Die Kantone sehen sich da als zuständig, wo es darum geht, Unterstützung beim Einsatz der E-ID für kantonale E-Government-Angebote zu leisten. Für Schwierigkeiten bei der Beantragung der E-ID oder bei der Nutzung der Vertrauensinfrastruktur muss dagegen der Bund eine Ansprechstelle schaffen. Eine solche ist im erläuternden Bericht zwar erwähnt, sie fehlt jedoch im Gesetzesentwurf ebenso wie der Second Level Support, den der Bund gemäss dem Bericht für die Kantone wahrnehmen soll.

Unter Bezugnahme auf die Ausführungen im erläuternden Bericht ist zudem darauf hinzuweisen, dass Personen, die bereit sind eine E-ID zu nutzen, üblicherweise auch in der Lage sind, einen Support per Telefon oder E-Mail in Anspruch zu nehmen. Es müssen dafür nicht zwingend physische Anlaufstellen geschaffen werden.

Art. 9 (Pflicht zur Akzeptanz der E-ID)

Art. 9 E-BGEID sieht vor, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Der Begriff der „öffentlichen Aufgabe“ wird im erläuternden Bericht mit „Verwaltungsaufgaben“ gleichgesetzt, was dem Begriff von Art. 178 Abs. 3 BV entspricht. Es empfiehlt sich, im BGEID ebenfalls von „Verwaltungsaufgaben“ zu sprechen, oder, falls der Begriff der „öffentlichen Aufgabe“ weiter gefasst werden soll, die Botschaft in diesem Punkt zu präzisieren. Es ist zu bedenken, dass unter anderem im Gesundheitswesen eine Vielzahl von privaten Akteuren öffentliche Aufgaben ausführen, so zum Beispiel Krankenkassenversicherer, Betreiber von Krebsregistern und Transplantationsregistern oder Anbieter des EPD. Die Pflicht zur Akzeptanz der zukünftigen E-ID bei all diesen Akteuren ist durchaus sinnvoll, wird aber Investitionen und Vorbereitungsarbeiten zur Folge haben, die den Betroffenen möglichst rasch klar kommuniziert werden müssen. Es ist somit wichtig, dass bei allen Beteiligten von Anfang an Klarheit herrscht über den Geltungsbereich von Art. 9 BGEID.

Die Umsetzung von Art. 9 BGEID bedingt eine Integration der E-ID in bestehende IT-Anwendungen von Kantonen und Gemeinden. Diesen ist dafür eine ausreichende Übergangsfrist einzuräumen.

Art. 10 (Vorweisen einer E-ID)

Der Kanton Obwalden begrüsst die in Art. 10 festgehaltene Wahlfreiheit zwischen E-ID und einem anderen Ausweisdokument und den damit einhergehenden Grundsatz der Nichtdiskriminierung zwischen Personen, die eine E-ID nutzen wollen, und Personen, die keine E-ID nutzen.

Art. 15 (Übertragbarkeit von elektronischen Nachweisen)

Die Hinweise zu Art. 15 Abs. 2 BGEID im erläuternden Bericht (S. 13) lassen sich nur schwer mit der Bestimmung im Entwurf selber vereinbaren. Während sich Art. 15 Abs. 2 mit der Übertragbarkeit von Nachweisen befasst, nimmt der erläuternde Bericht Bezug auf ein System für Sicherungskopien. Sollte mit der Bestimmung tatsächlich nur die Übertragbarkeit in ein System für Sicherungskopien gemeint sein, ist dies entsprechend zu formulieren.

Art. 16 (Vorweisen von elektronischen Nachweisen)

Art. 16 Abs. 1 bestimmt, dass die Inhaberin bzw. der Inhaber einer E-ID selber darüber bestimmt, welche Informationen an die betreffende Verifikatorin übermittelt werden. In der Praxis werden dennoch oft die Verifikatorinnen darüber bestimmen, da die Person ansonsten vom Angebot keinen Gebrauch machen kann. In der zu erarbeitenden Botschaft sind deshalb Ausführungen zu machen, wie die Beschränkung der Datenbearbeitung auf das Minimum bei privaten Verifikatorinnen sichergestellt werden soll und wie trotz der dezentralen Struktur des Systems eine wirksame Kontrolle möglich ist.

Art. 17 (Basisregister)

Wie der erläuternde Bericht (S. 14) ausführt, birgt die Tatsache, dass Ausstellerinnen ohne weitere Überprüfung ihre Daten selber ins Basisregister gemäss Art. 17 Abs. 3 BGEID eintragen können das Risiko, dass diese unter falscher Identität elektronische Beweismittel ausstellen können. Es liegt auf der Hand, dass dies für die betroffenen Personen unter Umständen weitreichende Folgen haben kann. Die Abfederung dieses Risikos durch Veröffentlichung bei begründetem Verdacht gemäss Art. 22 BGEID ist nicht ausreichend, da sie bereits eine Verletzung der Persönlichkeitsrechte von betroffenen Personen voraussetzt. Auch können durch blosses Öffentlichmachen erfahrungsgemäss nicht alle Nutzenden rechtzeitig erreicht werden. Ein Eintrag ins Vertrauensregister nach Art. 18 BGEID muss entsprechend auch für private Anbieter zwingend sein. Andernfalls können Missbräuche nicht verhindert werden.

Art. 20 (Anwendung zur Prüfung von elektronischen Nachweisen)

Aus dem Wortlaut von Art. 20 BGEID wird nicht klar, dass es dabei um eine Prüfung von elektronischen Nachweisen bei persönlichem Erscheinen und nicht um einen Online-Vorgang geht. Dies muss deutlicher ausgeführt werden. In jedem Fall ist bei der technischen Umsetzung – mithilfe einer Anwendung nach Art. 20 oder ohne – sicherzustellen, dass eine zuverlässige Überprüfung der Gültigkeit von elektronischen Nachweisen für die Verifikatorinnen ohne weiteres möglich ist.

Art. 23 (Quellcode der Vertrauensinfrastruktur)

Der Kanton Obwalden unterstützt die Veröffentlichung des Quellcodes der vom Bund zur Verfügung gestellten Elemente der Vertrauensinfrastruktur zur Umsetzung der E-ID gemäss Art. 23. Open Source Software und die damit einhergehende Transparenz trägt zum Vertrauen in technische Lösungen bei, was gerade im sensiblen Bereich des Nachweises der Identität von natürlichen Personen essentiell ist.

Art. 25 (Technische Entwicklung)

Die Funktionsweise von Abs. 2 dieser Bestimmung ist unklar: Wer entscheidet darüber, ob ein Anwendungsfall von Abs. 2 vorliegt? Entscheidet dies der Bundesrat bereits mit dem Erlass der Verordnung? Zudem ist der Zusammenhang zwischen Abs. 1 und Abs. 2 von Art. 25 im Text deutlicher hervorzuheben, und es sollte der Vollständigkeit halber der Fall des fakultativen Referendums miterfasst werden:

„² Sofern Bestimmungen, die gestützt auf Abs. 1 erlassen werden, einer weiteren Grundlage in einem Gesetz bedürfen, treten diese Bestimmungen ausser Kraft:

- a) [...]*
- b) mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung oder die Stimmberechtigten; oder [...]“*

Art. 26 (Gebühren)

Art. 26 BGEID sieht vor, dass von Ausstellerinnen und Verifikatorinnen elektronischer Nachweise Gebühren erhoben werden. Dies betrifft auch Stellen, die öffentliche Aufgaben erfüllen, obwohl diese gemäss Art. 9 BGEID zur Akzeptanz der E-ID verpflichtet sind. Gleichzeitig möchte der Bundesrat die E-ID durch Beiträge aus der Agenda DVS finanzieren, die von den Kantonen mitfinanziert wird. Gemäss Art. 3 Abs. 2 AllgGebV verzichtet die Bundesverwaltung auf die Erhebung von Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Dies soll auch vorliegend entsprechend gehandhabt und Verrechnungen zwischen den Gemeinwesen auf ein Minimum beschränkt werden.

Der Bundesrat soll darüber hinaus mit der Kompetenz ausgestattet werden, die Gebühren für weitere Akteure ganz oder teilweise zu erlassen, soweit diese öffentlichen Aufgaben erfüllen. Unter anderem besteht im Gesundheitsbereich ein grosses Interesse an einer breiten Nutzung der E-ID, um die Aufbereitung von Gesundheitsdaten zu erleichtern. Die Kosten für die betroffenen Stellen sind somit möglichst tief zu halten.

Die Vorlage und der erläuternde Bericht äussern sich nicht bzw. nur sehr vage über die Höhe der zu erhebenden Gebühren. Diese sollen auf Verordnungsstufe festgelegt werden. Die Kosten dürften jedoch einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben. Eine explizite Kostenfolgeschätzung für die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise aufgrund der Gebühren sollte deshalb in die Botschaft aufgenommen werden.

Art. 28 (Ausführungsbestimmungen)

Zahlreiche technische Aspekte zur Umsetzung der E-ID werden auf Verordnungsstufe geregelt. Aufgrund der unterschiedlichen bestehenden Lösungen in den einzelnen Kantonen, aber auch in den einzelnen Sektoren ist es unabdingbar, dass die zuständigen Akteure eng in die Erarbeitung der Vollzugsregelungen miteinbezogen werden. Es ist eine der Voraussetzungen einer breiten Akzeptanz der E-ID, dass diese unkompliziert in bestehende Anwendungen integriert werden kann.

Art. 29 (Änderung anderer Erlasse)


Gemäss dem erläuternden Bericht (Ziff. 3.1) wurde die Verwendung der E-ID in spezifischen Bereichen und damit die Änderung anderer Erlasse im Entwurf nur exemplarisch geregelt. Es ist unabdingbar, die Gesetzgebung des Bundes im weiteren Verfahren systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder eine qualifizierte elektronische Signatur verlangt

werden. Dies betrifft insbesondere auch die Verfahrensgesetzgebung des Bundes. Die entsprechenden Bestimmungen sind durchgehend anzupassen.


Wir danken Ihnen für die Möglichkeit zur Stellungnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Im Namen des Regierungsrats



Christoph Amstad
Landammann



Nicole Frunz Wallimann
Landschreiberin

Kanton Schaffhausen
Regierungsrat
Beckenstube 7
CH-8200 Schaffhausen
www.sh.ch

T +41 52 632 71 11
F +41 52 632 72 00
staatskanzlei@sh.ch



Regierungsrat

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
3003 Bern

per E-Mail an:
rechtsinformatik@bj.admin.ch

Schaffhausen, 4. Oktober 2022

Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 haben Sie die Kantonsregierungen zu einer Vernehmlassung in oben erwähnter Angelegenheit eingeladen. Wir bedanken uns für diese Möglichkeit und nehmen gerne wie folgt Stellung:

Wir unterstützen den unterbreiteten Vorentwurf zum E-ID-Gesetz. Im Einzelnen schliessen wir uns den Ausführungen der Konferenz der Kantonsregierungen (KdK) in der beiliegenden Stellungnahme vom 23. September 2022 vollumfänglich an.

Für die Kenntnisnahme und die Berücksichtigung unserer Stellungnahme danken wir Ihnen.



Freundliche Grüsse

Im Namen des Regierungsrates

Die Präsidentin:

Dr. Cornelia Stamm Hurter

Der Staatsschreiber-Stv.:

Christian Ritzmann

Beilage: Stellungnahme der KdK vom 23. September 2022



6431 Schwyz, Postfach 1260

per E-Mail

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus
3003 Bern

rechtsinformatik@bj.admin.ch

Schwyz, 27. September 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Vernehmlassung des Kantons Schwyz

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 29. Juni 2022 hat das Eidgenössische Justiz- und Polizeidepartement den Kantonsregierungen die Unterlagen zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) zur Vernehmlassung bis 20. Oktober 2022 unterbreitet.

Der Regierungsrat unterstützt die Vorlage zum neuen E-ID-Gesetz. Die Schaffung einer einheitlichen staatlichen E-ID ist zur Sicherung der Zukunftsfähigkeit der Schweiz und Förderung der digitalen Transformation unumgänglich. Ausdrücklich begrüsst wird, dass die E-ID durch den Bund ausgegeben und die Infrastruktur ebenfalls durch den Bund betrieben wird. Zu den einzelnen Artikeln bestehen seitens Regierungsrat nachfolgende Anmerkungen.

Ingress

Mit Blick auf die rechtsgeschäftliche Verwendung der elektronischen Nachweise und die zur Ausstellung der elektronischen Nachweise verwendeten Personendaten bzw. deren Kategorien ist die Gesetzgebungskompetenz des Bundes im Bereich des Zivilrechts gemäss Art. 122 Abs. 1 BV ebenfalls in den Ingress aufzunehmen.

1. Abschnitt

Im 1. Abschnitt wird eine zusätzliche Bestimmung mit Legaldefinitionen zu den verwendeten Begrifflichkeiten angeregt.

Art. 2

Die Aufnahme der AHV-Nummer (AHVN) in die E-ID birgt gewisse Risiken, die primär in der Möglichkeit der Verknüpfung verschiedener Datenbestände besteht. Mit Blick auf die Zielsetzungen der Revision des Bundesgesetzes über die AHV vom 20. Dezember 1946 (AHVG, SR 831.10) soll die

AHVN systematisch für die Verhinderung von kostenintensiven Verwaltungsfehlern sowie für mehr Effizienz dank automatisiertem Datenaustausch zwischen den Behörden und zur Vermeidung von Verwechslungen verwendet werden. Entsprechend bestehen wenig Vorbehalte, wenn es um die Identifikation zwischen Behörden und Privaten und die darauffolgende Verwendung beim elektronischen Behördengang geht, sofern es sich um öffentliche Organe handelt, die unter Art. 153c Abs. 1 AHVG fallen. Im Sinne der obigen Ausführung ist im Gesetz – z. B. in Art. 16 der Vorlage – ausdrücklich festzuhalten, dass die AHVN mit Hilfe von technischen Massnahmen nur jenen Verifikatoren zugänglich gemacht werden darf, für welche grundsätzlich die rechtlichen Grundlagen für die systematische Verwendung gemäss AHVG gegeben sind. Damit soll der ungehinderten Verbreitung der AHVN an private Verifikatoren vorgebeugt werden.

Art. 3

Der Regierungsrat hält die vorgesehenen persönlichen Voraussetzungen für die Ausstellung einer E-ID nachvollziehbar und zweckmässig.

Art. 5

Gemäss erläuterndem Bericht ist es aufgrund der dezentralen Art des Systems nicht möglich, die E-ID selber zu sperren. Aufgrund des erheblichen Missbrauchspotenzials im Falle eines Diebstahls der E-ID ist eine Supportorganisation aufzubauen, welche rund um die Uhr im Einsatz steht (vgl. Art. 8).

Art. 5 Bst. d Ziff. 2 legt fest, dass die E-ID widerrufen wird, wenn das Fedpol über eine Änderung der Personenidentifizierungsdaten des Inhabers oder der Inhaberin informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen profitieren so von erleichterten, digitalen Abläufen.

Art. 8

Mit der Bestimmung wird eine neue Kantonsaufgabe geschaffen. Um gesamtschweizerisch einen angemessenen Kundenservice gewährleisten zu können, ist eine einheitliche, permanente (24/7) Supportorganisation aufzubauen. Eine Schärfung der Bestimmung hinsichtlich dieses Ziels ist notwendig. Gemäss erläuterndem Bericht ist vorgesehen, die Investitionskosten des Bundes über finanzielle Beiträge der Digitalen Verwaltung Schweiz (DVS) zu finanzieren. Im Kontext der durch die Kantone zu schaffende Anlaufstelle ist zu prüfen, ob die entstehenden Kosten auf Seiten der Kantone ebenfalls über DVS finanziert werden können.

Art. 9

Neben der Pflicht der Behörden zur Akzeptanz der E-ID für die elektronische Identifikation von Personen soll klarer geregelt werden, dass eine Behörde bzw. andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID in keinem Fall als zwingend voraussetzen darf. Zudem ist den Kantonen und Gemeinden eine ausreichende Übergangsfrist einzuräumen.

Art. 10

In der Umsetzung ist darauf zu achten, dass durch den Einsatz der E-ID der Zugang zu öffentlichen Dienstleistungen nicht in unzumutbarer Weise eingeschränkt wird.

Art. 11

Diese Bestimmung ist systematisch nach Art. 5 einzuordnen.

Im Sinne der Umsetzung des Prinzips der dezentralen Datenhaltung wird zudem folgende Ergänzung von Art. 11 Abs. 4 vorgeschlagen: *«Die via Schnittstellen bezogenen Daten werden ausschliesslich zum Zweck der Ausstellung der E-ID bearbeitet und nicht im Informationssystem aufbewahrt.»*

Art. 16

Gemäss Art. 16 Abs. 1 bestimmt der Inhaber, welche Bestandteile des Nachweises und Informationen dem Verifikatoren übermittelt werden. Ein Unternehmen könnte jedoch mehr verlangen, als für den eigentlichen Zweck z. B. einer Anwendung erforderlich wäre. Der erläuternde Bericht hält dazu fest: *«Der Handlungsspielraum der Inhaberin oder des Inhabers wird somit durch die Anforderungen begrenzt, die die Verifikatoren für den Überprüfungsprozess festlegen»*. Diesbezüglich wird eine weitergehende Regelung angeregt, damit nicht der Verifikator einseitig die Anforderungen bestimmen kann.

Art. 26

Eine explizite Kostenfolgeschätzung für die Aussteller und Verifikatoren elektronischer Nachweise aufgrund der Gebühren sollte in die Botschaft aufgenommen werden, da die Kosten einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben dürften.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Frau Bundesrätin, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:



André Rüegsegger
Landammann



Dr. Mathias E. Brun
Staatsschreiber

Kopie an:

- die Schwyzer Mitglieder der Bundesversammlung.

Eidg. Justiz- und
Polizeidepartement EJPB
Bundesamt für Justiz
Bundesrain 20
3003 Bern

per Mail an:
rechtsinformatik@bj.admin.ch

27. September 2022

Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Wir nehmen Bezug auf Ihr Schreiben vom 29. Juni 2022 in oben genannter Angelegenheit, danken Ihnen für die Gelegenheit zur Stellungnahme und äussern uns dazu gerne wie folgt:

Grundsätzliches

Wir unterstützen eine staatlich geregelte E-ID für den medienbruchfreien Zugang zu Behördengeschäften als grundlegende Voraussetzung und sehen die Eröffnung der Vernehmlassung des Vorentwurfs für das Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) als wichtigen Meilenstein in der Entwicklung zu einer digitaleren Gesellschaft in der Schweiz.

Für den Erfolg der E-ID ist unserer Ansicht nach von besonderer Wichtigkeit, dass Nutzerinnen und Nutzern der zukünftigen staatlichen E-ID die grösstmögliche Kontrolle über ihre dezentral gespeicherten Daten haben und die E-ID nach den «Self-Sovereign Identity» und «Privacy by Design» Prinzipien umgesetzt wird.

Wir begrüssen es, wenn die zukünftige E-ID auf einer staatlich betriebenen Infrastruktur aufgebaut und betrieben wird, welche staatlichen und privaten Akteuren für die Ausstellung unterschiedlicher digitaler Nachweise standardisiert zur Verfügung steht. In diesem Kontext wird es wichtig sein, den Nutzerinnen und Nutzern ein bestmögliches Nutzererlebnis mit adäquaten Begleit- und Hilfestellungsmassnahmen während allen Prozessphasen der E-ID-Anwendung zu gewährleisten.

E-ID im Kontext des elektronischen Patientendossiers EPD

Ein zentraler Aspekt ist, dass die E-ID die Einführung und Ausbreitung des elektronischen Patientendossiers (EPD) unterstützt, einfach anwendbar ist und keine neuen Hürden entstehen lässt. Die Ausgestaltung der staatlichen E-ID als Self-Sovereign Identity lässt befürchten, dass für die EPD-Nutzung zusätzlich zur E-ID-Eröffnung noch ergänzende Informationen zur EPD Inhaberin/zum EPD Inhaber erhoben werden müssen. Ein zweistufiger Eröffnungsprozess, unter Umständen an zwei verschiedenen Stellen, wird die Ausbreitung des EPD nicht unterstützen und ist deshalb zu vermeiden.

Des Weiteren sollte die Verwendung der E-ID kostengünstiger sein, als die gegenwärtig für das EPD genutzten E-IDs. Dies ist unseres Erachtens entscheidend für den Erfolg des EPD und wichtig

für weitere gesundheitsbezogene Dienstleistungen, wie beispielsweise den Zugriff von Gesundheitsfachpersonen auf Gesundheitsdaten ihrer Patientinnen und Patienten. Es ist davon auszugehen, dass die Stammgemeinschaften gemäss Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015 (EPDG; SR 816.1) als Anbieterinnen einer Dienstleistung mit E-ID-Zugang zu Ausstellerinnen resp. Verifikatorinnen werden und gemäss dem vorliegenden Gesetzesentwurf Gebühren an den Bund entrichten müssen. Abhängig von deren Höhe kann dies zu finanziellen Problemen für das EPD führen. Deshalb ist eine Möglichkeit zu schaffen, dass bundesgesetzlich begründete Dienstleistungen, zu welchen auch das EPD zählt, von solchen Gebühren ausgenommen werden.

Bemerkungen zu einzelnen Bestimmungen

Zu Art. 8 (Anlaufstellen der Kantone)

Der Kanton Solothurn wird eine entsprechende Anlaufstelle für den First-Level-Support bezeichnen müssen. Derzeit scheint noch nicht klar zu sein, welche Stelle diese Aufgabe übernimmt. Ebenso ist noch unklar, mit welchen personellen und finanziellen Folgen dies verbunden ist.

Zu Art. 16 Abs. 3 (Vorweisen von elektronischen Nachweisen)

Die Regelung ist eine Ausprägung des Grundsatzes «Datenschutz durch Technik» (Art. 1 Abs. 2 Bst. b Ziff. 1). Unüblich ist in diesem Zusammenhang aber die Einschränkung durch das Wort «möglichst». Dieses ist wegzulassen und das System so zu erstellen, dass keine Rückschlüsse möglich sind.

Art. 17 Abs. 2 Buchstabe b Ziffer 1 (Basisregister)

Hier scheint das Wort «daraufhin» überflüssig zu sein, bzw. bleibt unklar, auf was sich dieses Wort bezieht.

Zu Art. 19 und Art. 20 (Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen; Anwendung zur Prüfung von elektronischen Nachweisen)

Art. 19 und Art. 20 erwähnen, dass der Bund je eine Anwendung zur Verfügung stellt, mittels derer elektronische Nachweise aufbewahrt und vorgewiesen werden können, bzw. die Gültigkeit der elektronischen Identifikation geprüft werden kann. Es erscheint uns wichtig, dass diese Anwendungen auf lokalen und mobilen Endgeräten installiert werden können und entsprechende Support-Prozesse für die Handhabung und bei Nicht-Funktionieren vorhanden sind.

Art. 21 (System für Sicherungskopien)

Es ist darauf zu achten, dass eine einheitliche Terminologie verwendet wird. In der Sachüberschrift wird von «Sicherungskopien» gesprochen, in den Absätzen 1 und 2 dann aber von «Sicherheitskopien».

Art. 24 (Betrieb der Vertrauensinfrastruktur)

«Elemente» scheint hier nicht der passende Begriff zu sein. Gemeint sein dürften am ehesten die «Grundlagen» der Vertrauensinfrastruktur.

Art. 25 Abs. 2 Buchstabe b (Technische Entwicklung)

Nicht abgedeckt ist der Fall, dass das Volk die Gesetzesbestimmung in einem Referendum ablehnt. Dies müsste noch ergänzt werden.

Im Übrigen verweisen wir auf die Stellungnahme der Konferenz der schweizerischen Datenschutzbeauftragten (Privatim), welcher wir uns anschliessen.

Gesamthaft erachten wir den vorgeschlagenen Vorentwurf als gelungene Umsetzung der vorgenommenen Ziele im Zeichen des digitalen Wandels.

Wir danken Ihnen für die uns zur Verfügung gestellten Dokumentationen und für die eingeräumte Gelegenheit zur Stellungnahme.

IM NAMEN DES REGIERUNGSRATES



Dr. Remo Ankli
Landammann



Andreas Eng
Staatsschreiber



Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Justiz-
und Polizeidepartement
Bundeshaus West
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 14. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 29. Juni 2022 laden Sie uns zur Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Wir unterstützen den unterbreiteten Vorentwurf und schliessen uns der von der Konferenz der Kantonsregierungen an der Plenarversammlung vom 23. September 2022 zu dieser Vorlage verabschiedeten Vernehmlassungsantwort an. Die Regierung des Kantons St.Gallen erachtet die Vorlage und ihre zeitnahe Umsetzung als sehr wichtig. Ergänzend haben wir folgende Bemerkungen:


Im Zusammenhang mit Art. 9 des Entwurfs möchten wir auf einen möglichen Änderungsbedarf von Art. 20a Ziff. 2 der eidgenössischen Arbeitslosenversicherungsverordnung (SR 837.02) sowie von Art. 17 Abs. 1 Bst. c der eidgenössischen Verordnung über das elektronische Patientendossier (SR 816.11) hinweisen. Allgemein und insbesondere im Hinblick auf Art. 8 des E-ID-Gesetzes, wonach die Kantone Anlaufstellen zu schaffen haben, wäre es für die Kantone hilfreich, wenn die Grundzüge der angedachten Verordnung bekannt wären.

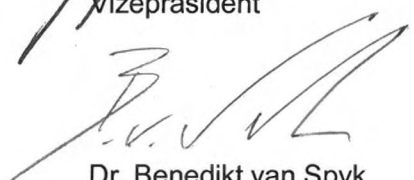
Innerhalb der Schweiz sollte es möglich werden, sich nur noch mit der digitalen Identität (E-ID) auszuweisen. Art. 3 des Entwurfs ist daher dahingehend zu erweitern, dass auch mit einer E-ID die persönlichen Voraussetzungen für den Erhalt einer (neuen) E-ID erfüllt sind.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.



Im Namen der Regierung


Marc Mächler
Vizepräsident


Dr. Benedikt van Spyk
Staatssekretär



Zustellung auch per E-Mail (pdf- und Word-Version) an:
rechtsinformatik@bj.admin.ch

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Onorevole Consigliera federale
Karin Keller-Sutter
Direttrice del Dipartimento federale
di Giustizia e Polizia
Bundesgasse 3
3003 Berna

rechtsinformatik@bj.admin.ch

Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (legge sull'Id-e, LIdE): avvio della procedura di consultazione

Signora Consigliera federale,

la ringraziamo per essere stati coinvolti nella procedura di consultazione. Lo scrivente Consiglio di Stato accoglie con favore il progetto di legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (legge sull'Id-e) proposto a seguito del rifiuto della legge federale sui servizi di identificazione elettronica (LSIE) da parte del popolo il 7 marzo 2021.

L'avamprogetto di legge posto in consultazione adotta un approccio incentrato sui bisogni della popolazione, propone una legislazione tecnologicamente neutra (ossia indipendente dalle tecnologie utilizzate) e ha un ruolo attivo nel creare la necessaria fiducia verso le istituzioni. Essa pone la giusta attenzione alle sfide del progresso tecnico e alla necessaria collaborazione internazionale. Salutiamo inoltre positivamente la procedura adottata che ha visto un coinvolgimento attivo dei Cantoni, del settore privato e della società civile, come pure i tempi ridotti con cui è stato sviluppato un nuovo ambizioso progetto legislativo.

Per quanto concerne le disposizioni proposte dall'avamprogetto di legge segnaliamo quanto segue:

- art. 3: osserviamo una discrepanza fra le persone che possono ottenere una e-ID e quelle che possono o devono interagire con le amministrazioni cantonali. Con questa distinzione i Cantoni potrebbero essere obbligati a dotarsi di mezzi di identificazione elettronica propri per soddisfare tutte le esigenze presenti sul territorio. Per il nostro Cantone questo è tanto più vero pensando a tutti i lavoratori frontalieri, ai proprietari di residenze secondarie o ai turisti cui sono destinati specifici servizi digitali.
- Art. 4: l'età minima proposta di 14 anni per richiedere l'identità elettronica senza avere il consenso dell'Autorità parentale appare in contrasto con la salvaguardia dei minori

da possibili utilizzi inappropriati dei loro dati personali e di un loro più ampio accesso ad Internet. Sugeriamo di fissare questo limite a 16 anni.

- Art. 8: l'avamprogetto di legge prevede la creazione di punti di contatto cantonali ai quali affidare il compito di assistenza sul posto in merito all'emissione e all'impiego dell'Id-e. A questo proposito, riteniamo necessario valutare una soluzione di sostegno nazionale che potrebbe rientrare fra i progetti finanziati tramite l'Amministrazione digitale svizzera (ADS).
- Art. 26: il progetto prevede dei costi per i cantoni e i comuni per l'iscrizione nell'albo di base e nel sistema di conferma degli identificatori come emittenti e verificatori a fronte dell'obbligo per le autorità di accettare l'e-ID (art. 9). L'art. 3 par. 2 dell'Ordinanza generale sugli emolumenti (OgeEm) prevede per contro che *"L'Amministrazione federale non riscuote emolumenti dagli organi intercantonali, dai Cantoni e dai Comuni per quanto gli stessi concedano il diritto di reciprocità"*. Occorre garantire che tale disposizione si applichi anche al caso specifico e quindi che le autorità pubbliche siano esentate da tali emolumenti o perlomeno che la compensazione tra le autorità pubbliche sia ridotta al minimo. Inoltre, gli altri attori che forniscono servizi pubblici digitali dovrebbero essere esentati dalle tasse, al fine di garantire un'elevata partecipazione a questo sistema, ad esempio nel campo della salute.

Prendiamo infine atto dell'intenzione di chiarire il ruolo dell'identità elettronica nazionale in relazione ai mezzi di identificazione settoriali, ad esempio in ambito sanitario, e sosteniamo questo orientamento, con lo scopo di evitare che parte dell'utenza possa essere esclusa dall'accesso di specifici servizi o prestazioni, ad esempio, alla cartella elettronica del paziente.

In allegato trasmettiamo la presa di posizione del delegato cantonale della protezione dei dati che è parzialmente in contrasto con la posizione dello scrivente Consiglio di Stato.

Voglia gradire, signora Consigliera federale, l'espressione della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente

Claudio Zali

Il Cancelliere

Arnoldo Coduri

Allegato:

- presa posizione del 05.10.2022 dell'incaricato cantonale della protezione dei dati

Copia a:

- Direzione del Dipartimento delle finanze e dell'economia (dfe-dir@ti.ch)
- Direzione del Dipartimento delle istituzioni (di-dir@ti.ch)
- Divisione delle risorse (dfe-dr@ti.ch)
- Centro sistemi informativi (csi@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in internet

telefono
web

Via Canonico Ghiringhelli 1
6501 Bellinzona

+41 91 814 45 01
www.ti.ch/protezionedati

Repubblica e Cantone Ticino
Cancelleria dello Stato
Servizi giuridici del Consiglio di Stato

persona
incaricata

Giordano Costa

**Incaricato cantonale della protezione dei dati
6501 Bellinzona**

telefono
e-mail

+41 91 814 45 01
giordano.costa@ti.ch

Dipartimento delle istituzioni
Direzione generale
Residenza

Bellinzona 5 ottobre 2022

Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici – Consultazione

Gentili signore,
egregi signori,

in merito alla summenzionata procedura di consultazione, formuliamo le seguenti osservazioni.

1. Considerazioni generali

La scrivente rimane perplessa sia in merito all'effettiva necessità dell'identificazione elettronica, sia in merito alla natura ibrida dell'intero progetto che affida parzialmente a dei privati compiti che dovrebbero, per la loro natura delicata e per i rischi che implicano, essere svolti esclusivamente dalle autorità. I rischi di abusi di dati rilevati nel primo progetto legislativo sono stati ridotti con il presente progetto ma non sono stati del tutto eliminati. Inoltre, la minimizzazione dei flussi di dati (principio della minimizzazione dei dati) e il salvataggio dei dati decentralizzato (presso il titolare dell'ID-e) non sono del tutto garantiti come si vedrà in seguito. Si teme inoltre che con il presente progetto legislativo – che prevede per ora la facoltatività dell'identificazione elettronica – il legislatore stia invero spianando la strada verso una futura obbligatorietà della stessa, sia nel settore pubblico sia in quello privato, ciò che implicherebbe nuovamente un ripensamento sia quanto all'implicazione di privati nella procedura di emissione dell'ID-e, sia quanto alle cautele tecniche di sicurezza da implementare.

DIREZIONE DI			
SG	<input checked="" type="checkbox"/>	SMPP	PolCa: _____
SEL	SC	SP	DirDI: _____
Ricevuto il: - 6 OTT. 2022			
<input checked="" type="checkbox"/> URGENTE			
Trasmesso per:			
<input checked="" type="checkbox"/> PROGETTO DI RISPOSTA		<input type="checkbox"/> ESAME E NOTA A DIRETTORE	
<input type="checkbox"/> EVASIONE DIRETTA		<input type="checkbox"/> CONOSCENZA E VOSTRI ATTI	

2. Considerazioni sugli articoli della legge

Ad art. 2 cpv.3 lett. a Forma e contenuto

L'inclusione del numero AVS nell'ID-e comporta alcuni rischi, soprattutto per quanto riguarda la possibilità di collegare tra loro diverse serie di dati in caso di furto dei dati.

Inoltre, nel messaggio concernente la modifica della legge federale sull'assicurazione per la vecchiaia e per i superstiti, il legislatore ha confermato che il numero AVS può essere utilizzato sistematicamente per evitare errori amministrativi che comportano costi elevati e per aumentare l'efficienza grazie allo scambio automatizzato di dati tra le autorità, evitando confusioni. Pertanto, l'elaborazione del numero AVS da parte degli enti pubblici di cui all'art. 153 c cpv. 1 LAVS non pone particolari problemi. Il problema si pone tuttavia per gli altri enti che non figurano nell'elenco di cui all'art. 153 c cpv.1 LAVS.

Infine, a fronte delle finalità dichiarate, ovvero garantire un'identificazione sicura tramite l'ID-e tra privati e con le autorità, la necessità dell'elaborazione del numero AVS per raggiungere lo scopo non risulta di primo acchito data. Il progetto non offre particolari delucidazioni in merito. In questo senso, l'utilizzo del numero AVS violerebbe il principio della minimizzazione dei dati sancito dalla legge stessa (art. 1 cpv. 2 lett. b cifra 3), poiché non risulta di primo acchito necessario per il perseguimento dello scopo.

Ad art. 3 e 4 Verifica dell'identità al momento del rilascio dell'ID-e

Stante il rapporto esplicativo, la procedura per ottenere l'ID-e si fonda principalmente sulla presentazione di un documento d'identità svizzero valido. In quanto al momento del rilascio dell'ID-e si rinuncia a una nuova verifica dell'identità del richiedente per motivi di costi, praticità e rapidità (vedi rapporto esplicativo pag. 9). È prevista solo la verifica dell'identità sulla base delle informazioni fornite e la verifica dell'immagine del viso. Nell'ottica della protezione dei dati, coloro che trattano dati personali per lo svolgimento dei propri compiti legali e/o compiti a loro demandati devono garantirne l'esattezza. L'adeguatezza delle misure per garantire l'esattezza dei dati dipende dal tipo e dalla portata del trattamento, nonché dal rischio che il trattamento comporta per i diritti fondamentali delle persone interessate. Un'ID-e rilasciata in modo errato comporta un rischio significativo per i diritti fondamentali dell'interessato (furto di identità). Di conseguenza, le misure per prevenire questo rischio devono essere accresciute e non possono essere ignorate per motivi di costi o celerità nel rilasciare l'ID-e. Il rapporto esplicativo è inoltre in contraddizione con quanto stabilito dall'art. 4 cpv. 3 lett. b della norma, stante il quale l'ID-e viene rilasciata solo dopo che si è potuto verificare l'identità del richiedente.

Ad art. 11 Sistema d'informazione per l'emissione e la revoca dell'ID-e

La norma deve precisare che, con l'interfacciamento, possono essere acquisiti dai sistemi d'informazione esterni secondo il capoverso 3 unicamente i dati previsti all'art. 2 della legge.

Ad Art. 13

Al cpv. 1 va precisato che la revoca avviene alle condizioni previste all'art. 5 della legge. Di conseguenza, può essere eliminato il cpv. 2 della norma.

Ad art. 16 Verifica dell'identità al momento del rilascio dell'ID-e

Il cpv.1 sancisce che il titolare del mezzo di autenticazione elettronico stabilisce quali componenti di tale mezzo o quali informazioni deducibili da esso sono trasmesse all'autorità o al privato che verifica i mezzi di autenticazione elettronici. Tuttavia, nelle spiegazioni dell'art. 16 si afferma che il verificatore determina quali dati sono necessari per l'accesso ai suoi servizi, ciò limita il margine di manovra del titolare. Le spiegazioni indicano chiaramente che un servizio non può essere utilizzato se il titolare decide di non presentare gli elementi richiesti dal verificatore. A nostro avviso, l'utilizzo dell'identificazione elettronica fa sorgere nuovi obblighi di identificazione ed incentiva la raccolta di dati che non sarebbero necessari con l'identificazione analogica. A fronte di ciò riteniamo fondamentale che la legge stabilisca esplicitamente ulteriori regole per la presentazione dell'ID-e: da un lato, il verificatore dovrebbe essere obbligato a richiedere l'ID-e solo se è assolutamente necessario, egli dovrebbe altresì essere obbligato a richiedere solo le parti dell'ID-e di cui non può fare a meno. Inoltre, il verificatore dovrebbe essere obbligato a non conservare, trasmettere o trattare in altro modo i dati di identificazione, a meno che un altro obbligo non lo richieda. Un'ulteriore raccolta di dati da parte del verificatore per scopi diversi dall'identificazione, sulla base del consenso della persona in un contesto di diritto privato, rimarrebbe ancora possibile in una seconda fase separata dopo l'identificazione.

Il cpv. 3 della norma stabilisce che l'operatore dei sistemi non è a conoscenza del contenuto delle prove elettroniche presentate e, per quanto possibile, non può trarre conclusioni sul loro utilizzo e sulle parti coinvolte. A nostro avviso per evitare dei rischi di profilazione delle persone la norma dovrebbe imporre l'utilizzo di sistemi che non permettano in nessun caso di tracciare gli utilizzi dell'ID-e o di altre prove elettroniche.

A tal proposito si ricorda che in materia di protezione dei dati, più il rischio per la confidenzialità dei dati è elevato, più elevato deve essere il grado di sicurezza che le misure adottate offrono. Gli accorgimenti tecnici devono perciò essere adeguati allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica per i diritti delle persone. Inoltre, la sicurezza dei dati deve essere garantita sin dalla progettazione di un sistema d'elaborazione di dati (privacy by design).

Ad art. 17 cpv. 3 Registro di base

A nostro avviso, la norma dovrebbe prevedere una verifica dell'identità degli emittenti e dei verificatori prima che essi possano inserire autonomamente i propri dati nel registro di base. Il rapporto esplicativo menziona che una procedura di autorizzazione richiederebbe molte risorse, ragion per cui l'ipotesi è stata scartata. Riteniamo che i costi elevati del processo di autorizzazione non dovrebbero essere un argomento per ignorare i rischi di abuso dell'infrastruttura fiduciaria. Inoltre, l'infrastruttura di fiducia si può definire tale unicamente se i rischi di abusi legati all'elaborazione dei dati sono ridotti con tutti i mezzi possibili. Ciò che non viene fatto nel caso di specie.

Cordiali saluti.

PER L'INCARICATO CANTONALE DELLA
PROTEZIONE DEI DATI

Carine Anato

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches
Justiz- und Polizeidepartement (EJPD)
Frau Karin Keller-Sutter
Bundesrätin
Bundeshaus West
3003 Bern

Frauenfeld, 4. Oktober 2022

589

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Vorentwurf für das E-ID-Gesetz (BGEID). Wir unterstützen die Bestrebungen, möglichst rasch eine Lösung für eine staatliche elektronische Identität zu erarbeiten und dafür die gesetzlichen Grundlagen zu schaffen. Wir erlauben uns aber den Hinweis, dass der Entwurf relativ abstrakt und eher schwer verständlich ist, und bitten Sie, die nachfolgenden Bemerkungen für die weiteren Rechtsetzungsarbeiten zu beachten.

1. Allgemeine Bemerkungen

Im Ingress werden als Verfassungsbestimmungen Art. 38 Abs. 1, Art. 81 und Art. 121 Abs. 1 der Bundesverfassung (BV; SR 101) angegeben. Diese Bestimmungen äussern sich allerdings nicht zu einer E-ID und bieten nach unserer Auffassung daher keine genügende verfassungsmässige Grundlage für das BGEID.

Art. 1 Abs. 1 lit. b bestimmt, dass das BGEID die Infrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen regelt. Im Anschluss an diese Bestimmung wird in Klammern der Begriff „Vertrauensinfrastruktur“ eingeführt. Im Gesetz werden jedoch die Begriffe „Infrastruktur“ oder „Vertrauensinfrastruktur“ in den nachfolgenden Artikeln uneinheitlich verwendet (vgl. Art. 2, Art. 12, Titel 5. Abschnitt, Art. 22 bis Art. 25 sowie Art. 28 BGEID). Wird ein Begriff am Anfang eines Erlasses eingeführt, sollte er im gesamten Erlass einheitlich verwendet werden.

2/5

Wir beantragen, dass im gesamten Erlass aufgrund der Einheitlichkeit und Klarheit der Begriff „Vertrauensinfrastruktur“, wie er in Art. 1 Abs. 1 lit. b BGEID eingeführt wurde, verwendet wird.

2. Bemerkungen zu einzelnen Artikeln

Art. 3

Es ist sinnvoll, die E-ID basierend auf einem bereits gültigen Schweizer Ausweis auszustellen und auf eine erneute Identitätsprüfung zu verzichten. Bezüglich der Ausweise für Asylsuchende im laufenden Verfahren (N-Ausweise) und Ausweise für vorläufig Aufgenommene (F-Ausweise) gilt es indessen zu erwähnen, dass diese zum jetzigen Zeitpunkt noch auf Papier und ohne im Zentralen Migrationsinformationssystem (ZEMIS) hinterlegte Gesichtsfotos ausgestellt werden. Die Umstellung der N- und F-Ausweise des Bundes auf moderne Plastikkarten mit Fotoerfassung direkt aus dem ZEMIS wird mutmasslich erst in den nächsten ein bis zwei Jahren erfolgen. Die letzten bis zu fünf Jahre gültigen EU/EFTA-Papierausweise werden schweizweit wohl erst bis 2026 durch Plastikkarten mit direkt im ZEMIS erfassten Fotos ersetzt sein.

Art. 4

Aus Effizienzgründen wäre es sinnvoll, wenn bei der Ausstellung einer klassischen Identitätskarte oder eines Passes die E-ID gleich mitgeneriert würde. Deren Aktivierung könnte dann später auf Wunsch der oder des Betroffenen erfolgen.

Soweit datenschutzrechtlich zulässig, wäre zudem zu begrüssen, wenn bereits bestehende (behördliche) E-ID Lösungen durch die neue E-ID des Bundes ersetzt würden. Dies hätte für die Bürgerinnen und Bürger den Vorteil, dass im Kontakt mit allen Behörden eine einheitliche E-ID verwendet werden könnte. In diesem Zusammenhang wäre es für die Kantone von Vorteil, wenn der Bund bei der Migration von kantonalen E-ID-Lösungen zur E-ID des Bundes mitwirken würde.

Art. 5

Bei Inaktivsetzung eines Ausländerausweises im ZEMIS oder eines Ausweises im Informationssystem Ausweisschriften (ISA) vor Ablauf der Gültigkeitsdauer gilt es, auch die E-ID zu widerrufen. Dies ist in den Ausführungsbestimmungen zu Art. 5 des Vorentwurfes zu berücksichtigen.

3/5

Art. 6

Ein Schweizer Pass ist bei volljährigen Personen zehn Jahre gültig, bei minderjährigen Personen fünf Jahre. Beim Ausländerausweis beträgt die Gültigkeitsdauer je nach ausländerrechtlicher Regelung zwischen vier Monaten und fünf Jahren oder bis zu dessen Widerruf oder Erlöschen.

Bei der Definition der Gültigkeitsdauer einer künftigen E-ID regen wir an, diese explizit mit der (verbleibenden) Gültigkeitsdauer eines Ausländerausweises im ZEMIS oder eines Ausweises im ISA zu koppeln. Bei Inaktivsetzung eines Ausländerausweises im ZEMIS oder eines Ausweises im ISA vor Ablauf der Gültigkeitsdauer gilt es auch die E-ID zu widerrufen. Dies wäre in den Ausführungsbestimmungen zu Art. 5, Art. 6 und Art. 11 Abs. 5 des Vorentwurfes zu berücksichtigen.

Art. 8

Wir teilen die im erläuternden Bericht vertretene Auffassung nicht, wonach Anlaufstellen in der Nähe der hilfesuchenden Personen (kantonale Ebene) zu schaffen sind. Es ist wenig sinnvoll, wenn das Bundesamt für Polizei (fedpol) zuständig für die Entgegennahme und Bearbeitung von (digitalen) Anträgen zur Ausstellung einer E-ID ist (vgl. Art. 4), aber eine Vielzahl kantonal unterschiedlich angesiedelter Beratungsstellen entkoppelt von diesem Antragsprozess „mitreden“. Dies verkompliziert den Prozess, schafft diffuse und unklare Zuständigkeiten und stiftet damit mehr Verwirrung als Klärung.

Personen, die sich für eine E-ID entscheiden und beantragen, wird es ohne Weiteres möglich sein, telefonisch oder online (ohne physische Anlaufstelle) eine entsprechende Beratung bei einer schweizweit zentralen Stelle einzuholen. Als die den Antrag bearbeitende Behörde wäre das fedpol geeigneter, die Hilfestellung nahe am digitalen Prozess und damit unmittelbar über eine Hotline sicherzustellen.

Würde an der dezentralen Lösung in den Kantonen festgehalten, müsste der Kanton Thurgau zuerst eine solche Stelle schaffen. Auch müsste diese Aufgabe unter Berücksichtigung der Kosten- und Entschädigungsfolgen (Gebührenteilung) ordentlich in die Zuständigkeit der Kantone übertragen werden.

Art. 10

Beim Bezug von rein digitalen Dienstleistungen wäre es angemessen, wenn von den Behörden zwingend eine E-ID verlangt werden kann.

Art. 11 Abs. 5

In Bezug auf Ausländerausweise gilt es zu beachten, dass die Ausweisdaten (Gesichtsfoto, Unterschrift, je nach Ausweisart auch Fingerabdrücke) für fünf Jahre im ZEMIS gespeichert werden. Die Ausführungsbestimmungen müssten festhalten, was gilt, wenn beispielsweise genau vier Jahre und 364 Tage nach Erfassung des Gesichtsfotos im ZEMIS eine E-ID beantragt würde. Richtet sich die Gültigkeitsdauer dann am Lösungszeitpunkt des Fotos im ZEMIS aus (in diesem Fall noch ein Tag) oder knüpft diese an die Gültigkeitsdauer eines noch mit alten Daten neu ausgestellten Ausländerausweises, der über die Löschung der Ausweisdaten im ZEMIS hinaus gültig bleibt?

Art. 13 Abs. 2

Analog zu Art. 5 ist zu prüfen, ob ein Widerruf zwingend und sofort zu erfolgen hat, wenn die Inhaberin oder der Inhaber verstorben ist.

Art. 14

Es ist nicht notwendig, dass das Gesetz vorschreibt, wie die Inhaberin oder der Inhaber eines anderen elektronischen Nachweises diesen aufzubewahren hat. Dies liegt in ihrer oder seiner Verantwortung.

Wir beantragen daher, dass Art. 14 wie folgt angepasst wird: „Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket.“

Art. 23

Wir begrüßen, dass der Quellcode veröffentlicht wird. Die Erfahrungen mit der Veröffentlichung des Quellcodes des E-Voting-Systems und des neuen Ergebnisermittlungssystems für Wahlen und Abstimmungen VOTING zeigen aber, dass nicht nur der Quellcode, sondern auch die Dokumentation vollständig offenzulegen ist. Der Quellcode ist so aufzubereiten, dass er von Expertinnen und Experten verstanden und nachvollzogen werden kann. Zudem muss er kompilierbar sein. Wir beantragen, bei Art. 23 folgende Formulierung zu verwenden:

„¹Der Bund veröffentlicht den vollständigen Quellcode, die Spezifikation, die Dokumentation und weitere Dateien mit relevanten Inputparametern der von ihm zur Verfügung gestellten Elemente der Vertrauensinfrastruktur und aller Elemente, die für den elektronischen Nachweis eingesetzt werden.

²Die Offenlegung erfolgt nach best practices. Dies bedeutet insbesondere:

5/5

- a. Quellcode, Spezifikation und Dokumentation sind so aufbereitet, dass Struktur und Inhalt von unabhängigen Expertinnen und Experten einfach nachvollzogen werden können.
- b. Quellcode und Dokumentation sind so aufbereitet, dass Dritte das System in der eigenen Infrastruktur effizient kompilieren, in Betrieb nehmen und analysieren können.
- c. Die Offenlegung erfolgt auf einer für Quellcode üblicherweise eingesetzten Plattform.
- c. Die Darstellung der offengelegten Unterlagen entspricht der gängigen Praxis.
- d. Die Offenlegung ist dauernd und wird regelmässig aktualisiert.
- e. Es wird ein detailliertes Änderungsprotokoll (changelog) geführt.
- f. Die offengelegten Dokumente sind anonym zugänglich.
- g. Die Nutzungsbedingungen müssen es erlauben, den Quellcode und die übrigen offengelegten Unterlagen vollständig zu prüfen, zu testen und zu analysieren.
- h. Der Quellcode darf für wissenschaftliche Zwecke genutzt werden.“

Im Übrigen verweisen wir auf die Stellungnahme der Konferenz der Kantonsregierungen (KdK) in dieser Sache, der wir uns anschliessen.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates



Der Staatsschreiber





Madame la Conseillère fédérale
Karin Keller-Suter
Cheffe du Département fédéral de justice
et police
DFJP
3000 Berne

Par courrier électronique à :
rechtsdienst@gs-efd.admin.ch

Lausanne, le 5 octobre 2022

Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID) – Avant-projet – Procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton de Vaud vous remercie d'avoir sollicité son avis dans le cadre de la procédure de consultation sur l'avant-projet de la loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID).

Une identité électronique fiable accélérera la numérisation des administrations publiques et participera grandement à la transition numérique de notre pays. Le Conseil d'Etat salue la diligence avec laquelle le Conseil fédéral, après le refus en votation populaire du précédent projet de loi en mars 2021, a su prioriser ce thème important. Il se réjouit de constater que ce nouveau projet prend en compte les éléments qui faisaient défaut dans le précédent projet, en particulier le rôle et la responsabilité de la Confédération dans la délivrance des identités et dans la mise à disposition et le maintien de l'infrastructure de confiance, le respect de la sphère privée par une décentralisation et une minimisation des données personnelles, l'extension du périmètre à un écosystème global qui inclura des moyens de preuve électroniques de tout type ou encore la gratuité pour l'ensemble des individus. Le Conseil d'Etat constate encore que l'avant-projet tient compte de la compatibilité de l'identité électronique avec les projets européens, ce qui est primordial dans un contexte de mobilité et d'amélioration de l'expérience utilisateur. Finalement, il reconnaît également l'importance que cette identité puisse être utilisée dans de nombreux domaines, en particulier celui de la santé numérique et du dossier électronique du patient.

Si le Conseil d'Etat soutient de manière générale cet avant-projet qui va dans le sens de la volonté populaire exprimée en votation, il formule toutefois les réserves et remarques suivantes qu'il vous prie de bien vouloir prendre en considération. Les observations ci-après sont d'ordre général. Une annexe à ce courrier regroupe les observations article par article et fait partie intégrante de cette prise de position.

Définitions et terminologie

Le Conseil d'Etat juge opportun d'introduire dans la loi une disposition spécifique destinée à définir certains termes, tels que « e-ID », « moyens de preuve électroniques », « registre de base » ou encore « clé cryptographique ». Le projet de loi gagnerait ainsi en clarté pour les personnes dont les connaissances ne permettent pas d'appréhender la complexité de ce thème.

Simplicité et convivialité

Le Conseil d'Etat est d'avis que le succès de la diffusion de l'e-ID au sein de la population sera possible uniquement si la procédure pour son obtention ainsi que son utilisation quotidienne sont rendues simples et conviviales mais également accessibles à l'ensemble de la population, indépendamment de la réalité de la fracture numérique dans notre pays. Il demande ainsi au Conseil fédéral de prévoir des dispositions d'exécution dans ce sens.

De plus, le Conseil d'Etat estime que la perception d'émoluments pour l'utilisation du système des copies de sécurité (article 26, alinéa 2) pourrait amener certaines personnes à renoncer à la sécurisation de leur e-ID et autres moyens de preuve électroniques, ce qui, à terme, pourrait prêter une partie de la population. A ce titre, il demande au Conseil fédéral de renoncer à ces émoluments.

D'un point de vue technique, pour que l'intégration de l'e-ID se passe au mieux dès son entrée en vigueur, le Conseil d'Etat souhaite obtenir rapidement de la Confédération les modèles d'échanges propres à assurer un interfaçage rapide et normalisé. Par ailleurs, pour encourager la population à adopter l'e-ID, il semble indispensable que les moyens de protection contre les abus d'identité et les procédures de révocation de l'e-ID fassent l'objet d'une information et d'une communication systématiques.

Conditions personnelles et solutions cantonales

Le Conseil d'Etat relève que l'article 3 de l'avant-projet précise que seules les personnes titulaires d'un document d'identité valable ou d'une pièce de légitimation valable pourront obtenir une e-ID, qui n'est dès lors pas qu'un simple login mais bien l'équivalent numérique de la pièce d'identité. Toutefois, il rappelle que le cercle des personnes interagissant avec les autorités cantonales et communales est plus large que celui prévu par cet article (frontaliers, personnes possédant une résidence secondaire, etc.). A ce jour, la loi sur la cyberadministration vaudoise permet d'attribuer des moyens d'identification électronique à l'ensemble de la population avec laquelle l'administration cantonale interagit. Le Conseil d'Etat estime donc indispensable que le Conseil fédéral examine la possibilité d'introduire une e-ID spécifique avec un champ d'application restreint pour la population qui ne remplit pas les conditions personnelles prévues à l'article 3 mais qui interagit régulièrement avec les administrations suisses.

Pour résoudre cette difficulté, il pourrait également se révéler indispensable que les cantons poursuivent l'exploitation de leur propre solution cantonale (moyens d'identification électronique) dans le cadre de leur cyberadministration. Ainsi, le Conseil d'Etat demande au Conseil fédéral de déterminer le statut de ces moyens d'identification électronique par rapport à la nouvelle e-ID et de préciser que ces derniers pourront toujours être utilisés pour des prestations nécessitant une authentification forte.

Mineurs

L'article 4 de l'avant-projet énonce que seuls les mineurs de moins de 14 ans devront avoir le consentement de leur représentant légal pour recevoir une e-ID. Pour le Conseil d'Etat, il est loin d'être certain que tous les adolescents dès l'âge de 14 ans soient à même de prendre la mesure du risque lié à l'usage de leurs données personnelles ou de « prêt » à un camarade de leurs e-ID. La responsabilité civile des mineurs incombe en règle générale à leurs parents et il ne semble donc pas que l'exigence d'une autorisation parentale pour tous les mineurs soit une exigence particulièrement insurmontable. Le Conseil d'Etat est d'avis que l'obtention d'une e-ID par un mineur doit remplir les mêmes conditions que celle pour l'obtention d'une carte d'identité ou d'un passeport dès l'instant où cette e-ID peut être utilisée de manière beaucoup plus large que dans une interaction avec une autorité publique.

Si l'objectif est aussi de permettre aux mineurs d'être les seuls à pouvoir accéder à la totalité de leur dossier électronique du patient, il semblerait alors préférable de prendre d'autres mesures, par exemple en rendant certains éléments du dossier du patient inaccessibles aux parents du patient.

Emoluments et coûts pour les cantons

L'article 9 de l'avant-projet prévoit que toute autorité ou tout service qui accomplit des tâches publiques doit accepter l'e-ID lorsqu'il recourt à l'identification électronique. Cette norme vise également les autorités cantonales et communales. Le Conseil d'Etat rappelle à ce titre que certains cantons ont déjà développé leur propre système de cyberadministration avec des solutions diverses de moyens d'identification électronique, pour lequel ils ont assumé des coûts de mise en œuvre puis des coûts de maintenance.

Ainsi, le Conseil d'Etat estime que le coût que représente l'introduction de l'e-ID pour les cantons n'est pas suffisamment pris en compte dans le projet mis en consultation. En effet, le rapport explicatif indique que les éventuels coûts d'adaptation des systèmes cantonaux seront contrebalancés par les gains d'efficacité en lien avec l'introduction de l'e-ID. Or, à ce stade, même s'il reste très difficile de prévoir les coûts des adaptations logicielles, il est probable que ceux-ci impacteront de nombreux services et seront vraisemblablement importants. De même, il est difficile d'affirmer que l'introduction de l'e-ID va forcément de pair avec des gains d'efficacité. Le Conseil d'Etat souhaite que le Conseil fédéral détaille ce point dans son message.

De plus, l'obligation faite aux cantons d'accepter l'e-ID fédérale a pour corollaire que les cantons auront l'obligation de s'inscrire sur le registre de base prévu à l'article 17 de l'avant-projet et donc seront obligatoirement astreints au paiement des émoluments prévus à l'article 26 de l'avant-projet. Ceci contrevient clairement au principe d'équivalence fiscale. S'agissant d'un projet fédéral, imposé aux cantons, la Confédération devrait assumer seule les effets financiers du projet ou tout au moins veiller à ce que l'art. 3, al. 2, Ordonnance générale sur les émoluments (OGEmol), qui énonce que l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes pour autant qu'ils lui accordent la réciprocité, s'applique également au cas présent et à ce que les compensations entre les collectivités publiques soient réduites au minimum.

Responsabilité des cantons

Le Conseil d'Etat note qu'à la question des coûts et des émoluments s'ajoute le fait que les cantons seront chargés, selon l'article 8 de l'avant-projet, d'offrir une assistance en relation avec l'émission et l'utilisation des e-ID. Ils devront pour ce faire désigner des services chargés de donner de l'assistance générale en lien avec différents processus cyberadministratifs ainsi que des points de contact à proximité des personnes qui pourraient en avoir besoin. Ces tâches nouvelles pourraient considérablement alourdir la charge de travail et nécessiter la création de postes supplémentaires. Dès lors, le Conseil d'Etat estime nécessaire d'examiner la possibilité de mettre sur pied un support au niveau fédéral (*service desk*) qui pourrait compléter le support local offert par les cantons sur la base de l'article 8.

Protection des données et application des lois cantonales de protection des données

De manière générale et au vu des finalités exprimées et de la portée du projet, qui tend à la délivrance d'une identité électronique, le Conseil d'Etat est d'avis que les dispositions légales relatives au traitement de données et à la communication dans le cadre du processus d'émission devraient être plus développées.

L'article 1, alinéa 2, liste les principes applicables, destinés à protéger la personnalité et les droits fondamentaux de la personne, et essentiels pour une acceptation du projet par la population. Alors que l'article 7 de la nouvelle loi fédérale sur la protection des données (nLPD) parle de « protection des données dès la conception et par défaut », le Conseil d'Etat note que la reprise du principe n'est que partielle à l'article 1 alinéa 2 lettre b chiffre 1 de l'avant-projet. Afin d'ancrer dans la loi le fait que la protection des données doit être systématiquement et automatiquement prise en compte, dans le cadre des développements informatiques notamment, le Conseil d'Etat demande au Conseil fédéral de reprendre les principes de la nLPD dans leur entier (dès la conception et par défaut).

De plus, au chapitre 6.7, le rapport explicatif indique que « la Confédération (fedpol et autres autorités), les émetteurs et les vérificateurs du secteur public sont soumis aux dispositions applicables aux organes fédéraux », soit à la loi fédérale sur la protection des données (LPD puis nLPD). Le Conseil d'Etat estime toutefois indispensable de préciser quelles seront les règles applicables aux traitements de données des titulaires d'e-ID et autres moyens de preuve électroniques lorsque leurs données seront traitées par les cantons et les communes, notamment sur les infrastructures propres (par exemple aux points de contact cantonaux définis à l'article 8).

En conclusion, le Conseil d'Etat réitère son soutien à cet avant-projet de loi qui va dans le sens de la volonté populaire exprimée lors de la votation du 7 mars 2021. Il salue la rapidité avec laquelle le Conseil fédéral a produit une nouvelle proposition afin de disposer rapidement d'une e-ID étatique et fiable pour faciliter les échanges en ligne et faire avancer la numérisation de notre pays. Il émet toutefois un certain nombre de remarques sur cet avant-projet et vous prie de bien vouloir les prendre en considération lors de l'élaboration du projet de loi et du message.

En vous remerciant de l'attention que vous porterez à ce courrier, nous vous adressons, Madame la Conseillère fédérale, nos salutations les meilleures.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE



Christelle Luisier Brodard

LE CHANCELIER



Aurélien Buffat

Annexe mentionnée

Copies

- Office des affaires extérieures
- Direction générale du numérique et des systèmes d'information

ANNEXE

Commentaires article par article

Article 1, alinéa 1, lettre a, alinéa 2, lettres a et b, et articles 4, 5, 13, 15, 16, 18 et 21 – notion de « personnes »

Le projet mentionne tantôt « personnes », « personnes physiques » ou « personnes privées ». Cela entraîne des difficultés de compréhension. Il serait préférable de se conformer à la terminologie du Code civil en distinguant personnes physiques et personnes morales.

Article 1, alinéa 2, lettre d

Il serait plus clair de scinder la lettre d en deux lettres supplémentaires : « e. à assurer la sécurité de l'infrastructure, f. à garantir une émission... ». Le commentaire précise : « Différents aspects à régler au niveau de l'ordonnance seront beaucoup plus équivoques sur le plan technologique, voire même plus spécifiques à la technologie ». Il faut se référer aux versions allemande et italienne pour comprendre le sens de cette phrase. Le texte pourrait être rédigé de la manière suivante pour plus de clarté : « Plusieurs aspects techniques, qui doivent être réglés par voie d'ordonnance, ne sont pas encore définitivement connus d'un point de vue technologique, voire dépendent de l'évolution de cette dernière. »

Article 2 (Forme et contenu)

Il est mentionné que les données personnelles viendront des registres officiels. A l'exception des photographies, qui viendront de ISA ou SYMIC, il n'est pas mentionné, à cet article, de quels registres viendront les autres informations. Une clarification sur ce point serait nécessaire, d'autant qu'à l'art. 11, il est indiqué qu'il s'agit des données d'ISA et de SYMIC. Il convient également d'être attentif aux éventuelles différences entre les sources de données.

Le commentaire ad article 2, alinéa 1 prévoit que la Confédération met en place une infrastructure de confiance qui permettra aux acteurs publics et privés d'émettre divers moyens de preuve électroniques. Le commentaire fait renvoi aux limitations posées par l'article 18, alinéa 3 du projet mais celui-ci ne pose pas de telles limitations. Il faudrait définir ces limitations.

L'alinéa 3, lettre e, impose que la pièce de légitimation qui a été utilisée pour l'émission de l'e-ID soit intégrée dans l'e-ID elle-même. Dans la mesure où les autorisations pour étrangers sont régulièrement sujettes à des modifications (non renouvellement, révocation, changement de statut etc.), il convient de définir si l'e-ID devra être mise à jour à chacune de ces modifications. Dans l'affirmative, il faudra définir si une solution technique permettra un échange d'informations entre SYMIC et l'autorité émettrice ou si les cantons seront tenus de signaler tous ces changements à fedpol, moyennant un surplus de travail très important pour les services cantonaux de migration.

Article 3 (Conditions personnelles)

L'utilisation de la terminologie « pièce de légitimation valable » ne convient pas pour définir une personne se trouvant légalement en Suisse. Au sens de la loi sur les étrangers et l'intégration (LEI), la « pièce de légitimation » correspond en effet à un passeport ou une pièce d'identité (art. 13 LEI). Par conséquent, il vaudrait mieux parler

de titulaire de « *titre de séjour valable* ». Cette remarque vaut également pour les articles 2 et 5 du projet de loi.

De plus, il apparaît par ailleurs nécessaire de préciser si les ressortissants suisses vivant à l'étranger auraient la possibilité de bénéficier d'une e-ID, et si tel devait être le cas, de préciser, à tout le moins, les conséquences au niveau de la communication des données transfrontières entre le pays de résidence du ressortissant suisse et la Suisse. De la même manière, il convient de prendre en compte également la situation des personnes bénéficiant d'une carte de légitimation du DFAE au sens de l'OLEH (enfants majeurs des fonctionnaires internationaux, par exemple).

Finalement, le commentaire ad article 3, lettre b prévoit : « *Lorsque cela est justifié et prévu expressément par la loi, il est possible de limiter l'accès à certains services aux titulaires d'un permis étranger dont l'identité n'a pas pu être vérifiée de façon fiable.* ». Le message ne saurait étendre le champ de la loi. Or, le projet ne prévoit pas expressément la limitation énoncée dans le commentaire.

Article 4 (Emission)

Concernant l'alinéa 2, il mériterait de clarifier comment le système saura qu'une personne est sous curatelle.

L'alinéa 4 prévoit la possibilité pour fedpol de prendre des données biométriques d'une personne pour pouvoir les comparer avec les données enregistrées dans SYMIC ou ISA et vérifier son identité. Or, il n'y a pas systématiquement, pour chaque bénéficiaire de titre de séjour, de photo enregistrée dans SYMIC. C'est en particulier le cas dans le domaine de l'asile, SYMIC ne prévoyant pas d'emplacement pour intégrer les photos des titulaires de permis F ou N. Pour cette catégorie de personnes, il n'y aura par conséquent jamais de photo qui permette de vérifier une identité. L'articulation de cette disposition avec la réalité du terrain devrait être précisé dans le message, ainsi que la mobilisation éventuelle des centres de biométrie cantonaux.

De plus, cette disposition constitue, selon le rapport explicatif, la concrétisation du principe de légalité consacré à l'art. 34 al. 2 let. c nLPD. Toutefois, en ce qui concerne la collecte et l'utilisation des données biométriques, la disposition légale, potestative, apparaît légère en termes de densité normative. Il serait nécessaire de préciser dans quels cas la biométrie sera utilisée et des comparaisons effectuées ainsi que le logiciel qui sera utilisé.

Article 5 (Révocation)

Concernant la révocation des e-ID, les éléments suivants devraient être précisés dans le projet de loi, respectivement dans le message :

- Les aspects relatifs au rapport de droit administratif qui existera entre les requérants et fedpol (dans le cas, par exemple, où fedpol révoque immédiatement l'e-ID car il existe un soupçon fondé - dont il serait d'ailleurs judicieux de préciser la nature - d'utilisation abusive de celle-ci, il serait nécessaire de préciser si une décision administrative doit être rendue, et si cas échéant, la personne concernée pourra contester).
- Les mécanismes prévus pour éviter des révocations systématiques lorsque les photos ne correspondent plus (lorsqu'une personne procède au renouvellement de son passeport ou de sa carte d'identité peu après avoir établi son e-ID, cette

dernière risque d'être révoqué dès lors que sa nouvelle photo ne correspondra plus à celle ayant servi à créer son e-ID).

- L'échange d'informations entre fedpol, SYMIC et l'autorité émettrice dans le cas du refus de renouvellement ou une révocation du titre de séjour par l'autorité cantonale de migration qui imposera à fedpol de mettre fin à l'e-ID.
- L'échange d'informations avec fedpol lors d'un décès ou du retrait du document d'identité utilisé lors de l'émission de l'e-ID. Dans ce contexte, il paraît essentiel que la désactivation soit immédiate et qu'il n'y ait pas de délai de latence.
- L'utilité d'autoriser la délivrance d'une nouvelle e-ID à quelqu'un qui en aurait déjà une.

A noter encore qu'en français, il est étrange de trouver une phrase qui débute par une minuscule (fedpol...). Le texte italien utilise une majuscule et le texte allemand précède l'abréviation d'un article. L'on pourrait soit utiliser la majuscule comme dans le texte italien soit formuler la phrase à la voie passive. La même remarque s'applique à l'article 11.

Article 6 (Durée de validité)

Si la durée de validité de l'e-ID est calquée sur celle du document d'identité, et si le document d'identité arrive à échéance et n'est encore valable que quelques semaines et que l'e-ID a été créé durant ce laps de temps, l'e-ID n'aura potentiellement que quelques semaines de validité. Il conviendrait ainsi d'attirer l'attention des personnes concernées à cet égard.

Article 8 (Points de contact cantonaux)

Les détails de la collaboration avec les cantons sont pour l'heure peu développés dans l'AP-LeID et dans le rapport explicatif. Il s'agit de préciser qui sera responsable du traitement des données effectué par les cantons aux points de contact et quelles données seront communiquées, respectivement rendues accessibles aux cantons, respectivement par les cantons.

Article 11 (Système d'information pour l'émission et la révocation des e-ID)

L'article 4, alinéa 1 pose le principe selon lequel celui qui souhaite obtenir une identité électronique doit en faire la demande à fedpol. Puis l'article 11, alinéa 1 pose le principe selon lequel fedpol gère un système d'information pour l'émission et la révocation des e-ID. Sur le plan légistique, il serait souhaitable de placer cet alinéa dans un article en début de loi (après l'article 1) instaurant les compétences de fedpol.

Concernant l'alinéa 2, il s'agit également de préciser si les données d'identification personnelle au sens de l'art. 2 al. 2 AP-LeID figureront dans le système d'information pour l'émission et la révocation des e-ID et en particulier ce qu'il en est de la photographie du requérant fournie lors de la procédure d'émission. Il n'est fait état de cette donnée à aucun moment dans le projet de loi. Il s'agit également de préciser si les cantons auront accès à ces données.

Concernant l'alinéa 3, il serait utile de préciser clairement dans la base légale que les données seront uniquement consultées et qu'elles ne sont donc ni dupliquées, ni sauvegardées dans le système d'information pour l'émission et la révocation des e-ID.

Il sied également de souligner que les données personnelles enregistrées dans SYMIC ne se fondent pas toujours sur un document d'identité ou un passeport. Dans le domaine de l'asile, l'identité peut se fonder sur les déclarations de la personne. Cela

implique que l'identité enregistrée dans SYMIC n'est pas fiable. Par ailleurs, il existe de nombreuses personnes qui disposent d'alias, c'est-à-dire plusieurs identités. Dans le meilleur des cas les alias sont identifiés comme tels, mais ce n'est pas toujours le cas.

Concernant l'alinéa 4, qui dispose du traitement *exclusif* de ces données dans le but d'émettre l'e-ID, il s'agirait de définir s'il ne faudrait pas prévoir des communications automatisées pour que fedpol soit automatiquement informé du cas lorsque le document d'identité ou la pièce de légitimation utilisée lors de l'émission de l'e-ID a été retiré.

Article 12 (Emission)

Il convient de préciser si les moyens de preuve électroniques visés à cet article pourront être intégrés dans le portefeuille d'une personne sans e-ID ou si seuls les détenteurs d'e-ID peuvent accéder aux autres moyens de preuve.

Article 13 (Révocation)

En lien avec les remarques à l'article 5, il s'agit de préciser la notion de « soupçon fondé », de définir si une décision administrative sera rendue, et le cas échéant, si la personne concernée pourra contester cette décision. Cet aspect relatif aux rapports de droit administratif devrait être précisé dans le message.

Articles 14 (Forme et conservation des moyens de preuve électroniques) et 19 (Application pour la conservation et la présentation des moyens de preuve électroniques)

La question qui se pose à la lecture de ces articles est de savoir s'il sera possible ou non de stocker les moyens de preuve électroniques sur plusieurs supports en même temps, et par analogie en dehors de l'application. La relation entre la règle inscrite à l'art. 14 AP-LeID et celle inscrite à l'art. 19 AP-LeID n'est pas claire. En effet, il est indiqué à l'art. 19 AP-LeID que l'application de la Confédération permettra justement de conserver le moyen d'identification électronique de son titulaire. Selon la réponse à ces questions, il pourrait être judicieux de coupler les articles 14 et 19.

Article 15 (Transmissibilité des moyens de preuve électroniques)

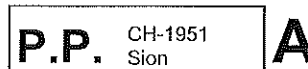
Le lien entre l'article 5, alinéa 2, et son commentaire n'est pas clair. Il s'agit de clarifier si un titulaire ne pourra restaurer que les moyens de preuve électroniques qui ne lui sont pas liés nommément.

Article 24 (Exploitation de l'infrastructure de confiance)

Il convient de préciser si le prestataire de service pourra sous-traiter certaines prestations. Dans l'affirmative, il pourrait être judicieux de limiter le choix du sous-traitant.



2022.04122



Poste CH SA

Département fédéral de justice et police
Madame Karin Keller-Sutter
Conseillère fédérale
Bundesgasse 3
3003 Berne



Date **28 SEP. 2022**

Avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID) : prise de position cantonale

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton du Valais vous remercie de lui avoir soumis l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID).

Le Gouvernement valaisan salue cet avant-projet. Il répond dans une très large mesure aux préoccupations formulées par la population lors du rejet de loi sur l'eID le 7 mars 2021. Il positionne notamment la Confédération comme autorité qui délivre une identité électronique étatique (e-ID) pour les titulaires d'un document d'identité émis par une autorité suisse et assure, par la conception de cette future e-ID, le respect de la vie privée, de l'économie et de l'enregistrement décentralisé des données. De plus, en mettant à disposition une infrastructure de confiance étatique et en exploitant les registres nécessaires, la Confédération permettra aux acteurs des secteurs public et privé d'émettre et d'utiliser des moyens de preuve électroniques lesquels pourront être contenus dans un portefeuille électronique qu'elle fournira également.

Malgré la très bonne qualité globale de l'avant-projet de loi, les documents mis en consultation soulèvent les remarques et questions suivantes :

1. AP-LeID

1.1. Article 3 : Conditions personnelles

Le projet de loi permet d'établir une identité numérique s'appuyant sur un permis délivré par l'autorité suisse compétente. Cette manière de faire pragmatique permettra d'éviter toute complexité inutile. Nous saluons cette proposition. Cependant, les cas d'usage de cette identité pourraient s'étendre au-delà des personnes disposant d'un tel permis. Il s'agit par exemple de propriétaires de résidences secondaires à qui des prestations numériques spécifiques sont également destinées. Le Conseil d'Etat souhaite donc qu'un concept visant à lier les moyens d'identification à différents types d'identité dont celle délivrée par la Confédération (mais pas uniquement) soit élaboré par les groupes de travail interinstitutionnels en charge de la mise en œuvre, notamment Administration numérique Suisse.

1.2. Article 4 alinéa 2 : Émission

L'art. 4 al. 2 prévoit qu'un enfant puisse obtenir une e-ID dès 14 sans consentement parental, pratique qui s'écarte de l'équivalence avec le monde physique pourtant défendu dans cet avant-projet de loi. Nous comprenons les raisons qui poussent de légiférer dans cette direction, mais estimons que les risques liés à une utilisation inappropriée, voire frauduleuse des données



personnelles (en raison du manque d'expérience et de la naïveté de cette classe d'âge, en particulier) comme suffisants pour maintenir cette limite d'âge à 18 ans.

1.3. Article 6 : Durée de validité

La durée de validité de l'e-ID étant laissée à la décision du Conseil fédéral, nous estimons qu'il serait intéressant de la coupler à celle du document utilisé pour sa création, afin d'éviter à l'utilisateur de devoir gérer des dates d'échéance différentes pour toutes ses preuves d'identités qu'elles soient physiques ou numériques.

1.4. Article 8 : Assistance par les cantons

La pertinence de laisser chaque canton organiser le support à la création et à l'utilisation de l'e-ID est discutable, en regard des importantes économies d'échelle qu'il pourrait y avoir à centraliser ce support dans un ServiceDesk global, dans les 4 langues nationales et, pourquoi pas, d'autres langues. La mutualisation de ce service pourrait être confiée à un organisme tel qu'eOperations Suisse SA.

1.5. Article 12 : Émission

La possibilité donnée à quiconque d'émettre des moyens de preuve électroniques à l'aide de l'infrastructure de confiance amène une grande souplesse pour des cas d'utilisation particuliers. Cependant, nous demandons qu'une évaluation plus précise des émoluments prélevés pour de telles utilisations soit communiquée lorsque les projets-pilotes auront abouti et que le message du Conseil fédéral sera transmis au Parlement. Ces émoluments devront être raisonnables afin d'inciter le plus grand nombre d'organisations possible à en faire usage.

1.6. Article 17 alinéa 3 : Registre de base

Le fait que les émetteurs et les vérificateurs inscrivent leurs données dans le registre de base peut amener un risque complémentaire d'usurpation d'identité. Nous demandons que la Confédération s'assure que les processus d'inscription soient fortement sécurisés.

1.7. Article 21 alinéa 2 : Systèmes de copies de sécurité

L'art. 21 prévoit de donner la possibilité aux titulaires de déposer une copie de sécurité de leurs moyens de preuves électroniques. Ceci est très intéressant mais nécessite, tout comme le registre de base visé à l'art. 17, une sécurisation très forte, en particulier pour l'accès à ces copies.

1.8. Article 26 : Emoluments

L'art. 26 prévoit qu'un émolument est perçu auprès des émetteurs et des vérificateurs de moyens de preuves électroniques. Cela concerne également les services qui s'acquittent de tâches publiques, quand bien même ils sont tenus d'accepter l'e-ID conformément à l'art. 9 de ladite loi. Dans le même temps, le Conseil fédéral entend financer l'e-ID par des contributions de l'Administration numérique suisse, alors que celle-ci est cofinancée par les cantons. Or, l'art. 3, al. 2, OGE mol énonce que l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes pour autant qu'ils lui accordent la réciprocité. Il convient de veiller à ce que cette disposition s'applique également au cas présent et à ce que les compensations entre les collectivités publiques soient réduites au minimum.

1.9. Article 27 : Conventions internationales

Le Conseil d'État salue la proposition de conventions internationales afin de favoriser au mieux la reconnaissance mutuelle des identités numériques dont découlera une possible simplification des procédures administratives numérisées, pour les usagers des pays concernés.

1.10. Modification d'autres actes : ch. 5. LDEP

Dans le cadre du dossier électronique du patient, la communauté Cara reconnaît aujourd'hui deux moyens d'identification électroniques pour les patients : la SwissId et la TrustId. Or, le rapport qui explique une modification de l'art. 11 let. c portant sur la terminologie (identité électronique vs moyen d'identification électronique MIE) mentionne que la Confédération émettra, à long terme, ces MIE en complément de l'e-ID, de l'infrastructure de confiance et du portefeuille et ceci en réponse à la volonté politique du souverain exprimée lors de la votation populaire du 7 mars 2021. En rappelant que l'e-ID n'est pas un MIE mais une preuve d'identité d'une personne sous forme électronique (ch. 5 art. 7), le rapport pose la question du rôle des MIE existants et des délais de mise en place d'un MIE national. Il conviendrait de préciser ces éléments dans le message.

2. Rapport explicatif:

2.1. Commentaires des dispositions (ch. 4), article 9, p. 11

L'art. 9 fixe l'obligation aux autorités d'accepter l'e-ID. Ceci est pertinent dans l'idée d'établir l'équivalence entre documents physique et électronique. Cependant, comme l'explique le rapport au sujet de l'art. 3 let. b, il serait sans doute utile de rappeler dans l'explication de cet article que certains services des autorités pourraient être limités aux titulaires d'e-ID établies sur la base de certains types de documents.


2.2. Conséquences (ch. 5): conséquences sur les finances et état du personnel pour la Confédération, p. 20

Le développement et la mise en service de l'infrastructure de confiance qui délivrera l'e-ID ainsi que le projet de portefeuille sont, de notre point de vue, financés par l'ANS. Il s'agit donc de l'exploitation et de la maintenance évolutive¹ qui doivent être financés par les émoluments. Il conviendra enfin d'assurer que ces aspects du sujet soient financés quelles que soient les recettes issues de ces émoluments. Nous vous prions de préciser ce point dans le message.

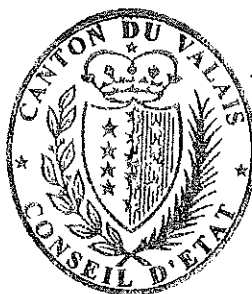
Nous vous remercions de nous avoir consultés et vous prions d'agréer, Madame la Conseillère fédérale, l'expression de notre considération distinguée.

Au nom du Conseil d'Etat

Le président



Roberto Schmidt



Le chancelier



Philipp Spörri

Copie à rechtsinformatik@bj.admin.ch

¹ Le ch. 5.1, dernière phrase, mentionne fautivement : « L'exploitation et le développement doivent être financés... ». Ce terme est néanmoins correct dans la version allemande et traduit par *Weiterentwicklung*



Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

Zug, 27. September 2022 rv

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Stellungnahme des Kantons Zug

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 hat uns das Eidgenössische Justiz- und Polizeidepartement eingeladen, zu oben erwähntem Gesetzesvorentwurf Stellung zu nehmen. Zum Vorentwurf äussern wir uns wie folgt:

1. Allgemeines

Der Regierungsrat des Kantons Zug begrüsst es, dass der staatliche elektronische Identitätsnachweis (E-ID) neu vom Bund herausgegeben und auf einer bundeseigenen Infrastruktur betrieben werden soll. Ebenso begrüsst er es, dass für den Erwerb neu keine Registrierung vor Ort mehr erforderlich ist. Die Schaffung eines staatlichen elektronischen Identitätsausweises ist ein eminent wichtiger Beitrag, um die Digitalisierung in der Schweiz voranzubringen. Der Regierungsrat hofft, dass die neue Bundeslösung in einem späteren Ausbauschritt nicht nur die elektronische Identifikation der Nutzenden, sondern auch die elektronische Unterzeichnung von Eingaben und Entscheiden ermöglichen wird, so wie dies mit «ZUGLOGIN» – der elektronischen Identität (E-ID) des Kantons Zug – schon seit 2016 möglich ist (<https://www.benutzerkonto.ch>).

Wie bereits bei der SuisseID wird der Kanton Zug auch die neue E-ID des Bundes in «ZUGLOGIN» integrieren bzw. freischalten, damit der Identitätsnachweis in «ZUGLOGIN» auch mit der neuen E-ID des Bundes erbracht werden kann.

2. Vorentwurf E-ID-Gesetz (BGEID)

Art. 3 Persönliche Voraussetzungen

Antrag: Die E-ID sei nur Personen auszustellen, deren Identität verlässlich festgestellt werden kann.

Begründung:

Soll wirklich Vertrauen in die E-ID geschaffen werden, so darf die E-ID nur Personen ausgestellt werden, deren Identität verlässlich festgestellt werden kann. Wer nicht sicher identifiziert werden kann (z. B. Ausweise N, F, S und Ci) hat keinen Anspruch auf eine elektronische Identität. Den öffentlichen und den privaten Anbietenden von eGovernment- bzw. Onlinediensten kann nicht zugemutet werden, dass sie die Unterschiede aller möglichen Ausweise von Ausländerinnen und Ausländern kennen und wissen, ob und in welchem Umfang sie ihre Dienste einschränken können bzw. müssen.

Art. 8 Anlaufstellen der Kantone

Antrag: Vom Bund sei ein einziger zentraler Helpdesk einzurichten, welcher 7x24h per Telefon, E-Mail oder weiteren Online-Kanälen erreichbar ist und der im Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung in allen Landessprachen und auf Englisch anbietet.

Begründung:

Wer eine Informatiklösung anbietet und betreibt, hat auch den entsprechenden First Level Support sicherzustellen. Es macht keinen Sinn, dass jeder Kanton (zusätzlich zum Bund) eine eigene Anlaufstelle schafft. Im Übrigen werden Bürgerinnen und Bürgern, die nicht bereit oder in der Lage sind, sich dem elektronischen Geschäftsprozess für die Ausstellung einer E-ID zu stellen, auch kaum Bedarf für eine elektronische E-ID haben.

Art. 10 Vorweisen einer E-ID

Antrag 1: Die Wahlmöglichkeit zwischen E-ID und physischem Ausweis sei auf zehn Jahre zu befristen.

Begründung:

Eine unbefristete Wahlmöglichkeit zwischen E-ID und physischem Ausweis hätte zur Folge, dass ein vollständiger Wechsel zur E-ID nie möglich würde. Zumindest sind die in Art. 10 erwähnten physischen Ausweise innert dieser Frist dahingehend weiterzuentwickeln, dass sie auch als E-ID genutzt werden können.

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Antrag: Art. 14 sei wie folgt zu ergänzen und zu präzisieren:

«¹ Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket.

² Der Bund stellt ein Identifikationsmittel als benutzerfreundliche Applikation (App) zur Verfügung. Damit können elektronische Nachweise aufbewahrt und vorgewiesen werden.

³ Die Inhaberin oder der Inhaber bewahrt die Dokumente mithilfe der vom Bund zertifizierten App unter ihrer oder seiner alleinigen Kontrolle auf.»

Begründung:

Wir erwarten, dass den Nutzenden ein vom Bund erstelltes und geprüftes Identifikationsmittel (z. B. analog der «COVID Cert» App) zur Verfügung gestellt wird. Mittel- und langfristig werden

auch wenig digitalaffine Personen mit dem Wallet den Zugang auf Ihre personenbezogenen Daten gewähren oder ablehnen. Daher ist auch die Benutzerfreundlichkeit explizit in die Formulierung dieser Bestimmung aufzunehmen. Die intuitive Bedienbarkeit ist ein entscheidender Faktor dafür.

Art. 18 System zur Bestätigung von Identifikatoren

Antrag: Art. 18 sei dahingehend zu ergänzen, dass klar wird, dass es sich beim «System zur Bestätigung von Identifikatoren» um das sogenannte «Vertrauensregister» handelt.

Begründung:

Gemäss der Abbildung auf Seite 14 besteht die «Vertrauensinfrastruktur» unter anderem aus den Elementen «Basisregister» und «Vertrauensregister». Abgesehen von dieser Abbildung findet sich der Begriff «Vertrauensregister», im Gegensatz zum Begriff «Basisregister», weder im E-ID-Gesetz, noch wird er im erläuternden Bericht erklärt.

Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Falls Art. 14 wie beantragt angepasst wird, kann Art. 19 ersatzlos gestrichen werden.

Art. 20 Anwendung zur Prüfung von elektronischen Nachweisen

Antrag: Art. 20 sei wie folgt zu ändern bzw. zu ergänzen:

«Der Bund stellt eine Anwendung zur Verfügung, mit der elektronische Nachweise von Bundes-, Kantons- und Gemeindebehörden auf ihre Gültigkeit überprüft werden können. Der Bundesrat kann vorsehen, dass der Bund auch für private Ausstellerinnen und Aussteller eine solche Anwendung zur Verfügung stellt, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können.»

Begründung:

Vor dem Hintergrund, dass gemäss Art. 17 nur geringe Anforderungen an die Eintragung von Ausstellerinnen und Ausstellern ins Basisregister gestellt werden, ist es nachvollziehbar, dass der Bund nicht für alle in der Vertrauensinfrastruktur enthaltenen elektronischen Nachweise eine Prüfanwendung zur Verfügung stellen kann. Zumindest für E-IDs einer Bundes-, Kantons- und Gemeindebehörde sollte dies jedoch möglich sein.

Art. 21 System für Sicherungskopien

Antrag 1: Die Schaffung einer Lösung für Sicherungskopien sei in Art. 21 Abs. 1 nicht als Option des Bundesrates, sondern als zwingender Bestandteil der Vertrauensinfrastruktur zu verankern.

Begründung zu Antrag 1:

Im regelmässigen Fall eines Wechsels des Smartphones und im weniger häufigen Fall des Verlustes hat die Inhaberin oder der Inhaber ein vitales Interesse, die Daten im Wallet risikoarm auf ein neues Gerät bringen zu können. Der Ansatz der selbstbestimmten Identität (Self-Sovereign Identity) verlangt von den Nutzenden digitale Kompetenzen und die Übernahme von

Verantwortung für die Sicherheit der eigenen Daten. Die Vertrauensinfrastruktur des Bundes darf die Nutzerin bzw. den Nutzer in diesem datensicherheitsrelevanten Bereich nicht alleine lassen.

Antrag 2: In Art. 21 Abs. 3 sei die Möglichkeit vorzusehen, dass Inhaberinnen und Inhaber die Vernichtung der Sicherheitskopie ihrer eigenen E-ID selber vornehmen können, ohne dass sie dafür einen Antrag stellen müssen.

Begründung zu Antrag 2:

Es ist nicht nachvollziehbar, warum die Inhaberin bzw. der Inhaber zwar die E-ID auf dem eigenen E-ID-Träger (z. B. Smartphone), nicht aber die Sicherungskopie löschen kann.

3. Erläuternder Bericht zum Vorentwurf E-ID-Gesetz (BGEID)

Bericht zu Art. 2 Abs. 1 und Art. 12 Abs. 1 Form und Inhalt der E-ID

Der Bericht verweist fälschlicherweise auf eine «Einschränkung in Art. 18 Abs. 3». Wahrscheinlich sollte sich der Verweis auf die Einschränkung in Art. 18 Abs. 2 beziehen.

Bericht zu Art. 4 Abs. 2 Ausstellung

Der Bericht sei dahingehend zu ergänzen, dass klar wird, wie für Minderjährige unter 14 Jahren und bei Personen mit umfassender Beistandschaft die benötigte Einwilligung ihrer gesetzlichen Vertretung im Onlineprozess abgebildet und durchgesetzt wird.

Bericht zu Art. 11 Abs. 3 Informationssystem zur Ausstellung und zum Widerruf der E-ID

Antrag: Der Bericht sei dahingehend zu ergänzen, dass der antragstellenden Person die Daten gemäss Art. 2 Abs. 2 und 3 übermittelt werden.

Begründung:

Gemäss Bericht werden der antragstellenden Personen nur die Daten gemäss Art. 2 Abs. 3 übermittelt, was nicht zutreffend ist.

Bericht zu Art. 22 Missbrauch der Vertrauensinfrastruktur

Antrag: Der Bericht zu Art. 22 sei dahingehend zu ergänzen, dass klar wird, warum der Ausschluss von Ausstellerinnen und Ausstellern aus dem Basisregister im Missbrauchsfall technisch nicht möglich ist.

Bericht zu Art. 26 Gebühren

Antrag: Das vorgesehene Gebührensystem sei detailliert und anhand von Beispielen zu erläutern, damit die finanziellen Auswirkungen auf die Kantone und Gemeinden nachvollzogen werden können. Der Verweis auf das Gebührensystem der Sovrin Foundation in Fussnote 32 auf Seite 17 des erläuternden Berichts hilft diesbezüglich nicht weiter.

Begründung:

Gemäss Art. 9 muss jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID des Bundes akzeptieren, wenn sie eine elektronische Identifizierung vornimmt. Dazu muss sie gemäss Art. 17 Abs. 3 ihre Daten als Verifikatorin in das Basisregister eintragen. Dies wiederum löst gemäss Art. 26 Abs. 1 eine Gebühr aus. Gemäss telefonischer Auskunft des Bundesamtes für Justiz (Rolf Rauschenbach) handelt es sich dabei um eine einmalige Gebühr, die erforderlich sei, damit sich nicht Bots als Verifikatorinnen oder Verifikatoren ins Basisregister eintragen. Wiederkehrende Gebühren würden im vorerwähnten Beispiel für die Behörden nicht anfallen. Dasselbe gelte, wenn der Kanton Zug die neue E-ID des Bundes in «ZUGLOGIN» integriere bzw. freischalte, so dass der Identitätsnachweis in «ZUGLOGIN» auch mit der neuen E-ID des Bundes erbracht werden könne.

4. Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier

Art. 11

Antrag: Art. 11 sei dahingehend zu ergänzen, dass auch öffentliche Herausgeberinnen und Herausgeber von Identifikationsmitteln zertifiziert sein müssen.

Begründung:

Aus dem Bericht zu Art. 11 geht nicht hervor, warum sich der Bund, wenn er ein Identifikationsmittel anbietet, nicht zertifizieren lassen muss. Eine Zertifizierung dient der Schaffung von Vertrauen.

Für die Berücksichtigung unserer Anliegen danken wir Ihnen zum Voraus bestens.

Zug, 27. September 2022

Freundliche Grüsse
Regierungsrat des Kantons Zug



Martin Pfister
Landammann



Renée Spillmann Siegwart
stv. Landschreiberin

Versand per E-Mail an:

- rechtsinformatik@bj.admin.ch (Word- und PDF-Format)
- Zuger Mitglieder der Bundesversammlung
- Staatskanzlei (info.staatskanzlei@zg.ch, Geschäftskontrolle)
- Datenschutzstelle (datenschutz.zug@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Amt für Informatik und Organisation (info.aio@zg.ch)



Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

5. Oktober 2022 (RRB Nr. 1330/2022)

**Bundesgesetz über den elektronischen Identitätsnachweis und
andere elektronische Nachweise (Vernehmlassung)**

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 29. Juni 2022 haben Sie uns den Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) zur Stellungnahme unterbreitet. Wir danken Ihnen für diese Gelegenheit und äussern uns wie folgt:

A. Allgemeine Bemerkungen

Wir begrüssen den vorliegenden Entwurf des E-ID-Gesetzes auf der Basis einer staatlich betriebenen Infrastruktur und den Grundsätzen der Privatsphäre durch Technik (privacy by design), der Datensparsamkeit und der dezentralen Datenspeicherung. Dies sind wichtige Grundvoraussetzungen für die Akzeptanz bei Bevölkerung und Wirtschaft.

Eine schnelle Umsetzung und Einführung der mit dem Gesetz ermöglichten Lösung erachten wir ebenfalls als zentralen Aspekt: Einerseits ist der Bedarf gross und dringend, andererseits muss vermieden werden, dass die Lösung schon bei der Einführung technisch überholt ist.

Zu bemängeln ist indessen, dass der erläuternde Bericht (S. 20–21) nur spärliche Angaben zu den finanziellen Auswirkungen auf die Kantone enthält. In der Botschaft zur Gesetzesvorlage sollten diese Auswirkungen auf die Kantone nach Möglichkeit genauer beziffert werden, insbesondere die Bruttokosten (ohne Einbezug allfälliger Effizienzgewinne).

Der «Self-sovereign Identity»-Ansatz ist unseres Erachtens in der Bevölkerung noch wenig bekannt und schafft dadurch einen erhöhten Informations- und Erklärungsbedarf, der bereits jetzt angesprochen werden sollte. Eine nationale Sensibilisierungskampagne wäre eine Möglichkeit dafür.

Darauf hinweisen möchten wir, dass die E-ID auch im Rahmen verdeckter Ermittlungsmassnahmen anwendbar sein muss und entsprechend eine Urkunde im Sinne von Art. 289 Abs. 4 Bst. a der Strafprozessordnung (SR 312.0) oder Art. 110 Abs. 4 und 317^{bis} des Schweizerischen Strafgesetzbuches (SR 311.0) darstellt. Dies sollte in der Botschaft festgehalten werden.

Schliesslich ist für den gesamten Gesundheitsbereich zentral, dass die Bundes-E-ID die Ausbreitung des elektronischen Patientendossiers (EPD) unterstützt, einfach anwendbar ist und keine neuen Hürden entstehen lässt. Deshalb sind die E-ID- und die EPD-Gesetzgebung gut aufeinander abzustimmen, sodass die nationale E-ID ohne Weiteres auch den Anforderungen des ebenfalls national geregelten EPD genügt. Zudem sollte der Anwendungsfall EPD insgesamt im Gesetz und in der Botschaft noch klarer dargestellt werden. Deutlich hervorgehen sollte, dass die Bundes-E-ID die heute zur Verfügung stehenden, für das EPD zertifizierten E-ID-Lösungen (SwissID, TrustID, HIN eID) ablösen wird und wie der EPD-Eröffnungsprozess mit der nationalen E-ID effizient und kundenorientiert unterstützt wird.

Neben diesen grundsätzlichen Bemerkungen bleibt allgemein anzufügen, dass im vorgelegten Vorentwurf in vielen (keineswegs nur untergeordneten) Fragen auf die noch zu erarbeitende Verordnung verwiesen wird, welche die erforderlichen Präzisierungen bringen soll. Unter diesen Umständen regen wir an, auch die noch auszuarbeitende Verordnung in die Vernehmlassung zu geben, damit dort die Bedürfnisse der Kantone und gegebenenfalls der Gemeinden eingebracht werden können.

B. Bemerkungen zu den einzelnen Bestimmungen

1. Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise

Art. 1 Abs. 2: Die Zweckumschreibung sollte klarer zum Ausdruck bringen, dass es um einen «Nutzen für alle» geht. Ausserdem erscheint die Formulierung «ohne die technische Entwicklung unnötig einzuschränken» (Bst. d) zu offen und unbestimmt. Sie könnte daher als Freipass verstanden werden, dass eben doch nicht die höchsten Anforderungen an die Sicherheit der Infrastruktur erforderlich seien. Stattdessen sollte ein Halbsatz angefügt werden, wonach Anpassungen an die technische Entwicklung möglich sein sollten.

Art. 2 Abs. 2: Zu den bereits aufgeführten Personenidentifizierungsdaten sollte bei Personen mit Schweizer Staatsbürgerschaft zusätzlich der Heimatort aufgenommen werden. Das Handelsregisteramt hat diesen gemäss Art. 24b Abs. 1 Bst. f der Handelsregisterverordnung (SR 221.411) «auf der Grundlage des Ausweisdokuments» zu erfassen.

Art. 2 Abs. 3: Wir begrüssen ausdrücklich, dass gemäss Art. 2 Abs. 3 Bst. a auch die AHV-Nummer zum Inhalt der E-ID gehören soll. Nur so ermöglicht die E-ID eine rasche und eindeutige Identifizierung im Verkehr mit Behörden, welche die AHV-Nummer in ihren Registern führen. Indessen begründen die Erläuterungen leider nicht, weshalb die AHV-Nummer verwendet werden soll; dies sollte in der Botschaft ausführlich nachgeholt werden.

Art. 5: Aus gesetzessystematischen Überlegungen sollte die Bestimmung über den Widerruf der E-ID unverändert nach Art. 6 zur Gültigkeitsdauer (der mit der Umstellung zu Art. 5 wird) platziert werden. Ausserdem wäre wünschenswert, wenn bei Änderung der Perso-

nenidentifizierungsdaten der Inhaberin oder dem Inhaber einer E-ID automatisch eine neue E-ID ausgestellt würde.

Gemäss Art. 5 Bst. d Ziff. 1 widerruft das Bundesamt für Polizei (fedpol) die E-ID u. a., wenn es informiert wird, dass der im Ausstellungsprozess der E-ID verwendete Ausländerausweis entzogen wurde. Wir regen an, die Systeme so aufzubauen, dass das fedpol automatisiert informiert wird oder dass das fedpol diese Daten aus dem zentralen Migrationsinformationssystem abrufen kann, ohne dass die Migrationsämter eine Meldung erstatten müssen.

Art. 6: Der Einfachheit halber sollte die Gültigkeitsdauer der E-ID mit der Gültigkeitsdauer des beim Ausstellungsprozess referenzierten physischen Ausweisdokuments gemäss Art. 2 Abs. 3 Bst. e des Vorentwurfs übereinstimmen.

Art. 7: Die Sorgfaltspflicht der Nutzenden einer E-ID sollte mit Massnahmen begleitet werden, welche die betroffenen Personen bei der Wahrnehmung dieser Sorgfaltspflichten unterstützen.

Art. 8: Grundsätzlich ist zu begrüssen, dass die Kantone den betroffenen Personen im Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten. Da jedoch die Aufgaben, Pflichten und Grenzen einer solchen Unterstützung derzeit nicht näher umschrieben sind und folglich auch die finanziellen Auswirkungen nicht beziffert werden können, sind hier entsprechende Vorbehalte anzubringen.

Art. 9: Die Tragweite dieser Bestimmung sollte in der Botschaft präzisiert werden, damit die betroffenen Stellen sich frühzeitig darauf einstellen können.

Art. 10: Die Wahlfreiheit der betroffenen Personen ist zu begrüssen und darf keinesfalls eingeschränkt werden. Denn es besteht die grosse Gefahr, dass die Freiwilligkeit der E-ID schon bald durch eine Pflicht zur E-ID abgelöst wird, wenn Dienstleistungen von öffentlichen oder privaten Anbietenden – bei elektronischem Verkehr – nur noch mit Verwendung der E-ID bezogen werden können. Dabei besteht die weitere Gefahr, dass Anbietende von Dienstleistungen sämtliche Personenidentifizierungsdaten verlangen, obwohl dies im konkreten Fall nicht nötig ist. Damit vergrössert sich auch die Gefahr des Missbrauchs dieser Personenidentifizierungsdaten. Um der Gefahr der «Überidentifikation» zu begegnen, müssen in diese Bestimmung weitere Regeln für das Vorweisen der E-ID eingefügt werden: Zum einen soll die Verifikatorin verpflichtet sein, die E-ID nur dann zu verlangen, wenn dies absolut notwendig ist, und zum anderen soll sie verpflichtet sein, nur diejenigen Teile der E-ID abzufragen, auf die sie nicht verzichten kann. Zusätzlich ist ihr die Verpflichtung aufzuerlegen, die Daten der Identifikation weder zu speichern noch weiterzugeben noch sonst wie zu bearbeiten, ausser eine anderweitige Pflicht verlangt dies.

Art. 11: Der wesentliche Punkt, dass die über die Schnittstellen zu ISA und ZEMIS abgerufenen Daten zur Ausstellung und zum Widerruf der E-ID im Informationssystem nicht aufbewahrt werden dürfen, sollte im Gesetzestext klar zum Ausdruck kommen. Art. 11 Abs. 4 sollte daher wie folgt lauten: «Die via Schnittstellen bezogenen Daten werden ausschliesslich zum Zweck der Ausstellung der E-ID bearbeitet und nicht im Informationssystem aufbewahrt.»

Gemäss Art. 11 Abs. 5 dürfen die Daten längstens bis fünf Jahre nach Ablauf der E-ID aufbewahrt werden. Dabei besteht jedoch die Gefahr, dass sie für Ermittlungen in Missbrauchsfällen (z. B. nach der Erschleichung einer falschen E-ID) nicht mehr zur Verfügung stehen. Wir schlagen deshalb vor, die Frist an Art. 37 Abs. 1 der Ausweisverordnung (SR 143.11) anzugleichen, der vorsieht, dass die zu einem Pass oder einer Identitätskarte gespeicherten Daten 20 Jahre aufbewahrt werden.

Art. 16: Es sind in Bezug auf Art. 16 Abs. 1 Massnahmen zu prüfen, wie die Beschränkung der Datenbearbeitung auch bei privaten Verifikatorinnen sichergestellt werden kann. Entsprechend ist ein eigener Absatz einzufügen, in dem ausdrücklich festgehalten wird, dass die Verifikatorin nur diejenigen Bestandteile des Nachweises verlangen darf, die sie für die Erbringung der Dienstleistung tatsächlich benötigt, und dass sie die ihr übermittelten «Bestandteile des Nachweises» nur mit ausdrücklicher Einwilligung der betroffenen Person für weitere bzw. andere Zwecke verwenden darf.

Bei Art. 16 Abs. 3 ist unklar, warum die Systeme nicht so gestaltet werden müssen, dass gar keine Rückschlüsse gezogen werden können. Daher ist auf das Wort «möglichst» im Text zu verzichten. Falls aus technischen oder rechtlichen Gründen nicht darauf verzichtet werden kann, ist klar darzulegen, warum eine Ausgestaltung eines Systems, das keine entsprechenden Rückschlüsse zulässt, nicht möglich ist.

Art. 17: Es sollte eine Verifizierung der Identität der privaten Ausstellerinnen und Verifikatorinnen vorgesehen werden. Daher sollte Art. 17 Abs. 3 so formuliert werden, dass die Ausstellerinnen und Verifikatorinnen ihre Daten nicht ohne Verifikation selbst in das Basisregister eintragen können. Ein nachträglicher Kommunikationsweg in Fällen von begründetem Verdacht, wie in Art. 22 vorgesehen, erscheint ungenügend, um dem Risiko zu begegnen, dass Ausstellerinnen oder Verifikatorinnen mit vorgetäuschter Identität elektronische Beweismittel ausstellen könnten. Dabei dürfen die hohen Kosten des Zulassungsprozesses kein Argument sein, grosse Risiken eines Missbrauchs der Vertrauensinfrastruktur in Kauf zu nehmen. Von einer Vertrauensinfrastruktur kann zudem nur gesprochen werden, wenn die Risiken des Missbrauchs mit allen möglichen Mitteln kleingehalten werden.

Art. 23: Wir begrüssen diese Bestimmung ausdrücklich, denn Open-Source-Software und die damit einhergehende Transparenz trägt zum Vertrauen in technische Lösungen bei, was gerade im sensiblen Bereich des Nachweises der Identität von natürlichen Personen wesentlich ist.

Art. 26: Dass beim Einsatz der E-ID für die sie nutzenden, natürlichen Personen keine Gebühr anfällt, begrüssen wir. Dies trägt zum breiten Einsatz der E-ID bei. Ausdrücklich verankert werden sollte in dieser Bestimmung indessen die Gebührenfreiheit für die Kantone und andere Stellen, die öffentliche Aufgaben erfüllen (und die gemäss Art. 9 zur Akzeptanz der E-ID verpflichtet sind). Zumindest in Abs. 4 wäre klarzustellen, dass insbesondere die Datenabfrage zur Identitätsprüfung für diese Stellen gebührenfrei ist. Von den übrigen Ausstellerinnen und Verifikatorinnen sollte nur eine geringe Gebühr verlangt werden, da die Kosten einen nicht unerheblichen Einfluss auf die künftige Verbreitung der E-ID und weiterer elektronischer Nachweise haben dürften. Eine Mindestgebühr zur Entgegenwirkung von Falscheinträgen scheint jedoch gerechtfertigt. Zudem sollte eine Kostenfolgenabschätzung für die Nutzerinnen und Nutzer der Vertrauensinfrastruktur in die Botschaft aufgenommen werden.



Schliesslich sollte aus Art. 26 klar hervorgehen, dass alle Leistungen um die E-ID gebührenfrei sind und Ausstellerinnen und Verifikatorinnen von anderen elektronischen Nachweisen (wie z. B. ein Universitätsdiplom) nur für die dafür notwendigen Einträge im Basisregister eine Gebühr zu entrichten haben. Wir beantragen daher, den Text von Art. 26 Abs. 1 wie folgt zu ändern: «Die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise entrichten für ihre Einträge im Basisregister und im System zur Bestätigung von Identifikatoren Nachweisen eine Gebühr.»

Art. 27: Im Hinblick auf die Rechtssicherheit regen wir an, zumindest in der Botschaft die Tragweite von Art. 27 Abs. 1 zu präzisieren.

2. Bundesgesetz über die elektronische Signatur

Wir begrüssen, dass das Gesetz über die elektronische Signatur (SR 943.03) dahingehend geändert werden soll, dass mit dem Vorweis einer E-ID für die Ausstellung einer digitalen Signatureinheit keine persönliche Vorsprache mehr erforderlich ist (Art. 9 Abs. 4^{bis}). Die Ausstellung einer qualifizierten elektronischen Signatur wird damit wesentlich vereinfacht. Indessen regen wir an, weitergehende Möglichkeiten zu prüfen, sodass die elektronische Signatur einem breiteren Personenkreis einfacher zugänglich gemacht werden kann (z. B. eine automatische Ausstellung einer qualifizierten elektronischen Signatur bei der Ausstellung einer E-ID). Zudem sollen alle Erlasse dahingehend angepasst werden, dass für eine elektronische Eingabe über ein Portal des Bundes oder der Kantone das Vorweisen einer E-ID genügt, d. h., keine qualifizierte elektronische Signatur mehr erforderlich ist.

Genehmigen Sie, sehr geehrte Frau Bundesrätin,
die Versicherung unserer ausgezeichneten Hochachtung.

Im Namen des Regierungsrates

Der Präsident:

Die Staatsschreiberin:

Ernst Stocker

Dr. Kathrin Arioli



Stellungnahme

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Plenarversammlung vom 23. September 2022

Am 29. Juni 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise. Die Kantonsregierungen nehmen zu dieser Vernehmlassungsvorlage wie folgt Stellung:

1. Grundsätzliches

1.1. Allgemeine Einschätzung

- 1 Die Kantonsregierungen unterstützen die Vorlage zum neuen E-ID-Gesetz. Sie begrüßen die rasche Erarbeitung einer neuen Vorlage, die unter dem umfassenden Einbezug kantonaler wie privater Akteure erfolgt ist. Aus Sicht der Kantonsregierungen ist die Schaffung einer einheitlichen staatlichen E-ID für die Schweiz unumgänglich, um zukunftsfähig zu bleiben und die Digitalisierung auch auf Ebene der öffentlichen Verwaltung voranzutreiben.
- 2 Die Kantonsregierungen sind der Ansicht, dass den Vorbehalten, die im März 2021 zur Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste geführt haben, mit dem vorliegenden Entwurf in angemessener und nachvollziehbarer Weise Rechnung getragen wird. Ausdrücklich begrüsst werden insbesondere die folgenden Punkte:
 - Im Gegensatz zur in der Volksabstimmung gescheiterten Vorlage sieht der neue Entwurf eine Ausstellung der E-ID durch eine staatliche Stelle vor. Auch die nötige Infrastruktur wird durch den Bund zur Verfügung gestellt.
 - Die Grundsätze von Datensparsamkeit, dezentraler Datenspeicherung und "privacy by design" entsprechen wichtigen Anliegen der Bevölkerung. Die Schweiz orientiert sich damit auch an den Vorgaben der europäischen Gesetzgebung (insbesondere der geplanten Revision der eIDAS-Verordnung).

- Die Vorlage berücksichtigt die Entwicklungen auf europäischer Ebene und ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um die Anerkennung der schweizerischen E-ID im Ausland bzw. die Anerkennung ausländischer elektronischer Identitätsnachweise in der Schweiz zu erleichtern.
- Die Möglichkeit, die Vertrauensstruktur für das Ausstellen weiterer elektronischer Nachweise zu nutzen, und die kostenlose Ausstellung der E-ID für Privatpersonen ermöglichen eine schnellere Verbreitung und Akzeptanz der Infrastruktur.

1.2. Begriffsdefinitionen

- 3 Das BGEID verwendet eine Vielzahl von technischen Begriffen wie "elektronischer Nachweis", "Verifikatorin", "Basisregister", "Vertrauensregister" oder "Identifikator". Diese sind im allgemeinen Sprachgebrauch nicht geläufig und bedürfen daher einer genaueren Definition. Die entsprechenden Begriffe werden zwar teilweise im Rahmen einzelner Artikel (z.B. "Verifikatorin" in Art. 16) oder im Rahmen des erläuternden Berichts definiert. Die Verständlichkeit des Gesetzes und die Systematik würden indes profitieren, wenn eine neue Bestimmung (z.B. als Art. 2) aufgenommen würde, welche die relevanten Definitionen für das gesamte Gesetz vornimmt. Zu achten ist dabei auch auf eine klare Unterscheidung zwischen "elektronischen Nachweisen" (als Oberbegriff, der die E-ID und andere elektronische Nachweise umfasst) und "anderen elektronischen Nachweisen".

1.3. Sicherheit und Benutzerfreundlichkeit

- 4 Mitentscheidend für die künftige Verbreitung der E-ID und der Vertrauensinfrastruktur wird die Benutzerfreundlichkeit der entsprechenden Applikationen sein. Sie müssen für alle Beteiligten möglichst unkompliziert und niederschwellig zugänglich und anwendbar sein. Unter anderem an diesem Punkt sind in der Vergangenheit Vorhaben wie die qualifizierte elektronische Signatur gescheitert. Gleichzeitig darf Benutzerfreundlichkeit nicht auf Kosten von Sicherheit und Datenschutz gehen. Hierbei ist den Schutzzielen der Authentizität und der Verbindlichkeit besonderes Gewicht beizumessen. Sind diese nicht gewährleistet, entstehen hohe Risiken, nicht nur für die betroffenen Personen, sondern auch für die öffentlichen Organe und die Privaten, die auf die Bestätigung der Identität des Gegenübers angewiesen sind. Spätestens bei Bekanntwerden vom Missbrauchsfällen hätten Sicherheitslücken zudem einen Vertrauensverlust zur Folge, mit den entsprechenden Konsequenzen für die Verbreitung der E-ID und die Nutzung der Vertrauensinfrastruktur. Den Aspekten der Benutzerfreundlichkeit und der Sicherheit wird somit bei der Ausarbeitung der bundesrätlichen Verordnung besondere Beachtung zu schenken sein. Die Infrastruktur muss laufend den technischen Veränderungen angepasst werden können.

1.4. Koordination mit Vollzugsträgern

- 5 Die Umsetzung des BGEID und insbesondere seiner Art. 8 und Art. 9 verlangt nach umfassenden Massnahmen auf Ebene der Kantone und Gemeinden. Im erläuternden Bericht fehlen jedoch Ausführungen zur Notwendigkeit, die Umsetzung mit den Vollzugsträgern koordiniert zu planen. Auch werden keine Angaben gemacht zum Zeitbedarf für die Umsetzung in den Kantonen und Gemeinden (gemäss Art. 8 VIV) sowie zum geplanten Zeitpunkt des Inkrafttretens. Die Kantonsregierungen erwarten in der Botschaft des Bundesrates entsprechende Ausführungen. Eine koordinierte Umsetzung gemäss dem Arbeitspapier von Bund und Kantonen vom 28. Oktober 2015 ist an die Hand zu nehmen.
- 6 Die Kantonsregierungen erinnern daran, dass die Digitalisierung der Verwaltung auf Kantons- und Gemeindeebene bereits in vollem Gange ist. Es wurden bereits und werden in den nächsten Jahren weitere grosse Investitionen vorgenommen. Für die Kantone ist es deshalb von entscheidender Bedeutung, dass die Identifizierung über die E-ID sich technisch problemlos in ihre bestehenden Anwendungen integrieren lässt. Der erläuternde Bericht (Kap. 5.2., S. 20-21) geht pauschal davon aus, dass Kantone und Gemeinden von der E-ID und der Vertrauensinfrastruktur profitieren werden, was ihre (nicht weiter bezifferten) Aufwände in jedem Fall rechtfertigen werde. Diese Ausführungen genügen nicht. Es ist eine detailliertere Kostenfolgeabschätzung vorzunehmen, und der Berücksichtigung der Anschlussfähigkeit bestehender Lösungen ist bei der Ausarbeitung der technischen Details vorrangige Beachtung zu schenken.

1.5. Haftung und Qualitätsstandards

- 7 Die E-ID wird zur Identifizierung in kantonalen elektronischen Diensten zur Anwendung kommen und kantonale Lösungen ergänzen. Im erläuternden Bericht fehlen jedoch Ausführungen zum Umgang mit Haftungsansprüchen, sollten Fehler im E-ID-System zu Lücken in den kantonalen Anwendungen führen. Entsprechende Angaben mit Bezug zu anerkannten Qualitätsstandards (Standard eCH-0170) sind im Hinblick auf nachfolgende Ausführungsbestimmungen in der Botschaft zu ergänzen.

1.6. Vollmacht und gesetzliche Vertretung

- 8 Weder im Entwurf noch im erläuternden Bericht sind Hinweise zu finden auf die Abläufe in Zusammenhang mit Vollmachten und der gesetzlichen Vertretung. Gemäss Art. 4 und Art. 5 BGEID ist zur Ausstellung einer E-ID für Minderjährige bis 14 Jahre und Personen unter umfassender Beistandschaft das Einverständnis der gesetzlichen Vertretung nötig. Es fehlen aber Aussagen zu späteren Vertretungs- und Delegationsmöglichkeiten in der Nutzung der E-ID oder in der Anwendung anderer Nachweise. Im Interesse einer einheitlichen Vollzugspraxis ist eine entsprechende Klärung in der Botschaft wichtig.

2. Bemerkungen zu einzelnen Artikeln des BGEID

2.1. Art. 1

- 9 Art. 7 des neuen Datenschutzgesetzes (nDSG) postuliert neben dem Grundsatz des "Datenschutz durch Technik" ("privacy by design") jenen der "datenschutzfreundlichen Voreinstellungen" ("privacy by default"). Letzterer ist in Art. 1 Abs. 2 Bst. b zusätzlich aufzuführen, um diesem zentralen Aspekt Betonung zu verleihen und eine Harmonisierung mit dem nDSG sicherzustellen.

2.2. Art. 3 (Persönliche Voraussetzungen)

- 10 Art. 3 BGEID sieht vor, dass nur Personen mit geregelter Aufenthalt in der Schweiz eine E-ID beantragen können. Der Kreis der Personen, die mit öffentlichen Verwaltungen interagieren, ist aber weiter gefasst. Zu denken ist unter anderem an Personen, die ohne geregelten Aufenthalt in der Schweiz wohnhaft sind, oder an Zweitwohnungsbesitzer. Es ist zumindest die Möglichkeit zu prüfen, für solche Fälle eine spezifische E-ID auszustellen. Die Gesetzesvorlage ist entsprechend so zu ergänzen, dass der Bundesrat ermächtigt wird, für weitere Personen mit Aufenthalt in der Schweiz eine spezielle E-ID mit eingeschränktem Einsatzbereich vorzusehen.
- 11 Gemäss dem erläuternden Bericht (S. 9 zu Art. 3) sollen Anbieterinnen die Möglichkeit haben, die Nutzung ihrer Dienste für die Inhaberinnen und Inhaber gewisser Ausweiskategorien zu beschränken. Der Bericht weist darauf hin, dass bei Ausweisen der Kategorien N, F, S und Ci nicht davon ausgegangen werden könne, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. Es ist festzuhalten, dass die Verlässlichkeit der Identifizierung einer Person nicht aus der Kategorie ihres Ausweises ersichtlich ist (nicht jede asylsuchende Person kann keine Identitätsdokumente vorweisen, während über eine Härtefallbewilligung auch Personen, deren Identität nicht abschliessend geklärt ist, unter Umständen einen Ausweis B erhalten können). Sollen Einschränkungen spezifisch aufgrund der Verlässlichkeit der Identitätsdokumente möglich sein, so ist dies im Gesetz auszuführen und eine entsprechende Angabe ist unter die Daten gemäss Art. 2 Abs. 3 BGEID aufzunehmen. Ein blosser Verzicht auf eine gesetzliche Regelung, ohne dass die entsprechende Angabe in der E-ID erfasst wird, geht am Ziel vorbei.
- 12 In Art. 3, Bst. a wird konkret das Ausweisgesetz (AwG) genannt. Es ist nicht nachvollziehbar, weshalb in Art. 3, Bst. b bloss allgemein auf die Ausländergesetzgebung verwiesen und nicht die konkreten Gesetze (Ausländer- und Integrationsgesetz und Asylgesetz) genannt werden. Für Aussenstehende ist mit der heutigen Formulierung nicht ersichtlich, welche gesetzlichen Bestimmungen angewendet werden.

2.3. Art. 4 (Ausstellung)

- 13 Der Ausstellungsprozess und damit verbunden die Frage, wie die Identifizierung der antragsstellenden Personen durchgeführt wird, sind für die Sicherheit und damit auch für die künftige Akzeptanz der E-ID zentral. Eine Regelung des Ausstellungsprozesses muss deshalb ins Gesetz aufgenommen werden. Dabei dürfen Sicherheitsüberlegungen nicht hinter Kosten- und Effizienzfragen zurückstehen. Art. 6 Abs. 5 nDSG statuiert die Pflicht des Datenbearbeiters oder der Datenbearbeiterin, sich über die Richtigkeit der Personendaten zu vergewissern. Die Angemessenheit der Massnahmen muss sich dabei auch nach dem – im Falle der E-ID erheblichen – Risiko für die Grundrechte der betroffenen Person richten.
- 14 Der Entwurf sieht gemäss Art. 4 Abs. 2 vor, dass ab dem 15. Altersjahr die E-ID eigenständig beantragt werden kann. Nach Art. 5 Abs. 1 AwG brauchen Minderjährige dagegen zum Bezug eines (physischen) Ausweises die Einwilligung ihres gesetzlichen Vertreters. Die Begründung des erläuternden Berichtes zu diesem Unterschied überzeugt nicht. Im Vordergrund sollten Sicherheitsüberlegungen stehen und nicht die Frage, welche Ausweisarten von Jugendlichen mehrheitlich genutzt werden. Die Altersgrenze zum selbständigen Bezug einer E-ID ist somit jener zum Bezug eines physischen Ausweises anzugleichen.

2.4. Art. 5 (Widerruf)

- 15 Art. 5 Bst. d Ziff. 2 legt fest, dass die E-ID widerrufen wird, wenn das fedpol über eine Änderung der Personenidentifizierungsdaten des Inhabers oder der Inhaberin informiert wird. Im Sinne einer Dienstleistung und des Mehrwerts, den die E-ID auch für die Bevölkerung schaffen soll, ist in solchen Fällen die automatische Ausstellung einer neuen E-ID ins Auge zu fassen. Die betroffenen Personen müssen sich dann nicht noch einmal um die Ausstellung einer neuen E-ID bemühen und profitieren so von den erleichterten Abläufen, die durch die Digitalisierung ermöglicht werden.

2.5. Art. 6 (Gültigkeitsdauer)

- 16 Neben der Gültigkeitsdauer ist im Entwurf auch die Frage der Verlängerung nicht geregelt. Es wird nicht klar, ob nach Ablauf des physischen Ausweisdokuments – sofern die Gültigkeit der E-ID an diese geknüpft wird – erneut eine E-ID beantragt werden muss oder ob dies bei Verlängerung des Ausweises automatisch geschieht. Dies ist spätestens in der Verordnung ebenfalls zu klären.

2.6. Art. 7 (Sorgfaltspflicht)

- 17 Art. 7 BGEID sieht eine Sorgfaltspflicht für Inhaberinnen und Inhaber einer E-ID vor. Nicht konkret geregelt sind dabei die Verpflichtungen bei Verlust des E-ID-Trägers, dies im Gegensatz zu Art. 8 AwG, das eine Meldepflicht bei Verlust eines (physischen) Ausweises vorsieht. Zur Konkretisierung der Sorgfaltspflichten ist dieser Fall auch im BGEID auszuführen.

2.7. Art. 8 (Anlaufstellen der Kantone)

- 18 Die Bestimmung sieht eine zusätzliche Aufgabe für die Kantone vor. Der erläuternde Bericht (S. 10 zu Art. 8) geht davon aus, dass die benötigten Strukturen in den Kantonen bereits vorhanden sind. Dies ist jedoch nicht notwendigerweise der Fall.

Als Vollzugsträger steht hier der Bund in der Verantwortung. Wer eine Informatiklösung anbietet und betreibt, hat auch den nötigen Support sicherzustellen, soweit die eigene Anwendung betroffen ist. Die Kantone sehen sich da als zuständig, wo es darum geht, Unterstützung beim Einsatz der E-ID für kantonale E-Government-Angebote zu leisten. Für Schwierigkeiten bei der Beantragung der E-ID oder bei der Nutzung der Vertrauensinfrastruktur muss dagegen der Bund eine Ansprechstelle schaffen. Eine solche ist im erläuternden Bericht zwar erwähnt, sie fehlt jedoch im Gesetzesentwurf ebenso wie der Second Level Support, den der Bund gemäss dem Bericht für die Kantone wahrnehmen soll.

Unter Bezugnahme auf die Ausführungen im erläuternden Bericht ist zudem darauf hinzuweisen, dass Personen, die bereit sind, eine E-ID zu nutzen, üblicherweise auch in der Lage sind, einen Support per Telefon oder E-Mail in Anspruch zu nehmen. Es müssen dafür nicht zwingend physische Anlaufstellen geschaffen werden.

2.8. Art. 9 (Pflicht zur Akzeptanz der E-ID)

- 19 Art. 9 E-BGEID sieht vor, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Der Begriff der «öffentlichen Aufgabe» wird im erläuternden Bericht mit «Verwaltungsaufgaben» gleichgesetzt, was dem Begriff von Art. 178 Abs. 3 BV entspricht. Es empfiehlt sich, im BGEID ebenfalls von "Verwaltungsaufgaben" zu sprechen, oder, falls der Begriff der «öffentlichen Aufgabe» weiter gefasst werden soll, die Botschaft in diesem Punkt zu präzisieren. Es ist zu bedenken, dass unter anderem im Gesundheitswesen eine Vielzahl von privaten Akteuren öffentliche Aufgaben ausführen, so zum Beispiel Krankenversicherer, Betreiber von Krebsregistern und Transplantationsregistern oder Anbieter des EPD. Die Pflicht zur Akzeptanz der zukünftigen E-ID bei all diesen Akteuren ist durchaus sinnvoll, wird aber Investitionen und Vorbereitungsarbeiten zur Folge haben, die den Betroffenen möglichst rasch klar kommuniziert werden müssen. Es ist somit wichtig, dass bei allen Beteiligten von Anfang an Klarheit herrscht über den Geltungsbereich von Art. 9 BGEID.

- 20 Die Umsetzung von Art. 9 BGEID bedingt eine Integration der E-ID in bestehende IT-Anwendungen von Kantonen und Gemeinden. Diesen ist dafür eine ausreichende Übergangsfrist einzuräumen.

2.9. Art. 15 (Übertragbarkeit von elektronischen Nachweisen)

- 21 Die Hinweise zu Art. 15 Abs. 2 BGEID im erläuternden Bericht (S. 13) lassen sich nur schwer mit der Bestimmung im Entwurf selber vereinbaren. Während sich Art. 15 Abs. 2 mit der Übertragbarkeit von Nachweisen befasst, nimmt der erläuternde Bericht Bezug auf ein System für Sicherungskopien. Sollte mit der Bestimmung tatsächlich nur die Übertragbarkeit in ein System für Sicherungskopien gemeint sein, ist dies entsprechend zu formulieren.

2.10. Art. 16 (Vorweisen von elektronischen Nachweisen)

- 22 Art. 16 Abs. 1 bestimmt, dass die Inhaberin bzw. der Inhaber einer E-ID selber darüber bestimmt, welche Informationen an die betreffende Verifikatorin übermittelt werden. In der Praxis werden dennoch oft die Verifikatorinnen darüber bestimmen, da die Person ansonsten vom Angebot keinen Gebrauch machen kann. In der zu erarbeitenden Botschaft sind deshalb Ausführungen zu machen, wie die Beschränkung der Datenbearbeitung auf das Minimum bei privaten Verifikatorinnen sichergestellt werden soll und wie trotz der dezentralen Struktur des Systems eine wirksame Kontrolle möglich ist.

2.11. Art. 17 (Basisregister)

- 23 Wie der erläuternde Bericht (S. 14) ausführt, birgt die Tatsache, dass Ausstellerinnen ohne weitere Überprüfung ihre Daten selber ins Basisregister gemäss Art. 17 Abs. 3 BGEID eintragen können, das Risiko, dass diese unter falscher Identität elektronische Beweismittel ausstellen können. Es liegt auf der Hand, dass dies für die betroffenen Personen unter Umständen weitreichende Folgen haben kann. Die Abfederung dieses Risikos durch Veröffentlichung bei begründetem Verdacht gemäss Art. 22 BGEID ist nicht ausreichend, da sie bereits eine Verletzung der Persönlichkeitsrechte von betroffenen Personen voraussetzt. Auch können durch blosses Öffentlichmachen erfahrungsgemäss nicht alle Nutzenden rechtzeitig erreicht werden. Ein Eintrag ins Vertrauensregister nach Art. 18 BGEID muss entsprechend auch für private Anbieter zwingend sein. Andernfalls können Missbräuche nicht verhindert werden.

2.12. Art. 20 (Anwendung zur Prüfung von elektronischen Nachweisen)

- 24 Aus dem Wortlaut von Art. 20 BGEID wird nicht klar, dass es dabei um eine Prüfung von elektronischen Nachweisen bei persönlichem Erscheinen und nicht um einen Online-Vorgang geht. Dies muss deutlicher ausgeführt werden. In jedem Fall ist bei der technischen Umsetzung – mithilfe einer Anwendung

nach Art. 20 oder ohne – sicherzustellen, dass eine zuverlässige Überprüfung der Gültigkeit von elektronischen Nachweisen für die Verifikatorinnen ohne weiteres möglich ist.

2.13. Art. 25 (Technische Entwicklung)

- 25 Die Funktionsweise von Abs. 2 dieser Bestimmung ist unklar: Wer entscheidet darüber, ob ein Anwendungsfall von Abs. 2 vorliegt? Entscheidet dies der Bundesrat bereits mit dem Erlass der Verordnung? Zudem ist der Zusammenhang zwischen Abs. 1 und Abs. 2 von Art. 25 im Text deutlicher hervorzuheben, und es sollte der Vollständigkeit halber der Fall des fakultativen Referendums miterfasst werden:

"² Sofern Bestimmungen, die gestützt auf Abs. 1 erlassen werden, einer weiteren Grundlage in einem Gesetz bedürfen, treten diese Bestimmungen ausser Kraft:

- a) [...]
- b) *mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung oder die Stimmberechtigten; oder [...]"*

2.14. Art. 26 (Gebühren)

- 26 Art. 26 BGEID sieht vor, dass von Ausstellerinnen und Verifikatorinnen elektronischer Nachweise Gebühren erhoben werden. Dies betrifft auch Stellen, die öffentliche Aufgaben erfüllen, obwohl diese gemäss Art. 9 BGEID zur Akzeptanz der E-ID verpflichtet sind. Gleichzeitig möchte der Bundesrat die E-ID durch Beiträge aus der Agenda DVS finanzieren, die von den Kantonen mitfinanziert wird. Gemäss Art. 3 Abs. 2 AllgGebV verzichtet die Bundesverwaltung auf die Erhebung von Gebühren von interkantonalen Organen, Kantonen und Gemeinden, soweit diese Gegenrecht gewähren. Dies soll auch vorliegend entsprechend gehandhabt und Verrechnungen zwischen den Gemeinwesen auf ein Minimum beschränkt werden.
- 27 Der Bundesrat soll darüber hinaus mit der Kompetenz ausgestattet werden, die Gebühren für weitere Akteure ganz oder teilweise zu erlassen, soweit diese öffentliche Aufgaben erfüllen. Unter anderem besteht im Gesundheitsbereich ein grosses Interesse an einer breiten Nutzung der E-ID, um die Aufbereitung von Gesundheitsdaten zu erleichtern. Die Kosten für die betroffenen Stellen sind somit möglichst tief zu halten.
- 28 Die Vorlage und der erläuternde Bericht äussern sich nicht bzw. nur sehr vage über die Höhe der zu erhebenden Gebühren. Diese sollen auf Verordnungsstufe festgelegt werden. Die Kosten dürften jedoch einen nicht unerheblichen Einfluss auf die künftige Akzeptanz und Verbreitung der E-ID und der Vertrauensinfrastruktur haben. Eine explizite Kostenfolgeschätzung für die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise aufgrund der Gebühren sollte deshalb in die Botschaft aufgenommen werden.

2.15. Art. 28 (Ausführungsbestimmungen)

- 29 Zahlreiche technische Aspekte zur Umsetzung der E-ID werden auf Verordnungsstufe geregelt. Aufgrund der unterschiedlichen bestehenden Lösungen in den einzelnen Kantonen, aber auch in den einzelnen Sektoren ist es unabdingbar, dass die zuständigen Akteure eng in die Erarbeitung der Vollzugsregelungen miteinbezogen werden. Es ist eine der Voraussetzungen einer breiten Akzeptanz der E-ID, dass diese unkompliziert in bestehende Anwendungen integriert werden kann.

2.16. Art. 29 (Änderung anderer Erlasse)

- 30 Gemäss dem erläuternden Bericht (Ziff. 3.1) wurde die Verwendung der E-ID in spezifischen Bereichen und damit die Änderung anderer Erlasse im Entwurf nur exemplarisch geregelt. Es ist unabdingbar, die Gesetzgebung des Bundes im weiteren Verfahren systematisch auf Bestimmungen hin zu überprüfen, in denen ein physischer Ausweis oder eine qualifizierte elektronische Signatur verlangt werden. Dies betrifft insbesondere auch die Verfahrensgesetzgebung des Bundes. Die entsprechenden Bestimmungen sind durchgehend anzupassen.

Prise de position

Consultation sur la loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (loi e-ID, LeID)

Assemblée plénière du 23 septembre 2022

Le Conseil fédéral a mis en consultation la loi fédérale sur l'identité électronique et autres moyens de preuve électroniques le 29 juin 2022. Les gouvernements cantonaux se prononcent comme suit sur le projet :

1. Remarques générales

1.1. Appréciation générale

- 1 Les gouvernements cantonaux soutiennent le projet de nouvelle loi e-ID. Ils constatent avec satisfaction qu'il a été élaboré rapidement et avec l'ensemble des acteurs cantonaux et privés. Ils estiment que l'introduction d'une identité numérique unique émise par l'État est indispensable à la Suisse si elle veut rester compétitive et faire progresser la numérisation de l'administration publique.
- 2 Les gouvernements cantonaux considèrent que le présent projet tient compte de manière appropriée et intelligible des réserves qui ont conduit au rejet de la loi fédérale sur les services d'identification électronique en mars 2021. Ils relèvent en particulier les points suivants :
 - contrairement à la loi rejetée en votation, le nouveau projet prévoit que l'émission de l'e-ID relève d'une instance publique et que l'infrastructure nécessaire sera fournie par la Confédération ;
 - les principes de minimisation des données, d'enregistrement décentralisé des données et de protection des données dès la conception (« *privacy by design* ») répondent à des préoccupations importantes de la population. La Suisse s'aligne ainsi également sur la législation européenne (en particulier sur la révision prévue du règlement eIDAS) ;
 - le projet prend en considération les développements européens et habilite le Conseil fédéral à conclure des accords internationaux afin de faciliter la reconnaissance mutuelle des preuves d'identité électroniques entre la Suisse et l'étranger ;
 - l'utilisation de l'infrastructure de confiance pour émettre d'autres moyens de preuve électroniques et la gratuité de l'e-ID pour les particuliers contribueront à une diffusion plus rapide du dispositif et renforceront l'adhésion.

1.2. Définitions

- 3 La LeID contient toute une série de termes techniques tels que *moyen de preuve électronique, vérificateur, registre, identificateur*. Peu courants, ils méritent une définition plus précise. Ils sont certes en partie définis dans certains articles (art. 16 « vérificateur ») ou dans le rapport explicatif, mais la loi serait plus intelligible et la systématique renforcée si une nouvelle clause (art. 2 par ex.) contenait une définition des principaux termes employés. À noter qu'il convient de faire une distinction précise entre « moyens de preuve électroniques » (terme générique qui comprend l'e-ID et les autres moyens de preuve électroniques) et « autres moyens de preuve électroniques ».

1.3. Sécurité et convivialité

- 4 La convivialité des applications comptera parmi les critères déterminantes de la diffusion à venir de l'e-ID et de l'infrastructure de confiance. L'accès et l'utilisation doivent être aussi simples et faciles que possible pour toutes les personnes concernées, un point sur lequel de précédents projets comme la *signature électronique qualifiée* ont échoué. Dans le même temps, la convivialité ne doit pas être réalisée au détriment de la sécurité et de la protection des données. On veillera ce faisant à accorder une importance particulière aux objectifs de protection que sont l'authenticité et la fiabilité. Si tel n'est pas le cas, les coûts pourraient être élevés pour les personnes concernées, mais aussi pour les organismes publics et les particuliers qui ont besoin de la confirmation de l'identité de leur interlocuteur. Pourraient apparaître, en cas d'abus avérés, des failles de sécurité susceptibles de porter préjudice à la confiance dans le dispositif, avec toutes les conséquences que cela impliquerait pour la diffusion de l'e-ID et l'utilisation de l'infrastructure de confiance. La convivialité et la sécurité devront faire l'objet d'une attention particulière lors de l'élaboration de l'ordonnance du Conseil fédéral. L'infrastructure doit pouvoir être adaptée en continu au progrès technique.

1.4. Coordination avec les organes d'exécution

- 5 La mise en œuvre de la LeID, en particulier des art. 8 et 9, suppose que les cantons et les communes engagent des mesures globales. À noter cependant que le rapport explicatif ne se prononce pas sur la nécessité de coordonner la mise en œuvre avec les organes d'exécution. Il ne donne aucune indication sur le temps nécessaire à la mise en œuvre dans les cantons et les communes (au sens de l'art. 8 OCo, ordonnance sur la consultation) ni sur la date d'entrée en vigueur. Les gouvernements cantonaux attendent du Conseil fédéral qu'il précise ces points dans son message. La mise en œuvre doit être coordonnée, comme le prévoit le document ad hoc de la Confédération et des cantons du 28 octobre 2015.
- 6 Les gouvernements cantonaux rappellent que le développement de la cyberadministration progresse bien à l'échelon tant cantonal que communal. De gros efforts financiers ont été consentis et le seront de nouveau dans les années à venir. Il est donc déterminant pour les cantons que l'identification via l'e-ID puisse être intégrée dans leurs applications sans la moindre difficulté. Le rapport explicatif (chap. 5.2.,

p. 20-21) part du principe que les cantons et les communes profiteront de la mise en place de l'e-ID et du recours à l'infrastructure de confiance, ce qui justifie leurs coûts (qui ne sont pas encore chiffrés). Ces explications sont insuffisantes. Il convient d'évaluer de manière plus détaillée les coûts engendrés par l'introduction de l'e-ID et d'accorder la priorité à l'adaptation des solutions utilisées actuellement lorsque seront définies les caractéristiques techniques.

1.5. Responsabilité et normes de qualité

- 7 L'e-ID servira à l'identification électronique dans les services cantonaux et complètera les solutions cantonales. Le rapport explicatif ne contient toutefois aucune indication sur les actions en responsabilité en cas de défauts du système de l'e-ID susceptibles d'entraîner des failles de sécurité dans les applications cantonales. Il convient donc de le préciser dans le message en se référant à des normes de qualité reconnues (norme eCH-0170), ce pour l'élaboration des dispositions d'exécution à venir.

1.6. Procuration et représentation légale

- 8 Le projet mis en consultation et le rapport explicatif ne contiennent aucune indication sur la procuration et la représentation légale. Les art. 4 et 5 LeID énoncent que les mineurs de moins de quatorze ans et les personnes sous curatelle de portée générale doivent avoir le consentement de leur représentant légal pour obtenir une e-ID. Rien n'est dit cependant des possibilités de représentation ou de délégation pour l'utilisation d'une e-ID ou d'autres moyens de preuve. Le message devra préciser ce point afin de permettre une mise en œuvre uniforme.

2. Remarques sur certains articles

2.1. Art. 1

- 9 L'art. 7 de la nouvelle loi sur les données personnelles (nLPD) énonce deux principes : celui de la protection des données « dès la conception » (« *privacy by design* ») et celui de la protection des données « par défaut » (« *privacy by default* »). Il convient d'ajouter le principe de protection des données « par défaut » à l'art. 1, al. 2, let. b, pour renforcer cet aspect central et être aligné avec la nLPD.

2.2. Art. 3 (Conditions personnelles)

- 10 L'art. 3 LeID énonce que seules les personnes justifiant d'un titre de séjour légal en Suisse peuvent demander une e-ID. Le cercle des personnes en contact avec les services administratifs publics est toutefois plus large. On pense notamment aux personnes qui résident en Suisse sans titre de séjour légal ou aux propriétaires de résidences secondaires. Il y a donc lieu de vérifier si ces personnes ne pourraient pas se voir délivrer une e-ID spécifique. Il convient par ailleurs de compléter le projet de loi de sorte à

habiliter le Conseil fédéral à prévoir une e-ID spécifique assortie d'un champ d'application restreint pour d'autres personnes séjournant en Suisse.

- 11 Selon le rapport explicatif (p. 9, art. 3), les fournisseurs doivent pouvoir limiter le recours à leurs services aux personnes titulaires de certaines catégories de documents d'identité. Il n'est pas certain d'emblée que l'identité ait pu être vérifiée de façon fiable pour les catégories de permis N, F, S et Ci. À noter que la fiabilité de l'identification d'une personne ne ressort pas de la catégorie de son document d'identité (les requérants ne sont pas tous dans l'incapacité de présenter un document d'identité, alors que les personnes dont l'identité n'est pas établie de manière définitive peuvent se voir délivrer dans certaines conditions un permis B, si elles sont titulaires d'une autorisation pour cas de rigueur). Si des restrictions sont envisageables en raison précisément de la fiabilité des documents d'identité, il faut le préciser dans la loi et le mentionner expressément parmi les données d'identification énoncées à l'art. 2, al. 3, LeID. Il serait contreproductif de renoncer purement et simplement à une disposition légale sans le préciser sur l'e-ID.
- 12 L'art. 3, let. a, LeID mentionne explicitement la loi sur les documents d'identité (LDI). On peut dès lors se demander pourquoi la let. b renvoie de manière générale à la législation sur les étrangers et non aux lois spécifiques (loi fédérale sur les étrangers et l'intégration et loi sur l'asile). La formulation actuelle ne permet pas au profane de savoir quelle législation appliquer.

2.3. Art. 4 (Émission)

- 13 Le processus d'établissement, et par conséquent la question de savoir comment identifier le demandeur, sont déterminants pour la sécurité, mais aussi pour l'acceptation future de l'e-ID. Une réglementation dudit processus doit donc figurer dans la loi. Les questions de sécurité ne doivent pas passer après les questions de coûts et d'efficacité. L'art. 6, al. 5, nLPD prévoit l'obligation pour la personne responsable du traitement de s'assurer de l'exactitude des données personnelles. L'adéquation des mesures n'est pas à dissocier du risque – considérable dans le cas de l'e-ID – encouru pour les droits fondamentaux de la personne concernée.
- 14 Selon l'art 4, al. 2, LeID, le projet de loi prévoit que toute personne de 15 ans et plus est autorisée à demander une e-ID de son propre chef. Selon l'art. 5, al. 1, LDI, les mineurs doivent produire l'autorisation de leur représentant légal pour déposer une demande d'établissement d'un document d'identité. Les arguments avancés dans le rapport explicatif pour justifier cette différence ne convainquent pas. La priorité devrait être la sécurité et non quelles catégories de documents sont majoritairement utilisées par les jeunes. La limite d'âge imposée pour avoir le droit de déposer une demande d'e-ID doit être la même que pour obtenir une pièce d'identité physique.

2.4. Art. 5 (Révocation)

- 15 L'art. 5, let. d, ch. 2, énonce que fedpol révoquera immédiatement l'e-ID s'il apprend que les données d'identification personnelles ont été modifiées. Il convient d'envisager dans de tels cas l'établissement automatique d'une nouvelle e-ID, dans la mesure où il s'agit d'une prestation et d'une plus-value dont doit aussi profiter la population. Cela évitera à la personne concernée de demander une nouvelle e-ID et elle bénéficiera ainsi de procédures facilitées par la numérisation.

2.5. Art. 6 (Durée de validité)

- 16 Le projet de loi ne règle ni la durée de validité de l'e-ID, ni la question de la prolongation. Il n'est pas précisé s'il faut demander une nouvelle e-ID dès que le document d'identité physique expire, à supposer que la validité de l'e-ID en dépende, ou si cela se fait automatiquement au moment de renouveler ledit document d'identité. Ce point devra être réglé au plus tard dans l'ordonnance.

2.6. Art. 7 (Devoir de diligence)

- 17 L'art. 7 LeID énonce un devoir de diligence pour toute personne titulaire d'une e-ID. Il ne se prononce pas sur les obligations résultant de la perte du document d'identité, contrairement à l'art. 8 LDI qui prévoit que toute perte d'un document d'identité (physique) doit être signalée. La mise en œuvre du devoir de diligence suppose que cette question soit précisée dans la LeID.

2.7. Art. 8 (Points de contact cantonaux)

- 18 Cette disposition implique une tâche supplémentaire pour les cantons. Le rapport explicatif part du principe que ceux-ci ont déjà les structures nécessaires. Or, ce n'est pas toujours le cas. Organe d'exécution, la Confédération doit prendre ses responsabilités. Qui propose et exploite une solution informatique doit assurer le support nécessaire si son application est concernée. Les cantons se considèrent compétents dès lors qu'il s'agit d'apporter un soutien à l'utilisation de l'e-ID pour les prestations cantonales de cyberadministration. On attend de la Confédération qu'elle mette en place un point de contact pour toute difficulté liée à la demande d'une e-ID ou à l'utilisation de l'infrastructure de confiance. Il en est certes question dans le rapport explicatif, mais pas dans le projet de loi (tout comme le second niveau de support que la Confédération doit fournir aux cantons).
En ce qui concerne les explications fournies dans le rapport explicatif, il convient de rappeler que les personnes prêtes à utiliser une e-ID sont aussi en mesure de recourir à une assistance téléphonique ou électronique. Il n'est donc pas nécessaire de créer un point de contact physique.

2.8. Art. 9 (Obligation d'accepter l'e-ID)

- 19 L'art. 9 LeID énonce que toute autorité ou tout service qui accomplit des tâches publiques doit accepter l'e-ID lorsqu'il recourt à l'identification électronique. Dans le rapport explicatif, la notion de « tâche publique » est assimilée à celle de « tâches administratives », qui correspond à celle de l'art. 178, al. 3, Cst. Il est par conséquent recommandé de parler également de « tâches administratives » dans la LeID, ou de préciser dans le message si la notion de « tâche publique » doit être comprise dans une acceptation plus large. Il convient de ne pas oublier que de nombreux acteurs privés, du secteur de la santé notamment, s'acquittent de tâches publiques (assureurs-maladie, exploitants des registres du cancer et des transplantations ou fournisseurs du DPE, etc.). Il est tout à fait loisible d'exiger d'eux qu'ils acceptent l'e-ID, mais cela supposera des investissements et des efforts de préparation qui devront être communiqués aux personnes concernées clairement et le plus rapidement possible. Il est important que les parties prenantes soient informées dès le début de la teneur du champ d'application de l'art. 9 LeID.
- 20 Appliquer l'art. 9 suppose que l'e-ID soit intégrée aux applications informatiques des cantons et des communes. Il convient donc de leur accorder une période de transition suffisante.

2.9. Art. 15 (Transmissibilité des moyens de preuve électroniques)

- 21 Les explications du rapport explicatif sur l'art. 15, al. 2 (p. 12) semblent difficilement conciliables avec les dispositions du projet de loi en lui-même. Alors que l'art. 15, al. 2 porte sur la transmissibilité des moyens de preuve, le rapport explicatif évoque un système de copies de sécurité. Si cette disposition ne concerne effectivement que la transmissibilité vers un système de copies de sécurité, la formulation doit être revue.

2.10. Art. 16 (Présentation des moyens de preuve électroniques)

- 22 L'art. 16, al. 1, énonce que lorsqu'il présente un moyen de preuve électronique, son titulaire détermine quelles informations sont transmises aux vérificateurs. Cependant, ce seront souvent ces derniers qui en décideront en pratique, étant donné que la personne ne pourra bénéficier de l'offre que si elle fournit les informations demandées. Le message à élaborer devra donc expliquer comment limiter au maximum le traitement des données par des vérificateurs privés et comment s'assurer que le contrôle sera efficace, malgré la structure décentralisée du système.

2.11. Art. 17 (Registre de base)

- 23 Comme le rapport explicatif l'indique (p. 14), le fait que les émetteurs inscrivent eux-mêmes leurs données dans le registre de base sans vérification de leur identité (art. 17, al. 3, LeID) induit le risque qu'ils délivrent des preuves électroniques sous une fausse identité. De toute évidence, les conséquences

pour les personnes concernées pourraient être lourdes dans certains cas. L'atténuation du risque par la publication d'informations en cas de soupçons fondés d'utilisation abusive de l'infrastructure de confiance au sens de l'art. 22 LeID ne suffit pas, puisqu'elle présuppose qu'il y a déjà eu violation des droits de la personnalité des personnes concernées. De plus, une simple publication ne suffira pas à avertir tous les utilisateurs à temps. L'inscription à un répertoire de confiance au sens de l'art. 18 LeID doit donc être obligatoire pour les acteurs privés aussi. Sinon, il sera impossible d'empêcher les abus.

2.12. Art. 20 (Système concernant la vérification des moyens de preuve électroniques)

- 24 Il ne ressort pas clairement de la formulation de l'art. 20 LeID que la vérification des moyens de preuve électroniques est une démarche effectuée en personne et non en ligne. La formulation doit être explicitée. Dans tous les cas, il faudra s'assurer lors de la mise en œuvre technique que les vérificateurs peuvent procéder sans difficultés à une vérification fiable de la validité des moyens de preuve électroniques – à l'aide d'une application au sens de l'art. 20, ou non.

2.13. Art. 25 (Progrès technique)

- 25 L'al. 2 de cette disposition n'est pas clair : qui décide s'il s'agit d'un cas d'application de l'al. 2 ? Est-ce le Conseil fédéral lorsqu'il édicte l'ordonnance ? Par ailleurs, le lien entre les al. 1 et 2 dudit article doit être précisé :

«² Si des dispositions édictées en vertu de l'al. 1 requièrent une base légale supplémentaire dans une loi, ces dispositions sont abrogées :

a) [...]

b) en cas de rejet du projet du Conseil fédéral par l'Assemblée fédérale ou par le peuple ; ou [...]

2.14. Art. 26 (Émoluments)

- 26 L'art. 26 LeID prévoit qu'un émolument est perçu auprès des émetteurs et des vérificateurs de moyens de preuves électroniques. Cela concerne également les services qui s'acquittent de tâches publiques, quand bien même ils sont tenus d'accepter l'e-ID conformément à l'art. 9 de ladite loi. Dans le même temps, le Conseil fédéral entend financer l'e-ID par des contributions de l'Administration numérique suisse, alors que celle-ci est cofinancée par les cantons. Or, l'art. 3, al. 2, OGE mol énonce que l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes pour autant qu'ils lui accordent la réciprocité. Il convient de veiller à ce que cette disposition s'applique également au cas présent et à ce que les compensations entre les collectivités publiques soient réduites au minimum.

- 27 Le Conseil fédéral se voit en outre confier la compétence d'exonérer d'autres acteurs prestataires de services publics de tout ou partie des émoluments. Il est dans l'intérêt du secteur de la santé en particulier que l'e-ID soit utilisée à large échelle pour faciliter le traitement des données. Les coûts des services concernés doivent donc être aussi bas que possible.
- 28 Le projet et le rapport explicatif ne se prononcent pas, ou avec peu de précision, sur le montant desdits émoluments. Celui-ci doit être fixé par voie d'ordonnance. Le message devrait contenir une estimation explicite des coûts auxquels les émetteurs et les vérificateurs de moyens de preuve électroniques peuvent s'attendre, d'autant que lesdits coûts pourraient avoir un impact considérable sur l'acceptation future et la diffusion de l'e-ID et de l'infrastructure de confiance.

2.15. Art. 28 (Dispositions d'exécution)

- 29 De nombreux aspects techniques propres à la mise en œuvre de l'e-ID sont réglés par voie d'ordonnance. Compte tenu de la diversité des solutions existant dans les cantons, mais aussi dans les différents secteurs, il est indispensable que les acteurs concernés soient étroitement associés à l'élaboration des dispositions d'exécution. L'e-ID ne pourra être largement acceptée que si elle s'intègre facilement aux applications existantes.

2.16. Art. 29 (Modification d'autres actes)

- 30 Selon le rapport explicatif (ch. 3.1), la question de l'utilisation de l'e-ID dans divers domaines n'est réglée qu'à titre indicatif dans l'avant-projet de loi, de même que celle de la modification d'autres actes législatifs. S'impose donc pour la suite de la procédure un examen systématique des dispositions fédérales contenant l'obligation de présenter un document d'identité physique ou exigeant une signature électronique qualifiée. Cela concerne en particulier la législation fédérale sur les procédures. Les dispositions afférentes doivent être adaptées en continu.

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Bern, 19. Oktober 2022
BGEID / MZ

Elektronischer Versand:
rechtsinformatik@bj.admin.ch

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)
Vernehmlassungsantwort der FDP.Die Liberalen

Sehr geehrte Damen und Herren

Für Ihre Einladung zur Vernehmlassung der oben genannten Vorlage danken wir Ihnen. Gerne geben wir Ihnen im Folgenden von unserer Position Kenntnis.

Langjährige Forderung der FDP

Bereits im Positionspapier „[Chancen der Digitalisierung](#)“ der FDP.Die Liberalen wurde gefordert, dass die Schweiz die Voraussetzungen für eine rein elektronische Abwicklung von privaten und öffentlichen Services schafft. Dafür ist ein funktionstüchtiges System der digitalen Identität (E-ID) und der elektronischen Signatur absolut zentral. Die FDP begrüsst heute, wie bereits im vorherigen Gesetzesprojekt, dass ein grosser Schritt bei der Digitalisierung gemacht wird.

Erneuter Versuch einer E-ID, neu mit staatlichem Anbieter

Die Vorteile einer elektronischen Identität in der heutigen Zeit sind nach wie vor unbestritten. Das Nein der Stimmbevölkerung im März 2021 hat lediglich gezeigt, dass die Wählerschaft keine reine private Lösung für diese hochsensiblen Daten wünscht. Aufgrund dieser Erkenntnisse hat das EJPD rasch einen neuen Anlauf gewagt und eine neue sowie vertrauenswürdige Vorlage ausgearbeitet. Das neue Projekt verfolgt einen Ansatz, der auf den Grundsätzen des Datenschutzes durch das System selbst (Privacy by Design & Privacy by Default), der Datensparsamkeit sowie der dezentralen Speicherung von Daten beruht. Der Staat übernimmt hier eine wichtige öffentliche Aufgabe, indem er den Ausstellungsprozess der E-ID und den Gesamtbetrieb der dazu nötigen, technischen Infrastruktur durch spezialisierte Behörden wahrnimmt. Der Erwerb und die Verwendung der E-ID sind insbesondere in der Anfangsphase unentgeltlich. Diese Erleichterung bei der Einführung des elektronischen Nachweises schafft einen Anreiz und verspricht eine rasche Verbreitung in der Bevölkerung.

Fraktionsmotion der FDP

Die in der Vorlage enthaltene Stossrichtung verfolgt auch sechs gleichlautende Motionen, die von allen Fraktionen im Parlament eingereicht wurden. Die FDP-Liberale Fraktion hat im Parlament kurz nach dem erfolglosen Urnengang zentrale Forderungen für eine erfolgreiche und rasche Implementierung einer elektronischen Identität gestellt und dementsprechend ihre Fraktionsmotion [21.3129](#) eingereicht. Die Ziele der FDP-Motion haben weiterhin Bestand: Chancen der Digitalisierung nutzen, Schutz der Privatsphäre berücksichtigen und sicherstellen, dass die Vergabe der E-ID und der Betrieb der Infrastruktur von spezialisierten öffentlichen Anbietern gewährleistet wird. Wir sind der Meinung, dass die vorliegende Vorlage diesen Grundsätzen gerecht wird und der politische Auftrag somit umgesetzt wurde.

Sichere, benutzerfreundliche und zukunftsgerichtete Lösungen für E-ID Ökosysteme

Zentral ist ausserdem, dass die gewählte Lösung vertrauenswürdig, sicher, benutzerfreundlich und einfach anpassbar bzw. erweiterbar ist. Fehler, die bei vielen IT-Projekten des Bundes in der Vergangenheit vorgefallen sind, dürfen sich keinesfalls wiederholen. Die konkrete Verwendung der E-ID muss möglichst praxisorientiert und anpassbar gestaltet werden, damit das Angebot für eine breite Bevölkerung sowie die Wirtschaft einen tatsächlichen Mehrwert bietet. Aufgrund dessen ist die FDP sehr erfreut, dass das vorliegende Gesetz technologie-neutral formuliert worden ist. So wird ermöglicht, agil auf technologische Änderungen zu reagieren. Da es sich bei der aufzubauenden Infrastruktur um eine kritische Komponente handelt, in welche ein hohes Vertrauen gesetzt wird, müssen bei Entwicklung und Betrieb der staatlichen E-ID regelmässig interne und externe Sicherheitstests (technisch und organisatorisch) durchgeführt werden. Damit einhergehend sollten sich zukünftig auch verschiedene bürokratische Abläufe zugunsten eines umfassenden eGovernments verbessern. Das Gesetz sollte daher nicht bloss eine Anbindung anderer elektronischer Nachweise und deren Ausstellung und Überprüfung technisch gewährleisten (Interoperabilität), sondern dies aktiv fördern bzw. unterstützen. Hierzu erachtet es die FDP als zielführend, im Rahmen der Zweckbestimmung zu ergänzen, dass das Gesetz künftig auch neue digitale Geschäftsmodelle fördern und ermöglichen soll.

Rasche Förderung der privaten Rechts- und Investitionssicherheit

Darüber hinaus stellt eine umfassende und funktionierende Vertrauensinfrastruktur die Basis für die notwendige Rechts- und Investitionssicherheit der privatwirtschaftlichen Akteure voraus. Bevor die Grundzüge der Ausgestaltung der Vertrauensinfrastruktur sowie die konkrete Rollenverteilung zwischen Staat und privaten Akteuren nicht hinreichend konkret definiert sind, können potenzielle Technologielieferanten und Dienstleistungserbringer ihre Geschäftsmodelle nur ungenügend ausarbeiten. Dadurch wird auch die Planung von potenziellen Dienstleistungen, welche die E-ID als digitalen Nachweis verwenden, erschwert. Die FDP regt daher an, dass der Bundesrat rasch mehr Klarheit in der Rollenverteilung schafft, um Investitions- und Rechtssicherheit sowie Planbarkeit sicherzustellen.

Nutzung der Synergien

Aufgrund der technologischen Dynamik sind privatwirtschaftliche Akteure oft geeigneter als der Staat, um Systeme auf agile Weise zu entwickeln und anzubieten. Der Vergleich mit anderen europäischen Ländern zeigt, dass eine staatliche Monopollösung teurer, weniger flexibel und daher nicht zielführend wäre. Der Bund soll sich um die Ausstellung und den Gesamtbetrieb der E-ID kümmern und dabei Synergien durch bereits bestehende Technologien und Methoden der Privatwirtschaft nutzen. Für die Erarbeitung der dazugehörigen Verordnung wird der Bundesrat angehalten, die Privatwirtschaft und die Wissenschaft für ihre Expertise beizuziehen.

Die Verbindung zwischen der digitalen und der physischen Welt bleibt ein entscheidendes Element der Vertrauensinfrastruktur. Es ist sinnvoll, dass dem Bund die Kompetenz übertragen wird, die Identität der Bundes-, Kanton- und Gemeindebehörden zu bestätigen (spez. Bestätigung der Identifikatoren). Gleichermaßen ist es essenziell, im Sinne des erstrebten E-ID Ökosystems, dass auch privatwirtschaftliche Akteure befähigt sind, separate und nicht-staatliche (private) Bestätigungsmechanismen bereitzustellen.

Offener und diskriminierungsfreier Zugang

Die FDP begrüsst, dass man sich mit der E-ID in der digitalen, wie auch in der realen Welt ausweisen kann und dadurch gemäss Art. 10 mittels Teilidentifikation die grösstmögliche Wahlfreiheit erhält. Dem Nutzer steht es frei, ob er sich weiterhin mit einem physischen Dokument oder der E-ID ausweisen möchte. Unter Hinweis auf das Diskriminierungsverbot (Art. 8 BV) und die behördliche Pflicht auf Rücksicht von Sprach-, Hör- oder Sehbehinderten (Art. 12 BehiG) ist ein diskriminierungsfreier Zugang zu Leistungen und deren Barrierefreiheit gesetzlich zu gewährleisten. Nebst den oben bereits erwähnten Grundsätzen ist unter diesem Aspekt das Prinzip «Design for all» zu wahren und die Informatikstrukturen sind auf sämtlichen Ebenen nachhaltig und barrierefrei zu planen.

Anwendungsbereich E-ID

Infolge schneller Digitalisierungsschritte im EU-Raum ist die Anwendung einer E-ID zukünftig auch grenzüberschreitend denkbar. Umso wichtiger ist eine frühe Koordination zwischen den Schweizer und EU-Be-

hörden im Gesetzgebungsprozess (eIDAS). Für die FDP erfreulich sind folglich sämtliche laufende und bevorstehende Bestrebungen des Bundesrates, Abkommen zur internationalen Anerkennung der E-ID zu erreichen.

Abschliessend weisen wir darauf hin, dass die Ausführungen zu Art. 9 mit Blick auf die Botschaft noch zu optimieren sind. Die aktuellen Erläuterungen zu Art. 9 (namentlich Absatz 1, letzten zwei Sätze) sind unklar oder gar widersprüchlich. Zum einen fehlt im zweitletzten Satz ein «oder». Zum andern ist unklar, warum auch das «persönliche Erscheinen» (Bericht) unter «elektronische Identifizierung» (Gesetzestext) fällt. Schliesslich ist inhaltlich zu prüfen, ob die behördliche Annahmepflicht nicht auszuweiten ist: Idealerweise sollten sich Bürgerinnen und Bürger überall dort mit der E-ID ausweisen können, wo sie sich gegenüber dem Staat zu erkennen geben, sei das beim persönlichen Erscheinen, der elektronischen Identifizierung oder weiteren staatlichen Logins.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Berücksichtigung unserer Argumente.

Freundliche Grüsse

FDP.Die Liberalen
Der Präsident

A handwritten signature in blue ink, appearing to read 'Thierry Burkart'.

Thierry Burkart
Ständerat

Der Generalsekretär

A handwritten signature in blue ink, appearing to read 'Jon Fanzun'.

Jon Fanzun

20. Oktober 2022

Ihr Kontakt: Noëmi Emmenegger, Geschäftsführerin der Bundeshausfraktion, Tel. +41 31 311 33 03, E-Mail: schweiz@grunliberale.ch

Stellungnahme der Grünliberalen zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Die Grünliberalen erachten die Möglichkeit für einen staatlich anerkannten elektronischen Identitätsnachweis (E-ID) als wichtiges Element in der digitalen Transformation. Wir sind deshalb erfreut, dass der Bund die Ausgestaltung der gesetzlichen Rahmenbedingungen für eine E-ID nach der Ablehnung durch die Stimmbevölkerung rasch wiederaufgenommen hat. Das Vertrauen der Bevölkerung in die E-ID ist essenziell, weshalb wir es als zwingend erachten, dass die neue Lösung die Bedürfnisse der Stimmbevölkerung berücksichtigt. Dies ist mit der vorliegenden Lösung gelungen, wonach die E-ID zwar auf privatwirtschaftlich entwickelten Produkten und Diensten beruhen darf, der Ausstellungsprozess und der Gesamtbetrieb der Lösung aber in der Verantwortung spezialisierter Behörden erfolgt. Dass die E-ID auf den Grundsätzen der Privacy by Design, der Datensicherheit, der Datensparsamkeit und der dezentralen Datenspeicherung beruht, unterstreicht diese Anforderungen und wird von uns ausdrücklich begrüsst. Zugleich orten wir in den folgenden vier Feldern Anpassungsbedarf:

- **Datensparsamkeit:** Die Datensparsamkeit ist wie erwähnt eines der Grundprinzipien, auf denen die E-ID beruht. Wir erachten sie als zentrales Element, um die Akzeptanz und Nutzung der E-ID in der Bevölkerung zu stärken. Im weiteren Sinn dient die Datensparsamkeit auch der Vermeidung einer Überidentifikation, die mit einer einfachen digitalen Identifikation potenziell besteht. Um einer solchen Entwicklung entgegenzuwirken, fordern wir eine Präzisierung im Gesetz, wonach der elektronische Nachweis als Voraussetzung für die Erbringung einer Dienstleistung oder die Gewährung eines Zugangs nur insoweit gestellt wird, als sie unbedingt erforderlich ist.
- **Diskriminierungsfreier Zugang:** Der Zugang zur E-ID ist gemäss Vorentwurf auf jene Personen begrenzt, die über eine Aufenthaltsbewilligung in der Schweiz verfügen. Damit werden gewisse Personen von der Nutzung einer E-ID per Gesetz ausgeschlossen. Zugleich gibt es auch Personen, welche aus persönlichen Gründen oder aufgrund mangelnder technischer Kenntnisse und Mittel auf eine E-ID verzichten. Der diskriminierungsfreie Zugang zu sämtlichen Dienstleistungen und Zugängen muss gewährleistet werden, indem eine attraktive und zumutbare Alternative zur Übermittlung der notwendigen Informationen zur Verfügung gestellt wird.
- **Sicherstellung der Barrierefreiheit:** Unter Berücksichtigung der UNO-Behindertenrechtskonvention sowie des Bundesgesetzes über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiG) ist das BGEID um den Grundsatz der barrierefreien Nutzbarkeit zu ergänzen. Die E-Accessibility ist Voraussetzung dafür, dass Menschen mit Sehbeeinträchtigung von der Nutzung eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Brieftasche nicht ausgeschlossen werden.
- **Ausweitung des Anwendungsbereichs:** Als Ergänzung möchten wir anregen, dass die Anwendung der E-ID auf Prozesse ausgeweitet werden können soll, in denen eine Identifikation über einen Pass/Ausweis nicht erforderlich ist, bspw. auf private Authentifizierungsmittel. In diesen Anwendungsbereichen soll die E-ID den Nutzerinnen und Nutzern als optionale Möglichkeit zur Verfügung stehen. Unter Berücksichtigung des Grundsatzes der Datensparsamkeit ist in diesem Bereich eine möglichst datensparsame Ausgestaltung anzustreben.

Wir begrüssen, dass mit der Vorlage ein schrittweiser Ausbau der Anwendungsfälle der E-ID ermöglicht wird. So kann der elektronische Ausweis, der für die Identifikation und Bestätigung verschiedener Merkmale verwendet werden kann, möglichst zeitnah umgesetzt werden. Für die Ausarbeitung eines integrierten Ökosystems digitaler Beweise (z.B. ärztliche Rezepte, Impfbüchlein), das ebenfalls Ziel des Vorhabens sein soll, steht mehr Zeit für Verfügung, was grundsätzlich sinnvoll ist. Sie muss aber zeitnah angegangen werden, um das Potenzial der E-ID vollumfänglich auszuschöpfen.

Ebenfalls unterstützen wir die internationale Interoperabilität unserer E-ID, möchten aber darauf hinweisen, dass diese künftig im Gleichschritt mit anderen Staaten, insbesondere mit der EU, weiterentwickelt werden muss.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und die Prüfung unserer Anmerkungen. Bei Fragen stehen Ihnen die Unterzeichnenden sowie unsere zuständigen Fraktionsmitglieder, Nationalrätin Judith Bellaiche und die Nationalräte Jörg Mäder und François Pointet, gerne zur Verfügung.

Mit freundlichen Grüssen

Jürg Grossen
Parteipräsident

Noëmi Emmenegger
Geschäftsführerin der Bundeshausfraktion



GRÜNE Schweiz

Waisenhausplatz 21
3011 Bern

rahel.estermann@gruene.ch
031 326 66 15

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
3003 Bern

per E-Mail an:
rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

Entwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID): Vernehmlassung

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Sie haben die GRÜNEN eingeladen, sich zum Entwurf für das Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) zu äussern. Wir danken Ihnen dafür und nehmen gerne Stellung.

Die GRÜNEN haben das ursprüngliche E-ID-Gesetz, welches eine Privatisierung und die zentrale Datenspeicherung vorsah, erfolgreich bekämpft (Referendumsabstimmung März 2021). Uns ist es wichtig, dass bald eine E-ID für die Schweizer Bevölkerung zugänglich ist. Wir begrüssen den nun vorliegenden zweiten Entwurf grundsätzlich, da massive Verbesserungen vorgenommen wurden. Wir GRÜNE unterstützen den gewählten Ansatz der Self Sovereign Identity (SSI) und die Idee eines Ökosystems der digitalen Basis-Infrastruktur. Jedoch fordern wir weitere Verbesserungen bezüglich Schutz der Daten und Datenkompetenz der Bevölkerung – die neue E-ID muss der Bund dazu nützen, das Wissen rund um Daten und Datenschutz in der Bevölkerung zu fördern. Ebenso muss die Barrierefreiheit gesetzlich verankert, eine Option für Menschen ohne Ausweis sowie ein Ausstellungsweg über Passbüros geschaffen werden. Die ganze Vertrauensinfrastruktur muss Open Source sein, um ihrem Namen gerecht zu werden. Wir schlagen zudem zwei zusätzliche Gesetzesartikel vor, um die Überidentifikation zu verhindern: Es darf nur dort eine E-ID verlangt werden, wo es für den Zweck auch erforderlich ist.

Allgemeine Anmerkungen

Die GRÜNEN gehörten zum erfolgreichen Referendumskomitee gegen die erste Version des E-ID-Gesetzes. Wir haben das im März 2021 gescheiterte Projekt erfolgreich bekämpft, weil es eine staatliche Kern-Dienstleistung unnötigerweise privatisiert hätte und dabei auch die Prinzipien der Datensparsamkeit, des «Privacy by Design» sowie der dezentralen

Speicherung nicht beachtet hat. Gleich im Anschluss an die Abstimmungen haben die GRÜNEN aber ein breit abgestütztes Projekt initiiert, um möglichst schnell ein neues E-ID-Gesetz aufzugleisen. Denn uns ist daran gelegen, dass die Einwohner*innen der Schweiz möglichst schnell über einen elektronischen staatlichen Ausweis verfügen können. Wir GRÜNE haben mehrfach den transparenten und partizipativen Prozess für eine neue E-ID positiv gewürdigt, der in den letzten Monaten stattfand. Wir finden es zentral, dass der Prozess auch nach der Vernehmlassung derart offen weitergeführt wird, beispielsweise bezüglich der Verordnung.

Wir GRÜNE haben uns im Rahmen der Konsultation des Zielbildes E-ID zustimmend geäußert zur Idee des SSI-Ansatzes (Self-Sovereign Identity) sowie derjenigen eines Ökosystems der digitalen Basis-Infrastruktur. Wir stehen auch dem jetzt vorliegenden Entwurf des E-ID-Gesetzes grundsätzlich positiv gegenüber und würdigen, dass im Vergleich zur Vorlage, welche die Bevölkerung ablehnte, massive Verbesserungen des Gesetzes vorgenommen wurden. Das jetzt vorliegende Gesetz ist eine gute Basis, um einen digitalen Identitätsnachweis zu schaffen und so den digitalen Wandel in der Schweiz im Sinne der Menschen und ihrer Bedürfnisse voranzubringen. Gleichwohl gibt es im vorliegenden Entwurf noch Lücken zu schliessen und Änderungen vorzunehmen.

Datenschutz

Mit der Anwendung der E-ID wird eine neue, spezifische Daten-Kategorie geschaffen: besonders schützenswerte Personendaten, die als solche in ihrer Korrektheit bestätigt wurden. Diese Daten sind äusserst wertvoll und verdienen auch einen besonderen Schutz, der durch das Datenschutzgesetz (auch in der revidierten Version) ungenügend gegeben ist. Wir verweisen hier auf die detaillierten Ausführungen der Vernehmlassungsantwort des Referendumskomitees E-ID. Aus Sicht der GRÜNEN muss das BGEID in dieser Hinsicht kritisch geprüft und überarbeitet werden.

Auch muss der Bund prüfen, ob das Vertrauen in die E-ID – gerade auch, wenn sie zu einem Öko-System mit vielen Schnittstellen ausgebaut wird – mit einer unabhängigen Aufsichtskommission gestärkt werden kann.

Datenkompetenz

Die Einführung der E-ID, die anfallenden besonders schützenswerten, bestätigten Personendaten und insbesondere der gewählte SSI-Ansatz – den wir begrüßen – sollte für den Bund ein Anlass sein, eine Kampagne für die Sensibilisierung und Kompetenzaneignung der eigenen digitalen Daten zu starten. Der SSI-Ansatz erfordert eine hohe Verantwortung der Nutzenden und die dafür nötigen Kompetenzen müssen vom Bund folgerichtig gefördert werden. Der Bund soll die Einführung der E-ID so zur Gelegenheit machen, die Daten- und Datenschutzkompetenz der Bevölkerung zu fördern.

Barrierefreiheit

Ohne Berücksichtigung der E-Accessibility wären Menschen mit Sehbeeinträchtigung vom staatlichen Angebot eines elektronischen Identitätsnachweises ausgeschlossen. Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Vor dem Start der E-ID muss eine Bestätigung der Barrierefreiheit des Systems durch Fachpersonen aus dem Kreis der Betroffenen erfolgen (siehe auch den Vorstoss [22.7406 der grünen Nationalrätin Franziska Ryser](#)).

Für die detaillierte Ausführungen zur Barrierefreiheit verweisen wir auf die Vernehmlassungsantwort von SZBLIND, die wir unterstützen.

Anmerkungen zu spezifischen Aspekten und Artikeln des BGEID

AHV-Nummer (Art. 2 Abs. 3)

Die GRÜNEN sehen die weitverbreitete Speicherung und Nutzung der AHV-Nummer kritisch. Sie soll beim Einsatz der E-ID nur dort zugänglich gemacht werden, wo die AHV-Nummer auch gesetzlich wirklich erforderlich ist.

Optionen für Personen ohne Schweizer Pass oder Aufenthaltsbewilligung (Art. 3)

Gemäss Art. 3 ist eine E-ID nur zugänglich für Personen, welche über einen Schweizer Pass oder eine gültige Aufenthaltsbewilligung verfügen. Von diesen zwei Optionen ist aber ein signifikanter Teil der Bevölkerung ausgeschlossen (der sich in seiner Grösse auch nicht messen lässt).

Um diese Personen, die hier leben und oft auch arbeiten, nicht von gewissen Dienstleistungen auszuschliessen, schlagen die GRÜNEN vor, dass das BGEID Möglichkeiten schaffen soll für Personen ohne Schweizer Pass oder gültige Aufenthaltsbewilligung – beispielsweise eine Ausstellung der E-ID aufgrund eines ausländischen Passes.

Ausstellung der E-ID (Art. 4)

Die GRÜNEN beantragen, dass im Ausstellungsprozess ein zweiter Weg geschaffen wird, auf dem die E-ID in einer physischen Anlaufstelle unter Begleitung bezogen werden kann. Die Art der Ausstellung soll zudem in der E-ID als Wert gespeichert werden.

Dieser zusätzliche Ausstellungsweg soll drei Zielen dienen:

- (1) dem Abbau von Hürden für Personen, für welche ein rein digitaler Ausstellungsprozess anspruchsvoll ist;
- (2) der Sicherung des Vertrauens in den Ausstellungsprozess durch eine geschulte und kompetente (physische anwesende, menschliche) Begleitung;
- (3) damit die E-ID auch bei einem regulären Besuch für die Ausstellung einer physischen ID oder Pass automatisch mit angeboten respektive im gleichen Prozess ausgestellt werden kann.

Die GRÜNEN schlagen vor, dafür die Passbüros der Kantone für diesen Prozess einzubinden. Dies könnte in Art. 8 (Anlaufstellen der Kantone) explizit festgehalten werden.

Vorweisen von elektronischen Nachweisen (Art. 16)

Im Sinne der Datensparsamkeit und der Datensicherheit darf eine E-ID nur dort zwingend sein, wo es für den Zweck auch erforderlich ist. Damit wird eine «Überidentifikation» verhindert. Ebenso braucht es ein Widerrufsrecht, damit die E-ID-Inhaber*innen jederzeit die Kontrolle über ihre Daten behalten. Zudem sind jeweils nur jene Attribute zu verlangen, welche für den Zweck tatsächlich erforderlich sind. So braucht zum Beispiel eine Altersfreigabe nur das beglaubigte Attribut des Alters, nicht aber den Namen oder weitere Identifikationsmerkmale.

Die Referendumsallianz macht zwei Ergänzungsvorschläge zu Art. 16, die wir GRÜNE unterstützen:

Art. 16^{bis} Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang

¹ Die Erfordernis eines elektronischen Nachweises darf von Behörden und Privaten als Voraussetzung für die Erbringung einer Leistung oder Gewährung eines Zugangs nur insoweit gestellt werden als sie für die Erbringung der Leistung oder der Gewährung des Zugangs unbedingt erforderlich ist.

² Falls die Übermittlung von Bestandteilen eines elektronischen Nachweises oder davon abgeleiteten Informationen unbedingt erforderlich ist, so ist stets die Möglichkeit vorzusehen, diese Bestandteile und Informationen ohne vermeidbare Nachteile auf andere Weise zu übermitteln.

Art. 16^{ter} Informations- und Zustimmungspflicht; Widerrufsrecht

Für Datenbearbeitungen, welche für die Erbringung der Leistung oder die Gewährung des Zugangs nicht unbedingt erforderlich sind, gelten nachfolgende Bestimmungen:

- a. Die Verifikatorin informiert die Inhaberin oder den Inhaber des Ausweises über Art, Zweck und Umfang der Datenbearbeitung.
- b. Die Datenbearbeitung bedarf der expliziten und jederzeit widerrufbaren Zustimmungen der Inhaberin und des Inhabers.
- c. Erfüllt die Bearbeitung verschiedene Zwecke, so hat die Inhaberin oder der Inhaber die Zustimmung zu jedem dieser Zwecke einzeln zu erteilen.
- d. Die Inhaberin oder der Inhaber kann die Zustimmung jederzeit und einzeln widerrufen.

Vertrauensinfrastruktur (5. Abschnitt)

Wir begrüßen es sehr, dass die Basisinfrastruktur für die E-ID nun eine Staatsaufgabe ist – dies ist eine der zentralen Errungenschaften der neuen E-ID-Vorlage. Das Vertrauen ist ein wichtiger Faktor für den Erfolg der E-ID und des gesamten Ökosystems.

Um das nötige Vertrauen in diese Infrastruktur auch wirklich zu schaffen, muss sie komplett – und nicht nur in Teilen – in der Verantwortung des Bundes liegen und Open Source sein.

Die GRÜNEN verlangen deshalb, dass auch die Funktionalität zur Prüfung der E-ID (in Form einer Anwendung/App, aber auch als Software Development Kit wie es beispielsweise beim Covid-Zertifikat der Fall war) vom Bund ausgestellt werden muss – dies hat sich bereits bei den Covid-Anwendungen bewährt. Die «kann-Formulierung» in Art. 20 ist zu ersetzen.

Dasselbe gilt auch für das System für Sicherungskopien (Art. 21): Auch hier ist die Kann-Formulierung zu ersetzen.

Neben den Quellcode der Vertrauensinfrastruktur muss auch der Quellcode der Apps gemäss Art. 19 (Anwendung zur Aufbewahrung und Vorweisen von elektronischen

Nachweisen) und Art. 20. (Anwendung zur Prüfung der elektronischen Nachweise) offengelegt werden.

Gebühren (Art. 26)

Die GRÜNEN beantragen, dass keine Gebühren erhoben werden. Das E-ID-Ökosystem ist eine Basisinfrastruktur für die Digitalisierung der Schweiz und damit für die Effizienz und Attraktivität der gesamten Volkswirtschaft. Aussteller*innen und Verifikator*innen investieren ihren Anteil am Ökosystem durch die Anpassung ihrer Systeme und Prozesse.

Wir danken Ihnen, Frau Bundesrätin, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Kritikpunkte an der vernehmlasssten Gesetzesvorlage.

Freundliche Grüsse



Balthasar Glättli
Präsident



Rahel Estermann
stv. Generalsekretärin, Leiterin Politik

Per Mail: rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

Vernehmlassung: Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Sie haben uns eingeladen, zur obengenannten Vernehmlassungsvorlage Stellung zu nehmen. Für diese Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens.

Allgemeine Bemerkungen

Obwohl das Bundesgesetz über die elektronischen Identifizierungsdienste (E-ID-Gesetz) in der Volksabstimmung vom 7. März 2021 abgelehnt wurde, besteht in der Gesellschaft und bei der Wirtschaft nach wie vor der Wunsch nach einem elektronischen Identitätsnachweis (E-ID). Mit vorliegendem Entwurf soll ein solcher Identitätsnachweis für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises eingeführt werden. Diese E-ID soll auf einer staatlich betriebenen Infrastruktur beruhen.

Die Mitte spricht sich für eine E-ID aus

Die Mitte spricht sich für die Einführung einer solchen E-ID aus. Dabei steht für sie der Schutz der Daten und das Vertrauen der Nutzer an oberster Stelle. Daher soll die eingeführte Vertrauensinfrastruktur offen, verlässlich und sicher gestaltet sein. Der Ansatz des Vorentwurfs beruht auf dem Grundsatz des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung. Der Mitte erscheint dadurch die nötige Sicherheit der Daten grundsätzlich gewährleistet zu sein. Jedoch würde sie eine regelmässige Überprüfung der Vertrauensinfrastruktur durch eine unabhängige Instanz sowie eine Anpassung der Infrastruktur an den aktuellen Stand der Technik begrüssen.

Aus Sicht der Mitte sollte zudem die Unterscheidung der E-ID als Identifikationsmittel zu einem Authentifikationsmittel deutlicher gemacht werden, handelt es sich bei der E-ID doch um einen digitalen Identitätsnachweis und nicht um ein Zugangsmittel. Des Weiteren sollte auch geprüft werden, wie der barrierefreie Zugang zur E-ID für Menschen mit Beeinträchtigungen sichergestellt werden kann. Dieser Aspekt fand im Vernehmlassungsentwurf keine Erwähnung, ist im Zusammenhang mit dem vorliegenden Gesetzesvorhaben jedoch von grosser Bedeutung.

Aufgrund der starken gesellschaftlichen und wirtschaftlichen Verflechtung der Schweiz mit dem Ausland, insbesondere mit der Europäischen Union (EU), ist es für die Mitte zudem essentiell, dass die Schweizer E-ID und ausländische E-ID gegenseitig anerkannt werden können. Dass eine Interoperabilität der E-ID-Systeme der EU und der Schweiz angestrebt wird, erachtet die Mitte daher als sinnvoll.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und verbleiben mit freundlichen Grüssen.



Die Mitte

Sig. Gerhard Pfister
Präsident Die Mitte Schweiz

Sig. Gianna Luzio
Generalsekretärin Die Mitte Schweiz



Per E-Mail

Bundesamt für Justiz

Bundesrain 20

3003 Bern

rechtsinformatik@bj.admin.ch

Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme, die wir gerne wahrnehmen:

1 Grundsätzliche Bemerkungen

Die SP Schweiz unterstützt diese Vorlage im Grundsatz. Wie der Abstimmungskampf und das Abstimmungsergebnis zum gescheiterten Bundesgesetz über die elektronischen Identifizierungsdiensten (BGEID) vom März 2021 gezeigt hat, ist es bei der Schaffung einer Rechtsgrundlage für einen elektronischen Identitätsnachweises für die Stimmbürger:innen entscheidend, dass eine solche E-ID von einer staatlichen Stelle herausgegeben wird.¹ Ebenfalls zentral sind für uns die Grundsätze der Datensparsamkeit, der bestmöglichen Selbstbestimmung der Nutzer:innen einer E-ID über ihre Daten, des "privacy by design" sowie der dezentralen Datenspeicherung², wie sie in den überparteilichen, auch von der SP eingebrachten und mittlerweile von beiden Räten angenommenen³ Motionen⁴ auch festgeschrieben ist. Schliesslich ist es für uns auch wichtig, dass auch in Zukunft sichergestellt wird, dass für die Inanspruchnahme von staatlichen Leistungen immer auch eine mit zumutbarem Aufwand benutzbare nicht-digitale Lösung zur Verfügung steht.⁵ Der

¹ Vgl. Demoscope Repräsentative Umfrage zu den elektronischen Identifizierungsdiensten (BGEID).

² Vgl. auch Art. 1 Abs. 2 lit. b VE-BGEID, Erläuternder Bericht, S. 7.

³ Vgl. Amtliches Bulletin Nationalrat vom 14.9.2021; Amtliches Bulletin Ständerat vom 13.6.2022.

⁴ Vgl. Motion Min Li Marti 21.3126 Vertrauenswürdige staatliche E-ID

⁵ Vgl. Vernehmlassungsantwort Digitale Gesellschaft, Oktober 2022, Abschnitt «Diskriminierungsfreier Zugang zu Leistungen»; siehe auch Stellungnahme der Fachkommission

vorliegende Vorentwurf des Bundesrates genügt nach Ansicht der SP Schweiz diesen Grundsätzen überwiegend. Ebenfalls erachten wir es als richtig und wichtig, dass diese Vorlage internationalen Entwicklungen insbesondere auf europäischer Ebene Rechnung trägt und der Bundesrat anstrebt, eine internationale Anerkennung der schweizerischen E-ID zu erreichen und gleichzeitig auch ausländische E-IDs anerkennen zu wollen.⁶ Wir begrüßen vor diesem Hintergrund ausdrücklich die rasche Neuauflage einer Vorlage für elektronische Identifizierungsdienste durch die Bundesverwaltung und den partizipativen Ansatz bei deren Ausarbeitung⁷. Konkreten Verbesserungsbedarf sehen wir insbesondere bei der Verhinderung des Identitätsdiebstahls durch persönliches Erscheinen der antragsstellenden Person für eine E-ID (siehe nachfolgend unter Ziff. 2.2.) sowie bei der Verhinderung einer Überidentifikation bei der Übermittlung der Bestandteile der elektronischen Nachweise an die Verifikator:innen (siehe Ziff. 2.4. unten stehend).

2 Kommentar zu den wichtigsten Bestimmungen

2.1. Persönliches Erscheinen der antragsstellenden Person zur Ausstellung einer E-ID (Art. 4 VE-BGEID)

Aus Sicht der SP Schweiz ist die Datensicherheit im Allgemeinen und die Vermeidung des Identitätsdiebstahls andererseits zentral für die Sicherheit und Glaubwürdigkeit einer staatlichen E-ID. Vor diesem Hintergrund finden wir es zur Verhinderung von Identitätsdiebstahl wichtig, dass auf eine vollständig automatisierte Video-Identifikation bei der Ausstellung einer E-ID⁸ verzichtet wird. Vielmehr sollte die persönliche Identifizierung der Antragssteller:innen mittels persönlichem Erscheinen bei einer entsprechenden Behördenstelle durchgeführt werden.⁹

Daher beantragt die SP Schweiz, **Art. 4 VE-BGEID** entsprechend zu **ergänzen**.

2.2. Identifikation durch physischen Ausweis (Art. 10 VE-BGEID)

Der in diesem Artikel festgeschriebene Grundsatz, dass eine Identifikation vor staatlichen Behörden neben der Möglichkeit der Verwendung einer E-ID immer auch mittels physischen Ausweisen und somit nicht-digital möglich sein muss¹⁰, ist für die SP Schweiz von eminenter Bedeutung und unterstützen wir deshalb auch nachdrücklich. Die

Netz- und Datenpolitik der SP Schweiz zur öffentlichen Konsultation zum «Zielbild E-ID», September 2021, Ziff. 1.

⁶ Vgl. Erläuternder Bericht, S. 3, 5.

⁷ Vgl. Erläuternder Bericht, S. 3.

⁸ Vgl. Erläuternder Bericht, S. 9f.

⁹ Vgl. Vernehmlassungsantwort Digitale Gesellschaft, Oktober 2022, zu Art. 4 Abs. 4.

¹⁰ Vgl. Erläuternder Bericht, S. 11.

entsprechende Einschränkung, wonach dies nur möglich sein soll, wenn die entsprechenden Anforderungen an die Prozesssicherheit gewährleistet sind, finden wir vor diesem Hintergrund verfehlt, da diese Anforderungen bei einer Identifikation durch physische Ausweisdokumente sowieso erfüllt sein müssten.¹¹

Die SP Schweiz beantragt deshalb, Art. 10 VE-BGEID folgendermassen zu ändern:

Art. 10 VE-BGEID

Wer in einem Prozess einer Person, die persönlich erscheint, die Möglichkeit bietet, die E-ID oder Teile davon vorzuweisen, muss dieser Person die Wahl lassen, sich stattdessen mit einem Ausweisdokument nach dem AwG6, einem Ausländerausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und

Asyl oder einem Ausweis nach Artikel 13 Absatz 1 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005⁷ auszuweisen, ~~sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können.~~

2.3. Risiko der Überidentifikation bei der Übermittlung der Bestandteile der elektronischen Nachweise an die Verifikator:innen (Art. 16 VE-BGEID)

Die Grundsätze der Datensparsamkeit und des «privacy by design» sind für die SP Schweiz zentrale Pfeiler für diese Vorlage (siehe dazu obenstehend unter Ziff. 1.). Der Vorschlag des Bundesrates zum Art. 16 BGEID¹² erachten wir vor diesem Hintergrund als ungenügend. Für uns ist es problematisch, dass die Verifikatorin frei über das Erfordernis des elektronischen Nachweises und deren Umfang bestimmen können soll. Vielmehr soll dieser Umfang gesetzlich auf das unbedingt Erforderliche beschränkt werden. Andernfalls soll eine informierte und explizite Zustimmung stattfinden müssen.

Folglich beantragt die SP Schweiz, die entsprechenden Bestimmungen folgendermassen zu ergänzen.¹³

Art. 16^{bis} Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang

1 Die Erfordernis eines elektronischen Nachweises darf von Behörden und Privaten als Voraussetzung für die Erbringung einer Leistung oder Gewährung eines Zugangs nur insoweit gestellt werden als sie für die Erbringung der Leistung oder der Gewährung des Zugangs unbedingt erforderlich ist.

¹¹ Vgl. Vernehmlassungsantwort Digitale Gesellschaft, Oktober 2022, zu Art. 10.

¹² Vgl. Erläuternder Bericht, S. 13.

¹³ Siehe Vernehmlassungsantwort Digitale Gesellschaft, Oktober 2022, zu Art. 16^{bis}, Art. 16^{ter}.

2 Falls die Übermittlung von Bestandteilen eines elektronischen Nachweises oder davon abgeleiteten Informationen unbedingt erforderlich ist, so ist stets die Möglichkeit vorzusehen, diese Bestandteile und Informationen ohne vermeidbare Nachteile auf andere Weise zu übermitteln.

Art. 16^{ter} Informations- und Zustimmungspflicht; Widerrufsrecht

Für Datenbearbeitungen, welche für die Erbringung der Leistung oder die Gewährung des Zugangs nicht unbedingt erforderlich sind, gelten nachfolgende Bestimmungen:

a Die Verifikatorin informiert die Inhaberin oder den Inhaber des Ausweises über Art, Zweck und Umfang der Datenbearbeitung.

b Die Datenbearbeitung bedarf der expliziten und jederzeit widerrufbaren Zustimmungen der Inhaberin und des Inhabers.

c Erfüllt die Bearbeitung verschiedene Zwecke, so hat die Inhaberin oder der Inhaber die Zustimmung zu jedem dieser Zwecke einzeln zu erteilen.

d Die Inhaberin oder der Inhaber kann die Zustimmung jederzeit und einzeln widerrufen.

2.4. Obligatorisches Angebot einer Anwendung zur Prüfung von elektronischen Nachweisen (Art. 20 VE-BGEID)

Die SP Schweiz findet es im Sinne der Benutzer:innenfreundlichkeit richtig, dass eine Anwendung zur Prüfung von elektronischen Nachweisen zur Verfügung gestellt werden soll. Allerdings soll der Bundesrat nicht bloss die Möglichkeit erhalten, eine solche Anwendung zur Verfügung zu stellen, sondern vielmehr dazu verpflichtet werden. Nur so kann die im Erläuternden Bericht richtigerweise gewünschte Vertrauen der Bevölkerung in die Vertrauensinfrastruktur¹⁴ gestärkt werden.

Daher beantragt die SP Schweiz, **Art. 20 VE-BGEID** entsprechend zu **ergänzen**.

Wir bitten Sie, unsere Anliegen bei der Überarbeitung der Vorlage zu berücksichtigen.

¹⁴ Vgl. Erläuternder Bericht, S. 16.

Mit freundlichen Grüssen

SOZIALDEMOKRATISCHE PARTEI DER SCHWEIZ

Handwritten signature of Mattea Meyer in blue ink.

Mattea Meyer

Co-Präsidentin

Handwritten signature of Cédric Wermuth in black ink.

Cédric Wermuth

Co-Präsident

Handwritten signature of Claudio Marti in black ink.

Claudio Marti

Politischer Fachsekretär

Madame la Conseillère fédérale Karin Keller-Sutter
Cheffe du Département fédéral de justice et police
DFJP
3000 Berne

Par courrier électronique :
rechtsinformatik@bj.admin.ch

Berne, le 20 octobre 2022

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID)

Réponse de l'UDC Suisse à la procédure de consultation

Madame la Conseillère fédérale,

Mesdames et Messieurs,

L'UDC Suisse vous remercie de l'avoir consultée au sujet de l'objet cité en titre. Après avoir examiné les détails du projet, elle a l'avantage de se prononcer comme suit :

L'UDC Suisse ne peut pas accepter la loi proposée en l'absence de base constitutionnelle claire. En effet, à la suite du refus de l'identité électronique par deux tiers des votants, il convient d'offrir à la population un projet fiable et transparent, fondé sur une compétence constitutionnelle indiscutable.

L'avant-projet de loi prévoit la mise en place d'une identité électronique étatique pour les titulaires d'un document d'identité émis par les autorités suisses. En outre, il vise à créer une infrastructure de confiance étatique étendue qui permettra aux acteurs de secteurs publics et privés d'émettre et d'utiliser des moyens de preuve électroniques aux personnes intéressées.

L'UDC Suisse est consciente de l'intérêt que peut représenter une identité électronique fiable. C'est à ce titre qu'elle avait soutenu à l'époque la loi sur les services d'identification électronique. Quoi qu'il en soit, de tels systèmes doivent être sûrs et se fonder sur une réglementation juridique saine.

Absence de base constitutionnelle claire

Comme le Conseil fédéral le reconnaît à la page 6 de son rapport, l'article 81 Cst vise des travaux publics et ouvrages de nature physique, au sens d'une construction. Le recours à cet article pour fonder de grands projets informatiques et autres éléments visant à créer un paysage administratif électronique uniforme n'est que partiellement soutenu par la doctrine.

L'UDC Suisse considère qu'il faut agir avec rigueur en matière de partage des compétences entre la Confédération et les cantons. En l'espèce, les réserves de la doctrine étant sérieuses¹, le projet doit se baser sur une nouvelle compétence constitutionnelle acceptée par le peuple et les cantons.

¹ EJPD, Bundesamt für Justiz, Rechtsgrundlagen für die IKR-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, JAAC 2012, p. 7-9.

L'accapuration de nouvelles tranches de compétence par les autorités fédérales sans réelle acceptation doctrinale n'a pas sa place dans un Etat fédéraliste.

Obtenir la confiance de la population

En l'absence d'un partage clair et transparent des compétences et d'une réponse satisfaisante aux doutes en matière de protection des données, le projet se heurtera à juste titre à une sérieuse opposition populaire. Pourtant, tout système d'identification est tributaire de la confiance qui lui est accordée.

En l'occurrence, deux tiers des citoyens suisses ont exprimé leur méfiance quant à un système de ce genre lors de la dernière votation correspondante. Une majorité d'entre eux a évoqué la question de la protection des données comme raison de son refus. Le fait de proposer une identité électronique étatique ne répond à l'évidence pas, en tant que tel, aux craintes de la population.

Eviter les dérapages

Nonobstant les observations mentionnées ci-dessus, l'UDC salue le fait que l'avant-projet s'adresse uniquement aux personnes de nationalité suisse ou disposant d'un permis valable. Les documents d'identité relevant de la seule compétence confédérale, les villes ne sauraient obtenir de passe-droits à ce sujet, notamment dans l'optique d'une légalisation de facto des clandestins.

En revanche, l'UDC émet de grandes réserves concernant les garanties du Conseil fédéral, selon lesquelles le système proposé demeurera effectivement facultatif à long terme. Le récent exemple de la poste, dont les clients ont été contraints d'adopter rapidement la solution SwissID sous peine de perdre leur accès en ligne et les remous occasionnés démontrent les limites des systèmes centralisés dits « volontaires ». Cet exemple donne un aperçu de ce à quoi peut ressembler une solution « volontaire », alors que certaines prestations sont certes accessibles dans les officines, mais à des tarifs plus élevés.

Réitérant ses remerciements de l'avoir associée à cette consultation, l'UDC Suisse vous prie de croire, Madame la Conseillère fédérale, Mesdames et Messieurs, à l'assurance de sa considération.

Avec nos meilleures salutations

UNION DÉMOCRATIQUE DU CENTRE

Le président du parti

Le secrétaire général



Marco Chiesa

Conseiller aux Etats



Peter Keller

Conseiller national



Schweizerische Arbeitsgemeinschaft für die Berggebiete
Groupement suisse pour les régions de montagne
Gruppo svizzero per le regioni di montagna
Gruppa svizra per las regiuns da muntogna

Schweizerische Arbeitsgemeinschaft für die Berggebiete, Postfach, 3001 Bern

Bundesamt für Justiz

3003 Bern

rechtsinformatik@bj.admin.ch

Bern, 30. September 2022
TE / C13

(avec un résumé en français à la fin du document)

Stellungnahme der SAB zum E-ID-Gesetz

Sehr geehrte Damen und Herren

Die Schweizerische Arbeitsgemeinschaft für die Berggebiete SAB bedankt sich für die Gelegenheit zur Stellungnahme zu randvermerktem Geschäft. Die SAB vertritt die Interessen der Berggebiete und ländlichen Räume in den wirtschaftlichen, sozialen und ökologischen Belangen. Mitglieder der SAB sind 22 Kantone, rund 600 Gemeinden sowie zahlreiche Organisationen und Einzelmitglieder.

Nach der Ablehnung des E-ID-Gesetzes in der Volksabstimmung vom 7. März 2021 nimmt der Bundesrat einen neuen Anlauf für die Einführung eines Elektronischen Identitätsnachweises. Ein wesentlicher Grund für die Ablehnung war damals, dass der Identitätsnachweis nicht durch die Bundesverwaltung, sondern durch beauftragte Dritte erstellt worden wäre. Die Mehrheit der Stimmbevölkerung ist offensichtlich der Auffassung, dass der Identitätsnachweis vollumfänglich in der Kontrolle der Bundesbehörden bleiben muss. Diesem Anliegen wird mit dem nun vorliegenden neuerlichen Vorschlag Rechnung getragen.

Aus Sicht der SAB entspricht die Einführung eines elektronischen Identitätsnachweises einem Bedürfnis der Bevölkerung. Immer mehr Behördengeschäfte werden ausschliesslich elektronisch abgewickelt. Davon profitiert auch die Bevölkerung in entlegeneren Landesgegenden, da sie sich den physischen Weg zu den Amtsstellen ersparen kann. Die SAB unterstützt deshalb grundsätzlich die Einführung einer E-ID, welche den Verkehr mit den Behörden weiter erleichtern wird.

Parallel zum Schutz der Persönlichkeit und der Grundrechte von Personen, ist ein weiteres wichtiges Ziel des Gesetzes eine umfassende 'Vertrauensinfrastruktur' aufzubauen, die einen klaren Nutzen für Bürgerinnen und Bürger hat. Die E-ID kann in diesem Sinne nicht nur für E-Government eine wichtige Voraussetzung sein, sondern auch für zahlreiche andere Geschäftsmodelle, die eine digitale Identifikation voraussetzen. Das Gesetz sollte daher nicht nur eine Anbindung anderer elektronischer Nachweise, und deren Ausstellung und Überprüfung gewährleisten, sondern dies aktiv fördern bzw. unterstützen. Wir erachten es daher für zielführend, im Rahmen der Zweckbestimmung zu ergänzen, dass das Gesetz neue digitale Geschäftsmodelle ermöglichen soll, die Vertrauen im digitalen Raum voraussetzen.

Wenn Vertrauen geschaffen werden soll, muss die Infrastruktur sicher und robust sein. Überlegungen zur Cybersicherheit müssen deshalb von Anfang an berücksichtigt und gesetzlich verankert werden. Im Gesetz sollte vorgeschrieben werden, dass die Cybersicherheit regelmässig durch externe Fachspezialisten getestet wird.

Mit freundlichen Grüssen

**SCHWEIZERISCHE ARBEITSGEMEINSCHAFT
FÜR DIE BERGGEBIETE (SAB)**

Die Präsidentin:

Der Direktor:

Christine Bulliard-Marbach
Nationalrätin

Thomas Egger

Résumé

Le SAB - Groupement suisse pour les régions de montagne - soutient globalement la mise en place d'une identité électronique pour les personnes. Cela permettra de régler de nombreuses questions administratives à distance, ce qui est dans l'intérêt des régions de montagne et de l'espace rural. Cependant, pour qu'un tel projet fonctionne, il est nécessaire d'assurer la protection des personnes et des droits qui en découlent. Il faut aussi mettre en place des infrastructures sûres et performantes. Enfin, le SAB estime que ce projet devrait contribuer à développer de nouveaux modèles commerciaux.

Eidg. Justiz- und
Polizeidepartement EJPD
Bundeshaus West
3003 Bern

per E-Mail an:
rechtsinformatik@bj.admin.ch

Bern, 18. Oktober 2022

**Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis
und andere elektronische Nachweise (E-ID-Gesetz, BGEID);
Stellungnahme des Schweizerischen Gemeindeverbands (SGV)**

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 haben Sie dem Schweizerischen Gemeindeverband (SGV) das oben erwähnte Geschäft zur Stellungnahme unterbreitet. Für die Gelegenheit, uns aus Sicht der rund 1'600 dem SGV angeschlossenen Gemeinden äussern zu können, danken wir Ihnen bestens.

Da die Gemeinden im Thema digitale Verwaltung (E-Government) institutionell stark mit den Kantonen zusammenarbeiten und verbunden sind, verweisen wir im Grundsatz auf die Stellungnahme der Konferenz der Kantonsregierungen KdK vom 23. September 2022; sie geht unter anderem auf die diversen Schnittstellen zwischen Bundesebene sowie kantonaler und kommunaler Ebene ein. Nachfolgend unterbreiten wir Ihnen unsere Stellungnahme:

Der Schweizerische Gemeindeverband SGV unterstützt seit Beginn der politischen Diskussion einen elektronischen Identifikationsnachweis E-ID mit der Überzeugung, dass ein gesicherter Zugang zu elektronischen, digitalen Behördenleistungen die digitale Verwaltung fördern und stärken wird – und dies auf allen Staatsebenen: Bund, Kantone und Gemeinden. **In diesem Sinne ist auch der Entwurf eines neuen Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) ganz prinzipiell zu begrüßen.** Der Vorentwurf des E-ID-Gesetzes wird insgesamt als gelungen betrachtet und kann bis auf wenige Details unterstützt werden.

In den weiteren Arbeiten wird es von grosser Wichtigkeit sein, dass die Schnittstellen insbesondere beim Betrieb eines elektronischen Identifikationsnachweises E-ID zu den anderen Staatsebenen (Kantone und Gemeinden) umfassend und schlüssig geklärt werden können. Dies soll entweder im Rahmen der (operativen) institutionellen Zusammenarbeit über bereits bestehende Gremien, wie der Digitalen Verwaltung Schweiz (DVS), oder bei der anstehenden Erarbeitung der bundesrätlichen Umsetzungsverordnung erfolgen.

Zusammen mit den Kantonen (KdK) fordern wir von Anfang weg einen festen Einbezug in die bevorstehenden Arbeiten, damit die operativen Belange des Vollzugs mit den betroffenen staatlichen Behörden im Vorhinein diskutiert und geklärt werden können. Dies soll rasch und, wenn möglich, bereits während der politischen Diskussion im Parlament erfolgen, damit die gute Dynamik des Projekts E-ID aufrechterhalten werden kann. Für den SGV ist es wichtig, dass ein elektronischer Identifikationsnachweis E-ID möglichst bald zur Verfügung steht, damit die Entwicklung zu immer mehr digitalen Behördendienstleistungen auf allen Staatsebenen weiter gefördert werden kann.

Als sehr wichtig betrachtet der SGV unter Bezugnahme auf die Ablehnung der E-ID-Vorlage (anlässlich der eidg. Volksabstimmung vom 7. März 2021) sowie auf die in der Frühjahrssession 2021 der eidg. Räte eingereichten Motionen für eine "Vertrauenswürdige, staatliche E-ID"¹ die Einhaltung der höheren Ansprüche und Kriterien, wie **eine staatliche Herausgabe des elektronischen Identifikationsnachweises E-ID (Ausstellung des Ausweises und Betrieb der Infrastruktur) sowie der sorgfältige Umgang mit den Personendaten (vor allem «Self-Sovereign Identity», dezentrale Speicherung, Datenschutz und Datensparsamkeit)**. Auch der praktische Zugang zum elektronischen Identifikationsnachweis E-ID soll simpel ausgestaltet sein, was den Bezug resp. das Ausstellen von weiteren elektronischen Nachweisen vereinfacht. Ferner soll sich die Schweiz an den Vorgaben der europäischen Gesetzgebung orientieren, um für die Zukunft die internationale Durchlässigkeit sicherstellen zu können. **Mit dem Vorentwurf zum E-ID-Gesetz wird all diesen Kriterien mehrheitlich und auf eine praktikable Art und Weise entsprochen.**

Zu einzelnen Punkten:

Art. 3 Persönliche Voraussetzungen

Unter Art. 3 Entwurf BGEID wird festgelegt, dass ausschliesslich Personen mit einem geregelten Aufenthalt die Möglichkeit zum Bezug eines elektronischen Identifikationsnachweises E-ID haben sollen. Aus kommunaler Sicht bleibt anzufügen, dass die üblichen Behördenkontakte aber einen weiteren Kreis umfassen, bspw. Personen mit einem nicht geregelten Aufenthalt in der Schweiz oder Zweitwohnungsbesitzer aus dem Ausland. Hier ist zu prüfen, ob nicht auch für solche Fälle ein **elektronischer Identifikationsnachweis E-ID in einem beschränkten Rahmen** vorgesehen werden kann. Ansonsten wird ein künstlicher, unnötiger «digitaler Medienbruch» im behördlichen Umgang mit Personen geschaffen, der nicht den Prinzipien einer durchgängigen digitalen/elektronischen Verwaltung entspricht.

Art. 4 Ausstellung

Die Ausstellung des elektronischen Identifikationsnachweises E-ID in Verbindung mit der Identifizierung der Person ist ein entscheidendes Moment, weshalb es eine klare Regelung der Prozesse und Abläufe benötigt – insbesondere auch in Verbindung mit Art. 8 Entwurf BGEID, welcher die Kantone als Anlaufstelle bezeichnet. Es ist nicht ausgeschlossen und aufgrund der kantonalen Organisationsfreiheit auch möglich, dass dabei die Gemeinden eine

¹ div. Motionen E-ID: [21.3124](#), [21.3125](#), [21.3126](#), [21.3127](#), [21.3128](#) und [21.3129](#)

wichtige Rolle einnehmen werden. Deshalb sind auch für die weiteren Arbeiten die kantonalen und kommunalen Behörden angemessen einzubeziehen.

Art. 8 Anlaufstelle der Kantone

Mit Art. 8 Entwurf BGEID wird den Kantonen eine neue Aufgabe übertragen. Mit Verweis auf die Ausführungen zu Art. 4 gilt es, diesen Sachverhalt klar und umfassend zu regeln. Das beinhaltet finanzielle Fragen, aber auch Fragen des Supports und des Betriebs. Von verschiedener Seite wird heute bereits der Anspruch angemeldet, dass auch sie als halbstaatliche oder private Unternehmen zukünftig einen elektronischen Identifikationsnachweis E-ID ausstellen könnten. Solchen Bestrebungen ist von Vornherein kritisch zu begegnen. Die politische Forderung nach der verlorenen Volksabstimmung von März 2021 war klar und eindeutig: **Die E-ID muss als staatliches Projekt umgesetzt werden. Das betrifft unseres Erachtens insbesondere auch die Stelle, wo eine Ausstellung eines Ausweises stattfinden soll. Neben den Kantonen können dies auch Gemeinden, also ebenfalls eine staatliche Behörde, sein, aber keine privaten Stellen.**

Art. 9 Pflicht zur Akzeptanz der E-ID

Mit Art. 9 Entwurf BGEID wird eine neue Pflicht begründet, die vorsieht, dass alle Behörden, welche «öffentliche Aufgaben» erfüllen, den elektronischen Identifikationsnachweis E-ID zu akzeptieren haben. Das betrifft ebenfalls kommunale Behörden. **Es ist aus Sicht des SGV wichtig, dass ein schweizerischer elektronischer Identifikationsnachweis E-ID zum nationalen Standard wird, weshalb der SGV diese neue Verpflichtung unterstützt.**

Bei der Definition wird explizit die «öffentliche Aufgabe» erwähnt. Es wird vorgeschlagen, dass gemäss Art. 178 Abs. 3 Bundesverfassung BV zur allgemeinen Klarheit der Begriffe im Speziellen von «Verwaltungsaufgaben» gesprochen wird. **Falls der Bundesgesetzgeber den Begriff bewusst weiterfassen möchte, benötigte es einen eindeutigen Beschrieb des Inhalts, damit allen Beteiligten klar ist, wofür ein elektronischer Identifikationsnachweis E-ID inskünftig verwendet werden kann.**

Art. 26 Gebühren

Gebühren sind spezielle staatliche Abgaben, die als Entgelt für bestimmte Dienstleistungen der öffentlichen Verwaltung oder für die Beanspruchung einer öffentlichen Einrichtung erhoben werden können. Die Erhebung derselben orientiert sich an verschiedenen Grundprinzipien, wie der Rechtmässigkeit, der Verursachergerechtigkeit sowie der Verhältnismässigkeit. **Die in Art. 26 Entwurf BGEID festgelegte Gebührenordnung zum elektronischen Identifikationsnachweis E-ID beinhaltet diesbezüglich noch verschiedene grundsätzliche Fragen, die im Einzelnen geklärt werden müssen. Dies soll im Rahmen der Arbeit an der Umsetzungsverordnung erfolgen.**

Unter anderen sind Gebühren unter den verschiedenen Staatsebenen vorgesehen, was im Prinzip sinnlos ist und wenn überhaupt nur im engsten Masse erfolgen sollte. Auch soll ein umfassender Gebührenerlass durch den Bundesrat für bestimmte Akteure möglich sein. Vorliegend soll ein solcher mit dem Verweis auf eine weite Verbreitung und der Steigerung

der Akzeptanz bei der Bevölkerung gerechtfertigt sein. **Dies wird von Seiten des SGV kritisch beurteilt.** Wer heute eine physische Identitätskarte bezieht, hat eine Gebühr im klassischen Sinne zu entrichten. Es ist im direkten Vergleich nicht einsehbar, weshalb nun eine elektronische Identität nicht auch gebührenpflichtig sein sollte, ansonsten eine rechtsungleiche Behandlung in Bezug auf eine analoge staatliche Leistung geschaffen wird. **Der Vorschlag des SGV geht dahin, dass viel eher bei der Höhe der Gebühr (Verhältnismässigkeit) anzusetzen ist.** Je tiefer eine solche ausfällt, umso grösser wird der Anreiz sein, einen elektronischen Identifikationsnachweis E-ID zu beziehen. Es handelt sich aber keineswegs um eine «Gratis»-Dienstleistung des Staates, da der schweizweite Betrieb und die Herausgabe hohe Kosten generieren werden.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Gemeindeverband

Präsident

Direktor



Hannes Germann
Ständerat

Christoph Niederberger

Kopie an: Schweizerischer Städteverband SSV / Konferenz der Kantonsregierungen KdK / Digitale Verwaltung Schweiz DVS



Département fédéral de justice et police DFJP

Par e-mail : rechtsinformatik@bj.admin.ch

Berne, le 18 octobre 2022

**Loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques
(loi sur l'e-ID, LeID)**

Madame la Conseillère fédérale,

Nous vous remercions de nous donner l'occasion de prendre position sur cette proposition de loi fédérale sur l'identité électronique. L'Union des villes suisses représente les villes, les communes urbaines et les agglomérations de notre pays, soit bien trois quarts de la population suisse.

Considérations générales

L'UVS salue cet avant-projet de qualité, mis en consultation à peine plus d'un an seulement après le rejet par le peuple de la première monture. Les doutes exprimés par la population lors de la votation de mars 2021 ont été pris en compte, puisque c'est désormais une infrastructure d'identité électronique étatique, gérée par la Confédération et qui pourra être utilisée par les acteurs du secteur privé et public, qui est proposée.

Les villes partagent également les principes de base de ce nouveau projet, à savoir le respect de la vie privée dès la conception (*privacy by design*), de l'économie et de l'enregistrement décentralisé des données.

Plusieurs villes soulignent l'importance de reprendre les derniers standards internationaux au moment de concrétiser la mise en œuvre de l'identité électronique. Le Conseil fédéral devra veiller à ce que le système suisse soit compatible avec les systèmes multilatéraux. Il devra par ailleurs dialoguer de manière proactive avec les entités publiques – cantons et communes - qui connaissent déjà des solutions numériques sur leur territoire, afin de chercher des synergies et d'assurer une continuité entre les deux systèmes.



Demandes concernant les différentes dispositions

- **Art. 2 al. 3 (contenu de l'E-ID)** : il est indiqué dans le rapport que le numéro AVS sera collecté, mais sans qu'il soit fait mention d'une possible utilisation de ce numéro comme clé d'appariement. Le Conseil fédéral est invité à préciser cet élément dans son message. Par ailleurs le Conseil fédéral devra également éclaircir la situation des personnes ne bénéficiant pas (encore) de numéro AVS au moment de l'établissement de l'identité électronique : est-ce que l'E-ID ne contiendra dans ce cas pas de numéro AVS ou est-ce qu'un numéro AVS devra en parallèle être créé ?
- **Art. 3 let. a et art. 18 al. 1 (personnes morales)** : les formulations retenues à ces articles ne sont pas suffisamment claires en ce qui concerne les personnes morales. Le fonctionnement concret de l'identité électronique au sein des entreprises, ainsi que le lien entre personnes physiques et morales dans cette situation, devront être expliqués de manière plus détaillée dans le message du Conseil fédéral.
- **Art 5 « Révocation »** : En cas de révocation de l'E-ID, utilisateurs et utilisatrices devraient en être informés de manière active. Le projet de loi devra prévoir un tel mécanisme.
- **Art. 6 « Durée de validité »** : il serait judicieux de faire coïncider la durée de validité de l'E-ID avec celle du document physique sur laquelle elle repose (carte d'identité, passeport, etc.). Cette précision pourrait être apportée au niveau de la loi.
- **Art. 8 « Points de contact cantonaux »** : les villes doivent pouvoir assumer ce rôle de coordination, afin que l'E-ID puisse y être commandée comme les cartes d'identité et passeports actuels. Cette précision pourrait être apportée au niveau législatif.
- **Art. 11 al. 5 (conservation des données)** : le Conseil fédéral propose de limiter à cinq ans la durée de conservation des données autorisée après la date de validité ou révocation de l'E-ID. Des recherches sur l'existence d'une identification électronique devant toutefois pouvoir être réalisées au-delà de cette période, l'UVS invite le Conseil fédéral à prévoir un délai plus long.
- **Art. 15 « Transmissibilité des moyens de preuve électroniques »** : à l'al. 2 de cet article, il devrait être précisé qu'une transmission des moyens de preuve électronique est autorisée dans tous les cas. La possibilité de transférer l'E-ID sur un autre support technique doit faire partie de ses fonctionnalités de base. Renoncer à cette fonctionnalité pourrait remettre en question l'acceptation de ce nouvel instrument par les détenteurs d'identités électroniques et donc sa diffusion à grande échelle.
Proposition :
Art. 15 al.2 : Le Conseil fédéral autorise la transmission des moyens de preuve électroniques qui ne sont pas émis au nom d'une personne physique.
- **Art. 20 « Application pour la vérification des moyens de preuve électronique »** : Le système devrait être construit dès le départ de manière à inspirer confiance. Par ailleurs, pour des raisons de coûts, il faudrait éviter que chaque service de vérification doive mettre à



disposition ses propres applications de vérification de manière décentralisée. Une possibilité de vérification indépendante et crédible fait partie intégrante d'une infrastructure de confiance.

Proposition :

Art. 20 : La Confédération met à disposition une application permettant de vérifier la validité des moyens de preuve électronique.

- **Art. 21 « Système des copies de sécurité »** : suivant la même logique qu'à l'art. 15, le Conseil fédéral devrait mettre à disposition un système de copies de sécurité.

Proposition :

Art. 21 al. 1 : la Confédération met à disposition un système informatique dans lequel les titulaires de moyens de preuves électroniques peuvent en déposer une copie de sécurité pour qu'elle y soit conservée.

- **Art. 24 « Exploitation de l'infrastructure de confiance »** : L'UVS soutient la formulation proposée, mais souhaiterait apporter la précision suivante : une externalisation – partielle ou complète - de l'infrastructure vers des fournisseurs de services extérieurs à l'administration fédérale devrait être explicitement rendue impossible, ceci afin de préserver la souveraineté numérique de la Suisse.
- **Art. 8a, al. 2^{bis} Loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite (demande d'extrait)** : dans son commentaire de cette disposition, le Conseil fédéral cite les portails de la Confédération, des cantons et du secteur privé pour le dépôt d'une demande d'informations tirées du registre des poursuites. Or, certaines villes et communes disposent également d'un portail propre. Cela devra être précisé dans le message.

Union des villes suisses

Président

Anders Stokholm

Directeur

Martin Flügel

Copie Association des Communes suisses

Bundesrätin
Karin Keller-Sutter
Bundeshaus West
3003 Bern

Brugg, 5. August 2022

Zuständig: Martin Brugger
Dokument: SN SBV_E ID.docx

PDF und Word an:
rechtsinformatik@bj.admin.ch

Vernehmlassung des Schweizer Bauernverbandes zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter,
sehr geehrte Damen und Herren,

Mit Ihrem Schreiben vom 29. Juni 2022 laden Sie den Schweizer Bauernverband (SBV) ein, zur oben genannten Vorlage Stellung zu nehmen. Für die uns gegebene Möglichkeit danken wir Ihnen bestens und sind gerne bereit, uns in dieser Angelegenheit zu äussern.

Grundsätzliche Erwägungen

Der Schweizer Bauernverband vertritt die Interessen des Landwirtschaftssektors und der rund fünfzigtausend landwirtschaftlichen Betriebe und Bauernfamilien in der Schweiz.

Der Austausch von Daten zwischen Personen, Marktpartnern oder öffentlichen Behörden auf elektronischem Weg gehört bereits heute für Landwirtschaftsbetriebe zum Alltag. Je wichtiger die Authentizität von Informationen ist, desto wichtiger ist eine verlässliche und eindeutige Identifikation von Personen (und Betrieben). Eine einfach handhabbare, sichere und eindeutige Identifikation von natürlichen Personen auf der Basis einer zuverlässigen Vertrauensinfrastruktur ist für die weitere positive Entwicklung im elektronischen Verkehr und die rasch voranschreitende Digitalisierung eine Grundvoraussetzung.

Nach der deutlichen Ablehnung des Bundesgesetzes über elektronische Identifizierungsdienste in der Volksabstimmung vom 7. März 2021 erhielt der Bundesrat aus beiden Räten in diversen Motionen den Auftrag, für eine Neuauflage der rechtlichen Bestimmungen zu einer E-ID zu sorgen. Wir begrüssen, dass der Bundesrat dieses Heft rasch in die Hand nahm, und sind der Ansicht, dass mit der nun aufgelegten Gesetzesvorlage den wichtigsten Kritikpunkten, welche in der Abstimmung zur Ablehnung führten, begegnet wird – insbesondere, dass die Herausgabe der E-ID und die Schaffung der Vertrauensinfrastruktur als staatliche Aufgaben wahrgenommen werden.

Stellungnahme zu den einzelnen Bestimmungen

Der auf den Grundsätzen Datenschutz durch Technik, Datensicherheit, Datensparsamkeit und dezentrale Datenspeicherung beruhende Schutz der Persönlichkeit und der Grundrechte von Personen (Art. 1, Abs. 2) sorgt dafür, das nötige Vertrauen in ein solches System zu gewährleisten.

Der Bauernverband begrüsst insbesondere die Freiwilligkeit eine E-ID zu erstellen und Rückzug einer E-ID und die Wahlfreiheit zwischen Vorweisen einer E-ID oder anderen Ausweisdokumenten. (Art. 4, Art. 5 und Art. 10, Art. 16).

Seite 2 | 2

Wir begrüßen in der Vorlage, dass jede Person ihre E-ID in einer elektronischen Börse («Anwendung») selber verwalten kann (Art. 14) und diese vom Bund gestellt wird (Art. 19).

Für den Schweizer Bauernverband wertet auch positiv, dass das System gegenüber anderen elektronischen Nachweisen (3. Abschnitt) offen angedacht ist.

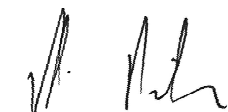
Schlussbemerkungen

Aus Sicht der Landwirtschaft begrüßen wir den Vorentwurf über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID). Wir vertreten die Ansicht, dass eine Umsetzung gemäss Vorlage für die Landwirtschaft und die ganze Gesellschaft förderlich ist, weil es den digitalen Verkehr mit Behörden vereinfacht, beziehungsweise überhaupt erst ermöglicht. Die Vorlage trägt auch dazu bei, die Rahmenbedingungen für die Digitalisierung in weiteren Projekten zu verbessern wie z.B. dem elektronischen Patientendossier oder dem digitalen Austausch von vertraulichen Daten zwischen privaten Akteuren.

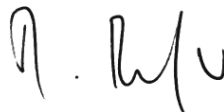
Wir hoffen, dass Sie unsere Anliegen berücksichtigen werden und danken Ihnen nochmals für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Schweizer Bauernverband



Markus Ritter
Präsident



Martin Rufer
Direktor

Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Rolf Rauschenbach
Bundeshaus West
3003 Bern

Per E-Mail an: rechtsinformatik@bj.admin.ch

19. Oktober 2022

Stellungnahme zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrter Herr Rauschenbach, sehr geehrte Damen und Herren

Wir beziehen uns auf die am 29. Juni 2022 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartements zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (VE-E-ID-Gesetz, VE-BGEID). Gestützt auf die Rückmeldungen unserer Mitglieder nehmen wir zum Vorschlag gerne wie folgt Stellung.

Zusammenfassung

Eine elektronische Identität erleichtert die Identifikation im Internet und den Austausch mit den staatlichen Behörden. Immer mehr Geschäfte werden heute online abgewickelt. Damit steigt das Bedürfnis nach einer sicheren, staatlich kontrollierten elektronischen Identität immer mehr. Die Schweiz ist eines der wenigen Industrieländer, welches noch über kein entsprechendes Instrument verfügt.

Da eine Überprüfung der Identität im Internet nur schwer möglich ist, benötigen Wirtschaft und Verwaltung und gerade auch die Bürgerinnen und Bürger schnell eine zuverlässige elektronische Möglichkeit zur Identifikation von Personen (E-ID). Dies ist schliesslich auch im Interesse aller, da bislang verwendete Alternativen wie die Logins grosser Plattformanbieter unsicherer sind und dabei Daten ins Ausland fliessen. Nach der Ablehnung des Bundesgesetzes über eine E-ID am 7. März 2021 hat der Bundesrat erfreulich schnell reagiert.

Er schlägt nun eine Lösung vor, welche die an der Urne zum Ausdruck gebrachten Bedenken der Bürgerinnen und Bürger aufgreift und es Nutzerinnen und Nutzern schnell und unkompliziert ermöglichen soll, sich digital auszuweisen. Alle Personen, die über eine Schweizer Identitätskarte, einen Schweizer Pass oder einen von der Schweiz ausgestellten Ausländerausweis verfügen, sollen eine E-ID beantragen können.

economiesuisse unterstützt den Vorschlag des Bundesrates in wesentlichen Punkten. Es besteht nur geringfügiger Anpassungsbedarf. Entscheidend ist in jedem Fall, dass der Vorschlag schnell und pragmatisch umgesetzt wird, damit die Schweiz möglichst zeitnah über eine E-ID verfügt.

Die aus unserer Sicht wichtigsten Anliegen lauten wie folgt:

- Das Gesetz ist als Rahmengesetz ausgestaltet. Damit muss es die wichtigsten Regulierungsgrundsätze auf ausreichender Abstraktionsstufe enthalten. Entscheidend ist dabei, dass die Umsetzung technologie-neutral ausgestaltet ist.
- Die Ausführungsbestimmungen, die in der Verordnung enthalten sein werden, müssen sodann angesichts der Komplexität der Materie zusammen mit Experten aus der Privatwirtschaft und Wissenschaft erstellt werden. Im Zentrum stehen hier die Sicherheit, die Anwenderfreundlichkeit und damit die Akzeptanz der Lösung im Verkehr.
- Die Regeln müssen mit anderen Gesetzen, welche eine Identifizierung vorsehen, abgestimmt sein. Dies gilt beispielsweise für den Bereich des Geldwäschereigesetzes oder den Bereich der digitalen Signaturen gemäss Bundesgesetz über die elektronische Signatur.
- Es darf keine Schweizer Insellösung geschaffen werden. Die internationale Interoperabilität und Anerkennung vergleichbarer ausländischer E-ID muss sichergestellt sein.
- Darüber hinaus gilt es Vertretungsrechte von natürlichen Personen an juristische Personen auf der E-ID der natürlichen Person abzubilden.

Bei allen Ansprüchen an Qualität sowohl auf Stufe Gesetz als auch Verordnung müssen die rechtlichen Grundlagen zeitnah und pragmatisch in die Praxis umgesetzt werden. Die Schweiz ist in dieser Frage bereits massiv im Hintertreffen.

1 Einleitende Bemerkungen

Die Schaffung einer E-ID mit der vorgesehenen, umfassenden staatlichen Vertrauensinfrastruktur und der Ermöglichung, dass Akteure sowohl des öffentlichen als auch des privaten Sektors die E-ID bzw. weitere elektronische Nachweise verwenden bzw. ausstellen können, ist sehr zu begrüßen. Die Wirtschaft begrüsst insbesondere das Ambitionsniveau, das mit der Vorlage nochmals bestärkt wird: Die E-ID soll keine starre Insellösung sein, sondern Teil eines dynamischen Ökosystems der digitalen Nachweise. Diese "Vision" sollte bei der Gestaltung der Rahmenbedingungen immer im Gedächtnis bleiben. Wichtig ist aus unserer Sicht zunächst eine schnelle und pragmatische Umsetzung der rechtlichen Grundlagen in die Praxis, damit die Schweiz in diesem Bereich nicht (noch weiter) ins Hintertreffen gerät. Zudem sollte die neue E-ID bei den Benutzerinnen und Benutzern rasch zum Standard werden. Deren Verwendung muss daher leicht zugänglich und verständlich, zuverlässig und weit verbreitet sein. Während wir die Vorlage im Wesentlichen unterstützen, möchten wir dennoch einzelne Verbesserungsvorschläge anbringen. Diese betreffen folgende Bereiche:

Vertretungsrechte an juristische Personen

Die E-ID ist richtigerweise nur für natürliche Personen konzipiert. Damit eine erwartungsgemäss wichtige Verwendungsform im Verkehr aber möglich ist, sollten auch allfällige Vertretungsrechte dieser natürlichen Personen an juristische Personen auf der E-ID der natürlichen Person abgebildet werden. Dies könnte insbesondere durch eine Verbindung des Basisregisters mit dem Handelsregister oder dem SHAB erfolgen.

Keine Schweizer Insellösung

Die Schweizer E-ID muss zwingend international operabel sein. Vergleichbare ausländische E-ID sollten in der Schweiz explizit anerkannt werden. In einer international ausgerichteten Volkswirtschaft und einem kleinen Land wie der Schweiz dürfen keine Insellösungen geschaffen werden. Es gilt, dass auch grenzüberschreitende Prozesse in diesem Bereich durch technische Lösungen vereinfacht werden.

Sicherung des breiten Vertrauens in die angebotene Lösung

Datenschutz und Datensicherheit: Dem Datenschutz sollte insbesondere in Bezug auf die Aufbewahrungsfristen noch mehr Rechnung getragen werden. Die vorgeschlagenen Fristen erachten wir als zu lange.

Technologieneutralität

Wir sehen in Bezug auf das Kriterium der Technologieneutralität bereits jetzt Anpassungsbedarf. So wird festgeschrieben, dass die neue E-ID durch kryptographische Verschlüsselung geschützt wird (vgl. Art. 17 VE-BGEID). Dabei werden technologisch überlegene Methoden, welche in Zukunft allenfalls verfügbar sind, nicht berücksichtigt. Die an sich gut gemeinte Formulierung in Art. 1 Abs. 2 Bst. c VE-BGEID, dass die E-ID dem Stand der Technik entsprechen muss, verhindert ebenfalls eine technologieneutrale Umsetzung.

Einbezug von Experten bei der Erarbeitung der Ausführungsbestimmungen

Von grosser Relevanz werden die Ausführungsbestimmungen zum Rahmengesetz sein, die in der Verordnung spezifiziert werden. Bei deren Erarbeitung ist ein enger Einbezug der Wirtschaft und der Forschung zwingend, damit die E-ID in Bezug auf ihre konkrete Anwendung, Sicherheit und Nutzerfreundlichkeit funktioniert und eine breite Akzeptanz entwickeln kann. Gleichzeitig gilt es die Prozesse zum Einbezug solcher Spezialitäten derart auszugestalten, dass eine effiziente Arbeit ermöglicht wird und das Inkrafttreten der neuen Bestimmungen und damit die Verfügbarkeit der E-ID möglichst zeitnah erfolgen kann.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse



Erich Herzog
Mitglied der Geschäftsleitung



Lukas Federer
Projektleiter Infrastruktur



Office fédérale de la justice
Département fédéral de justice et police DFJP
3003 Berne

rechtsinformatik@bj.admin.ch

Berne, le 18 octobre 2022 usam-MH/cp

Réponse à la procédure de consultation :

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID)

Madame, Monsieur,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et plus de 600 000 PME, soit 99,8% des entreprises de notre pays. La plus grande organisation faîtière de l'économie suisse s'engage sans répit pour l'aménagement d'un environnement économique et politique favorable au développement des petites et moyennes entreprises.

Le 29 juin 2022, l'Office fédéral de la justice nous a convié à prendre position dans le cadre de la procédure de consultation sur l'avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID).

L'usam plaide pour une mise en place rapide de l'e-ID avec les moyens technologies à la pointe du savoir-faire en matière d'authentification. Ceci suppose que l'administration fédérale collabore activement avec le secteur privé pour qu'une solution efficace, *user friendly* et sûre voit le jour au plus vite. Les technologies choisies doivent être communiqué rapidement à l'économie privée afin qu'elle puisse mettre en place les infrastructures informatiques correspondantes.

I. Point de situation

L'usam se présente pour une e-ID portée par les compétences et le savoir du secteur privé. L'e-ID a malheureusement échoué dans les urnes en 2021, raison pour laquelle l'administration fédérale présente ici une copie en stipulant que l'Etat a le contrôle sur les données d'identification des citoyens suisses.

L'économie privée attend impatiemment que le dossier de la numérisation avance rapidement. L'enjeu consiste à enfin satisfaire la demande des milieux économiques de pouvoir pleinement saisir les chances de l'authentification numérique d'un bout à l'autre des chaînes de commercialisation des biens et services pour tous les usagers potentiels. Sans cet instrument de l'e-ID et la possibilité générale d'utiliser une signature électronique qualifiée, l'économie suisse risque de prendre un retard conséquent sur le dossier de la numérisation, ce qui se traduirait concrètement par un manque d'attractivité ainsi qu'une baisse de la compétitivité internationale de nos entreprises par rapport aux autres pays.

II. Appréciation de l'usam

A l'avis de l'usam, l'e-ID ne pourra pousser la numérisation de la Suisse et devenir un facteur d'implantation important pour l'économie Suisse qu'à la condition qu'elle soit largement diffusée et facilement utilisable. Cela suppose que les domaines suivants doivent également être couverts par l'e-ID ou les autres moyens de preuve électroniques :

- l'interopérabilité des technologies sous-jacentes à la mise en place de l'e-ID doivent être impérativement garantie au niveau international ;
- les normes technologiques doivent correspondre entre aux standards internationaux sans faire le moindre compromis quant à la sécurité et la protection de la sphère privée ;
- l'e-ID doit également servir à la signature de contrat ;
- la signature électronique qualifiée doit parallèlement être mise en place ;
- une procédure d'identification standardisée doit obligatoirement être mise en place pour les personnes sans e-ID.

Concernant l'art. 19 « Application pour la conservation et la présentation des justificatifs électroniques », il faudrait exploiter toute la portée de l'écosystème, à savoir que l'e-ID devient une preuve numérique de base pour de nombreuses autres preuves numériques (p. ex. billet pour une manifestation, titre de transports publics, carte de membre, carnet de vaccination d'un animal de compagnie, permis de circulation ou rapport du contrôle technique réussi d'un véhicule, etc.). En plus du portefeuille électronique de l'Etat, les utilisateurs doivent pouvoir, selon les explications relatives à l'art. 19, utiliser d'autres applications pour la conservation et la présentation de leurs justificatifs électroniques. L'usam exige à cet égard d'inscrire dans la loi l'utilisation de portefeuilles électroniques proposés par des acteurs privés, afin de démontrer l'équivalence des solutions privées correspondantes et d'en favoriser ainsi leur acceptation. Si tel n'est pas le cas, l'Etat pourrait tirer tous les compétences de gestion de données d'identité électronique à soi, ce que l'usam refuse catégoriquement au motif de la protection de la sphère privée.

L'article 16, alinéa 1, de l'avant-projet relatif à la présentation de preuves électroniques ne mentionne pas explicitement le principe de protection des données concernant l'utilisation de preuves numériques ; ailleurs aussi, on se réfère au fait que les principes généraux relatifs à la protection des données personnelles ne doivent pas être répétés dans le LeID pour rester valables. En effet, le principe de minimisation des données prévu par le droit de la protection des données exige que le traitement des données personnelles soit proportionné à la finalité et limité à ce qui est nécessaire aux fins du traitement. En conséquence, le droit de la protection des données impose des limites aux vérificateurs potentiels dans le choix des preuves qu'ils peuvent exiger pour accéder à leurs services, qu'il serait plus circonspect d'intégrer dans le projet de loi pour en augmenter l'acceptabilité générale.

L'usam salue l'article 9 alinéa 4 de la « Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques » qui stipule que la preuve d'identité lors de l'enregistrement pour la signature électronique qualifiée pourra être apportée par une preuve d'identité électronique en général. Il ne faut toutefois pas oublier que, même pour les personnes n'ayant pas d'e-ID, la signature électronique qualifiée doit être facilement proposée. Il y a certes une signature électronique légalement admissible, qui est assimilée à la signature manuscrite (art. 14 al. 2 bis CO). Cependant, les exigences posées à la signature électronique qualifiée selon ZertES sont si élevées qu'elle ne s'est pas encore imposée en pratique, que ce soit auprès des particuliers ou des entreprises. Cela s'explique notamment par le fait que la signature électronique qualifiée selon ZertES engendre des coûts conséquents pour l'entreprise et implique un effort organisationnel et technique important. Même si les signatures électroniques devaient largement s'imposer auprès des entreprises, la pénétration du marché quasi inexistante chez les particuliers représenterait toujours un obstacle au commerce numérique. Dans cette optique, l'usam exige que la nouvelle loi fédérale sur

les services d'identification électronique (loi E-ID) tiennent compte de ce problème et y remédient, en intégrant la signature électronique qualifiée selon ZertES au processus de l'e-ID, respectivement en facilitant grandement l'accès à la signature électronique qualifiée pour les particuliers (processus, coût, etc.). Aussi longtemps que les contrats exigeront encore une signature manuscrite, les milieux économiques et la société en général seront privés de la possibilité de travailler et de faire des affaires de manière numérique et devront donc continuer à imprimer, à signer et à envoyer par la poste les documents contractuels.

Finalement, l'avant-projet en reste aux valeurs juridiques de la caractérisation de l'e-ID, il est toutefois primordial que les milieux économiques puissent être immédiatement informés des détails lisibles de la technologie choisie pour l'e-ID. Les PME doivent en effet pouvoir se préparer à l'avance à un développement rapide de systèmes compatibles avec la nouvelle e-ID.

II. Conclusion

L'usam exige que la transformation numérique au sein des autorités publiques conduise à des allègements dans les procédures administratives. A ce titre, cet avant-projet e-ID et des moyens de preuve électroniques est une pierre angulaire qu'il faudrait pouvoir étendre au maximum dans les procédures nécessitant l'authentification et ce, dans les meilleurs délais. Toutes les bases légales portant sur l'identification doivent être adaptées à ces nouvelles dimensions numériques.

Le projet présente cependant trois écueils : le portefeuille étatique de l'e-ID ne doit pas occulter la mise en place de l'utilisation de portefeuilles électroniques proposés par des acteurs privés, la signature électronique qualifiée doit impérativement devenir facilement utilisable et la technologie choisie doit impérativement être partagée à l'avance avec l'économie privée.

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Madame, Monsieur, nos respectueuses salutations.

Union suisse des arts et métiers usam



Hans-Ulrich Bigler
Directeur



Mikael Huber
Responsable du dossier

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
3003 Bern

per Mail an:
rechtsinformatik@bj.admin.ch

Bern, 19. Oktober 2022

E-ID-Gesetz: Vernehmlassung

Sehr geehrte Frau Bundesrätin

Besten Dank für die Einladung zur oben erwähnten Vernehmlassung. Der Schweizerische Gewerkschaftsbund (SGB) nimmt dazu im Folgenden gerne Stellung.

Nach der Ablehnung des auch von den Gewerkschaften mit einer Kampagne bekämpften "Bundesgesetzes über elektronische Identifizierungsdienste" durch die Stimmbevölkerung hat sich der SGB am 7. März 2021 wie folgt geäußert:

*"Mit dem heute zur Abstimmung vorgelegten E-ID-Gesetz hätte der Staat eine seiner zentralen Aufgaben – die Identifizierung der eigenen BürgerInnen – zugunsten privater Akteure aufgegeben. Unter dem Vorwand der Modernisierung hätte dies zur Schaffung eines privaten Monopols oder Oligopols geführt, das mit den von der Bundesverwaltung bereitgestellten Daten Profite macht. [...] **Es ist Aufgabe des Staates und nicht der Banken und Versicherungen, die Identität der BürgerInnen zu bescheinigen:** Die Botschaft der Stimmbevölkerung ist in diesem Punkt völlig eindeutig. Darum braucht es nun schnell eine amtliche elektronische Identifizierung, die öffentlich und transparent ist und dem öffentlichen Interesse dient. Eine solche, für alle zugängliche Grundversorgung ist ein wichtiger Schritt in Richtung einer gerechten Digitalisierung und wird auch der Schweizer Wirtschaft nützen."*

Mit dem aktuellen Vorliegen des Entwurfs über ein "Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise" können wir nun erfreut feststellen, dass der **Bundesrat aus der vergangenen Abstimmungsniederlage die richtigen Lehren gezogen** und darauf aufbauend schnell eine umfassende neue Vorlage über ein E-ID-Gesetz ausgearbeitet hat. **Absolut zentral dabei ist erstens, dass der Staat mit dem neuen Gesetz alleiniger Herausgeber der E-ID werden wird** und auch die für deren Verwendung und Verbreitung benötigten "Vertrauensinfrastruktur zur Verfügung stellt", wohingegen es dem Bund gemäss abgelehntem E-ID-Gesetz sogar explizit verboten gewesen wäre, nur schon eine eigene E-ID auszugeben. **Die neue Vorlage genügt zweitens überwiegend auch den wichtigen Forderungen der sechs gleichlautenden, vom Parlament überwiesenen Motionen** mit dem

Titel "*Vertrauenswürdige staatliche E-ID*" (21.3124-29), welche für eine neue E-ID insbesondere die drei Grundsätze der Datensparsamkeit, der dezentralen Datenspeicherung sowie des Datenschutzes durch Technik (*privacy by design*) festlegen. **Drittens ist es von entscheidender Bedeutung, dass dieser Vorentwurf auch die Entwicklungen auf europäischer Ebene massgebend berücksichtigt** und insbesondere mit der eIDAS-Verordnung der Europäischen Union kompatibel ist und somit die Interoperabilität mit den elektronischen Identitätsnachweisen der Europäischen Union grundsätzlich – beziehungsweise technisch – gewährleisten kann.

Trotz dieser grundsätzlich wohlwollenden Zustimmung zur neuen Vorlage, erachten wir den Schutz der Persönlichkeit und der Personendaten im vorliegenden Gesetzesentwurf als noch unzureichend umgesetzt. Die gesetzlich vorgesehene Erhebung von Daten sowie ihre Bearbeitung muss jeweils zwingend auf das zu ihrem Zweck unbedingt Erforderliche reduziert werden, das Wort "Datenschutz" erscheint im vorliegenden E-BGEID allerdings lediglich zweimal. Letzteres ist zwar namentlich deshalb der Fall, weil grundsätzlich auch im Bereich des elektronischen Identitätsnachweises sämtliche Bestimmungen des kürzlich revidierten Bundesgesetzes über den Datenschutz (DSG) Anwendung finden, jedoch ist genau dies aus zwei Gründen unzureichend: Erstens handelt es sich bei Personendaten, welche in Bezug auf einen elektronischen amtlichen Nachweis erhoben und verarbeitet werden um eine neue, besonders schützenswerte und vom DSG nur unzureichend erfasste Datenkategorie und zweitens geht das Schweizer DSG bewusst ganz grundsätzlich weniger weit als die entsprechend relevante neue EU-Richtlinie DSGVO (mit welcher die E-ID ja – gemäss anderweitiger Ausführungen im Erläuternden Bericht – kompatibel sein soll). **Vor diesem Hintergrund unterstützen wir die von der Digitalen Gesellschaft in ihrer Stellungnahme gemachten Vorschläge für die Ergänzung des Vierten Abschnittes des Gesetzesentwurfs um einen Artikel 16^{bis} "Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang" sowie einen Artikel 16^{ter} "Informations- und Zustimmungspflicht; Widerrufsrecht".**

Darüber hinaus sehen wir bei weiteren Artikeln des vorliegenden Gesetzesentwurfes Anpassungsbedarf und nehmen im Folgenden spezifisch dazu Stellung:

- **Art. 2 Abs. 2, ergänzende Daten:** Die Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde sowie die Angaben zum Ausstellungsprozess sind für die Ausstellung und Verwendung der E-ID nicht erforderlich und stellen somit Daten dar, die nicht Teil der E-ID sein sollten; die Buchstaben e und f sind daher zu streichen. Was die – bezüglich Datenschutz und -sarsamkeit keineswegs unproblematische – Verwendung der AHV-Nummer als singulären numerischen Identifikator betrifft, regen wir alternativ an, die Einführung eine neuen "**E-ID-Nummer**" zu prüfen.
- **Art. 3, Persönliche Voraussetzungen:** Gemäss Erläuterndem Bericht sollen Anbieterinnen die Möglichkeit haben, die Nutzung ihrer Dienste für die InhaberInnen gewisser Ausweiskategorien zu beschränken. Dies deshalb, weil bei Ausweisen der Kategorien N, F, S und Ci nicht davon ausgegangen werden könne, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. Dazu ist erstens anzumerken, dass die **Verlässlichkeit der Identifizierung einer Person nicht aus der Kategorie ihres Ausweises ersichtlich** ist und dass zweitens der Anwendungssperimeter der E-ID diskriminierungsfrei zu erfolgen hat. Allfällige

Einschränkungen müssen deshalb spezifisch begründet und im Gesetz ausdrücklich aufgeführt sein. Letzteres wird im Erläuternden Bericht zwar auch ausgeführt, nur fehlt im Vorentwurf die gesetzliche Bestimmung dazu. Darüber hinaus sei an dieser Stelle grundsätzlich angemerkt, dass gemäss den vorgeschlagenen Bestimmungen nur Personen Anrecht auf eine E-ID haben, welche in der Schweiz über eine Aufenthaltsbewilligung verfügen. Dies schliesst alle Personen aus, welche sich unter einem anderen Titel als einer ordentlichen Aufenthaltsbewilligung in der (digitalen) Schweiz aufhalten. Das Gesetz könnte eine Möglichkeit vorsehen, dass bei genügender Identifikation (etwa über einen ausländischen Pass) ebenfalls eine E-ID ausgestellt werden kann.

- **Art. 4, Ausstellung:** Gemäss Abs. 2 sollen Minderjährige ab dem 15. Altersjahr die E-ID eigenständig beantragen können, wohingegen physische Ausweisdokumente gemäss Ausweisgesetz nur von Volljährigen bezogen werden können. Es ist uns kein Grund ersichtlich, weshalb für den Bezug einer E-ID – an die die genannten hohen Sicherheitsanforderungen gestellt werden – eine tiefere Altersgrenze gelten soll, weshalb wir deren **Anpassung an die Volljährigkeit** fordern.
- **Art. 6, Gültigkeitsdauer:** Gemäss diesem Artikel ist die E-ID befristet gültig, wobei der Bundesrat die genaue **Gültigkeitsdauer** regelt. Letzteres können wir nicht nachvollziehen und fordern stattdessen **eine klare gesetzliche Bestimmung**, dass die Gültigkeitsdauer der E-ID jener des Dokuments entsprechen muss, das für deren Ausstellung verwendet wurde.
- **Art. 9, Pflicht zur Akzeptanz der E-ID:** Die E-ID muss gemäss diesem Artikel von *"jeder Behörde oder anderen Stelle, die öffentliche Aufgaben erfüllt"* akzeptiert werden, was grundsätzlich zu begrüssen ist. Wir wünschen uns aber auf Verordnungsebene eine möglichst **klare und weitgehende Definition dieser "anderen Stellen"**. Beispielsweise könnte festgelegt werden, dass alle Stellen beziehungsweise alle Unternehmen, deren Dienstleistungen sich teilweise über öffentliche Gelder finanzieren, zur Akzeptanz der E-ID verpflichtet sind.
- **Art. 24, Betrieb der Vertrauensinfrastruktur:** Gemäss diesem Artikel soll die Vertrauensinfrastruktur durch *"eine Leistungserbringerin innerhalb der Bundesverwaltung"* betrieben werden. Wir wünschen uns hierzu ebenfalls mehr Klarheit und **bestenfalls die direkte gesetzlich Definition der zuständigen Leistungserbringerin**. Vor dem Hintergrund der mittlerweile klar geregelten Verantwortlichkeiten innerhalb der "digitalen Bundesverwaltung" müsste dies eigentlich möglich sein.
- **EPDG Art. 11 Bst c, Zertifizierungspflicht:** Die im Erläuternden Bericht zu diesem Artikel des Bundesgesetzes über das elektronische Patientendossier gemachte Aussage, dass langfristig auch dieses Identifikationsmittel vom Bund herausgegeben werden soll, ist sehr positiv. Nur ist der neue, vom Bund und den Kantonen vorgesehene **Zeitplan für die Einführung eines funktionierenden und vertrauenswürdigen elektronischen Patientendossiers zu Recht ambitioniert**, weshalb hier – auch vor dem Hintergrund von dessen grundsätzlich hoher Dringlichkeit – keineswegs von "Langfristigkeit" gesprochen werden sollte.

In diesem Sinne hoffen wir auf die Berücksichtigung unserer Stellungnahme und danken Ihnen herzlich.

Freundliche Grüsse

SCHWEIZERISCHER GEWERKSCHAFTSBUND



Pierre-Yves Maillard
Präsident



Reto Wyss
Zentralsekretär

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundeshaus West
3003 Bern

Per Mail zugestellt an: rechtsinformatik@bj.admin.ch

Basel, 20. Oktober 2022
RHE / NGR I +41 58 330 62 51

Stellungnahme zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (VE-E-ID-Gesetz, VE-BGEID)

Sehr geehrte Frau Bundesrätin,
sehr geehrte Damen und Herren

Wir beziehen uns auf die am 29. Juni 2022 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartements zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (VE-E-ID-Gesetz, VE-BGEID).

Wir bedanken uns bestens für die Konsultation in dieser für die Finanzbranche wichtigen Vernehmlassung. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen nachfolgend unsere Anliegen.

Die aus unserer Sicht wichtigsten Anliegen lauten wie folgt:

- Der VE-BGEID muss als **Rahmengesetz** die wichtigsten Regulierungsgrundsätze enthalten, die eine **allgemeine Tragweite haben** und **technologieneutral** ausgestaltet sind. Von entscheidender Bedeutung sind die **Ausführungsbestimmungen**, die in der Verordnung enthalten sein werden. Bei der Erarbeitung derselben sind angesichts der Komplexität der Materie **Experten aus der Privatwirtschaft und Wissenschaft beizuziehen**.
- Die rechtlichen Grundlagen sollten **schnell und pragmatisch in die Praxis umgesetzt** werden, damit die Schweiz in diesem Bereich nicht (noch weiter) ins Hintertreffen gerät.
- Die **Konsistenz mit anderen Gesetzen**, welche eine Identifizierung vorsehen, muss sichergestellt werden, namentlich im Bereich des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG) und im Bereich der digitalen Signaturen gemäss Bundesgesetz über die elektronische Signatur (ZertES).

• Swiss Banking

- Die **internationale Interoperabilität** und **Anerkennung** vergleichbarer ausländischer E-ID in der Schweiz und vice versa soll sichergestellt werden.
- Allfällige **Vertretungsrechte von natürlichen Personen an juristischen Personen** sollten auf der E-ID der natürlichen Person abgebildet werden.

A. Grundsätzliche Bemerkungen

Die Schaffung einer E-ID mit der vorgesehenen, **umfassenden staatlichen Vertrauensinfrastruktur** und der Ermöglichung, dass **Akteure sowohl des öffentlichen als auch des privaten Sektors** die E-ID bzw. weitere elektronische Nachweise verwenden bzw. ausstellen können, ist sehr zu begrüßen.

Wichtig ist aus unserer Sicht eine **schnelle und pragmatische Umsetzung der rechtlichen Grundlagen** in die Praxis, damit die Schweiz in diesem Bereich nicht (noch weiter) ins Hintertreffen gerät. Zudem sollte die neue E-ID bei den Benutzerinnen und Benutzern **rasch zum Standard werden**. Deren Verwendung muss daher **leicht zugänglich und verständlich, zuverlässig** und **weit verbreitet** sein.

Während wir die Vorlage im Wesentlichen unterstützen, möchten wir dennoch **einzelne Verbesserungsvorschläge** anbringen. Diese betreffen folgende Bereiche:

- **Förderung der E-ID und der Entwicklung neuer Geschäftsmodelle:** Ein staatlich anerkannter elektronischer Nachweis ist auch ein wichtiger Baustein von innovativen Geschäftsmodellen, namentlich von solchen, die von privatwirtschaftlichen Akteuren entwickelt werden. In diesem Sinne sollte die aktive Förderung der Akzeptanz und Weiterentwicklung der E-ID als Zweckbestimmung im Gesetz festgehalten werden (siehe nachfolgend Ziffer B.1).
- **Abbildung von Vertretungsrechten an juristischen Personen:** Auch wenn die E-ID richtigerweise nur für natürliche Personen konzipiert ist, müsste es aus unserer Sicht dennoch möglich sein, auch allfällige Vertretungsrechte dieser natürlichen Personen an juristischen Personen auf der E-ID (der natürlichen Person) abzubilden, allenfalls durch eine Verbindung des Basisregisters mit dem Handelsregister und/oder dem SHAB (siehe nachfolgend Ziffer B.2).
- **Gültigkeitsdauer der E-ID:** Die Gültigkeitsdauer der E-ID darf jene des Identitäts- oder Legitimationsdokuments, welches im Rahmen der Ausstellung der E-ID verwendet wurde, nicht überschreiten. Zudem sollte die zeitliche Kontinuität der Gültigkeit einer E-ID gewährleistet werden, d.h. ein zu einem bestimmten Zeitpunkt überprüfter und zertifizierter Ausweis soll beispielsweise auch 10 Jahre später als überprüft und zertifiziert gelten (siehe nachfolgend Ziffer B.3).
- **Internationale Interoperabilität:** Vergleichbare ausländische E-ID sollten in der Schweiz explizit anerkannt werden. In einer international verwobenen Wirtschaft ist es unabdingbar, dass die Prozesse auch in diesem Bereich durch technische Lösungen vereinfacht werden (siehe nachfolgend Ziffer B.4).
- **Datenschutz und Datensicherheit:** Dem Datenschutz sollte insbesondere in Bezug auf die Aufbewahrungsfristen noch mehr Rechnung getragen werden. Die vorgeschlagenen Fristen erachten wir als zu lange (siehe nachfolgend Ziffer B.5)

• Swiss Banking

- **Vorweisen von elektronischen Nachweisen:** Es sollte festgehalten werden, dass der Aussteller weder einen Nachweis noch spezifische Daten für die Validierung aufbewahren darf. Zudem eröffnet der Wortlaut der Vorschrift der Betreiberin der Systeme über den gewählten Begriff «möglichst» die Möglichkeit, einen Rückschluss zur Verwendung des elektronischen Nachweises ziehen zu können (siehe nachfolgend Ziffer B.6).
- **Rechtssicherheit und Verantwortlichkeit:** Die Folgen des Missbrauchs der E-ID sowie weiterer elektronischer Nachweise sind im Gesetz nur marginal geregelt. Vor diesem Hintergrund schlagen wir vor, im Gesetz eine Haftungsnorm aufzunehmen. Zudem soll auch über die privaten Identifikatoren und Nachweise eine gewisse Kontrolle bestehen, weshalb dies im Gesetz besser reflektiert werden sollte (siehe nachfolgend Ziffer B.7).
- **Konsequente Umsetzung der Technologieneutralität:** Zukünftige Entwicklungen sollten weder vorweggenommen noch durch ein zu eng formuliertes Gesetz verhindert werden. Wir sehen diesbezüglich vereinzelt noch Verbesserungspotenzial (siehe nachfolgend Ziffer B.8).
- **Weitere Verbesserungsvorschläge:** Wir schlagen Ergänzungen zu Form und Inhalt, Akzeptanz und Vorweisung einer E-ID sowie der Ausstellung anderer elektronischer Nachweise, der Nutzung von elektronischen Nachweisen und der Verbesserung in Bezug auf die Vertrauensinfrastruktur vor (siehe nachfolgend Ziffer B.9).
- **Änderung weiterer Erlasse** (siehe nachfolgend Ziffer B.10).
 - **Verwendung der E-ID im Finanzsektor:** Die Schaffung der E-ID kann im Finanzbereich (vor allem beim Onboarding) viel Effizienz schaffen. Entsprechend sollten bereits mit dem BGEID die entsprechenden expliziten rechtlichen Grundlagen im Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG) geschaffen werden.
 - **Abstimmung mit dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate** (Bundesgesetz über die elektronische Signatur, ZertES): Die Voraussetzungen zur Erlangung einer E-ID und einer qualifizierten elektronischen Signatur (QES) müssen aufeinander abgestimmt werden. Die Identifizierung mit der E-ID muss der Identifikation durch persönliches Erscheinen gleichgestellt sein.
- **Periodische Überprüfung:** Der Sicherheitsaspekt, insbesondere im Bereich der Cybersicherheit, muss selbstverständlich eine kontinuierliche Priorität bleiben. Dies nicht nur bei der Einführung der elektronischen Identität, sondern auch während ihrer gesamten Anwendung. Die angewandten Standards müssen regelmässig überprüft werden, um einen hohen Schutz der Privatsphäre und eine hohe Widerstandsfähigkeit gegen Cyberangriffe zu gewährleisten (siehe nachfolgend Ziffer B.11).

Wir erlauben uns schliesslich den Hinweis, dass der VE-BGEID ein **Rahmengesetz** ist, das die wichtigsten Regulierungsgrundsätze im Zusammenhang mit der elektronischen Identität enthalten muss. Diese haben daher eine **allgemeine Tragweite** und müssen **technologieneutral** sein. Von noch grösserer Bedeutung sind hingegen die **Ausführungsbestimmungen**, die in der Verordnung enthalten sein werden. Bei der Erarbeitung derselben sind angesichts der Komplexität der Materie **Experten aus der Privatwirtschaft und Wissenschaft beizuziehen** (siehe nachfolgend Ziffer B.12).

B. Im Einzelnen

1. Förderung der E-ID und der Entwicklung neuer Geschäftsmodelle

Damit eine staatlich anerkannte elektronische Identität rasch in der Breite angewandt wird, muss sie einfach erhältlich sowie weit verbreitet und akzeptiert sein. Die aktive Förderung der Akzeptanz und Weiterentwicklung der E-ID sollte daher im Zweck des Gesetzes festgehalten werden.

Ein staatlich anerkannter elektronischer Nachweis ist auch ein wichtiger Baustein von zukünftigen innovativen Geschäftsmodellen, namentlich von solchen, die von privatwirtschaftlichen Akteuren entwickelt werden. Innovative Geschäftsmodelle sollten wo immer möglich und sinnvoll weiter gefördert werden und entsprechend als Zweckbestimmung im Gesetz festgehalten werden. Wir schlagen folgende Ergänzung im Gesetzestext vor:

Art. 1 Abs. 2 VE-BGEID

[...]

² Es hat zum Zweck:

[...]

e. die Akzeptanz und Weiterentwicklung der E-ID sowie auf der E-ID basierende Geschäftsmodelle laufend zu fördern.

2. Vertretungsrechte an juristischen Personen

Die digitale Abbildung der Vertretungsrechte für eine juristische Person entspricht einem grossen Bedürfnis der Wirtschaft. Während eine E-ID für juristische Personen kaum zu realisieren ist, wäre es dennoch denkbar, solche Vertretungsrechte auf der E-ID der natürlichen Personen abzubilden und entsprechend im Basisregister als Nachweis einzutragen. Vorstellbar wäre dabei, das Basisregister mit HR und SHAB zu verbinden, damit die entsprechenden Identifikatoren im Register abgebildet werden können. Eine solche Lösung würde den Schweizer Standort bezüglich Digitalisierung wesentlich stärken und wäre zudem auch im Interesse der Verbreitung der E-ID, da man diese nicht nur für private, sondern auch für kommerzielle Zwecke einsetzen könnte. Wir schlagen daher eine Ergänzung von Art. 1 Abs. 1 VE-BGEID sowie einen neuen Art. 12bis VE-BGEID vor:

Art. 1 Abs. 1 VE-BGEID

¹ Dieses Gesetz regelt:

- a. den staatlichen elektronischen Identitätsnachweis natürlicher Personen (E-ID) und andere elektronische Nachweise;
- b. die Infrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen (Vertrauensinfrastruktur);
- c. die Rollen und Verantwortlichkeiten bei der Bereitstellung und Nutzung dieser Infrastruktur.

d. den Nachweis der Vertretungsrechte an juristischen Personen.

[...]

Art. 12bis VE-BGEID (neu)

Vertretungsrechte an juristischen Personen, können als Nachweise auf der E-ID geführt werden. Der Bundesrat regelt die Einzelheiten, insbesondere den dafür notwendigen Datenaustausch zwischen den Handelsregistern und dem Basisregister gemäss diesem Gesetz.

3. Gültigkeitsdauer der E-ID

Es ist aus unserer Sicht sehr wichtig, dass die Gültigkeitsdauer der E-ID gemäss Art. 6 VE-BGEID die Gültigkeitsdauer des Identitäts- oder Legitimationsdokuments, das im Rahmen der Ausstellung/Erstellung der E-ID verwendet wurde, nicht überschreiten darf.

Zudem ist sicherzustellen, dass auch die zeitliche Kontinuität der Gültigkeit einer E-ID gewährleistet werden kann, das heisst, dass ein zu einem bestimmten Zeitpunkt überprüfter und zertifizierter Ausweis auch zum Beispiel 10 Jahre später als überprüft und zertifiziert gilt. Es sollte eine Vorgabe bestehen, dass ein entsprechendes technisches Verfahren vorhanden sein muss, analog zur heutigen Long Term Validation (LTV) im Bereich der elektronischen Signaturen.

4. Internationale Interoperabilität

Die Interoperabilität mit vergleichbaren ausländischen E-ID-Lösungen ist für die international stark verbundene Schweizer Wirtschaft wichtig. Damit könnten die ohnehin schon komplexen grenzüberschreitenden Wirtschaftsprozesse zumindest in diesem Bereich vereinfacht werden. In Frage für eine Anerkennung kämen dabei insbesondere die nach der eIDAS ausgestellten Identitäten in der EU. Wir schlagen daher vor, die Anerkennung und Herstellung der Interoperabilität mit vergleichbaren ausländischen E-ID-Systemen bereits bei der Zielsetzung des Gesetzes aufzunehmen und Art. 1 VE-BGEID entsprechend zu ergänzen.

Aus unserer Sicht käme zudem eine einseitige Anerkennung durch die Schweiz in Frage (vgl. Art. 27 VE-BGEID). Dies könnte relativ unkompliziert geschehen. Ein Staatsvertrag wäre dazu nicht notwendig. Art. 27 VE-BGEID müsste daher entsprechend erweitert und dem Bundesrat die Kompetenz einer einseitigen Anerkennung eingeräumt werden.

Wir schlagen vor, Art. 1 Abs. 2 VE-BGEID und Art. 27 VE-BGEID (inkl. Überschrift des 7. Abschnitts) wie folgt zu ergänzen resp. anzupassen:

Art. 1 Abs. 2 VE-BGEID

[...]

² Es hat zum Zweck:

[...]

f. Interoperabilität und Anerkennung mit vergleichbaren ausländischen Identitätsnachweisen sicherzustellen.

7. Abschnitt: Internationale ~~Abkommen~~Anerkennung

Art. 27 VE-BGEID

[...]

³ Der Bundesrat kann vergleichbare ausländische E-ID anerkennen.

5. Datenschutz und Datensicherheit

5.1 Widerruf einer E-ID und anderer elektronischer Nachweise

Der Widerruf einer E-ID (nach Art. 5 VE-BGEID) und anderer elektronischer Nachweise (Art. 13 VE-BGEID) sollte auch bei einer betrügerischen Erlangung der E-ID resp. des elektronischen Nachweises und nicht nur bei Missbrauch der E-ID resp. des elektronischen Nachweises möglich sein. Eine betrügerisch erlangte E-ID ebenso wie deren Missbrauch rechtfertigen auf jeden Fall deren Widerruf. Art. 5 und Art. 13 VE-BGEID sind daher wie folgt zu ergänzen:

Art. 5 lit. f VE-BGEID

[...]

f. der begründete Verdacht besteht, dass die E-ID betrügerisch erlangt wurde.

Art. 13 Abs. 2 lit. d VE-BGEID

[...]

d. der begründete Verdacht besteht, dass der elektronische Nachweis betrügerisch erlangt wurde.

5.2 Sorgfaltspflichten

Im dezentralen System kommt den Sorgfaltspflichten der Inhaberinnen und Inhaber besondere Bedeutung zu. Sie sind damit selber verantwortlich für die Sicherheit der E-ID-Träger und der darauf gespeicherten Daten, gerade weil diese dezentral, d.h. bei der Nutzerin oder beim Nutzer gespeichert werden. Entsprechend müssten diese Pflichten der Inhaberinnen und Inhaber genauer definiert werden. Diese müssen genau wissen, welche Sorgfaltspflichten sie treffen. Wir schlagen daher folgende Ergänzung von Art. 7 Abs. 1 VE-BGEID vor:

Art. 7 VE-BGEID

¹ Die Inhaberin oder der Inhaber einer E-ID muss die notwendigen und zumutbaren Massnahmen treffen, damit ihre oder seine E-ID nicht missbräuchlich verwendet werden kann. Der Bundesrat regelt die notwendigen Massnahmen, welche die E-ID Träger ausreichend schützen.

5.3 Aufbewahrungsfristen

Gemäss Art. 11 Abs. 5 BGEID obliegt dem Bund die Kompetenz zur Regelung der Aufbewahrungsfrist der E-ID. Eine solche Aufbewahrung soll gemäss BGEID höchstens bis fünf Jahre nach Ablauf oder Widerruf der E-ID gestattet sein. Laut Erläuterungsbericht (vgl. Seite 11) verfolgt die Datenaufbewahrung den Zweck, «*all-fällige Fälle von Missbrauch untersuchen zu können*».

Erklärungsbedürftig erscheint uns, weshalb die Daten noch weitere fünf Jahre nach Ablauf der E-ID aufbewahrt werden sollen, wenn der ursprüngliche Zweck bereits erloschen ist. Auch erscheint uns eine Aufbewahrungsfrist von 5 Jahren grundsätzlich zu lang. Wir sehen keine Rechtfertigung für eine über ein Jahr dauernde Frist. So sind beispielsweise Randdaten des Fernmeldeverkehrs durch die Anbieterinnen von Fernmeldediensten während 6 Monaten aufzubewahren (siehe Art. 26 Abs. 5 BÜPF).

Aus unserer Sicht sollte die Datenerhebung Anknüpfungspunkt für den Beginn der Frist sein und nicht der Ablauf oder der Widerruf der E-ID. Nur Daten, die zum Betrieb der E-ID notwendig sind, sollen selbstverständlich während der Gültigkeit der E-ID weiter aufbewahrt werden dürfen, allerdings erscheint auch hier eine Aufbewahrung von 5 Jahren über die Gültigkeit der E-ID hinaus als unverhältnismässig, mehr als ein Jahr ist aus unserer Sicht nicht zu rechtfertigen.

Art. 11 VE-BGEID

[...]

⁵ Der Bundesrat regelt die Aufbewahrungsfristen. Die Daten dürfen längstens ~~bis fünf Jahre nach Ablauf oder Widerruf der E-ID~~ bis ein Jahr ab deren Erhebung aufbewahrt werden, sofern sie nicht zur Nutzung der E-ID unabdingbar sind. Die zur Nutzung notwendigen Daten dürfen längstens bis ein Jahr nach Ablauf oder Widerruf der E-ID aufbewahrt werden.

6. Vorweisen von elektronischen Nachweisen

Ein wichtiger Grundsatz der E-ID ist die Gewährleistung des Datenschutzes durch eine dezentrale Datenverwaltung (vgl. Art. 1 Abs. 2 lit. b Ziff. 4 VE-BGEID).

Klärungsbedürftig ist aus unserer Sicht, ob die Hinterlassung von Spuren bei der Verwendung des digitalen Ausweises (beispielsweise beim Abschluss eines Vertrages zur Eröffnung einer Bankbeziehung oder bei der Inanspruchnahme einer Dienstleistung) gänzlich ausgeschlossen werden kann.

Damit zusammenhängend stellt sich die Frage, ob allenfalls durch den Staat oder durch Private (z.B. Verifikatorinnen) Daten getrackt resp. gespeichert werden. Diese Frage ist unseres Erachtens aufgrund des Bankkundengeheimnis von zentraler Bedeutung, da es um eine Offenbarung von Daten geht. Aus dem erläuternden Bericht ist diesbezüglich keine hinreichende Erklärung erkennbar.

Weiter ist aus unserer Sicht unklar, wie ein Aussteller einen Beweis "zertifizieren" bzw. mit seiner Datenbank überprüfen kann, ob das Zertifikat korrekt ist, ohne Kenntnis von diesem Zertifikat zu haben. Es sollte im Gesetz festgehalten werden, dass der Aussteller weder einen Nachweis noch spezifische Daten für die Validierung aufbewahren darf. Dies bedeutet aber auch, dass es nach der "Zertifizierung" schwierig sein wird, den Beweis zu erbringen, dass der Aussteller die Daten validiert hat.

Die aktuelle Formulierung in Art. 16 Abs. 3 VE-BGEID mindert unter Umständen die Beweiskraft dieser Aussage. Der Wortlaut der Vorschrift eröffnet der Betreiberin der Systeme über den gewählten Begriff «möglichst» die Möglichkeit, einen Rückschluss zur Verwendung des elektronischen Nachweises ziehen zu können. Unseres Erachtens bedarf es in diesem Zusammenhang jedoch einer klaren Verbotsnorm, die - soweit erforderlich - mit Ausnahmetatbeständen versehen wird. Der Bundesrat soll diese regeln. Er muss prüfen, in welchen Fällen es Ausnahmen braucht und diese auf Verordnungsstufe regeln. Grundsätzlich sind aus unserer Sicht zwei Grundkategorien an Ausnahmefällen denkbar: Einerseits aufgrund zwingender rechtlicher Anforderungen und andererseits in begründeten Ausnahmefällen (bspw. aus Sicherheitsgründen). Es ist wichtig, diese Ausnahmetatbestände eng mit der Wirtschaft abzustimmen. Wir würden hierbei unterstützen. Wir schlagen daher folgende präzisierende Formulierung vor:

Art. 16 VE-BGEID

- ¹ Die Inhaberin oder der Inhaber des elektronischen Nachweises bestimmt, welche Bestandteile des Nachweises oder davon abgeleiteten Informationen an die Behörde oder den Privaten, die oder der elektronische Nachweise überprüft (Verifikatorin), übermittelt werden.
- ² Das Vorweisen und Überprüfen eines elektronischen Nachweises erfolgt ohne dass die Ausstellerin davon Kenntnis hat.
- ³ Die Betreiberin der Systeme nach dem 5. Abschnitt muss durch technische und organisatorische Massnahmen sicherstellen, dass sie weder hat keine Kenntnis zum des Inhalts der vorgewiesenen elektronischen Nachweise erlangt, und kann-möglichst keine noch Rückschlüsse über deren Verwendung und die Beteiligten zieh~~te~~en.

7. Rechtssicherheit und Verantwortlichkeit

Das Basisregister wird durch den Bund geführt und muss daher gewissen inhaltlichen Anforderungen genügen. Das gilt sowohl für die öffentlichen als auch für die privaten Identifikatoren und Nachweise, die im Register enthalten sind. Wer das Basisregister nutzt, muss auf die Richtigkeit des Inhaltes vertrauen können. Klar ist, dass der Bund selbst nicht absolute Richtigkeit garantieren kann. Er sollte allerdings einen Prüfmechanismus einführen, um zumindest Missbräuche zu vermeiden und eine hohe Qualität des Registers zu gewährleisten. Sofern das Vertrauen in diese Einträge öfters enttäuscht wird, wird es auch nicht benutzt werden. Es ist daher im Interesse der Herausgeber der E-ID als auch der Nutzenden, dass die Qualität des Registers stimmt. Vor diesem Hintergrund schlagen wir vor, in Art. 18 VE-BGEID anstelle einer «kann»-Formulierung eine Pflicht vorzusehen.

Art. 18 Abs. 2 VE-BGEID

- ¹ Der Bund stellt ein System zur Verfügung, mit dem er bestätigt, dass ein im Basisregister enthaltener Identifikator und allfällige kryptografische Schlüssel einer Bundes-, Kantons- oder Gemeindebehörde zugeordnet sind.
- ² Der Bundesrat ~~kann-vorsehen~~ regelt das Verfahren und die Voraussetzungen, wonach dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.
- ³ Alle Behörden und Privaten können die Zuordnungen durch Abfragen im System überprüfen.

Darüber hinaus muss sich die Relying Party auf die Gültigkeit der elektronischen Nachweise sowie die im Basisregister eingetragenen Informationen verlassen können. D.h. es darf keine Haftbarkeit zu Lasten desjenigen entstehen, der sich auf diese elektronischen Nachweise und Informationen verlässt, wenn sich später ein Mangel manifestiert. Wenn ein Schaden entsteht, soll dafür jene Partei haften, die die inhaltlich falsche Information eingeliefert hat. Aus Gründen der Rechts(-verkehrs)sicherheit ist dies so im Gesetz aufzunehmen.

Art. 18^{bis} Haftung VE-BGEID (neu)

Wenn ein Schaden entsteht, haftet dafür jene Partei, die die inhaltlich falsche Information eingeliefert hat.

8. Technologieneutralität

Gemäss Erläuternder Bericht soll die Vorlage technologieneutral ausgestaltet sein (vgl. bspw. Erläuternder Bericht, S. 22). Dies ist allerdings nur sehr bedingt der Fall, da diese auf die kryptographische Verschlüsselung gestützt wird (vgl. Art. 17 VE-BGEID). Daher wird nicht berücksichtigt, dass künftig allenfalls bessere technische Möglichkeiten bestehen als die kryptographische Verschlüsselung. Ausserdem ist dies auch vor dem Hintergrund problematisch, dass die Ausgestaltung der E-ID dem aktuellen Stand der Technik entsprechen soll (vgl. Art. 1 Abs. 2 Bst. c VE-BGEID; Erläuternder Bericht, S. 23).

Art. 17 VE-BGEID

¹ Der Bund stellt ein öffentlich zugängliches Register (Basisregister) zur Verfügung, das Daten enthält über:

- a. die Ausstellerinnen elektronischer Nachweise;
- b. die Verifikatorinnen;
- c. den Widerruf von elektronischen Nachweisen.

² Die Daten umfassen:

- a. die Identifikatoren der Ausstellerinnen und Verifikatorinnen;
- b. die ~~kryptografischen Schlüssel der Ausstellerinnen~~ Informationen, die erforderlich sind, um
 - 1. die Authentizität und Integrität der ausgestellten elektronischen Nachweise darauf hin zu überprüfen,
 - 2. deren Identifikatoren zu überprüfen;
- c. die ~~kryptografischen Schlüssel der~~ Informationen zu den Verifikatorinnen, die erforderlich sind, um deren Identifikatoren zu überprüfen;
- d. Daten über widerrufene elektronische Nachweise; diese dürfen keine Rückschlüsse über die Inhaberin oder den Inhaber oder über den Inhalt ermöglichen.

³ Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.

⁴ Das Basisregister enthält keine Daten über die einzelnen elektronischen Nachweise mit Ausnahme über deren Widerruf.

9. Weitere Verbesserungsvorschläge

9.1 E-ID und andere elektronische Nachweise

a) Form und Inhalt der E-ID

Im VE-BGEID ist vom Ausstellungsdatum der E-ID die Rede (siehe Art. 2 Abs. 3 lit. c VE-BGEID). Unseres Erachtens wird damit wohl eher das Datum der Zertifizierung der Daten gemeint sein.

Des Weiteren sollten idealerweise die nachfolgenden Daten sowohl für den physischen Ausweis als auch für die E-ID vorhanden sein:

- Ausstellungsdatum;
- Datum des Gültigkeitsendes;
- Datum der Zertifizierung (für die E-ID; auch wenn diese später ausgestellt wird);
- Datum der Annullierung (sofern eine regelmässige automatische Aktualisierung der E-ID möglich ist).

Schliesslich bestimmt jeweils die Inhaberin oder der Inhaber die Informationen, welche er einer Privatperson, einer juristischen Person oder einer Behörde übermitteln möchte (Art. 16 Abs. 1 VE-BGEID). Die Adresse des Wohnsitzes könnte u.a. auch für die Aufenthalts- oder Arbeitsgenehmigung sinnvoll sein. Wir schlagen daher vor, die Adresse des Wohnsitzes in Art. 2 Abs. 2 VE-BGEID aufzunehmen.

b) Akzeptanz der E-ID

Der Vorentwurf des E-ID-Gesetzes hält nicht klar fest, ob die E-ID "nur" als elektronisches Identifikationsmittel in der virtuellen Welt ausgestaltet werden soll (als Gegenstück zu ID/Pass in der physischen Welt) oder auch in der physischen Welt einsetzbar sein soll (E-ID als umfassendes Identifikationsmittel für physische und virtuelle Welt; vgl. bspw. den erläuternden Bericht zu Art. 1 Abs. 2 Bst. a VE-BGEID [*«Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden.»*, S. 7] und zu Art. 9 [*«(...) die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet (...)»* [S. 11]). Eine Verwendung der E-ID auch in der physischen Welt wäre wünschenswert und würde nicht zuletzt auch zu deren Verbreitung beitragen. Entsprechend wäre die Pflicht zur Akzeptanz der E-ID nicht an eine elektronische Identifizierung zu koppeln. Wir schlagen daher folgende Anpassung von Art. 9 VE-BGEID vor:

Art. 9 VE-BGEID

Jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, muss die E-ID akzeptieren, wenn sie eine **elektronische** Identifizierung vornimmt.

Der VE-BGEID hat namentlich den Zweck, eine «sichere Identifizierung» mittels E-ID unter Privaten und mit Behörden zu gewährleisten (vgl. Art. 1 Abs. 2 lit. a VE-BGEID). Zudem beruht die E-ID auf Ausweisen gemäss AwG oder nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl (vgl. Art. 3 VE-BGEID). Es ist daher angebracht, dass überall, wo im Geschäftsverkehr eine Identifikationspflicht besteht, diese hinsichtlich der Personenidentifizierungsdaten ohne weitere Massnahmen (wie bspw. ein persönliches Erscheinen der betreffenden Person) mit der E-ID erfüllt werden kann. Damit wird die effiziente Digitalisierung von Geschäftsprozessen möglich, so zum Beispiel im Rahmen der Identifikation nach

GwG. Zur Sicherstellung der Harmonisierung und da sich solche Pflichten nicht ausschliesslich aus Gesetzen ergeben, erachten wir eine generelle Auffangnorm für die Identifizierung unter Abwesenden als sinnvoll.

Art. 9^{bis} Nachweis der Identität unter Abwesenden VE-BGEID (neu)

Sofern eine Pflicht zur Identifikation besteht und die Ausweise gemäss Art. 3 dieses Gesetzes akzeptiert werden, ist die E-ID für die Personenidentifizierungsdaten ohne weitere Massnahmen ausreichend. Insbesondere besteht keine Pflicht des persönlichen Erscheinens der betreffenden Person.

c) Vorweisen einer E-ID

Die Formulierung von Art. 10 VE-BGEID scheint uns unklar, da er insbesondere Wiederholungen enthält. Er sollte daher vereinfacht werden.

d) Ausstellung anderer elektronischer Nachweise

Die Ausführungen zur Nutzung der Infrastruktur zur Ausstellung von elektronischen Nachweisen gemäss Art. 12 Abs. 1 VE-BGEID sind sehr weit gefasst. Gleichzeitig sollten neben dem Ausstellungsdatum auch Angaben zur Validierung der Daten enthalten sein. Dementsprechend schlagen wir für Art. 12 Abs. 1 VE-BGEID folgende Ergänzungen vor:

Art. 12 VE-BGEID

¹ Wer als staatliche Stelle oder als Teil der Privatwirtschaft elektronische Nachweise ausstellen möchte, kann die Infrastruktur nach dem 5. Abschnitt nutzen.

² Diese elektronischen Nachweise müssen neben dem von der Ausstellerin festgelegten Inhalt den Identifikator der Ausstellerin, ~~sowie~~ das Ausstellungsdatum sowie das Datum der Validierung der Daten enthalten.

9.2 Nutzung von elektronischen Nachweisen

a) Aufbewahrung von elektronischen Nachweisen

Art. 14 VE-BGEID sollte um den Begriff der Sicherheit ergänzt werden:

Art. 14 VE-BGEID

Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe ~~selbst-gewählter~~ gesicherter technischer Mittel seiner Wahl und unter ihrer oder seiner alleinigen Kontrolle auf.

b) Übertragbarkeit von elektronischen Nachweisen

Es sollte möglich sein, bestimmte elektronische Beweismittel an eine andere Inhaberin oder an einen anderen Inhaber zu übertragen, wenn diese gesetzliche Vertreterin bzw. dieser gesetzliche Vertreter der- oder desselben ist (Eltern, gesetzliche Vertreterin bzw. gesetzlicher Vertreter von Personen unter Beistandschaft, eingetragene Ehepartnerin oder eingetragener Ehepartner).

9.3 Verbesserungsvorschläge in Bezug auf die Vertrauensinfrastruktur

a) *Missbrauch der Vertrauensinfrastruktur*

Der Zeitpunkt, ab dem eine Nutzung missbräuchlich wird, ist nicht eindeutig festgelegt. Zudem suggeriert der erläuternde Bericht, dass mit Missbrauchsfällen gerechnet werden muss, was unbefriedigend ist. Es geht vielmehr darum, solche Fälle so wirksam wie möglich zu bekämpfen. Wir empfehlen daher, diesen Umstand im Gesetzestext entsprechend zu berücksichtigen.

b) *Quellcode der Vertrauensinfrastruktur*

Die Veröffentlichung des Quellcodes der Elemente der Vertrauensinfrastruktur im Internet ist grundsätzlich begrüssenswert. Aus Gründen der Technologieneutralität empfehlen wir für Art. 25 VE-BGEID eine «kann»-Formulierung.

Art. 25 VE-BGEID

Der Bund kann veröffentlichen den Quellcode der von ihm zur Verfügung gestellten Elemente der Vertrauensinfrastruktur veröffentlichen.

10. Änderung weiterer Erlasse

10.1 Verwendung der E-ID im Finanzsektor

Im Bereich des Finanzsektors könnten mit der Einführung der E-ID wesentliche Effizienzgewinne resultieren. Im Allgemeinen sollte eine E-ID, die die Informationen eines Ausweises enthält, diesem gleichwertig sein, so dass auch andere Erlasse (z.B. GwG/GwV) abgedeckt sind – es sei denn, es ist bspw. eine Beglaubigung durch einen Notar erforderlich. Das GwG geht in Art. 3 von einer Identifikation durch beweiskräftige Dokumente aus. Es stellt sich daher die Frage, ob die E-ID als solches Dokument gilt. Wir schlagen vor, hier Klarheit zu schaffen und die Identifikation durch die E-ID ausdrücklich vorzusehen. Damit hätte diese Art der Identifikation ihre Grundlage auf der richtigen Stufe, d.h. im formellen Gesetz.

Art. 3 GwG

¹ Der Finanzintermediär muss bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines beweiskräftigen Dokumentes oder einer E-ID gemäss Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise vom... identifizieren. Handelt es sich bei der Vertragspartei um eine juristische Person, so muss der Finanzintermediär die Bevollmächtigungsbestimmungen der Vertragspartei zur Kenntnis nehmen und die Identität der Personen überprüfen, die im Namen der juristischen Person die Geschäftsbeziehung aufnehmen.

10.2 Abstimmung mit dem ZertES

Die Anpassung von Art. 9 ZertES (vgl. Erläuternder Bericht, S. 20) sollte klar festhalten, dass eine Identifizierung mit der E-ID der Identifikation durch persönliches Erscheinen gleichgestellt ist. Wichtig ist, dass klar

festgehalten wird, dass mit einer Identifizierung mittels E-ID die Anforderungen an die Ausstellung einer QES erfüllt werden (vgl. Bericht, S. 7: "So können die bestehenden (Online)-Identifizierungsprozesse, die viel komplexer sind, ersetzt werden. Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden.").

Art. 9 ZertES

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines geregelten Zertifikats stellen, verlangen:

- a. bei natürlichen Personen: dass sie persönlich erscheinen ~~und~~ oder durch eine E-ID gemäss dem Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise vom ... den Nachweis ihrer Identität erbringen;
[...]

11. Periodische Überprüfung

Das BGEID und die darauf basierenden technischen Infrastrukturen müssen einer periodischen Überprüfung unterzogen werden, welche klären soll, ob die technischen Funktionalitäten zur Sicherstellung von Datenschutz (inkl. Bankkundengeheimnis) und Cybersicherheit jeweils dem aktuellen Stand der Technik entsprechen und somit «state of the art» sind (Art. 1 Abs. 2 lit. c VE-BGEID) und die E-ID ihren Zweck zur Förderung digitaler Geschäftsmodelle erfüllen kann.

12. Beizug von Experten bei der Erarbeitung der Ausführungsbestimmungen

Wir erlauben uns schliesslich den Hinweis, dass der VE-BGEID ein Rahmengesetz ist, das die wichtigsten Regulierungsgrundsätze im Zusammenhang mit der elektronischen Identität enthalten muss. Diese haben daher eine allgemeine Tragweite und müssen technologieneutral sein. Von noch grösserer Bedeutung sind hingegen die Ausführungsbestimmungen, die in der Verordnung enthalten sein werden. Bei der Erarbeitung derselben sind angesichts der Komplexität der Materie Experten aus der Privatwirtschaft und Wissenschaft beizuziehen.

Dementsprechend schlagen wir eine entsprechende Ausführungsbestimmung als neuen Absatz 2 von Art. 28 VE-BGEID vor:

Art. 28 VE-BGEID

¹ Der Bundesrat erlässt die Ausführungsbestimmungen, insbesondere: [...]

² Der Bundesrat zieht bei der Erarbeitung der Ausführungsbestimmungen Experten der Privatwirtschaft und der Wissenschaft bei.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen für die weiteren Arbeiten. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung



Richard Hess
Leiter Digitalisierung



Natalie Graf
Fachverantwortliche Legal

Hopfenweg 21
PF/CP 5775
CH-3001 Bern
T 031 370 21 11
info@travailsuisse.ch
www.travailsuisse.ch

Madame Karin Keller-Sutter
Cheffe du DFJP
Conseillère fédérale

Courriel: rechtsinformatik@bj.admin.ch

Berne, le 18 octobre 2022

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électronique (loi sur l'e-ID, LeID). Consultation.

Madame la Conseillère fédérale,
Madame, Monsieur,

Nous vous remercions de nous donner la possibilité d'exprimer notre avis sur cet avant-projet de loi et c'est bien volontiers que nous vous faisons part de notre avis.

Le 7 mars 2021, la loi fédérale sur les services d'identification électroniques (LSIE) a été clairement rejetée par presque 65 % des votants. Travail.Suisse avait proposé lors de la campagne de votation sur la LSIE le rejet car elle ne répondait pas aux critères de service public et faisait peser un risque trop grand sur la protection des données. Pour Travail.Suisse, la convivialité de la future application et le respect de la protection des données doivent être garanties pour les utilisatrices et les utilisateurs.

Le nouveau projet de LeID a dûment tenu compte de l'échec en votation de mars 2021 et satisfait aux principales exigences de service public et de protection des données. C'est pourquoi, Travail.Suisse soutient cet avant-projet de loi.

Nous saluons en particulier le fait que l'avant-projet de loi :

- Prévoit la mise en place d'une identité électronique étatique, gratuite et volontaire pour les titulaires d'un document d'identité émis par les autorités suisses. Dans ce cadre, l'État continue d'assumer sa tâche centrale, qui est la vérification de l'identité d'une personne ainsi que l'émission du moyen de preuve électronique s'y rapportant.
- Règle convenablement les questions de protection des données avec le respect des principes suivants: prendre en compte la protection de la vie privée dès la conception du produit (privacy by design), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification).
- Tienne compte du règlement no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions

électroniques au sein du marché intérieur et prévoit une compétence du Conseil fédéral pour conclure des accords internationaux afin d'obtenir une reconnaissance internationale de l'e-ID et une reconnaissance en Suisse des e-ID étrangères.

- Développe une infrastructure de confiance qui permettra aux cantons, communes et villes d'accomplir certaines tâches plus efficacement. Dans cette optique, l'infrastructure de confiance permettra de progresser en matière de numérisation des activités publiques.

La transformation numérique est en cours aux différents échelons de la sphère publique. Mais certaines catégories de la population ont toujours de la peine à maîtriser ce changement. Il subsiste un besoin important pour consulter une autorité dans le monde réel. Les cantons ont déjà mis en place différents services et offres destinés aux personnes souhaitant obtenir un soutien ou des informations générales. Ces points de contact existants pourront et devront également être utilisés pour offrir une assistance en rapport avec l'E-ID. Pour Travail.Suisse, il est important de continuer à garantir aussi un service public physique pour différentes catégories de personnes ayant des difficultés à s'adapter à la numérisation des services publics. Par ailleurs, il ne faut pas oublier que des points de contact physiques jouent aussi un rôle de lien social et le service public doit continuer, malgré le développement de sa numérisation, à offrir ce lien par le biais de prestations physiques.

En vous remerciant de réserver un bon accueil à notre réponse, nous vous adressons, Madame la Conseillère fédérale, Madame, Monsieur, nos salutations distinguées.



Adrian Wüthrich, président



Denis Torche, responsable du dossier service public

T +41(0)31 390 39 39
E catherine.rouvenaz@agile.ch

Eidgenössisches Justiz- und
Polizeidepartement – EJPD
Per E-Mail an :
rolf.rauschenbach@bj.admin.ch

Berne, 10. Oktober 2022

Stellungnahme im Rahmen der Vernehmlassung zur elektronischen Identität

Sehr geehrte Damen und Herren

Wir bedanken uns für die Vorlage und den erläuternden Bericht zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

AGILE.CH begrüsst die Einführung eines staatlichen elektronischen Identitätsnachweises grundsätzlich. In unserer Stellungnahme beschränken wir uns auf den Aspekt der Barrierefreiheit, der beim hier vorliegenden Gesetzesvorhaben von grosser Bedeutung ist.

Grundsätzliche Erwägungen:

AGILE.CH ist überrascht, dass der Aspekt der E-Accessibility keine Erwähnung in der Vorlage findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt wird. In der Entwicklung sind sämtliche Umsetzungsschritte im Hinblick auf den Standard eCH-0059 Version 3.0 (oder spätere Versionen) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG 2.1 des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, welche von der E-Accessibility-Richtlinie der EU inspiriert sind.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK) unterzeichnet. Artikel 9 der UNO-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies schliessen auch die Information

und Kommunikation, einschliesslich der entsprechenden Technologien und -systeme ein. Das Behindertengleichstellungsgesetz (BehiG) schreibt in Art. 14 vor, dass die Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten nehmen müssen. Ohne Gewährleistung der E-Accessibility wären vor allem Menschen mit Sehbeeinträchtigung vom staatlichen Angebot in Form eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Briefftasche ausgeschlossen.

Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Praktische Überlegungen:

Für Menschen mit Sehbeeinträchtigung stellt die Digitalisierung eine Chance dar zu einem breiteren Zugang zu Dienstleistungen aller Art. Die digitalen Kommunikationskanäle sind das eigentliche Tor zu den Informationen für die sehbehinderten Menschen. Zwingende Voraussetzung für die Nutzbarkeit der digitalen Angebote ist aber, dass diese barrierefrei zur Verfügung stehen. Deshalb muss vor jeder Publikation eines Web-basierten Produkts und auch vor jedem Update geprüft werden, ob dieses barrierefrei zugänglich ist. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das design-for-all-Prinzip zur Anwendung kommen, analog dem europäischen Recht.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Wir verweisen diesbezüglich auch auf die Antwort des Bundesrates auf die Frage [22.7406](#) von Nationalrätin Franziska Ryser, in der er ausführt, dass der standardmässige Einsatz von Usability-Tests im Rahmen der Weiterentwicklung der Instrumente zur Gewährleistung der Barrierefreiheit geprüft wird. Die Freigabe bzw. **Lancierung der E-ID darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist**. Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet.

Anträge:

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein **eigener Artikel «Barrierefreiheit»** aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen die


von Antragstellenden, Inhaber:innen einer E-ID, Aussteller:innen, Verifikator:innen und weiteren Usergruppen genutzt oder betrieben werden können.

2. In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein **eigenes Kapitel zur Barrierefreiheit** aufzunehmen. Dieses beschreibt detailliert, wie die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
3. Zur Kontrolle der Barrierefreiheit sei ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die **zusammen mit betroffenen Personen** die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Wir danken Ihnen für die Betrachtung unserer Stellungnahme.

AGILE.CH Die Organisationen von Menschen mit Behinderungen

Raphaël de Riedmatten



Geschäftsleiter

Catherine Rouvenaz



Secrétaire romande



Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
CHF-3003 Bern

Per Email versandt:
rechtsinformatik@bj.admin.ch

Bern, der 10. Oktober 2022

Vernehmlassung zum Vorentwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (nachfolgend "Vorentwurf" bzw. "VE")

Sehr geehrter Frau Bundesrätin,

Sehr geehrte Damen und Herren

Der Schweizerische Anwaltsverband (SAV) dankt Ihnen für die Gelegenheit in der obgenannten Vernehmlassung Stellung nehmen zu können. Für den SAV ist die E-ID insbesondere im Zusammenhang mit dem Projekt Justitia 4.0 von besonderer Relevanz, da mit der E-ID der Zugang für Anwälte zur Plattform erfolgen soll.

1. Vorbemerkungen

Der Vorentwurf scheint uns insgesamt sehr gelungen und den Anregungen in der öffentlichen Konsultation wurde Rechnung getragen. Insbesondere wurden die Weichen im Vorentwurf derart gestellt, dass einer grossen Verbreitung der E-ID und deren Akzeptanz in der Bevölkerung nichts im Weg steht. Weiter wurden auch der technologischen Weiterentwicklung sowie der Anbindung an internationale Systeme Rechnung getragen.

Wir haben lediglich einige wenige Punkte, die unseres Erachtens im Gesetzesentwurf noch zu berücksichtigen sind.

2. Datenschutz

Im Vorentwurf wird auf die Grundsätze im Datenschutz verwiesen (Art. 1 Abs. 2 Vorentwurf). Wir teilen die Ansicht, dass ein Verweis auf die Regelung im DSG mit minimalen spezifischen Regelungen im Vorentwurf in den meisten Fällen ausreichend ist. Es kann jedoch nicht übersehen werden, dass Personendaten durch die verifizierbare staatliche Bestätigung eine besondere Qualität erlangen, welche das DSG bisher nicht abbildet. Dies weil die Verifikation später immer noch nachvollzogen werden kann. Bezüglich der nachfolgenden zwei spezifischen Themen regen wir deshalb eine Ergänzung an.

2.1 Speicherung und Weitergabe von Daten bei der Verifikatorin

Auch nachträglich noch verifizierbare, elektronisch verfügbare und staatlich bestätigte Identitätsdaten können von besonderem Interesse sein oder einen grossen Wert aufweisen, weshalb auch entsprechende Vorkehrungen in einem Erlass geregelt werden sollten. Der Hinweis auf den Grundsatz der Datensparsamkeit, bzw. die Regelung im (neuen) Datenschutzgesetz genügen hier deshalb nicht.

Es rechtfertigt sich vielmehr, dem besonderen Risiko mit spezifischen Regelungen zu begegnen. Insbesondere sollte die Weitergabe solcher auch nachträglich noch verifizierbarer, elektronischer Nachweise und auch die Verwendung zu neuen Zwecken nur nach informierter, expliziter Einwilligung zulässig sein.

Andererseits sollte sichergestellt werden, dass bisher gar nicht systematisch erfasste Identifikationen (z.B. bei der Altersverifikation beim Alkoholkau im Ladengeschäft) auch zukünftig nicht erfasst werden. Im physischen Verkehr muss eine Verifikations-App zur Anwendung gelangen, aber eine informierte Einwilligung zur Speicherung ist in diesen Situationen kaum je möglich. Es rechtfertigt sich deshalb vorzuschreiben, dass die mit einer E-ID anfallenden elektronischen Identifikationsmerkmale in diesen Fällen grundsätzlich nicht dauerhaft gespeichert werden dürfen. Eine Speicherung sollte nur zulässig sein, insoweit damit gesetzliche Pflichten erfüllt werden und eine informierte Einwilligung tatsächlich eingeholt werden kann (z.B. Kauf von SIM-Karten).

2.2 «Overidentification»

Das Thema "*Overidentification*", d.h. die Grenzen welche elektronischen Nachweise von einer Verifikatorin erhoben werden dürfen, wird im Vorentwurf bewusst nicht geregelt. Im erläuternden Bericht wird ausgeführt, dass hierzu die allgemeinen Regeln des Datenschutzes ausreichend sind.

Dies greift unserer Ansicht nach zu kurz. Insbesondere im Falle der – beabsichtigten – breiten Verfügbarkeit der E-ID ist zu erwarten, dass Anbieter elektronischer Dienste überhaupt beginnen würden, Nutzer staatlich zu identifizieren oder aber im Zweifel zusätzliche verifizierte Identitätselemente zu verlangen. Eine Rechtfertigung nach DSG wäre für ein solches Vorgehen meist problemlos möglich – was aber der besonderen Qualität keine Rechnung trägt.

Nach der vom SAV vertretenen Ansicht, sollte die Bestimmung in Ziffer 16 VE daher um eine Bestimmung ergänzt werden, die festhält, dass die Identifikation mittels E-ID nur dann obligatorisch vorausgesetzt werden darf, wenn und soweit dies zur Erfüllung einer gesetzlichen Pflicht notwendig ist (wie z.B. beim Erwerb einer SIM-Karte, wo zwingend die Identität der erwerbenden Person zu erheben ist). In allen anderen Fällen muss das Recht bestehen, einen geforderten Nachweis diskriminierungsfrei auch mit anderen Mitteln beibringen zu können. Für den Fall eines Verstosses kann auf die Sanktionsvorschriften des DSG verwiesen werden.

3. Föderalisierte Vertrauensinfrastruktur | Ausgestaltung der Wallet (Art. 19 VE)

Es wird sehr begrüsst, dass der Bund eine Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen, d.h. eine Wallet, zur Verfügung stellt. Dabei ist sicherzustellen, dass diese so ausgestaltet ist, dass sich auch elektronische Nachweise anderer Aussteller aus fremden Registern darin abspeichern lassen. Die Vertrauensinfrastruktur sollte dazu so gefördert ausgestaltet werden, dass auch fremde Register – z.B. aus dem Ausland – unterstützt werden können.

4. Anwendung zur Prüfung von elektronischen Nachweisen (Art. 20 VE)

Es scheint grundsätzlich sinnvoll, wenn der Bund ebenfalls eine Anwendung zur Prüfung von elektronischen Nachweisen zur Verfügung stellt. Dies kann einer schnelleren Verbreitung nur dienlich sein. Es stellt sich danach die Frage, ob nicht von einer "kann"-Bestimmung

abgesehen werden soll und der Bund nicht angewiesen werden müsste eine solche zur Verfügung zu stellen.

5. Sicherungskopien (Art. 21 VE / Art. 26 Abs. 2 VE)

Man kann sich fragen, ob es tatsächlich Aufgabe des Bund sein muss, ein System für Sicherungskopien zur Verfügung zu stellen. Es ist sicher notwendig, dass es dem Inhaber von elektronischen Nachweisen möglich sein muss, eine Sicherungskopie seiner Wallet zu erstellen, da bei Verlust zwar eine neue E-ID bestellt werden kann, aber auch alle zusätzlichen elektronischen Nachweise neu beschafft und sämtliche Verknüpfungen wieder neu hergestellt werden müssen, was ausserordentlich zeitraubend sein kann. Die Regelungen im Vorentwurf sowie den Ausführungen im erläuternden Bericht entnehmen wir jedenfalls, dass zurzeit kein *Hardware Security Element* geplant ist.

Für den Fall, dass tatsächlich ein vom Bund betriebenes System für Sicherungskopien in Betrieb genommen wird, ist sicherzustellen, dass sämtliche dort hochgeladenen Daten verschlüsselt sind und auch vom Bund nicht darauf zugegriffen werden kann. Insofern wäre Art. 21 Abs. 2 VE noch zu ergänzen.

Nachdem es sich beim angedachten System für Sicherungskopien grundsätzlich darum handelt eine verschlüsselte Kopie der Wallet zu speichern, d.h. Speicherplatz zur Verfügung gestellt wird, kann eine kleine Gebühr erhoben werden.

6. Gebühren (Art. 26 VE)

Damit der E-ID zu einer möglichst grossen Verbreitung verholfen werden kann, sollten die Kosten so tief wie möglich gehalten werden. Der SAV begrüsst, dass insbesondere der Bezug der E-ID kostenfrei möglich sein soll.

Nach Ansicht des SAV, sollte auch der einfache Eintrag ins Basisregister kostenfrei angeboten werden. Dieser Prozess kann vollumfänglich automatisiert werden und es Bedarf diesbezüglich keinerlei besonderer Dienstleistungen des Betreibers der Vertrauensinfrastruktur. Dies könnte die niederschwellige Verbreitung von elektronischen Nachweisen dienlich sein, wo eine Bestätigung der Identifikatoren nicht zwingend notwendig ist (z.B. ein Verein, der seine Mitgliederausweise in Form von elektronischen Nachweisen gestalten möchte).

Dahingegen scheint es sinnvoll, eine (möglichst tiefe) Gebühr für die Bestätigung von Identifikatoren einzufordern. Hier wird tatsächlich eine Leistung des Bundes eingefordert. Nachdem dies primär im kommerziellen Einsatzbereich notwendig sein wird, dürfte eine solche Gebühr auch keinen Hinderungsgrund für die Verbreitung der E-ID darstellen.

Bezüglich Gebühren für Sicherungskopien, siehe Ziffer 5 vorstehend.

Mit dem nochmaligen Dank für die Einräumung zur Gelegenheit zur Vernehmlassung verbleiben wir namens des Schweizerischen Anwaltsverbandes

Präsidentin SAV

Birgit Sambeth



Generalsekretär SAV

René Rall



Bern, 18. Oktober 2022

Stellungnahme zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zum Vorentwurf für das neue Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID) Stellung zu nehmen.

Die Auslandschweizer-Organisation (ASO) ist eine private Stiftung, welche die Interessen von rund 788 000 ausserhalb unserer Landesgrenzen lebenden Schweizer:innen vertritt. Die Kommunikation zwischen Auslandschweizer:innen und Schweizer Behörden gestaltet sich häufig schwierig. E-Government-Dienste können dem entgegenwirken: Sie ermöglichen einen unkomplizierten Behördenkontakt trotz Zeitverschiebung und räumlicher Distanz. Die Einführung einer elektronischen Identität (E-ID) und anderer elektronischer Nachweise würde das Anbieten von E-Government-Lösungen bedeutend vereinfachen und den Auslandschweizer:innen somit die Betreuung ihrer Verwaltungsakten und den Behördenkontakt in besonderem Masse erleichtern. Die ASO begrüsst daher die Schaffung einer gesetzlichen Grundlage für elektronische Identitätsnachweise und andere elektronische Nachweise.

Eine sichere Identifizierung im Netz ermöglicht durchgehend digital ausgestaltete E-Voting-Verfahren. Die Einführung des E-Votings als ordentlicher Stimmkanal ist für die Auslandschweizer:innen von enormer Bedeutung. Ihre verfassungsmässig garantierten politischen Rechte sind in der Praxis oft schwer wahrnehmbar, weil die Wahl- und Abstimmungsunterlagen per Briefpost je nach Wohnort zu spät eintreffen. Eine vertrauenswürdige staatliche E-ID könnte ein vollständig papierloses E-Voting-Verfahren ermöglichen. Die ASO ermutigt den Bund, diese Chance zu nutzen, um den Auslandschweizer:innen ihr Stimm- und Wahlrecht effektiv zu garantieren.

Weiterhin könnte eine E-ID Auslandschweizer:innen den Zugang zu Schweizer Banken erleichtern. Die aus Gründen der Prävention von Geldwäscherei und Steuerhinterziehung verlangte eindeutige Identifizierung neuer Kund:innen ist für Banken insbesondere dann teuer, wenn die Kund:innen im Ausland leben. Viele



Banken schränken deshalb ihre Dienste diesbezüglich stark ein. Solche Identifizierungsprozesse werden durch eine E-ID einfacher und günstiger; somit bestünde die Hoffnung, dass die Schweizer Banken den Auslandschweizer:innen wieder vereinfacht Zugang gewähren.

Insbesondere begrüsst die ASO, dass der Bund die Bedenken der Schweizer Bevölkerung berücksichtigt hat und neu eine staatliche E-ID vorschlägt, welche ein hohes Sicherheitsniveau garantiert. Während sich der Auslandschweizerrat (ASR), höchstes Organ der ASO, nur zögerlich für den ersten Gesetzesentwurf ausgesprochen hatte, wird die neue Vorlage von einer überwältigenden Mehrheit befürwortet. Die im aktuellen Entwurf angestrebte internationale Kompatibilität der E-ID stellt für Auslandschweizer:innen einen grossen Fortschritt dar und fördert die internationale Mobilität.

Der Datenschutz bleibt weiterhin zentral und die diesbezüglichen Verbesserungen begrüssen wir grundsätzlich sehr. So erscheint uns überzeugend, dass die Bürger:innen dank des gewählten Self-Sovereign-Identity-Ansatzes selbst bestimmen können, welche Daten sie an wen weitergeben. Um der Gefahr der Überidentifikation vorzubeugen, erachten wir es aber als unerlässlich, diesen Ansatz – insbesondere bei einer Öffnung der Vertrauensinfrastruktur für Private – mit Massnahmen zur Förderung der digitalen Mündigkeit zu verbinden. 2021 waren rund 22.5 % der Auslandschweizer:innen über 65 Jahre alt. Ein nicht unbedeutender Teil der Auslandschweizer:innen gehört also einer Generation an, die nicht mit digitalen Technologien aufgewachsen ist und somit teilweise auf Unterstützung sowie Aufklärung angewiesen ist. Analog zu den geplanten kantonalen Anlaufstellen (Art. 8), benötigen auch Auslandschweizer:innen gut zugängliche Anlaufstellen zur Unterstützung im Umgang mit E-Government-Angeboten. Hier würde sich etwa eine Einbindung der konsularischen Vertretungen anbieten. Zudem wäre eine breit angelegte Informations- und Sensibilisierungskampagne, die sich auch an Auslandschweizer:innen richtet, zur Förderung der digitalen Mündigkeit wünschenswert.

Damit Fälle des Missbrauches der Vertrauensinfrastruktur tatsächlich an die Öffentlichkeit gelangen, sind niederschwellige Angebote vonnöten, bei denen betroffene Bürger:innen Verdachtsfälle melden können – beispielsweise ein Meldeformular, ähnlich demjenigen des Nationalen Zentrums für Cybersicherheit. Wir ermuntern den Bund, eine solche Struktur zur Verfügung zu stellen.

Zusammenfassend ist festzuhalten, dass die ASO die neuen gesetzlichen Grundlagen zu einer staatlichen E-ID und anderen elektronischen Nachweisen begrüsst. Wir sind überzeugt, dass die Schweizer Bevölkerung von der voranschreitenden Digitalisierung profitieren wird. Insbesondere für die Auslandschweizer:innen ist der Zugang zu E-



Government-Diensten und zur E-Democracy von grosser Bedeutung. Die Aspekte der Sicherheit und die Einhaltung der internationalen Standards müssen gewährleistet sein.

Wir danken für Ihre Kenntnisnahme.

Freundliche Grüsse

A handwritten signature in black ink, appearing to read "Filippo Lombardi".

Filippo Lombardi
Präsident

A handwritten signature in black ink, appearing to read "A. Rustichelli".

Ariane Rustichelli
Direktorin



Berne, le 18 octobre 2022

Prise de position relative à la loi fédérale sur l'identité électronique et autres moyens de preuve électroniques

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Nous vous remercions de nous donner la possibilité de prendre position au sujet de l'avant-projet de loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID).

L'Organisation des Suisses de l'étranger (OSE) est une fondation privée qui représente les intérêts des quelque 788 000 Suisses-ses résidant en dehors des frontières nationales. La communication entre les Suisses-ses de l'étranger et les autorités suisses s'avère souvent difficile. Des services de cyberadministration pourraient contribuer à améliorer la situation, car ils facilitent le contact avec les autorités, malgré le décalage horaire et la distance géographique. L'introduction d'une identité électronique (e-ID) et d'autres moyens de preuve électroniques simplifierait considérablement la fourniture de solutions de cyberadministration et faciliterait également le suivi des dossiers administratifs des Suisses-ses de l'étranger et leurs contacts avec les autorités. L'OSE salue donc la création d'une base légale pour les preuves d'identité numériques et autres moyens de preuve électroniques.

Une identification sécurisée sur internet permet de mettre en place des procédures de vote électronique numériques complètes. L'introduction du vote électronique en tant que canal de vote ordinaire est d'une importance capitale pour les Suisses-ses de l'étranger. Souvent, ils ont beaucoup de peine à exercer leurs droits politiques, pourtant garantis dans la Constitution fédérale, le matériel d'élection et de vote envoyé par la poste leur parvenant trop tard selon le lieu de résidence. Une identité électronique émise par l'État, digne de confiance, pourrait permettre le vote électronique et rendre l'envoi du matériel de vote et d'élection sur papier superflu. L'OSE encourage la Confédération à saisir cette opportunité pour garantir véritablement le droit de vote et d'élection des Suisses-ses de l'étranger.

En outre, une e-ID pourrait améliorer l'accès des Suisses-ses de l'étranger aux banques suisses. L'identification claire des nouvelles clientes et des nouveaux clients



en vue de prévenir le blanchiment d'argent et l'évasion fiscale est particulièrement onéreuse pour les banques lorsque ces personnes vivent à l'étranger. Par conséquent, de nombreuses banques limitent fortement leurs services dans ce domaine. Une e-ID simplifiera de telles procédures d'identification et en diminuera les coûts, de sorte que l'on peut espérer que les banques suisses accorderont à nouveau un accès simplifié à leurs services aux Suisses·ses de l'étranger.

L'OSE salue en particulier le fait que la Confédération a tenu compte des préoccupations de la population suisse et qu'elle propose désormais une e-ID émise par l'État, qui garantit un niveau de sécurité élevé. Alors que le Conseil des Suisses de l'étranger (CSE), l'organe suprême de l'OSE, ne s'était prononcé que de façon hésitante en faveur du premier projet de loi, le projet actuel est soutenu par une très large majorité. La compatibilité de l'e-ID sur le plan international, telle qu'elle est visée dans le projet actuel, représente un grand progrès pour les Suisses·ses de l'étranger et facilite la mobilité internationale.

La protection des données reste essentielle et nous saluons vivement les améliorations en la matière. Le fait que les citoyen·nes puissent décider des données qu'ils transmettent et à qui ils les transmettent, grâce au principe adopté de l'identité auto-souveraine (self-sovereign identity), nous paraît convaincant. Pour éviter un risque de suridentification, nous considérons qu'il est indispensable de lier ce principe – en particulier en cas d'ouverture de l'infrastructure de confiance aux particuliers – avec des mesures visant à promouvoir la maturité numérique. En 2021, environ 22,5% des Suisses·ses de l'étranger étaient âgés de plus de 65 ans. Une part non négligeable des Suisses·ses de l'étranger appartient donc à une génération qui n'a pas grandi avec les technologies numériques et qui a donc en partie besoin d'être soutenue et informée. De manière analogue aux points de contact cantonaux (art. 8), les Suisses·ses de l'étranger ont aussi besoin de points de contact facilement accessibles pour les aider à utiliser les offres de cyberadministration. L'intégration des représentations consulaires serait judicieuse à cet égard. De plus, une campagne d'information et de sensibilisation de grande ampleur, s'adressant aussi aux Suisses·ses de l'étranger, afin d'encourager la maturité numérique, serait également souhaitable.

En outre, pour que les cas d'abus de l'infrastructure de confiance soient effectivement rendus publics, il est nécessaire de disposer d'offres faciles d'accès, pour permettre aux citoyen·nes concernés de déclarer les cas suspects, par exemple un formulaire de déclaration, similaire à celui du Centre national pour la cybersécurité. Nous encourageons la Confédération à mettre une telle structure à disposition.

En résumé, l'OSE salue les nouvelles bases légales relatives à une e-ID émise par l'État et d'autres moyens de preuves électroniques. Nous sommes convaincus que la



population suisse profitera des progrès en matière de numérisation. Pour les Suisses·ses de l'étranger, l'accès aux services de cyberadministration et à la cyberdémocratie revêt une grande importance. Les aspects de la sécurité et le respect des normes internationales doivent être garantis.

Nous vous remercions par avance de l'attention que vous porterez à nos considérations.

Veuillez agréer, Madame la Conseillère fédérale, Mesdames, Messieurs, nos salutations distinguées,

A handwritten signature in black ink, appearing to read "Filippo Lombardi".

Filippo Lombardi
Président

A handwritten signature in black ink, appearing to read "A. Rustichelli".

Ariane Rustichelli
Directrice



Könizstrasse 23, Postfach, 3001 Bern

EJPD
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Generalsekretariat
Könizstrasse 23
Postfach
3001 Bern

Martin Abele
Bereichsleiter / GL-Mitglied
+41 31 390 88 17
martin.abele@sbv-fsa.ch

Bern, 28. September 2022/ MA

E-ID Gesetz, BGEID, Vernehmlassung

Sehr geehrte Damen und Herren

Wir bedanken uns für die Vorlage und den erläuternden Bericht zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Der SBV begrüsst die Einführung eines staatlichen elektronischen Identitätsnachweises grundsätzlich. In unserer Stellungnahme beschränken wir uns auf den Aspekt der Barrierefreiheit, der beim hier vorliegenden Gesetzesvorhaben von grosser Bedeutung ist.

Grundsätzliche Erwägungen:

Der SBV ist überrascht, dass der Aspekt der E-Accessibility keine Erwähnung in der Vorlage findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt wird. In der Entwicklung sind sämtliche Umsetzungsschritte im Hinblick auf den Standard eCH-0059 Version 3.0 (oder spätere Versionen) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG 2.1 des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, welche von der E-Accessibility-Richtlinie der EU inspiriert sind.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK, Übereinkommen über die Rechte von Menschen mit Behinderungen) unterzeichnet. Artikel 9 der UNO-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies schliesst auch die Information und Kommunikation, einschliesslich der entsprechenden Technologien und -systeme ein. Das Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen, kurz BehiG, schreibt in Art. 14 vor, dass die Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten nehmen müssen. Ohne Garantierung der E-Accessibility wären Menschen mit Sehbeeinträchtigung vom staatlichen Angebot in Form eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Briefta-sche ausgeschlossen.

Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Praktische Überlegungen:

Für Menschen mit Sehbeeinträchtigung stellt die Digitalisierung eine Chance dar zu einem breiteren Zugang zu Dienstleistungen aller Art. Die digitalen Kommunikationskanäle sind das eigentliche Tor zu den Informationen für die sehbehinderten Menschen. Zwingende Voraussetzung für die Nutzbarkeit der digitalen Angebote ist aber, dass diese barrierefrei zur Verfügung stehen. Deshalb muss vor jeder Publikation eines Web-basierten Produkts und auch vor jedem Update geprüft werden, ob dieses barrierefrei zugänglich ist. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das design-for-all-Prinzip zur Anwendung kommen, analog dem europäischen Recht.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Wir verweisen diesbezüglich auch auf die Antwort des Bundesrates auf die Frage [22.7406](#) von Nationalrätin Franziska Ryser, in der er ausführt, dass der standardmässige Einsatz von Usability-Tests im Rahmen der Weiterentwicklung der Instrumente zur Gewährleistung der Barrierefreiheit geprüft wird. Die Freigabe bzw. Lancierung der E-ID darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet, wie aktuelle Beispiele beim Bund (z.B. beim elektronischen Patientendossier, beim elektronischen Einreiseformular oder beim Covid-Zertifikat) oder in den Kantonen (kantonale e-ID Schaffhausen) zeigen.

Anträge:

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein eigener Artikel «Barrierefreiheit» aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen die von Antragstellenden, Inhaber:innen einer E-ID, Aussteller:innen, Verifikator:innen und weiteren Usergruppen genutzt oder betrieben werden können.
2. In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein eigenes Kapitel zur Barrierefreiheit aufzunehmen. Dieses beschreibt detailliert, wie die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
3. Zur Kontrolle der Barrierefreiheit sei ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Freundliche Grüsse



Kannarath Meystre
Generalsekretär



Martin Abele
Bereichsleiter Interessenvertretung

Zürich, 17. Oktober 2022



GEMEINSAM NACH VORNE SEHEN.

Geschäftsstelle

Friedackerstrasse 8

8050 Zürich

Tel. 044 317 90 00; Fax 044 317 90 01

info@blind.ch; www.blind.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundesamt für Justiz

Per E-Mail an: rechtsinformatik@bj.admin.ch
Dateiformate: gleichlautend als PDF und Word



Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Karin Keller-Sutter

Sehr geehrte Damen und Herren

Der Schweizerische Blindenbund (SBb) ist eine Selbsthilfeorganisation blinder und sehbehinderter Menschen mit rund 40 Mitarbeiterinnen und Mitarbeitern. Er gewährleistet in 8 Beratungsstellen die professionelle Durchführung von Massnahmen, die eine weitgehende Selbständigkeit blinder und sehbehinderter Menschen in materieller, beruflicher, gesellschaftlicher und kultureller Hinsicht ermöglichen und unterstützen sollen.

Mit Schreiben vom 29.06.2022 haben Sie den Schweizerischen Blindenbund zur Stellungnahme zur rubrizierten Vernehmlassung eingeladen. Dafür bedanken wir uns bestens.

Grundsätzlich begrüsst der SBb die Einführung eines staatlichen elektronischen Identitätsnachweises.

Der Schweizerische Blindenbund (SBb) unterstützt die Positionen von Procap Schweiz und dem SBV und folgen diesen weitestgehend in unserer Vernehmlassungsantwort.

Wir beschränken uns in unserer Antwort auf den Bereich der Barrierefreiheit, der beim hier vorliegenden Gesetzesvorhaben für Menschen mit Behinderungen - insbesondere Blinde und Sehbehinderte - von äusserst grosser Wichtigkeit ist.

Grundsätzliche Erwägungen:

Der SBb ist erstaunt, dass der Aspekt der E-Accessibility keine Erwähnung in der Vorlage findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-

Accessibility) auf allen Ebenen sichergestellt wird. In der Entwicklung sind sämtliche Umsetzungsschritte im Hinblick auf den Standard eCH-0059 Version 3.0 (oder spätere Versionen) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG 2.1 des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, welche von der E-Accessibility-Richtlinie der EU inspiriert sind.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK, Übereinkommen über die Rechte von Menschen mit Behinderungen) ratifiziert. Artikel 9 der UNO-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies schliesst auch die Information und Kommunikation, einschliesslich der entsprechenden Technologien und -systeme ein. Das Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (BehiG) schreibt in Art. 14 vor, dass die Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten nehmen müssen. Ohne Garantierung der E-Accessibility wären Menschen mit Sehbeeinträchtigung vom staatlichen Angebot in Form eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Brieftasche ausgeschlossen.

Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Praktische Überlegungen:

Für Menschen mit Sehbeeinträchtigung ist die Digitalisierung eine Chance für einen umfassenden Zugang zu Dienstleistungen aller Art. Die digitalen Kommunikationskanäle sind das eigentliche Tor zu den Informationen für die blinden und sehbehinderten Menschen. Zwingende Voraussetzung für die Nutzbarkeit der digitalen Angebote ist aber, dass diese barrierefrei zur Verfügung stehen. Deshalb muss vor jeder Publikation eines Web-basierten Produkts und auch vor jedem Update geprüft werden, ob dieses barrierefrei zugänglich ist. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das design-for-all-Prinzip zur Anwendung kommen, analog europäischem Recht.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Auf die Frage [22.7406](#) von Nationalrätin Franziska Ryser antwortet der Bundesrat, dass der standardmässige Einsatz von Usability-Tests im Rahmen der Weiterentwicklung der Instrumente zur Gewährleistung der Barrierefreiheit geprüft wird. Die Freigabe bzw. Lancierung der E-ID darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet, wie aktuelle Beispiele beim Bund (z.B. beim elektronischen Patientendossier, beim elektronischen Einreiseformular oder beim Covid-Zertifikat) oder in den Kantonen (kantonale E-ID Schaffhausen) zeigen.

Anträge:

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) ist ein eigener Artikel «Barrierefreiheit» aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen, die von

Antragstellenden, InhaberInnen einer E-ID, AusstellerInnen, VerifikatorInnen und weiteren Usergruppen genutzt oder betrieben werden können.

2. In den Ausführungsbestimmungen zum E-ID-Gesetz ist ein eigenes Kapitel zur Barrierefreiheit aufzunehmen. Dieses beschreibt detailliert, wie die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
3. Zur Kontrolle der Barrierefreiheit ist ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Nachträgliche Massnahmen zur Gewährleistung der Zugänglichkeit von IT-Projekten bleiben lückenhaft, unbefriedigend und verursachen hohe Kosten, die verhindert werden können.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Freundliche Grüsse

Schweizerischer Blindenbund



Paul Cuska
Stv. Geschäftsführer



Roland Gossweiler
Delegierter des Vorstandes für Sozialpolitik und Interessensvertretung

DIDAS Stellungnahme
zur
Vernehmlassung BGEID – Oktober 2022

Eingereicht an:
Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern
per Mail an: rechtsinformatik@bj.admin.ch

Eingereicht durch:
Digital Identity and Data Sovereignty Association (www.didas.swiss)
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
info@didas.swiss

Sehr geehrte Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir bedanken uns hiermit, in Fortsetzung unserer Stellungnahme zum Diskussionspapier «Zielbild E-ID», im Rahmen der Vernehmlassung zum BGEID erneut Stellung nehmen zu dürfen.

Die Digital Identity and Data Sovereignty Association (DIDAS) ist ein gemeinnütziger und nicht gewinnorientierter schweizerischer Verein, der mit dem Ziel gegründet wurde, "Die Etablierung und Förderung der Schweiz als führendes Ökosystem bei der Entwicklung und Einführung von Technologien, Dienstleistungen und Produkten zur Wahrung der Privatsphäre, welche die digitale Identität und elektronisch überprüfbare Daten bewahren sowie anwenden."

Wir würdigen die offene Vorgehensweise der Bundesverwaltung und die hohe Qualität des Gesetzesentwurfs. Zudem ist das Verständnis und die Anwendung eines prinzipienbasierten, iterativen und kollaborativen Vorgehens, als kritische Erfolgsfaktoren für die Planung und Einführung einer nachhaltigen Vertrauensinfrastruktur, der Etablierung einer elektronischen Identität und weiterer digitaler Nachweise, sowie deren flächendeckende Verwendung, zu würdigen.

Es freut uns ausserordentlich, dass sich DIDAS und seine Mitglieder im vergangenen Jahr wertschaffend in den Prozess einbringen konnte. So ist die vorliegende Stellungnahme als eine Gemeinschaftsarbeit aller Mitglieder des Vereins DIDAS unter der Federführung des Vorstandes anzusehen.

Rotkreuz, im Oktober 2022



Daniel Säuberli
Präsident



Ursula Sury
Vizepräsidentin



Marco Dütsch
Vorstand



Vasily Suvorov
Vorstand



Tim Weingärtner
Vorstand



I. Rekapitulation/Zusammenfassung unserer Stellungnahme zum Diskussionspapier «Zielbild E-ID» im Jahr 2021

Wir sind fest davon überzeugt, dass Ökosysteme digitaler Attribute nach den Prinzipien von SSI (Self Sovereign Identity resp. die der selbstbestimmten digitalen Identität) in Kontext mit dem schweizerischen Wertesystem und unserem föderalistischen Staatskonstrukt sowie unserer internationalen Positionierung, den aktuell bestmöglichen Ansatz darstellen, um eine nachhaltig zukunftsfähige, flexible, datenschutzfreundliche und umfangreiche E-ID Funktionalität in der Schweiz zu etablieren.

Daher fordern wir, dass der Staat sich mindestens auf die Herausgabe von digitalen Identitätsattributen (oder digitalen Nachweisen) in Kontext der Weiterentwicklung der Vision E-ID, sowie auf die relevanten Gesetze auf Ambitions-Niveau 3 konzentriert. Wir sind der Überzeugung, dass der Erfolg der E-ID Initiative in der Schweiz nur dann erzielt werden kann, wenn Public-Private-Partnerships ermöglicht werden (PPP, als Zusammenarbeits-, nicht als Rechtskonstrukt), welche die staatlichen Identitätsattribute als Vertrauensanker resp. als Basis für den Aufbau eines oder mehrerer Ökosysteme verwenden können. Wichtig in diesem Zusammenhang ist auch zu verstehen, dass Ökosysteme bereits ohne diese Attribute entstehen und genutzt werden können, die durch die spätere Verfügbarkeit dieser staatlichen Attribute an Vertrauenswürdigkeit gewinnen können.

Wir sehen also die Rolle des Staats als einen wichtigen Teil des künftigen Ökosystems digitaler Nachweise, der dieses durch die relevanten, hoheitlich herausgegebenen und elektronisch verifizierbaren Attribute ermöglicht. Die SSI-Mechanismen machen es dann weiteren Akteuren möglich, ihre Anwendungsfälle darauf auf- und auszubauen und durch Marktmechanismen und technologische Fortschritte (z.B. via digitaler Brieftaschen oder «Wallets») diese möglichst umfangreich der Gesellschaft zur Verfügung zu stellen. Aufgrund der konsumentenzentrierten Adaption von Wallets ist es in diesem Zusammenhang ausserordentlich wichtig, die Zivilgesellschaft von Anfang an in den Prozess einzubeziehen. Es ist zudem vorteilhaft zu fordern, die Wallets mit einem technologischen Vertrauensanker durch die Nutzung von Open Source Communities und -Lizenzen zu entwickeln.

Einer der wichtigsten Eigenschaften von SSI ist, dass sich die Entwicklung nachhaltig über eine solide Governance und den eingebetteten technologischen Möglichkeiten (wie z.B. Zero Knowledge Proof-Verfahren) sowie der Etablierung von Prinzipien steuern lässt, sodass die Grundrechte, Datenschutz, Privatsphäre und andere hoheitliche Anforderungen «by design» gewährleistet werden können. Dies gleichzeitig, ohne dass Wettbewerbsfähigkeiten verschiedener Marktakteure oder die Souveränität der Gesellschaft reglementiert oder eingeschränkt werden - oder werden müssen, sodass wir national und international digital agil und handlungsfäh bleiben.



Unsere Stellungnahme zum Zielbild E-ID kann unter folgendem Link nachgeschlagen werden: <https://www.didas.swiss/wp-content/uploads/2021/10/Stellungnahme-DIDAS-FINAL-V1.0-website.pdf>

II. Stellungnahme zur Vernehmlassung BGEID

Die in unserer Stellungnahme zum Diskussionspapier E-ID veröffentlichte Meinung hat demnach weiterhin Gültigkeit. Für die nachhaltige Meinungsbildung und Lösungsfindung gelten die SSI-Prinzipien.

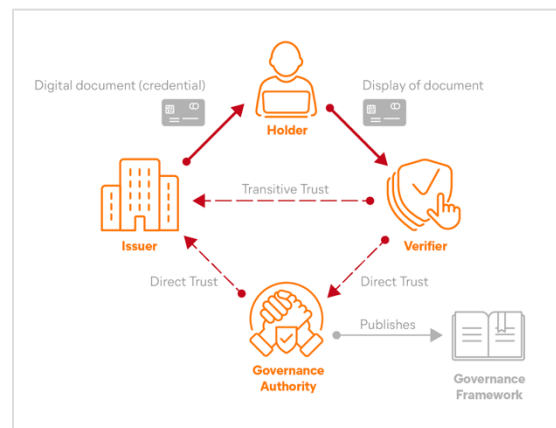
Es ist uns zudem ein Bestreben, einen «Balanced-approach» anzuwenden, der eine zeitnahe Etablierung des Ambitionsniveaus 3 ermöglicht und gleichzeitig die nötige Flexibilität im Gesetz verankert, um den sich schnell entwickelnden technologischen Möglichkeiten und der fortschreitenden Digitalisierung (resp. deren Akzeptanz in der Gesellschaft) gerecht zu werden.

Der vorliegende Vorentwurf des Bundesgesetzes enthält die zwingend notwendigen gesetzlichen Grundlagen, ist aber auch genügend offen formuliert und wird deshalb von unseren Mitgliedern als sehr gut beurteilt. Wir sind der Überzeugung, dass der Vorschlag für das E-ID-Gesetz eine solide Basis darstellt und den Rahmen für eine zukunftssträchtige Vertrauensinfrastruktur setzt, in welchem eine staatlich herausgegebene E-ID das Kernelement darstellt. Wir begrüßen die Schaffung eines Rechtsrahmens für diese Vertrauensinfrastruktur.

Die E-ID werden gemäss Vorentwurf BGEID in einigen Belangen als digitale Kopie eines anderen gültigen Ausweises realisiert (Art. 3). Dies betrachten wir nur dann als sinnvoll, wenn dadurch eine Umsetzung substanziell schneller erfolgen kann. Künftige Anpassungen sollen aufgrund der fortschreitenden Digitalisierung die E-ID als eigenständigen Nachweis etablieren können, ohne sich zwingend auf andere Ausweise abzustützen. Dadurch kann z.B. die E-ID einen eigenen Lebenszyklus erhalten und als gleichwertiges Ausweisdokument anerkannt werden, wobei den Inhaberinnen und Inhabern grundsätzlich in jeder Situation die Wahl des Nachweises zu gewähren ist.

In Ökosystemen elektronischer Nachweise kann somit der Staat die Rolle des «Enablers» übernehmen und das Ziel verfolgen, ein attraktives Umfeld für vielfältigste Anwendungen zu schaffen. Der Staat übernimmt zudem die Rolle der Governance Authority im sogenannten «Trust Diamond» und erlässt ein einheitliches Governance Framework.

Ein erfolgreiches Ökosystem elektronischer Nachweise lässt sich jedoch nur gemeinsam mit den beteiligten Aussteller/innen, Verifikator/innen und Inhaber/innen elektronischer Nachweise konzipieren, pilotieren und umsetzen. Um den Reifungsprozess entlang aller involvierter Stakeholder zu beschleunigen (aber auch um den Nutzenden die Möglichkeiten aufzuzeigen), sind explorative Pilotprojekte des Bundes in Zusammenarbeit mit Stakeholdern aus dem privaten



und öffentlichen Sektor von grosser Bedeutung. Damit kann das Ziel verfolgt werden gemeinsam zu lernen, ohne die Wahl spezifischer Technologien bereits in dieser Phase zu präjudizieren. Diese Projekte sollten vom Bund mit den nötigen finanziellen Mitteln ausgestattet werden. Wünschenswert wäre daher die Verankerung einer gemeinsamen Pilotierung mit gemischter Beteiligung der Akteure aus öffentlichem und privatem Sektor entlang einheitlicher Prinzipien, z.B. an geeigneter Stelle auf Verordnungsstufe.

Als weitere Massnahme zur Beschleunigung der Adaption elektronischer Nachweise, empfehlen wir einen weiterhin offenen und partizipativen Prozess und den Einbezug von Expertengruppen in die Gestaltung der Verordnungen und die weitere BGEID-Umsetzung. Eine Organisation wie DIDAS oder andere Expertennetzwerke könnten sich demnach dazu eignen, partnerschaftlich mit bestehenden Gremien und Institutionen wie z.B. Innosuisse, kollaborativ Projekte mit klarem Nutzen zu begleiten resp. zu orchestrieren.

Wir empfehlen es zudem, die im Ökosystem verwendeten Begrifflichkeiten einheitlich und angelehnt an internationale Standards zu definieren, wie z.B. Verifizierer, Vertrauensregister, Basisregister etc. In diesem Zusammenhang sollten auch Rahmenthemen wie Datensparsamkeit nicht im BGEID verankert werden, da sie ohnehin bereits durch bestehende Gesetze wie das DSG Gültigkeit haben. Sie sollten jedoch im Kontext mit neuen technologischen Mechanismen klar definiert werden.

Im Rahmen weiterer elektronischer Nachweise, ist es essenziell, wo möglich einheitliche Standards zu definieren wie auch Unterschiede in sektorieller Governance im Ökosystem zu ermöglichen. So sollen z.B. für eine Wohnsitzbestätigung immer die gleichen Attribute genutzt werden, währenddem in verschiedenen Sektoren unterschiedliche Attribute, z.B. für den Nachweis einer bestimmten Kompetenz (z.B. Spezialisierungen FMH bei Ärzten) verwendet werden sollen. Diese sektoriellen Unterschiede sollen sich möglichst nach internationalen Standards im jeweiligen Sektor ohne "Swiss Finish" richten. Diese Standards sollen durch eine autoritative Instanz in einem offenen und partizipativen Prozess verwaltet und kommuniziert werden.

Wir unterstützen zudem das Nutzen der AHV Nummer als einheitlichen Identifikator. Das Nutzen der AHV Nummer muss jedoch zwingend im Gesetz erwähnt werden, damit diese als interne Verifizierung überhaupt verwendet werden darf.

Wir unterstützen eine Ablauffrist für die E-ID, da sie ggf nicht widerrufen wird und auch über ihr Ablaufdatum hinaus als Identifikationsmittel akzeptiert werden könnte. Dabei sollten die technischen Möglichkeiten (z.B. expiration Date) genutzt werden.

DIDAS freut sich auf die weiteren Schritte und empfiehlt eine prioritäre Behandlung im Bundesrat. Weiterhin empfehlen wir das Vorantreiben von technischen Proof of Concepts und Minimal Viable Products (MVPs) unter Einbezug aller Stakeholder und der Zivilgesellschaft, um die vorgeschriebenen Perioden für den politischen Entscheid bestmöglich zu nutzen.



Detaillierte Stellungnahme zu relevanten Abschnitten und Artikeln im Vorentwurf:

Artikel	Vorentwurf Bundesgesetz	DIDAS Stellungnahme
1.1	<p>Art. 1</p> <p>1 Dieses Gesetz regelt:</p> <p>a. den staatlichen elektronischen Identitätsnachweis natürlicher Personen (E-ID) und andere elektronische Nachweise;</p> <p>b. die Infrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen (Vertrauensinfrastruktur);</p> <p>c. die Rollen und Verantwortlichkeiten bei der Bereitstellung und Nutzung dieser Infrastruktur.</p>	<p>Anpassung: a. den staatlichen elektronischen Identitätsnachweis natürlicher Personen (E-ID) und weiterer elektronischer Nachweise</p>
1.2	<p>2 Es hat zum Zweck:</p> <p>a. die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten;</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik 2. Datensicherheit, 3. Datensparsamkeit, und 4. dezentrale Datenspeicherung; <p>c. zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen;</p> <p>d. die Standardisierung der E-ID sowie die Sicherheit der Infrastruktur und der Ausstellung und Überprüfung der elektronischen Nachweise zu gewährleisten, ohne die technische Entwicklung unnötig einzuschränken.</p>	<p>Ergänzung: e. die Rechtmässigkeit und Gültigkeit von elektronischen Nachweisen in digitalen sowie im physischen Räumen zu ermöglichen und diese auf Basis einer elektronischen Vertrauensinfrastruktur physischen Nachweisen gleichzustellen.</p>
2.3	<p>Sie enthält zudem die folgenden Daten: a. AHV-Nummer;</p> <p>b. E-ID-Nummer;</p> <p>c. Ausstellungsdatum der E-ID;</p> <p>d. Ablaufdatum der E-ID;</p> <p>e. f.</p> <p>SR 142.51 2 / 12</p> <p>3 4</p> <p>Angaben zum Ausweis, der im Ausstellungsprozess der E-ID verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises;</p> <p>Angaben zum Ausstellungsprozess</p>	<p>Ergänzung: Art. 25 Technische Entwicklung und fortschreitende Digitalisierung</p> <p>Zu ergänzen 25.3: Der Bundesrat kann vorsehen, der E-ID mit einem eigenen Lebenszyklus bzw. einem direkten Ausstellungsprozess zu versehen, falls die Zivilgesellschaft dies im Rahmen der fortschreitenden Digitalisierung fordert.</p>
4.1	<p>Art 4 Ausstellung</p> <p>1 Wer eine E-ID will, muss deren Ausstellung dem Bundesamt für Polizei (fedpol) beantragen.</p>	<p>Ergänzung Art 4.5. - Es können zum Ausstellungszeitpunkt mehrere E-ID (oder weitere elektronische Nachweise) ausgestellt werden (z.B. für Multi-Device Unterstützung oder auch um die Ausstellung von Ausweisen minderjähriger an ihre gesetzlichen Vertreter zu ermöglichen).</p>

4.4	4 Zum Zweck der Gesichtsbildverifikation der antragstellenden Person können während dem Ausstellungsprozess biometrische Daten erhoben und mit dem Gesichtsbild aus dem ISA oder dem ZEMIS verglichen werden.	Ergänzung: Die biometrischen Daten können nach der Verifikation an einem revisionssicheren Ort ausserhalb des täglichen Zugriffs aufbewahrt werden oder sind zu vernichten.
7.1	Art. 7 Sorgfaltspflicht 1 Die Inhaberin oder der Inhaber einer E-ID muss die notwendigen und zumutbaren Massnahmen treffen, damit ihre oder seine E-ID nicht missbräuchlich verwendet werden kann.	Ergänzung Sorgfaltspflicht: Die Ausstellerin der E-ID hat die Pflicht die Inhaberin auf dem aktuellen Informationsstand bezüglich der verantwortungsvollen Nutzung der E-ID in physischen und digitalen Räumen zu halten.
8	Art. 8 Anlaufstellen der Kantone Die Kantone bezeichnen die Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.	Ergänzung: Die Ausstellerin stellt die dazu benötigten technischen Schnittstellen einheitlich zu Verfügung.
9	Art. 9 Pflicht zur Akzeptanz der E-ID Jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, muss die E-ID akzeptieren, wenn sie eine elektronische Identifizierung vornimmt.	Art 9 und 10: Die Freiwilligkeit der Nutzung der E-ID für Inhaberinnen und die Pflicht zur Akzeptanz der E-ID durch Träger öffentlicher Aufgaben sollen möglichst umfassend gelten. Die Akzeptanzpflicht soll sich auch auf Prozesse erstrecken, bei denen eine Person persönlich erscheint.
10	Art. 10 Vorweisen einer E-ID Wer in einem Prozess einer Person, die persönlich erscheint, die Möglichkeit bietet, die E-ID oder Teile davon vorzuweisen, muss dieser Person die Wahl lassen, sich stattdessen mit einem Ausweisdokument nach dem AwG6, einem Ausländerausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl oder einem Ausweis nach Artikel 13 Absatz 1 des Ausländer- und Integrationsgesetzes vom 16. Dezember 20057 auszuweisen, sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können.	Anpassung: Die Inhaberin einer E-ID kann bei einer Interaktion in der physischen Welt nicht dazu verpflichtet werden, sich mithilfe der E-ID auszuweisen. Sie kann sich stattdessen mit einem gleichwertigen gültigen Ausweis gemäss AwG oder einem Ausländerausweis nach der Bundesgesetzgebung über Ausländerinnen und Ausländer, Integration und Asyl oder einem Ausweis nach Artikel 13 Absatz 1 des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005 ausweisen.

13.1	<p>Art. 13 Widerruf</p> <p>1 Die Ausstellerinnen können die von ihnen ausgestellten elektronischen Nachweise widerrufen.</p>	<p>Ergänzung: Inhaber können die erhaltenen elektronischen Nachweise ohne Kenntnis der Ausstellerin löschen.</p>
13.2	<p>2 Sie widerrufen diese unverzüglich, wenn:</p> <p>a. die Inhaberin oder der Inhaber dies verlangt;</p> <p>b. die gesetzliche Vertretung von Minderjährigen bis zum vollendeten vierzehnten Lebensjahr oder von Personen unter umfassender Beistandschaft dies verlangt;</p> <p>c. der begründete Verdacht auf Missbrauch des elektronischen Nachweises besteht;</p>	<p>Ergänzung: Es sollte auch möglich sein, nicht—revozierbare elektronische Nachweise auszustellen, ggw benötigen diese den Konsensus der Inhaberin und Ausstellerin beim Ausstellungsprozess.</p>
14	<p>Art. 14 Form und Aufbewahrung von elektronischen Nachweisen</p> <p>Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.</p>	<p>Art. 14 Form und Aufbewahrung von elektronischen Nachweisen</p> <p>Die Inhaberin oder der Inhaber erhält den elektronischen Nachweisen als Datenpakete und bewahrt sie mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.</p> <p>Ergänzung: Die technischen Mittel, insbesondere elektronische Brieftaschen, müssen Zertifizierungsanforderungen erfüllen, falls die E-ID mit anderen elektronischen Nachweisen in derselben Brieftasche interagieren soll.</p> <p>oder: Die technischen Mittel, insbesondere elektronische Brieftaschen, müssen Zertifizierungsanforderungen erfüllen, falls eine E-ID darin gespeichert ist oder gespeichert werden kann.</p>
15.1	<p>Art. 15 Übertragbarkeit von elektronischen Nachweisen</p> <p>1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden.</p>	<p>Input: Im Falle einer gesetzlichen Vertretung soll für den Vertreter ein elektronischer Nachweis ausgestellt werden können, der ihn als Vertreter eines Subjekts resp. Inhabers ausweist.</p> <p>Des Weiteren sollen Mechanismen zur Verfügung gestellt werden können, die es einem Vertreter ermöglichen im Namen eines vertretenen Subjekts zu handeln.</p> <p>Dies soll für personenbezogene elektronische Nachweise gelten.</p>
16	<p>Art. 16 Vorweisen von elektronischen Nachweisen</p>	<p>Ergänzung 16.4: Verifikatoren dürfen im Sinne der Datensparsamkeit zu jedem Zeitpunkt nur die Daten abfragen, welche für die Erfüllung des jeweiligen kommunizierten Geschäftsfalls im Sinne des Inhabers nötig sind. —> Wird im Datenschutzgesetz bereits zu genüge abgedeckt, sollte ggf im digitalen Raum in Zusammenhang mit der E-ID jedoch speziell behandelt werden.</p>

16.2	2 Das Vorweisen und Überprüfen eines elektronischen Nachweises erfolgt ohne dass die Ausstellerin davon Kenntnis hat.	Anpassung: 2 Das Vorweisen und Überprüfen eines elektronischen Nachweises erfolgt ohne dass die Ausstellerin oder dritte davon Kenntnis haben, ausser der Inhaber erwünscht dies explizit. Ergänzung 16.4. Ein expliziter Wunsch muss für jeden Geschäftsfall einzeln geäussert werden. Deren Verweigerung darf durch die Ausstellerin oder Verifikatorin nicht als Hindernis für den Bezug eines bestimmten Dienstes verwendet werden.
17.1	1 Der Bund stellt ein öffentlich zugängliches Register (Basisregister) zur Verfügung, das Daten enthält über: a. die Ausstellerinnen elektronischer Nachweise; b. die Verifikatorinnen; c. den Widerruf von elektronischen Nachweisen.	Input: Die Daten der Verifikatorinnen müssen nicht zwingend im Basisregister publiziert werden.
17.3	3 Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.	Input: Diese Eintragungen müssen freiwillig sein. Es besteht Wahlmöglichkeit für die eingesetzten Wallets, aber auch bei der Wahl der Issuer und Verifier. Somit könnten auch Issuer oder Verifier gewählt werden, die andere Basisregister (als das hier geregelte) oder andere Methoden verwenden. Dies ist auch in Bezug auf eine Internationalisierung wichtig.
18	Art. 18 System zur Bestätigung von Identifikatoren	Input: Diese Begrifflichkeit erscheint uns sehr umständlich. Wir schlagen den Begriff "Vertrauensregister" vor.
18.2	2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.	Input: Aus unserer Sicht ist der Einbezug bzw. die Zulassung und Bestätigung von ausgewählten privaten Ausstellerinnen und Verifikatorinnen für ein erfolgreiches E-ID-Ökosystem zwingend notwendig. Dies darf daher nicht nur als Möglichkeit formuliert werden. So soll die Rolle von Akkreditierungsstellen bereits frühzeitig ermöglicht werden und z.B. Daten aus relevanten Registern (z.B UID-Register, dem Handelsregister, etc.) weiterverwendet werden.

23	Art. 23 Quellcode der Vertrauensinfrastruktur Der Bund veröffentlicht den Quellcode der von ihm zur Verfügung gestellten Elemente der Vertrauensinfrastruktur.	Ergänzung: und die Rechte Dritter gewahrt werden.
26.1	Art. 26 1 Die Ausstellerinnen und Verifikatorinnen elektronischer Nachweise entrichten für ihre Einträge im Basisregister und im System zur Bestätigung von Identifikatoren eine Gebühr.	Ergänzung: Die Preisgestaltung, insbesondere für Einträge in das Basisregister, hat moderat zu erfolgen.
27	Art. 27 Internationale Abkommen	Ergänzung 27.3: Es ist sicherzustellen, dass sich die benötigten technischen Mittel zur Erfüllung der Verträge im Sinne dieses Bundesgesetzes bereits gestellt werden und die Prinzipien von Privacy-by-design, der Offenheit (Code), Interoperabilität und Portabilität von digitalen Nachweisen in verbundenen Netzwerken beibehalten werden.

Die Stellungnahme ist eine Gemeinschaftsarbeit aller Mitglieder des Vereins DIDAS unter der Federführung des Vorstandes. Da DIDAS als unabhängige Expertengruppe aus Mitgliedern aller Stakeholdergruppen besteht, steht es unseren Mitgliedern frei auf eine Nennung zu verzichten. Um jedoch das Gewicht von DIDAS zu veranschaulichen, freuen wir uns folgend einige unserer Mitglieder explizit zu nennen:



Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an: rechtsinformatik@bj.admin.ch

18. Oktober 2022

Stellungnahme zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Am 29. Juni 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID). Wir bedanken uns für die Einladung zur Stellungnahme.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Entwurf wie folgt Stellung:

Grundsätzliches

Die Digitale Gesellschaft hat die gesellschaftliche, politische und technische Debatte zum Bundesgesetz über elektronische Identifizierungsdienste (BGEID) eng begleitet und das Referendum sowie die Volksabstimmung massgeblich geprägt. Die Hauptkritikpunkte des Gesetzes betrafen den Zweck und die Herausgeberschaft («staatlicher, elektronischer Ausweis» anstatt «privates Login») sowie den mangelnden Datenschutz (Datenschutz durch Technik/Privacy-by-Design und Datensparsamkeit/Privacy-by-Default). Dies waren dann auch die Gründe, weshalb das Gesetz mit grosser Mehrheit an der Urne abgelehnt wurde.

Die Digitale Gesellschaft begrüsst die Neuauflage des E-ID-Gesetzes und ist mit der Stossrichtung einverstanden.

Wir vertreten jedoch die Auffassung, dass der Schutz der Persönlichkeit und der Personendaten im vorliegenden Vorentwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise noch unzureichend umgesetzt sowie der Schutz vor Missbrauch der Daten noch unzureichend gewährleistet ist. Dies betrifft insbesondere die drohende «Überidentifikation».

Im Nachfolgenden werden wir dies an den einzelnen Artikeln erörtern und Änderungsvorschläge anbringen.

Bearbeitung von Personendaten

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht, abgeleitet von Art. 13 Abs. 2 der Bundesverfassung (BV). Ein elektronischer Nachweis ist ein Eingriff in dieses Grundrecht und hat gemäss Art. 36 BV verhältnismässig zu erfolgen; im Speziellen sollte die Grundrechtseinschränkung nicht weiter gehen, als notwendig und sachlich gerechtfertigt ist. Diesem Grundsatz ist im vorgeschlagenen Gesetz ungenügend Rechnung getragen. Wir vertreten die Auffassung, dass die gesetzlich vorgesehene Erhebung von Daten sowie ihre Bearbeitung auf das zu ihrem Zweck unbedingt Erforderliche reduziert werden muss, um dem Gehalt von Art. 13 Abs. 2 BV zu wahren.

Personendaten, welche in Bezug auf einen elektronischen amtlichen Nachweis erhoben und verarbeitet werden, erfordern zudem einen höheren und spezifischeren Schutz, als es das (revidierte) Datenschutzgesetz (DSG) bietet – und demnach eine ungenügende Grundlage für den Schutz der Personendaten nach dem BGEID darstellt.

Wir sind der Auffassung, dass amtlich erhobene, verwaltete und bereitgestellte Daten ein erhöhter Schutz beizumessen ist und dass dies im BGEID selbst vorzusehen ist.

Dass BGEID schafft eine neue Kategorie von Daten: Daten, die erstens besonders schutzwerten Charakter haben, zweitens auch behördlich verifiziert sind und drittens, für welche eine breite private Verwendung vorgesehen ist. Sie bilden eine neue Kategorie an Daten, welche durch das DSG nicht gedeckt sind. Das allgemein formulierte Datenschutzgesetz sowohl in der derzeitigen als auch in der künftigen, revidierten Fassung vermag nicht, einen adäquaten Schutz zu liefern, gerade betreffend der Überidentifizierung.

Nach dem DSG kann eine Datenbearbeitung erfolgen, sofern ein überwiegendes privates oder öffentliches Interesse eine solche rechtfertigt. Hier besteht ein erheblicher Interpretationsspielraum der Beteiligten und lässt in der Praxis auch zweckfremde Datenbearbeitungen zu, soweit sie etwa aufgrund eines wirtschaftlichen Interesses der Inhaberin oder des Inhabers der Datensammlung für verhältnismässig angesehen werden können (Beispiel: Online-Tracking, Kreditwürdigkeit). Meist wird zudem eine Einwilligung durch das Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) und/oder der Datenschutzerklärung eingeholt, ohne dass diesem Vorgang widersprochen werden könnte. Das DSG schafft auch keinen Anspruch auf ein Widerspruchsrecht, wonach der Bearbeitung – mindestens im Nachhinein – (einfach, also ohne Klage auf Persönlichkeitsverletzung) widersprochen werden könnte.

Das Schweizer DSG geht überdies betreffend Vorschriften hinsichtlich Identifikation und Tracking deutlich weniger weit als die EU-Richtlinie (DSGVO). Namentlich entfällt in der Schweiz das Kopplungsverbot, welches in der Praxis verhindert, dass eine Einwilligung in eine zweckfremde Datenbearbeitung über eine Kopplung an die Leistung selbst abgenötigt wird. Dies kann dazu führen, dass Private Daten sammeln und gebrauchen können, welche nicht für die Erbringung von Leistungen erforderlich sind und für welche keine eigentliche Freiwilligkeit besteht.

Damit verletzt nach unserer Ansicht die vorgeschlagene Fassung des BGEID sowohl den Grundsatz der Datensparsamkeit als auch der informationellen Selbstbestimmung. Neben der Verletzung der genannten Grundrechte und Grundsätze würde die drohende Überidentifikation das Vertrauen in die elektronische Identifikation schädigen. Die Akzeptanz würde darunter insgesamt stark leiden. Im BGEID sind deshalb ausgestaltete, konkrete Bestimmung betreffend diesen Grundsätzen

vorzusehen; Vorschläge zu diesen Bestimmungen werden weiter unten konkretisiert.

Rechtssystematisch stehen solche Bestimmungen ohne Kollision mit dem Datenschutzgesetz. Art. 4 DSG (Art. 6 nDSG) bestimmt, dass die Bearbeitung von Personendaten nur rechtmässig erfolgen darf, äussert sich zum rechtlichen Rahmen aber nicht. Damit besteht Gestaltungsspielraum des rechtlichen Rahmens durch das BGEID, wobei zu betonen ist, dass im heutigen rechtlichen Rahmen die konkrete Ausgestaltung des rechtlichen Rahmens einer Datenbearbeitung spezialgesetzlich, und nicht durch das DSG, vorgenommen wird.

Diskriminierungsfreier Zugang zu Leistungen

Unter mehreren Gesichtspunkten erweist sich für problematisch, wenn der Erhalt von Leistungen vom Besitz einer E-ID abhängig gemacht werden. Damit werden einerseits Menschen ausgeschlossen, welche nach geltender Gesetzgebung kein Anrecht auf eine E-ID haben, andererseits aber auch solche, welche nicht über die technischen Kenntnisse oder die Mittel verfügen, eine E-ID zu beantragen, oder dies aus persönlichen Gründen ablehnen. Unter Hinweis auf das Diskriminierungsverbot (Art. 8 BV) ist ein diskriminierungsfreier Zugang zu Leistungen deshalb gesetzlich zu gewährleisten.

Hierzu sei noch angemerkt, dass nach den vorgeschlagenen Bestimmungen nur Menschen Anrecht auf eine E-ID haben, welche in der Schweiz über eine Aufenthaltsbewilligung verfügen. Dies schliesst alle Menschen aus, welche über eine solche nicht verfügen und sich unter einem anderen Titel als einer ordentlichen Aufenthaltsbewilligung in der (digitalen) Schweiz aufhalten. Das Gesetz könnte eine Möglichkeiten vorsehen, dass bei genügender Identifikation (etwa über einen ausländischen Pass) eine elektronische ID ausgestellt werden kann, wobei bei unsicherer Identifikation diesem Umstand mit einer Anmerkung Rechnung getragen werden könnte.

Durchsetzbarkeit

Damit Gesetzesbestimmungen wirksam sind, müssen sie durchsetzbar sein. Das vorgeschlagene Gesetz verzichtet vollständig auf spezifische Bestimmungen, um Bestimmungen durchzusetzen und Verletzungen beheben zu können. Wir sehen es als wichtig an, dass juristische und natürliche Anbieterinnen (Ausstellerinnen, Verifikatorinnen), welche Bestimmungen verletzen, einer Strafbestimmung unterliegen, und dass ein vereinfachter und kostenfreier Zugang zu Verfahren zur

Behebung von Verletzung sowohl für die Subjekte des elektronischen Identitätsnachweises als auch für Verbände, die sich im Bereich Daten- und Persönlichkeitsschutz engagieren, im Gesetz geschaffen werden.

Erster Abschnitt

Art. 1

Art. 1 Abs. 2 BGEID hält als Ziel des Gesetzes fest, den Schutz der Persönlichkeit und der Grundrechte im Zusammenhang mit der Verwendung der E-ID zu gewährleisten. Diese explizite Zweckbindung halten wir für unabdingbar.

Wie nachfolgend erläutert, tragen verschiedene Bestimmungen des Gesetzes dem in Art. 1 Abs. 2 BGEID beschriebenen Grundsatz ungenügend Rechnung, namentlich betreffend der Datensparsamkeit.

Zweiter Abschnitt

Art. 2 Abs. 3

Die AHV-Nummer, die Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde, und die Angaben zum Ausstellungsprozess sind für die Ausstellung und Verwendung der E-ID nicht erforderlich und stellen damit Daten dar, die nicht Teil der E-ID sein sollten; darüber ist darauf hinzuweisen, dass die AHV-Nummer auch üblicherweise auf amtlichen Ausweisen nicht ersichtlich ist. Sollte die AHV-Nummer auf der E-ID enthalten sein, sollte eine Verwendung auf Vorgänge beschränkt sein, bei welchen die AHV-Nummer gesetzlich vorgesehen ist.

Art. 4 Abs. 4

Der Ausstellungsprozess ist im erläuternden Bericht nicht genauer beschrieben. Art. 4 Abs. 4 lässt jedoch vermuten, dass die Verifikation der antragstellenden Person und die Ausstellung der E-ID online und komplett automatisch vonstatten gehen soll – und kein Besuch auf der Gemeinde oder im Passbüro vorgesehen ist. Wie eine aktuelle Untersuchung des deutschen Chaos Computer Club (CCC) zeigt, weisen sämtliche gängigen Systeme zur «Video-Identifikation» Schwachstellen auf, die einen Identitätsdiebstahl möglich machen. Auf die Technik der «Video-Identifikation» und vergleichbare Verfahren ist daher zu verzichten. Auch wenn ein Identitätsdiebstahl durch einen «Deep-Fake» in Verbindung mit dem Abgleich des Gesichtsbild aus dem

ISA oder dem ZEMIS allenfalls schwieriger durchzuführen ist, wäre eine erfolgreiche Demonstration eines Identitätsdiebstahls verheerend für das Vertrauen und die Akzeptanz der E-ID.

Ein Vergleich der Bilder mit den Datenbanken ZEMIS und ISA sehen wir als überflüssig an, weil er für den Ausstellungsprozess nicht unbedingt erforderlich ist. Auf jeden Fall – und unabhängig vom gewählten Verfahren – müssen allfällig erhobene biometrische Daten unmittelbar im Anschluss an die Ausstellung (und der Übertragung der Daten in die E-ID nach Art. 2 Abs. 2 lit. g.) vernichtet werden.

Art. 10

Wir schlagen die Streichung des letzten Satzes («sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können») vor, da ein nicht-elektronischer amtlicher Ausweis dieses Kriterium ohnehin erfüllen sollte und ein diskriminierungsfreier Zugang für Personen ohne E-ID gewährleistet sein soll.

Art. 11 Abs. 3

Ein Abgleich mit den Datenbanken ISA und ZEMIS sowie dem Versichertenregister sehen wir, wie bereits ausgeführt, für nicht notwendig an.

Vierter Abschnitt

Den vierten Abschnitt sehen wir als stark ergänzungsbedürftig an.

Art. 1 Abs. 2 lit. b des Vorschlags zum BGEID setzt als Ziel des Gesetzes fest, dass der Schutz der Persönlichkeit und der Grundrechte der Personen, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, gewahrt werden solle. In dieser Hinsicht ist aber die momentane Fassung des Art. 16 des Vorschlags, welche festlegt, dass die Inhaberin oder der Inhaber frei darüber entscheiden kann, welche Bestandteile des Nachweises sie bekanntgibt, ungenügend. Es droht eine Überidentifikation.

Es ist für den Persönlichkeitsschutz essentiell, dass die Verifikatorin nicht frei über die Erfordernis des elektronischen Nachweises und deren Umfang bestimmen kann, sondern diese gesetzlich auf das unbedingt Erforderliche beschränkt wird, und dass andernfalls eine informierte und explizite Zustimmung stattfindet. Betreffend Einschränkung der Datenmenge auf das Notwendige lässt der Vorentwurf zum BGEID

zu, dass mehr Daten als notwendig verarbeitet werden, und damit mehr Möglichkeit für deren Missbrauch eröffnet werden. Um den geforderten Prinzipien «privacy by design» und Datensparsamkeit gerecht zu werden, ist eine Ergänzung notwendig.

Ergänzungsvorschlag zu Art. 16

Es werden zwei neue Gesetzesbestimmung in Ergänzung zu Art. 16 vorgeschlagen.

Art. 16^{bis} bestimmt, dass Umfang und Erfordernis von Seiten der Verifikatorin auf das unbedingt Erforderliche beschränkt wird. Er enthält auch eine Bestimmung des diskriminierungsfreien Zugangs zu Leistungen für Menschen ohne E-ID, welches vor allem Personen ohne Wohnsitz und Aufenthaltsbewilligung in der Schweiz sowie Menschen ohne Zugang zu technischen Mitteln betrifft. Der Absatz ist auch daraufhin ausgerichtet, dass sichergestellt ist, dass die Ausweiserfordernis von Privaten und Behörden nur dann besteht, wenn es die Umstände rechtfertigen.

Art. 16^{ter} verankert das Informations-, Zustimmung- und Widerrufbarkeitsprinzip, namentlich beim Gebrauch der Daten über ihren gesetzlichen und unbedingt erforderlichen Zweck hinaus. Dem Umstand, dass ein Ausweisen verschiedene Zwecke erfüllen kann, wird mit der Bestimmung Rechnung getragen, dass die Zustimmung und Widerrufung auf jeden einzelnen Zweck anwendbar ist.

Gesetzestext

Art. 16^{bis} Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang

¹ Die Erfordernis eines elektronischen Nachweises darf von Behörden und Privaten als Voraussetzung für die Erbringung einer Leistung oder Gewährung eines Zugangs nur insoweit gestellt werden als sie für die Erbringung der Leistung oder der Gewährung des Zugangs unbedingt erforderlich ist.

² Falls die Übermittlung von Bestandteilen eines elektronischen Nachweises oder davon abgeleiteten Informationen unbedingt erforderlich ist, so ist stets die Möglichkeit vorzusehen, diese Bestandteile und Informationen ohne vermeidbare Nachteile auf andere Weise zu übermitteln.

Art. 16^{ter} Informations- und Zustimmungspflicht; Widerrufsrecht

Für Datenbearbeitungen, welche für die Erbringung der Leistung oder die

Gewährung des Zugangs nicht unbedingt erforderlich sind, gelten nachfolgende Bestimmungen:

a Die Verifikatorin informiert die Inhaberin oder den Inhaber des Ausweises über Art, Zweck und Umfang der Datenbearbeitung.

b Die Datenbearbeitung bedarf der expliziten und jederzeit widerrufbaren Zustimmungen der Inhaberin und des Inhabers.

c Erfüllt die Bearbeitung verschiedene Zwecke, so hat die Inhaberin oder der Inhaber die Zustimmung zu jedem dieser Zwecke einzeln zu erteilen.

d Die Inhaberin oder der Inhaber kann die Zustimmung jederzeit und einzeln widerrufen.

Art. 16 Abs. 3

Streichen von «möglichst», da eine Vermeidung der Kenntnisnahme, beispielsweise durch Einsatz eines Proxys, technisch möglich ist.

Fünfter Abschnitt

Art. 20

Die Fakultativbestimmung sollte mit einer obligatorischen Bestimmung ersetzt werden. Der Bund sollte die Infrastruktur und alle benötigten Anwendungen (als Beispielapplikation) zur Verfügung stellen, damit ein vielfältiges Ökosystem und das nötige Vertrauen entstehen kann.

Art. 21 Abs. 2

Aus der Bestimmung ergibt sich noch nicht eindeutig, dass der Zugriff auf die Sicherheitskopien durch andere Personen nicht möglich sein darf; dies ist entsprechend zu ergänzen. (Die benötigten Keys oder Informationen sind bei den Inhaberinnen; zur Not könnten Nachweise auch neu ausgestellt werden.)

Art. 25

Art. 25 BGEID kann dahingehend interpretiert werden, dass sie dem Bundesrat eine Gesetzgebungskompetenz delegiert. Mit Hinweis darauf ist es problematisch, wenn der Bundesrat selbständig Erweiterungen vornehmen kann, insbesondere weil der Rechtsweg betreffend Bundesratserlasse üblicherweise ausgeschlossen oder schwierig

wahrzunehmen ist. Um die Möglichkeit unvorhergesehener technische Erneuerungen zu berücksichtigen, sei deshalb eine Methode vorzuschlagen, bei welcher die gerichtliche Überprüfung sowohl der Notwendigkeit als auch der Verhältnismässigkeit möglich ist.

Sechster Abschnitt

Art. 26

Es sei die Kostenlosigkeit aller Handlungen vorzusehen, welche die Zustimmung oder den Widerruf einer bestimmten Datenbearbeitung durch die Inhaberin oder den Inhaber eines elektronisches Ausweises erwirkt.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger

Madame la Conseillère fédérale Karin Keller-Sutter
Cheffe du Département fédéral suisse de justice et police DFJP
Palais fédéral ouest
CH-3003 Berne

Soumission par e-mail à l'adresse:
rechtsinformatik@bj.admin.ch

Zurich, le 29 septembre 2022

Consultation Loi fédérale sur la preuve d'identité électronique et autres services d'identification électronique (loi e-ID, LSIE)

Madame la Conseillère fédérale,
Mesdames, Messieurs,

Nous vous remercions de nous donner l'opportunité de prendre position sur la nouvelle proposition de loi e-ID, opportunité que nous souhaitons saisir ici au nom de digitalswitzerland.

Cette proposition définissant le cadre d'une infrastructure de confiance dont l'élément clé est un e-ID émis par l'État, nous constatons de manière générale qu'elle rencontre un écho favorable auprès des membres de digitalswitzerland. Cependant, nous sommes convaincus que l'identité électronique ne peut s'établir en Suisse que si elle est ancrée dans un écosystème de justificatifs électroniques inclusif. Nous considérons donc comme essentiel de mentionner cet aspect dans l'article énonçant le but de la loi (voir remarque A). Par ailleurs, un contrôle régulier de l'infrastructure étatique, un véhicule de saisie de contributions d'expertes et experts pour la mise en œuvre technologique de la loi, une structure tarifaire répondant aux normes internationales et une réglementation des mécanismes de confirmation privés nous paraissent judicieux (voir les remarques correspondantes B, C, D et E).

Comptant plus de 240 organisations par son réseau intersectoriel, digitalswitzerland se voit comme une plateforme de dialogue mettant ses services à disposition pour simplifier le passage au numérique de la Suisse. Le 28 avril dernier, digitalswitzerland a pu fournir une première contribution aux réflexions sur plusieurs plans menées sur le développement de l'écosystème e-ID en Suisse. Ce livre blanc a été rédigé par dix spécialistes de l'identité numérique du secteur privé et du domaine scientifique. Celui-ci est disponible à l'adresse suivante: <https://digitalswitzerland.com/building-a-swiss-digital-trust-ecosystem/>

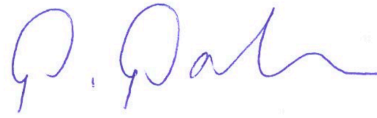
Nous souhaitons tirer parti de notre réseau et de notre position de plateforme de dialogue pour contribuer activement et de manière constructive au passage au numérique de la Suisse.

Nous vous remercions de votre attention et restons à votre disposition pour tout renseignement complémentaire.

Meilleures salutations,



Stefan Metzger
Managing Director digitalswitzerland



Guillaume Gabus
Extended Management, Public Affairs

Informations complémentaires
Guillaume Gabus, Extended Management, Public Affairs, digitalswitzerland
Tel. +41 76 589 71 99 | guillaume@digitalswitzerland.com

I. Informations sur digitalswitzerland

digitalswitzerland est une initiative intersectorielle nationale qui vise à faire de la Suisse un pôle d'innovation mondial leader dans le domaine du numérique. Sous l'égide de digitalswitzerland, plus de 240 adhérents de l'association et partenaires non politiques de la fondation collaborent de façon transversale pour atteindre cet objectif. digitalswitzerland aborde tous les aspects de la numérisation et s'attelle à résoudre divers défis.

Du point de vue de digitalswitzerland, l'infrastructure de confiance constitue un élément essentiel de l'avancée numérique de la société et de l'économie suisses. digitalswitzerland salue la rapidité du processus et l'axe stratégique de l'avant-projet.

II. Remarques sur la loi e-ID

A. Même importance accordée à l'e-ID et à l'écosystème e-ID

Parallèlement à la protection de la personnalité et des droits fondamentaux des personnes, la loi vise la mise en place d'une infrastructure de confiance étendue, présentant des avantages manifestes pour les citoyennes et citoyens. Seul un écosystème permettant l'interaction d'un grand nombre d'émetteurs et émettrices, d'une part, et de vérificateurs et vérificatrices de l'autre, peut apporter à la population la valeur ajoutée nécessaire pour prospérer. La loi ne doit donc pas se limiter au rattachement d'autres justificatifs électroniques, à leur délivrance et à leur vérification, mais doit également encourager et soutenir activement ce processus. Le fait que l'e-ID ne soit pas uniquement utilisé pour les processus liés à l'e-gouvernement, mais soit largement acceptée dans le secteur privé, constitue une responsabilité commune qui requiert une étroite collaboration. Nous considérons donc comme judicieux que, dans le cadre de sa finalité, la loi doive permettre de nouveaux modèles économiques numériques imposant la confiance dans l'espace numérique comme condition préalable. Dans ce contexte, la diversité et le nombre de modèles commerciaux numériques mis à disposition sur l'infrastructure étatique devraient également permettre de déterminer le degré de réalisation de la loi. Par ailleurs, une infrastructure de confiance étendue supposerait la sécurité juridique, mais aussi des investissements pour les acteurs du secteur privé. Tant que les principes de base de l'aménagement de l'infrastructure de confiance et la répartition des rôles entre l'État et les acteurs du secteur privé ne seront pas formulés de manière suffisamment concrète, les fournisseurs de technologie et de services potentiels ne pourront pas élaborer leurs modèles commerciaux de

manière satisfaisante. Cet état de fait pèse également sur la planification de services et offres de services potentiels basés sur l'e-ID dans le domaine des justificatifs numériques. digitalswitzerland souhaite inciter la Confédération à clarifier rapidement la situation et à assurer ainsi la sécurité des investissements.

B. Un contrôle régulier de l'infrastructure étatique

Pour s'établir, la confiance requiert une infrastructure sûre et robuste. Il est donc essentiel que les réflexions sur la cybersécurité soient d'emblée prises en compte et inscrites dans la loi. L'avant-projet de loi décrit deux systèmes: le système Fedpol d'émission des e-ID (voir section 2) et l'infrastructure de confiance (voir section 5). La loi devrait prévoir un contrôle régulier (probablement annuel) de la sécurité de ces deux éléments par des spécialistes qualifiés. Une mise en œuvre correcte permet d'assurer l'absence de données sensibles sur l'infrastructure de confiance. Cet élément doit être vérifié et doit être prévu par la loi. Il nous semble en outre judicieux de soumettre également la structure du système Fedpol à un contrôle technique et procédural. Ce point devrait être inscrit dans la loi. Outre la nécessité d'un contrôle, le besoin de protection devrait lui aussi faire l'objet d'une description explicite. Bien que l'ordonnance régit les détails de la réalisation des contrôles par des spécialistes, nous considérons des tests dits «Red Team Tests» comme particulièrement pertinents. Un organe de contrôle externe tel que l'institut national de test pour la cybersécurité (NTC) serait également envisageable afin de renforcer encore la confiance

C. Véhicule de contributions d'experts sur la mise en œuvre technologique de la loi

De l'avis de digitalswitzerland, il serait judicieux de ne pas réglementer la mise en œuvre technologique à l'échelon de la loi. Étant donné la rapidité de l'évolution technologique, la Confédération devrait veiller à pouvoir opter pour le contexte technologique correspondant au mieux aux objectifs de la loi et à ses exigences, au moment de son introduction (protection technique spécifique des données, sécurité des données, économie des données et enregistrement décentralisé des données). C'est pourquoi digitalswitzerland salue l'article 25 de la loi. Dans un même temps, il convient de noter que pour établir l'infrastructure de confiance, la loi devra convaincre les citoyennes et citoyens quant à la cohérence et la sophistication de son implémentation (portefeuille électronique, système de copies de sauvegarde, etc.). La mise en œuvre technologique de la loi comprend tant la User Experience (UX) de manière générale, que des moments décisifs du parcours client, notamment parce que les principes de l'identité auto-souveraine transmettent la responsabilité de l'identité à l'utilisateur. Le champ de tension entre la sécurité, la User Experience et l'approche de la décentralisation n'a pas encore été suffisamment clarifié. C'est précisément parce que la plupart de ces questions liées à la mise en œuvre technologique ne sont pas réglementées à l'échelon de la loi que nous aspirons à la mise en place d'un véhicule permettant au secteur privé et du domaine scientifique de contribuer au débat. Cela simplifierait la tâche de la Confédération en termes de mise en œuvre dans le cadre du champ de tension mentionné, voire permettrait d'éviter certaines zones d'ombre. Cette approche pourrait prendre la forme d'un groupe de spécialistes élargi ou avoir lieu via la plateforme GitHub actuelle. Ces spécialistes permettent également de faire état des connaissances existantes et des investissements réalisés. digitalswitzerland saluerait l'ajout d'une disposition d'exécution correspondante à l'article 28.

D. Structure tarifaire selon les normes internationales

digitalswitzerland est d'avis que les coûts et les prix des vérificatrices et vérificateurs ont un impact direct sur le succès de l'ensemble du projet. Ces réflexions d'ordre commercial sont particulièrement pertinentes pour les entreprises connectant leurs justificatifs avec l'e-ID, constituant ainsi l'écosystème e-ID recherché. La perception d'une taxe minimale pour l'émettrice ou l'émetteur et la vérificatrice ou le vérificateur pour (1) l'enregistrement des données (identificateur spécifique) dans le Registre de base et pour (2) l'inscription au Registre de confiance nous semble judicieuse. digitalswitzerland est d'avis que le montant de la taxe doit s'aligner sur les lignes directrices de la Fondation Sovrin. Cela signifie concrètement: une taxe minimale pour l'inscription au Registre de base, mais pas de taxe pour l'émission ou la vérification d'un justificatif. La révocation de justificatifs électroniques serait communiquée au système dans le cadre de l'actualisation quotidienne. Des frais seraient facturés aux émettrices ou émetteurs pour la mise à jour (Revocation Update) correspondante. Il importe ici que le montant total des frais ne dépende donc pas du nombre d'utilisatrices et utilisateurs, ni du nombre d'interactions pour un justificatif spécifique. Cet élément est essentiel tant pour l'évolutivité de l'écosystème que pour les réflexions commerciales des vérificatrices et vérificateurs, ainsi que des émettrices et émetteurs.

digitalswitzerland recommande l'intégration des principes susmentionnés à l'échelon de la loi, et espère par ailleurs que les produits des modèles commerciaux numériques désormais possibles, et l'économie de coûts liée à l'optimisation de l'identification viendront largement compenser ces taxes minimales. digitalswitzerland salue également l'absence de taxes prélevées pour l'émission de l'e-ID, pour son utilisation et pour le portefeuille électronique de la Confédération. Du point de vue de l'utilisatrice ou utilisateur final(e), ces points sont essentiels.

E. Réglementation des mécanismes de confirmation privés

La connexion entre le monde virtuel et le monde physique reste un élément décisif de l'infrastructure de confiance. Sur ce point, digitalswitzerland est d'avis que chaque instance bénéficiant actuellement de notre confiance (pour l'accréditation des émettrices et émetteurs, par exemple) doit également bénéficier de cette confiance au niveau virtuel. Cet élément est capital pour les utilisatrices et utilisateurs ainsi que pour les vérificatrices et vérificateurs, qui n'ont souvent pas de lien direct avec l'émettrice ou l'émetteur. Il est opportun que la Confédération transfère la compétence de confirmation de l'identité des autorités fédérales, cantonales et communales (confirmation spécifique des identificateurs). Il n'est pas moins essentiel au sens de l'écosystème e-ID recherché que les acteurs du secteur privé soient habilités à mettre des mécanismes distincts, non étatiques (privés) à disposition. Exemple: la liste des hautes écoles reconnues et accréditées en Suisse tenue par la Conférence des Recteurs des Universités Suisses (swissuniversities) représente une importante source d'informations pour la validation des diplômes d'écoles supérieures. Cet organe de confiance spécifique au secteur doit pouvoir continuer à exercer cette fonction via le numérique. Cela importe pour la mise en place d'écosystèmes multisectoriels, qui préparent la voie à des cas d'application à l'échelle sectorielle et au-delà. Comme mentionné à la remarque A, l'e-ID est un module central pour un grand nombre d'écosystèmes sectoriels (y compris les domaines de la santé, de la mobilité, des finances, etc.). Ce n'est que si nous évitons de construire des mondes cloisonnés, mais tendons à mettre en place une infrastructure de confiance, que nous pourrions créer une valeur ajoutée concrète pour les citoyennes et citoyens. Même si le projet actuel ne limite pas explicitement la possibilité de confiance privée spécifique à un secteur (article 18, al. 2), cela pourrait être mentionné également à l'échelon de la loi. Parallèlement, une plus grande clarté quant au processus d'accréditation d'émetteurs (privés) est souhaitable, notamment en ce qui concerne les conditions à remplir pour devenir émetteur et la manière de traiter les faux émetteurs. Concrètement, il pourrait être mentionné à l'article 12 alinéa 1 que les autorités et les personnes privées peuvent utiliser l'infrastructure de confiance de la Confédération conformément aux termes de la section 5, pour émettre des justificatifs électroniques non étatiques.

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern

Einreichung per Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zum neuen Vorschlag für ein E-ID-Gesetz äussern zu können, welche wir hiermit für digitalswitzerland wahrnehmen.

Zusammenfassend stellen wir fest, dass der Vorschlag für ein neues E-ID-Gesetz in der Mitgliedschaft von digitalswitzerland auf breite Resonanz stösst, indem es den Rahmen setzt für eine Vertrauensinfrastruktur, deren Kernelement eine staatlich herausgegebene e-ID ist. Allerdings sind wir der Überzeugung, dass sich die elektronische Identität in der Schweiz nur dann in der Breite durchsetzen kann, wenn sie in ein inklusives Ökosystem von elektronischen Nachweisen eingebettet ist. Darum erachten wir es für zentral, diesen Aspekt bereits in den Zweckartikel des Gesetzes aufzunehmen (siehe Anmerkung A). Des Weiteren erachten wir die regelmässige Prüfung der staatlich-betriebenen Infrastruktur, ein Vehikel für Experten-Input zur technologischen Gesetzesumsetzung, Gebührenstruktur nach internationalen Standards, und Regelung von privaten Bestätigungsmechanismen als sinnvoll (siehe jeweils Anmerkung B, C, D und E).

digitalswitzerland versteht sich als Dialogplattform, welche mit seinem branchenübergreifenden Netzwerk von über 240 Organisationen zur Verfügung steht, die Digitalisierung der Schweiz zu erleichtern. Am 28. April konnte digitalswitzerland einen ersten Beitrag zur laufenden Metaebene-Debatte über die Entwicklung des E-ID-Ökosystems in der Schweiz leisten. Dieses Whitepaper wurde gemeinsam von zehn Experten für digitale Identität aus dem privaten Sektor und der Wissenschaft verfasst. Es kann hier abgerufen werden: <https://digitalswitzerland.com/building-a-swiss-digital-trust-ecosystem/>

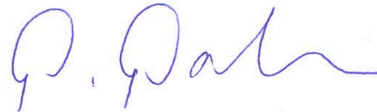
Mit unserem Netzwerk und unserer Position als Dialogplattform wollen wir einen aktiven und konstruktiven Beitrag zur Digitalisierung der Schweiz leisten.

Wir danken für die Aufmerksamkeit und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse,



Stefan Metzger
Managing Director digitalswitzerland



Guillaume Gabus
Extended Management, Public Affairs,
digitalswitzerland

Für weitere Auskünfte
Guillaume Gabus, Extended Management, Public Affairs, digitalswitzerland
Tel. +41 76 589 71 99 | guillaume@digitalswitzerland.com

I. Hintergrund zu digitalswitzerland

digitalswitzerland ist eine schweizweite, branchenübergreifende Initiative, welche die Schweiz als weltweit führenden digitalen Innovationsstandort stärken und verankern will. Unter dem Dach von digitalswitzerland arbeiten an diesem Ziel mehr als 240 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

Aus Sicht von digitalswitzerland ist die Vertrauensinfrastruktur eine wichtige Komponente, um die Schweizer Gesellschaft und Wirtschaft bei der Digitalisierung voranzubringen. digitalswitzerland begrüsst die Geschwindigkeit des Prozesses und die Stossrichtung des Vorentwurfs.

II. Anmerkungen zum E-ID Gesetz

A. Gleicher Stellenwert für E-ID und E-ID Ökosystem

Parallel zum Schutz der Persönlichkeit und der Grundrechte von Personen, ist ein weiteres wichtiges Ziel des Gesetzes eine umfassende 'Vertrauensinfrastruktur' aufzubauen, die einen klaren Nutzen für Bürger:innen hat. Nur ein Ökosystem, in dem es eine Vielzahl unterschiedlichster Aussteller:innen und Verifikator:innen aufeinandertreffen, kann der Bevölkerung jene Mehrwerte bieten, die es für dessen Florieren benötigt. Das Gesetz sollte daher nicht nur eine Anbindung anderer elektronischer Nachweise, und deren Ausstellung und Überprüfung gewährleisten, sondern dies aktiv fördern bzw. unterstützen. Dass die E-ID hier nicht nur für E-Government-Prozesse genutzt wird und in der Privatwirtschaft breiten Anklang findet, ist eine gemeinsame Verantwortung und bedarf enge Zusammenarbeit. Wir erachten es daher für zielführend, im Rahmen der Zweckbestimmung zu ergänzen, dass das Gesetz neue digitale Geschäftsmodelle ermöglichen soll, die Vertrauen im digitalen Raum voraussetzen. In diesem Sinne sollte die Zielerreichung des Gesetzes auch daran gemessen werden können, wie vielfältig und zahlreich die digitalen Geschäftsmodelle sind, welche auf der staatlich

betriebenen Infrastruktur zukünftig bereitgestellt werden. Darüber hinaus setzte eine umfassende 'Vertrauensinfrastruktur' die Rechts- und Investitionssicherheit für privatwirtschaftliche Akteure voraus. Bevor die Grundzüge der Ausgestaltung der Vertrauensinfrastruktur sowie die konkrete Rollenverteilung zwischen Staat und privaten Akteuren nicht hinreichend konkret sind, können potenzielle Technologielieferanten und Dienstleistungserbringer ihre Geschäftsmodelle nur ungenügend ausarbeiten. Dadurch wird auch die Planung von potenziellen E-ID-verwendenden Diensten und Dienstleistungsangeboten im Bereich der digitalen Nachweise erschwert. digitalswitzerland möchte den Bund anregen, rasch mehr Klarheit zu schaffen, um Investitionssicherheit zu erzeugen.

B. Regelmässige Prüfung der staatlich betriebenen Infrastruktur

Wenn Vertrauen geschaffen werden soll, muss die Infrastruktur sicher und robust sein. Überlegungen zur Cybersicherheit müssen deshalb von Anfang an berücksichtigt und gesetzlich verankert werden. Im Vorentwurf des Gesetzes werden zwei Systeme beschrieben, das Fedpol-System zur Ausstellung von E-IDs (gemäss Abschnitt 2) und die Vertrauensinfrastruktur (gemäss Abschnitt 5). Im Gesetz sollte vorgeschrieben werden, dass beide Elemente regelmässig (wahrscheinlich jährlich) von Fachspezialisten einem Sicherheitsreview unterzogen werden. Wenn richtig implementiert, dann liegen in der Vertrauensinfrastruktur keine sensitiven Daten vor. Dies gilt es zu überprüfen und sollte gesetzlich vorgeschrieben sein. Des Weiteren halten wir es für sinnvoll, dass die Struktur des Fedpol-Systems ebenfalls technisch und prozessual auf Sicherheitsfragen überprüft wird. Dies sollte gesetzlich verankert sein. Neben der Notwendigkeit einer Überprüfung sollte auch der Schutzbedarf klar beschrieben sein. Obwohl die Details der Umsetzungsweise für die Expertenprüfungen auf Verordnungsebene geregelt werden, halten wir hier sogenannte Red-Team-Tests für besonders zielführend. Eine externe Prüfstelle wie beispielsweise das Nationale Testinstitut für Cybersicherheit NTC wäre auch denkbar, um das Vertrauen weiter auszubauen.

C. Vehikel für Experten-Input zur technologischen Gesetzesumsetzung

digitalswitzerland erachtet es als sinnvoll, dass die technologische Umsetzung nicht auf Gesetzesstufe geregelt ist. Aufgrund des raschen technischen Fortschritts soll sich der Bund die Kompetenzen nehmen können, einen Technologie-Kontext zu wählen zum Zeitpunkt der Einführung, welche dem Zweck des Gesetzes und den Anforderungen (spez. Datenschutz durch Technik, Datensicherheit, Datensparsamkeit und dezentrale Datenspeicherung) am besten gerecht wird. digitalswitzerland begrüsst deshalb den Artikel 25 im Gesetz. Gleichzeitig muss angemerkt werden, dass der Erfolg der Vertrauensinfrastruktur davon abhängt, wie konsequent und überzeugend das Gesetz aus der Perspektive der Bürger:innen zu Ende gedacht und umgesetzt wird (z.B. elektronische Brieftasche, System für Sicherungskopien, etc.). Die technologische Gesetzesumsetzung beinhaltet sowohl die User Experience (UX) im Generellen, aber auch matchentscheidende 'Momente' in der Customer Journey, besonders weil SSI die Verantwortung der Identität dem User überträgt. Das Spannungsfeld zwischen Sicherheit, User Experience und dem Ansatz der Dezentralität ist noch nicht abschliessend geklärt. Genau weil die Mehrheit solcher Fragen im Zusammenhang mit der technologischen Umsetzung nicht auf Gesetzesstufe geregelt ist, erhoffen wir uns ein Vehikel für den Privatsektor und die Wissenschaft, welche es erlaubt, Diskussionsbeiträge beizusteuern und somit die Umsetzung – innerhalb des erwähnten Spannungsfeldes – für den Bund zu erleichtern bzw. allfällige Blindspots zu vermeiden. Dies könnte in Form einer erweiterten Expertengruppe oder über die bestehende GitHub-Plattform geschehen. Diese Experten helfen auch auf bestehendes Wissen und getätigte Investitionen hinzuweisen. digitalswitzerland würde eine entsprechende Ausführungsbestimmung als Zusatz in Artikel 28 begrüssen.

D. Gebührenstruktur nach internationalen Standards

digitalswitzerland ist der Überzeugung, dass die Kosten und Preise für Verifikator:innen und Aussteller:innen einen direkten Einfluss auf den Erfolg des Gesamtprojektes haben. Diese kommerziellen Überlegungen sind hochrelevant für jene Firmen, welche ihre Nachweise mit der E-ID verbinden und somit das erstrebte E-ID Ökosystem ausmachen. Eine minimale Gebühr für die Aussteller:innen und Verifikator:innen für (1) die Eintragung der Daten (spez. Identifikator) im Basisregister und für (2) die Aufnahme ins Vertrauensregister erscheint als sinnvoll. digitalswitzerland ist der Auffassung, dass sich die Höhe der Gebühren an den Leitlinien der Sovrin Foundation orientieren soll. Konkret heisst das: Eine minimale Gebühr für den Eintrag ins Basisregister, aber keine Gebühr für die Ausstellung oder die Verifikation eines Nachweises. Die Widerrufe der elektronischen Nachweise

würden durch tägliche Aktualisierungen zum System kommuniziert. Für Aussteller:innen wären auf den verbunden 'Revocation Update' Gebühren erhoben. Wichtig hier ist, dass der Gesamtbetrag der Gebühren somit nicht abhängig ist von der Anzahl der Nutzer:innen oder der Anzahl an Interaktionen für einen spezifischen Nachweis. Das ist essentiell für die Skalierbarkeit des Ökosystems und für die kommerziellen Überlegungen der Verifikator:innen und Aussteller:innen. digitalswitzerland würde die Aufnahme der genannten Grundsätze auf Gesetzesstufe empfehlen. digitalswitzerland erhofft sich zudem, dass die Erzeugnisse der neu-ermöglichten digitalen Geschäftsmodelle und die Kosteneinsparungen aufgrund optimierter Identifizierung, diese minimalen Gebühren weitgehend kompensieren. digitalswitzerland begrüsst auch, dass für die Ausstellung der E-ID, für deren Nutzung und für die elektronische Brieftasche des Bundes keine Gebühren erhoben werden. Dies ist aus einer Endnutzer-Perspektive essenziell.

E. Regelung von privaten Bestätigungsmechanismen

Die Verbindung zwischen der virtuellen und der physischen Welt bleibt ein entscheidendes Element der Vertrauensinfrastruktur. Hier ist digitalswitzerland der Meinung, dass jene Instanzen, welche momentan unser Vertrauen geniessen (z.B. um Aussteller:innen zu akkreditieren), diese Verantwortung auch virtuell erhalten sollen. Dies ist von zentraler Bedeutung für Nutzer:innen und Verifikator:innen, welche oft keine direkte Beziehung zu den Aussteller:innen haben. Es ist sinnvoll, dass dem Bund die Kompetenz übertragen wird, die Identität der Bundes-, Kanton- und Gemeindebehörden zu bestätigen (spez. Bestätigung der Identifikatoren). Gleichermassen ist es essenziell, im Sinne des erstrebten E-ID Ökosystem, dass auch Akteure des privaten Sektors befähigt sind, separate, nicht staatliche (private) Mechanismen bereitzustellen. Als Beispiel: Die Rektorenkonferenz der Schweizer Universitäten (swissuniversities) führt eine Liste der anerkannten oder akkreditierten Hochschulen in der Schweiz, die eine wichtige Informationsquelle für die Validierung von Hochschulabschlüssen darstellt. Diese sektorspezifischen Vertrauensstelle muss auch weiterhin die Funktion digital ausüben können. Dies ist wichtig für den Aufbau von multisektoralen Ökosystemen, welche den Weg für Anwendungsfälle innerhalb und über sektorale Grenzen hinweg ebnen. Wie in Anmerkung A erwähnt, dient die E-ID als zentraler Baustein für eine Vielzahl von sektoralen Ökosystemen (einschließlich Gesundheit, Mobilität, Finanzen usw.). Nur wenn wir es vermeiden, getrennte Welten aufzubauen und stattdessen nach einer umfassenden Vertrauensinfrastruktur streben, können wir einen konkreten Mehrwert für die Bürger:innen schaffen. Auch wenn der momentane Entwurf die Möglichkeit diese sektorspezifischen privaten Vertrauensstellung nicht explizit einschränkt (in Artikel 18, Absatz 2), könnte dies auf Gesetzesebene zusätzlich erwähnt werden. Parallel dazu ist mehr Klarheit über den Akkreditierungsprozess von (privaten) Ausstellern wünschenswert, insbesondere darüber, wer Aussteller werden kann und wie wir mit gefälschten Ausstellern umgehen. Konkret könnte in Artikel 12 Absatz 1 angemerkt werden, dass Behörden und Private die Vertrauensinfrastruktur des Bundes gemäss dem 5. Abschnitt nutzen können, um elektronische nicht-staatliche Nachweise auszustellen.

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per E-Mail an: rechtsinformatik@bj.admin.ch

18. Oktober 2022

Stellungnahme zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Am 29. Juni 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID). Wir bedanken uns für die Einladung zur Stellungnahme.

Hinter dem E-ID-Referendum steht ein überparteilicher, breit abgestützter Zusammenschluss von Organisationen und Netzwerken, der sich dafür einsetzt, dass die E-ID vom Staat an die Bevölkerung herausgegeben wird und der Datenschutz im Zentrum steht. Das Referendum wurde getragen von der Digitalen Gesellschaft, der unabhängigen Schweizer Kampagnenorganisation Campax, der Demokratie-Plattform WeCollect und dem Verein Public Beta. Unterstützt wurden sie von der SP Schweiz, der Grünliberalen Partei, den Grünen und der Piratenpartei, dem Verband Schweizerischer Polizei-Beamter VSPB, VPOD, von Syndicom, der Internet Society Switzerland, von grundrechte.ch, dem Schweizer Seniorenrat (SSR), dem Schweizer Verband für Seniorenfragen (SVS), der Vereinigung aktiver Senioren- und Selbsthilfeorganisationen der Schweiz (VASOS) sowie engagierten Mitgliedern aus allen Parteien.

Gerne nehmen wir zum Entwurf wie folgt Stellung:

Grundsätzliches

Die Organisationen und Personen des E-ID-Referendums haben die gesellschaftliche, politische und technische Debatte zum Bundesgesetz über elektronische Identifizierungsdienste (BGEID) eng begleitet, das Referendum gegen das Gesetz ergriffen sowie die Volksabstimmung massgeblich geprägt. Die Hauptkritikpunkte des Gesetzes betrafen den Zweck und die Herausgeberschaft («staatlicher, elektronischer Ausweis» anstatt «privates Login») sowie den mangelnden Datenschutz (Datenschutz durch Technik/Privacy-by-Design und Datensparsamkeit/Privacy-by-Default). Dies waren dann auch die Gründe, weshalb das Gesetz mit grosser Mehrheit an der Urne abgelehnt wurde.

Die Organisationen des E-ID-Referendums begrüssen die Neuauflage des E-ID-Gesetzes und sind mit der Stossrichtung einverstanden.

Wir vertreten jedoch die Auffassung, dass der Schutz der Persönlichkeit und der Personendaten im vorliegenden Vorentwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise noch unzureichend umgesetzt sowie der Schutz vor Missbrauch der Daten noch unzureichend gewährleistet ist. Dies betrifft insbesondere die drohende «Überidentifikation».

Im Nachfolgenden werden wir dies an den einzelnen Artikeln erörtern und Änderungsvorschläge anbringen.

Bearbeitung von Personendaten

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht, abgeleitet von Art. 13 Abs. 2 der Bundesverfassung (BV). Ein elektronischer Nachweis ist ein Eingriff in dieses Grundrecht und hat gemäss Art. 36 BV verhältnismässig zu erfolgen; im Speziellen sollte die Grundrechtseinschränkung nicht weiter gehen, als notwendig und sachlich gerechtfertigt ist. Diesem Grundsatz ist im vorgeschlagenen Gesetz ungenügend Rechnung getragen. Wir vertreten die Auffassung, dass die gesetzlich vorgesehene Erhebung von Daten sowie ihre Bearbeitung auf das zu ihrem Zweck unbedingt Erforderliche reduziert werden muss, um dem Gehalt von Art. 13 Abs. 2 BV zu wahren.

Personendaten, welche in Bezug auf einen elektronischen amtlichen Nachweis erhoben und verarbeitet werden, erfordern zudem einen höheren und spezifischeren Schutz, als es das (revidierte) Datenschutzgesetz (DSG) bietet – und demnach eine

ungenügende Grundlage für den Schutz der Personendaten nach dem BGEID darstellt. Wir sind der Auffassung, dass amtlich erhobene, verwaltete und bereitgestellte Daten ein erhöhter Schutz beizumessen ist und dass dies im BGEID selbst vorzusehen ist.

Dass BGEID schafft eine neue Kategorie von Daten: Daten, die erstens besonders schutzwerten Charakter haben, zweitens auch behördlich verifiziert sind und drittens, für welche eine breite private Verwendung vorgesehen ist. Sie bilden eine neue Kategorie an Daten, welche durch das DSG nicht gedeckt sind. Das allgemein formulierte Datenschutzgesetz sowohl in der derzeitigen als auch in der künftigen, revidierten Fassung vermag nicht, einen adäquaten Schutz zu liefern, gerade betreffend der Überidentifizierung.

Nach dem DSG kann eine Datenbearbeitung erfolgen, sofern ein überwiegendes privates oder öffentliches Interesse eine solche rechtfertigt. Hier besteht ein erheblicher Interpretationsspielraum der Beteiligten und lässt in der Praxis auch zweckfremde Datenbearbeitungen zu, soweit sie etwa aufgrund eines wirtschaftlichen Interesses der Inhaberin oder des Inhabers der Datensammlung für verhältnismässig angesehen werden können (Beispiel: Online-Tracking, Kreditwürdigkeit). Meist wird zudem eine Einwilligung durch das Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) und/oder der Datenschutzerklärung eingeholt, ohne dass diesem Vorgang widersprochen werden könnte. Das DSG schafft auch keinen Anspruch auf ein Widerspruchsrecht, wonach der Bearbeitung – mindestens im Nachhinein – (einfach, also ohne Klage auf Persönlichkeitsverletzung) widersprochen werden könnte.

Das Schweizer DSG geht überdies betreffend Vorschriften hinsichtlich Identifikation und Tracking deutlich weniger weit als die EU-Richtlinie (DSGVO). Namentlich entfällt in der Schweiz das Kopplungsverbot, welches in der Praxis verhindert, dass eine Einwilligung in eine zweckfremde Datenbearbeitung über eine Kopplung an die Leistung selbst abgenötigt wird. Dies kann dazu führen, dass Private Daten sammeln und gebrauchen können, welche nicht für die Erbringung von Leistungen erforderlich sind und für welche keine eigentliche Freiwilligkeit besteht.

Damit verletzt nach unserer Ansicht die vorgeschlagene Fassung des BGEID sowohl den Grundsatz der Datensparsamkeit als auch der informationellen Selbstbestimmung. Neben der Verletzung der genannten Grundrechte und Grundsätze würde die drohende Überidentifikation das Vertrauen in die elektronische Identifikation schädigen. Die Akzeptanz würde darunter insgesamt stark leiden. Im BGEID sind

deshalb ausgestaltete, konkrete Bestimmung betreffend diesen Grundsätzen vorzusehen; Vorschläge zu diesen Bestimmungen werden weiter unten konkretisiert.

Rechtssystematisch stehen solche Bestimmungen ohne Kollision mit dem Datenschutzgesetz. Art. 4 DSG (Art. 6 nDSG) bestimmt, dass die Bearbeitung von Personendaten nur rechtmässig erfolgen darf, äussert sich zum rechtlichen Rahmen aber nicht. Damit besteht Gestaltungsspielraum des rechtlichen Rahmens durch das BGEID, wobei zu betonen ist, dass im heutigen rechtlichen Rahmen die konkrete Ausgestaltung des rechtlichen Rahmens einer Datenbearbeitung spezialgesetzlich, und nicht durch das DSG, vorgenommen wird.

Diskriminierungsfreier Zugang zu Leistungen

Unter mehreren Gesichtspunkten erweist sich für problematisch, wenn der Erhalt von Leistungen vom Besitz einer E-ID abhängig gemacht werden. Damit werden einerseits Menschen ausgeschlossen, welche nach geltender Gesetzgebung kein Anrecht auf eine E-ID haben, andererseits aber auch solche, welche nicht über die technischen Kenntnisse oder die Mittel verfügen, eine E-ID zu beantragen, oder dies aus persönlichen Gründen ablehnen. Unter Hinweis auf das Diskriminierungsverbot (Art. 8 BV) ist ein diskriminierungsfreier Zugang zu Leistungen deshalb gesetzlich zu gewährleisten.

Hierzu sei noch angemerkt, dass nach den vorgeschlagenen Bestimmungen nur Menschen Anrecht auf eine E-ID haben, welche in der Schweiz über eine Aufenthaltsbewilligung verfügen. Dies schliesst alle Menschen aus, welche über eine solche nicht verfügen und sich unter einem anderen Titel als einer ordentlichen Aufenthaltsbewilligung in der (digitalen) Schweiz aufhalten. Das Gesetz könnte eine Möglichkeiten vorsehen, dass bei genügender Identifikation (etwa über einen ausländischen Pass) eine elektronische ID ausgestellt werden kann, wobei bei unsicherer Identifikation diesem Umstand mit einer Anmerkung Rechnung getragen werden könnte.

Durchsetzbarkeit

Damit Gesetzesbestimmungen wirksam sind, müssen sie durchsetzbar sein. Das vorgeschlagene Gesetz verzichtet vollständig auf spezifische Bestimmungen, um Bestimmungen durchzusetzen und Verletzungen beheben zu können. Wir sehen es als wichtig an, dass juristische und natürliche Anbieterinnen (Ausstellerinnen, Verifikatorinnen), welche Bestimmungen verletzen, einer Strafbestimmung

unterliegen, und dass ein vereinfachter und kostenfreier Zugang zu Verfahren zur Behebung von Verletzung sowohl für die Subjekte des elektronischen Identitätsnachweises als auch für Verbände, die sich im Bereich Daten- und Persönlichkeitsschutz engagieren, im Gesetz geschaffen werden.

Erster Abschnitt

Art. 1

Art. 1 Abs. 2 BGEID hält als Ziel des Gesetzes fest, den Schutz der Persönlichkeit und der Grundrechte im Zusammenhang mit der Verwendung der E-ID zu gewährleisten. Diese explizite Zweckbindung halten wir für unabdingbar.

Wie nachfolgend erläutert, tragen verschiedene Bestimmungen des Gesetzes dem in Art. 1 Abs. 2 BGEID beschriebenen Grundsatz ungenügend Rechnung, namentlich betreffend der Datensparsamkeit.

Zweiter Abschnitt

Art. 2 Abs. 3

Die AHV-Nummer, die Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde, und die Angaben zum Ausstellungsprozess sind für die Ausstellung und Verwendung der E-ID nicht erforderlich und stellen damit Daten dar, die nicht Teil der E-ID sein sollten; darüber ist darauf hinzuweisen, dass die AHV-Nummer auch üblicherweise auf amtlichen Ausweisen nicht ersichtlich ist. Sollte die AHV-Nummer auf der E-ID enthalten sein, sollte eine Verwendung auf Vorgänge beschränkt sein, bei welchen die AHV-Nummer gesetzlich vorgesehen ist.

Art. 4 Abs. 4

Der Ausstellungsprozess ist im erläuternden Bericht nicht genauer beschrieben. Art. 4 Abs. 4 lässt jedoch vermuten, dass die Verifikation der antragstellenden Person und die Ausstellung der E-ID online und komplett automatisch vonstatten gehen soll – und kein Besuch auf der Gemeinde oder im Passbüro vorgesehen ist. Wie eine aktuelle Untersuchung des deutschen Chaos Computer Club (CCC) zeigt, weisen sämtliche gängigen Systeme zur «Video-Identifikation» Schwachstellen auf, die einen Identitätsdiebstahl möglich machen. Auf die Technik der «Video-Identifikation» und vergleichbare Verfahren ist daher zu verzichten. Auch wenn ein Identitätsdiebstahl

durch einen «Deep-Fake» in Verbindung mit dem Abgleich des Gesichtsbild aus dem ISA oder dem ZEMIS allenfalls schwieriger durchzuführen ist, wäre eine erfolgreiche Demonstration eines Identitätsdiebstahls verheerend für das Vertrauen und die Akzeptanz der E-ID.

Ein Vergleich der Bilder mit den Datenbanken ZEMIS und ISA sehen wir als überflüssig an, weil er für den Ausstellungsprozess nicht unbedingt erforderlich ist. Auf jeden Fall – und unabhängig vom gewählten Verfahren – müssen allfällig erhobene biometrische Daten unmittelbar im Anschluss an die Ausstellung (und der Übertragung der Daten in die E-ID nach Art. 2 Abs. 2 lit. g.) vernichtet werden.

Art. 10

Wir schlagen die Streichung des letzten Satzes («sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können») vor, da ein nicht-elektronischer amtlicher Ausweis dieses Kriterium ohnehin erfüllen sollte und ein diskriminierungsfreier Zugang für Personen ohne E-ID gewährleistet sein soll.

Art. 11 Abs. 3

Ein Abgleich mit den Datenbanken ISA und ZEMIS sowie dem Versichertenregister sehen wir, wie bereits ausgeführt, für nicht notwendig an.

Vierter Abschnitt

Den vierten Abschnitt sehen wir als stark ergänzungsbedürftig an.

Art. 1 Abs. 2 lit. b des Vorschlags zum BGEID setzt als Ziel des Gesetzes fest, dass der Schutz der Persönlichkeit und der Grundrechte der Personen, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, gewahrt werden solle. In dieser Hinsicht ist aber die momentane Fassung des Art. 16 des Vorschlags, welche festlegt, dass die Inhaberin oder der Inhaber frei darüber entscheiden kann, welche Bestandteile des Nachweises sie bekanntgibt, ungenügend. Es droht eine Überidentifikation.

Es ist für den Persönlichkeitsschutz essentiell, dass die Verifikatorin nicht frei über die Erfordernis des elektronischen Nachweises und deren Umfang bestimmen kann, sondern diese gesetzlich auf das unbedingt Erforderliche beschränkt wird, und dass andernfalls eine informierte und explizite Zustimmung stattfindet. Betreffend

Einschränkung der Datenmenge auf das Notwendige lässt der Vorentwurf zum BGEID zu, dass mehr Daten als notwendig verarbeitet werden, und damit mehr Möglichkeit für deren Missbrauch eröffnet werden. Um den geforderten Prinzipien «privacy by design» und Datensparsamkeit gerecht zu werden, ist eine Ergänzung notwendig.

Ergänzungsvorschlag zu Art. 16

Es werden zwei neue Gesetzesbestimmung in Ergänzung zu Art. 16 vorgeschlagen.

Art. 16^{bis} bestimmt, dass Umfang und Erfordernis von Seiten der Verifikatorin auf das unbedingt Erforderliche beschränkt wird. Er enthält auch eine Bestimmung des diskriminierungsfreien Zugangs zu Leistungen für Menschen ohne E-ID, welches vor allem Personen ohne Wohnsitz und Aufenthaltsbewilligung in der Schweiz sowie Menschen ohne Zugang zu technischen Mitteln betrifft. Der Absatz ist auch daraufhin ausgerichtet, dass sichergestellt ist, dass die Ausweiserfordernis von Privaten und Behörden nur dann besteht, wenn es die Umstände rechtfertigen.

Art. 16^{ter} verankert das Informations-, Zustimmungs- und Widerrufbarkeitsprinzip, namentlich beim Gebrauch der Daten über ihren gesetzlichen und unbedingt erforderlichen Zweck hinaus. Dem Umstand, dass ein Ausweisen verschiedene Zwecke erfüllen kann, wird mit der Bestimmung Rechnung getragen, dass die Zustimmung und Widerrufung auf jeden einzelnen Zweck anwendbar ist.

Gesetzestext

Art. 16^{bis} Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang

¹ Die Erfordernis eines elektronischen Nachweises darf von Behörden und Privaten als Voraussetzung für die Erbringung einer Leistung oder Gewährung eines Zugangs nur insoweit gestellt werden als sie für die Erbringung der Leistung oder der Gewährung des Zugangs unbedingt erforderlich ist.

² Falls die Übermittlung von Bestandteilen eines elektronischen Nachweises oder davon abgeleiteten Informationen unbedingt erforderlich ist, so ist stets die Möglichkeit vorzusehen, diese Bestandteile und Informationen ohne vermeidbare Nachteile auf andere Weise zu übermitteln.

Art. 16^{ter} Informations- und Zustimmungspflicht; Widerrufsrecht

Für Datenbearbeitungen, welche für die Erbringung der Leistung oder die Gewährung des Zugangs nicht unbedingt erforderlich sind, gelten nachfolgende Bestimmungen:

a Die Verifikatorin informiert die Inhaberin oder den Inhaber des Ausweises über Art, Zweck und Umfang der Datenbearbeitung.

b Die Datenbearbeitung bedarf der expliziten und jederzeit widerrufbaren Zustimmungen der Inhaberin und des Inhabers.

c Erfüllt die Bearbeitung verschiedene Zwecke, so hat die Inhaberin oder der Inhaber die Zustimmung zu jedem dieser Zwecke einzeln zu erteilen.

d Die Inhaberin oder der Inhaber kann die Zustimmung jederzeit und einzeln widerrufen.

Art. 16 Abs. 3

Streichen von «möglichst», da eine Vermeidung der Kenntnisnahme, beispielsweise durch Einsatz eines Proxys, technisch möglich ist.

Fünfter Abschnitt

Art. 20

Die Fakultativbestimmung sollte mit einer obligatorischen Bestimmung ersetzt werden. Der Bund sollte die Infrastruktur und alle benötigten Anwendungen (als Beispielapplikation) zur Verfügung stellen, damit ein vielfältiges Ökosystem und das nötige Vertrauen entstehen kann.

Art. 21 Abs. 2

Aus der Bestimmung ergibt sich noch nicht eindeutig, dass der Zugriff auf die Sicherheitskopien durch andere Personen nicht möglich sein darf; dies ist entsprechend zu ergänzen. (Die benötigten Keys oder Informationen sind bei den Inhaberinnen; zur Not könnten Nachweise auch neu ausgestellt werden.)

Art. 25

Art. 25 BGEID kann dahingehend interpretiert werden, dass sie dem Bundesrat eine Gesetzgebungskompetenz delegiert. Mit Hinweis darauf ist es problematisch, wenn der Bundesrat selbständig Erweiterungen vornehmen kann, insbesondere weil der

Rechtsweg betreffend Bundesratserlasse üblicherweise ausgeschlossen oder schwierig wahrzunehmen ist. Um die Möglichkeit unvorhergesehener technische Erneuerungen zu berücksichtigen, sei deshalb eine Methode vorzuschlagen, bei welcher die gerichtliche Überprüfung sowohl der Notwendigkeit als auch der Verhältnismässigkeit möglich ist.

Sechster Abschnitt

Art. 26

Es sei die Kostenlosigkeit aller Handlungen vorzusehen, welche die Zustimmung oder den Widerruf einer bestimmten Datenbearbeitung durch die Inhaberin oder den Inhaber eines elektronisches Ausweises erwirkt.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung des E-ID-Referendums.

Freundliche Grüsse

Daniel Graf
Co-Kampagnenleiter

Erik Schönenberger
Co-Kampagnenleiter

Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen
Justiz- und Polizeidepartementes EJPD
Bundeshaus West
3003 Bern

Direkt per E-Mail an:
rechtsinformatik@bj.admin.ch

Lausanne, 20. Oktober 2022

CGR / SUTC

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Stellungnahme zur Vernehmlassung V1.3

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Zusammenfassung

Wir danken Ihnen für die Möglichkeit, an dieser Vernehmlassung zur eID teilzunehmen. Als ELCA Security - eine Tochterfirma des privaten Schweizer Informatikunternehmens ELCA Informatik - sehen wir unsere Verantwortung weniger in der Bereitstellung von politischer Expertise, sondern wir konzentrieren uns voll und ganz auf unsere Cybersecurity- und Business-Fachwissen. Wir sind stolz, einige der talentiertesten Entwickler, Ingenieure, Analysten und IT-Berater der Schweiz als Teil unseres Teams zu nennen, denn es ist unsere Mission unseren Kunden die bestmöglichen Lösungen auf dem Markt zu bieten. Deshalb ist es uns eine Ehre, unser Fachwissen mit Ihnen zu teilen. Neben unserer reinen Cybersecurity-Expertise sind wir auch als anerkannter Identity Provider in der Schweiz tätig. Seit mehr als drei Jahren betreuen wir

öffentliche Verwaltungen, alle Stammgemeinschaften sowie private Unternehmen. Wir sind daher überzeugt, dass unsere eID Marktexpertise und -erfahrung einen zusätzlichen wertvollen Input für diese Vernehmlassung bietet.

Wir möchten uns zu den folgenden acht Punkten, ohne Prioritätsreihenfolge, positionieren:

1. Sicherung und Speicherung kritischer Daten

Gemäss Artikel 21 muss ein Sicherungssystem entweder vom Bund selbst und/oder von zertifizierten und von der Regierung ernannten Anbietern bereitgestellt werden. Die Speicherung dieser kritischen Daten muss den höchsten Sicherheitsstandards entsprechen: Strenge - zertifizierte und geprüfte - Vorschriften sind erforderlich, um Sicherheitsverletzungen und Missbrauch zu verhindern.

2. Sicherheit und Kontrollen

Der Bund hat die Zuständigkeit und muss die Einhaltung und Authentizität, sowie die Sicherheit der künftigen Wallets zu garantieren. Gemäss Artikel 14 würde das Gesetz jedoch grundsätzlich jeder Applikation erlauben, kritische Daten zu speichern. Unserer Meinung nach muss das Gesetz die Zertifizierung von Applikationen und/oder Wallets klar definieren. Das bedeutet, dass Applikationen bestimmten Sicherheitsmassnahmen unterzogen werden müssen, um verwendet und installiert werden zu dürfen. Dies kann entweder durch die Regierung oder durch private Anbieter erfolgen, die bestimmte Sicherheits-, Authentifizierungs- und Akkreditierungsstandards einhalten.

Darüber hinaus würde die Regierung ein öffentliches Register mit akkreditierten Anbietern führen. Darüber hinaus müssten technische Massnahmen entwickelt werden, um die Nutzung unsicherer und nicht akkreditierter Anwendungen zu verhindern.

In einem Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) über die digitale Identität wird folgende Erklärung abgegeben: *"Ein Wallet ist die Hauptkomponente der Lösung und muss den Anforderungen der Verordnung entsprechend zertifiziert sein. Eine Wallet wird vom Nutzer gehalten und betrieben. Der Nutzer sollte sich der Downloads bewusst sein und nur legitime Wallet-Anwendungen verwenden, die Schlüssel, Identität und Identifizierungsprozesse sichern. Ein nicht-autorisiertes Wallet kann für den Nutzer einen tatsächlichen Sicherheitsverlust bedeuten, was zu Risiken wie mangelnder Vertraulichkeit seiner Daten und einer möglichen Komprimierung seines Sicherheitsschlüssel führt."*

3. Prüfbarkeit

Aufgrund des dezentralen Charakters des Systems wird es schwierig sein, im Streitfall Ermittlungen durchzuführen. Folglich müssen die Strafverfolgungsbehörden in der Lage sein, festzustellen, wo und wann eine bestimmte SSI verwendet wurde (z. B. zum Zwecke der Ermittlung bei Identitätsdiebstahl). Dies ist besonders wichtig für Aussteller und Prüfer von Attributen.

4. Information und Sensibilisierung der Bürger

Die Vergangenheit hat gezeigt, dass die jüngsten Initiativen rund um die eID und das elektronische Patientendossier (EPD) zum Teil daran gescheitert sind, dass die Bürgerinnen und Bürger nicht gezielt informiert wurden. Der Bund muss regelmässige und - was noch wichtiger ist - effiziente Kommunikationskampagnen durchführen, um die Akzeptanz bei den Bürgern zu erhöhen.

Da wir zu einem dezentraleren Ansatz übergehen, wird sich die Verantwortung linear auf den Bürger selbst verlagern. Die Schweizer Bevölkerung muss sich also der Risiken und der Verantwortung bewusst werden, die mit diesem Schritt einhergehen! Dies sollte durch eine effektive Kommunikation und nationale Sensibilisierungskampagnen geschehen.

5. SSI Reifegrad

Als Technologieanbieter und Cybersicherheitsexperte fördern wir die Dezentralisierung und Datenminimierung. Unsere Erfahrung zeigt jedoch, dass sich diese Technologien noch in einem sehr frühen Stadium befinden und noch nicht ausgereift sind. Daher unterstützen wir die folgenden zwei Massnahmen:

- a. Vermeiden Sie sowohl im Gesetzestext als auch in der Verordnung jegliche Technologieaussagen (z.B. Erwähnung der SSI-Infrastruktur).
- b. Fortlaufende Forschungsprojekte zur Überprüfung der Durchführbarkeit des genannten SII-Konzepts.

Darüber hinaus möchten wir auf die Notwendigkeit hinweisen, die Sicherheitsauswirkungen dieser Dezentralisierung von Anfang an zu berücksichtigen.

6. Monetarisierung

Wir stimmen zu, dass die eID, wie in Artikel 26 dargelegt, für alle Bürger und Aussteller kostenlos sein muss. Eine Gebühr sollte überall dort erhoben werden, wo ein Attribut ausgegeben oder im Gegenzug erfragt wird.

Dennoch sollte es eine klare Unterscheidung zwischen regulierten und nicht regulierten Attributen geben, wie sie auch in der "Verordnung zur europäischen digitalen Identität" beschrieben wird:

"Bei einem frei verteilten Dienst und einem freien und liberalen Markt besteht die Gefahr, dass der Bürger zu einer Geisel internationaler Technologieanbieter wird, die seine Daten zu Geld machen und den Datenschutz verletzen würden."

Grundsätzlich gilt: Wenn es kostenlos ist, wird der Nutzer zum Produkt.

Der Bund muss Kontrollmassnahmen ergreifen, um solche Entwicklungen zu vermeiden.

7. Offline-Modus

Die Nutzung der eID und der Prozess der Identitätsüberprüfung müssen sowohl im Offline- als auch im Online-Modus funktionieren: In einem Land wie dem unseren, mit weitläufiger und rauer Natur (Alpen), muss das System im Offline-Modus voll funktionsfähig sein und darf auf keinen Fall vom Netzzugang und dessen Verfügbarkeit abhängig sein! Dies ist besonders wichtig, weil die vorgesehene Nutzung einer eID immer mehr mit realen Anwendungsfällen verbunden sein wird, bei denen wir nicht erwarten können, dass der Bürger Zugang zum Internet/Netzwerk hat.

8. Abwärtskompatibilität und Interoperabilität

Als IdP-Anbieter mit umfassender Erfahrung in der Ausstellung von Ausweisen, z. B. für den Zugang zum elektronischen Patientendossier (EPD), fordern wir, dass das neue eID-Gesetz einen kontinuierlichen Zugang für solche bestehenden verifizierten Identitäten vorsieht und sicherstellt; zumindest für einen bestimmten Zeitraum. Wir empfehlen mindestens 5 Jahre.

Viele Akteure - wie z.B. die Kantone - sind heute bereits aktive Identitätsanbieter. Deshalb ist diese Anforderung besonders wichtig, um die laufenden Digitalisierungsbemühungen nicht zu unterbrechen oder zu gefährden. Auch, weil es in der Zwischenzeit und in den nächsten Jahren keine alternativen Lösungen gibt und geben wird! Diesen Identitätsanbieter muss zugesichert sein, dass das neue System interoperabel sein wird. Eine vollständige Migration der bestehenden eID wird für sie nicht akzeptabel sein.

Noch wichtiger ist, dass eine Rückwärtskompatibilität mit bereits zertifizierten Identitäten, die im Gesundheitsbereich, insbesondere dem elektronischen

Patientendossier (EPD), verwendet werden, gewährleistet und eine Neuregistrierung dieser Bürger vermieden werden muss.

Schlussfolgerung

Wir freuen uns sehr, dass dieses Thema an Bedeutung gewonnen hat, und hoffen, dass wir bald Klarheit über das weitere Vorgehen haben werden. Wir gehören zu den Akteuren auf dem Markt, die in den letzten Jahren viel in dieses Thema investiert haben → eID und EPD. Wir erwarten, dass diese Anstrengungen anerkannt werden und dass Unternehmen wie unseres so bald wie möglich in die Entwicklung des neuen Systems miteinbezogen werden. Wir glauben, dass eine privat-öffentliche Partnerschaft in diesem Fall eine gute Lösung ist! Wir danken Ihnen für Ihre Zeit und Ihre Bemühungen.

Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössisches
Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Directly per email to:
rechtsinformatik@bj.admin.ch

Lausanne, October 20, 2022

CGR / SUTC

Federal Law on Electronic Proof of Identity and Other Electronic Proofs of Identity (E-ID-Gesetz, BGEID)

Response to the Consultation V1.3

Dear President Keller-Sutter
Ladies and Gentlemen

Management Summary

We thank you for the opportunity given to us to participate in this eID consultation. As ELCA Security – a daughter company of the privately owned information technology firm in Switzerland ELCA Informatique - we see our responsibility less in providing political expertise and to focus full heartedly on our cybersecurity and business expertise. We are proud to call some of the most talented developers, engineers, analysts and IT consultants of Switzerland as part of our team and it is our mission to provide our clients with the best solutions possible in the market. Hence, why we are honored to share our expertise with you.

Besides our pure cybersecurity expertise, we are also active as a recognized identity provider in Switzerland. Since more than three years we are serving public administrations, all health communities as well as private companies. Thus,

we strongly believe that our eID market expertise and experience offers additionally valuable input for this consultation.

We would like to position ourselves on following eight points, in no order of priorities:

1. Backup and Critical Data Storage

Referring to article 21, a system of backup must be provided either by the Confederation itself and/or certified providers, appointed by the government. The storage of such critical data must comply with the highest level of security standards: strict regulations – certified and audited – are required to prevent security breaches and abuse.

2. Security and Controls

The Confederation is responsible and must guarantee compliance and authenticity as well as security of future wallets. Yet, as per article 14, the law would basically allow any application to store critical data. In our opinion, the law needs to clearly define the certification of applications and/or wallets. Meaning: applications must undergo specific security measures to be allowed to be used and installed. This can either be done by the government or by private providers complying with defined security, authentication and accreditation standards.

In addition, the government would operate a public register with accredited providers. In addition, technical measure would have to be developed, to prevent the usage of unsecure and not accredited applications.

Following statement, as issued in a report by the European Union Agency for Cybersecurity (ENISA) on digital identity, outlines:

"A wallet is the main component of the solution and is required to be certified as meeting the requirements of the regulation. A wallet is held and operated by the user. The user should be aware of downloads and use legitimate wallet applications that secure keys, identity, and identification processes. An unauthorized wallet can cause an actual security loss for the user, leading to risks that include a lack of confidentiality of their data and a possible key compromise."

3. Auditability

Due to the decentralized nature of the system, it will be hard to perform investigation in case of dispute. Consequently, law enforcement must have the capability to see where and when a given SSI was used (e.g. for the purpose of an identity theft investigation). This is especially important for issuers and verifiers of attributes.

4. Information and Citizen Awareness

Past shows that the recent initiatives around eID and Electronic Patient Record (EPR) failed partially because of lack of targeted information to the citizen. The Confederation needs put in place regular and – even more importantly - efficient communication campaigns to enhance adoption by the citizens.

In addition, as we are moving to a more decentralized approach, the responsibility will linearly move to the citizen itself. Hence, the Swiss population must be made aware of the risks and responsibilities implicated through this move! This should occur via effective communication and national sensibilization campaigns.

5. SSI Maturity

As a technology provider and cybersecurity expert, we are encouraging decentralization and data minimization. However, our experience shows that these technologies are at a very early stage and not yet mature. Therefore we support following two actions:

- a. Avoid any technology statements within the legal text as well as the ordonnance (e.g., mentioning of SSI infrastructure).
- b. Continuous research projects to verify the feasibility of mentioned SII approach.

Furthermore, we would like to highlight the requirement, to take security impact of this decentralization into account from the very beginning.

6. Monetization

We agree, as outlined in article 26, that the eID must be free for all citizen and issuers. A fee should be applied wherever an attribute is issued or in return is consumed.

Yet, there should be a clear distinction between regulated and non-regulated attributes as it is also described in the "Regulation for European Digital Identity": *"With a free distributed service and a free and liberal market, the risk is that the citizen becomes a hostage of international tech providers that would monetize their data and breach data privacy."* Basically, if it's free then the user becomes the product. The Confederation must put in place control measures to avoid this kind of developments.

7. Offline Mode

The use of the eID and its identification verification process must operate equally offline as well as in online mode: In a country like ours, with extensive and rough nature (Alps), the system must be fully operational in offline mode and must in no case dependent on network access and availability! This is especially important because the foreseen usage of an eID will be more and more linked to physical real life use cases, where we cannot expect the citizen to have internet/network access.

8. Backwards Compatibility and Interoperability

As an IdP provider with extensive experience as issuer of ID e.g., for Electronic Patient Record (EPR) access, we ask that the new eID law will foresee and ensure continuous access for such existing verified identities, at least for a certain period of time: we recommend a minimum of 5 years.

Today, many actors - such as cantons - are already active identity providers. Therefore, this requirement is especially important, not to interrupt or risk continuous digitalization efforts. Also, because there are and will not be any alternative solutions available meanwhile and for the coming few years! These identity providers need to be certain that the new system will be interoperable. A complete migration of existing eID will not be acceptable for them. Even more important: a backward compatibility with already certified identities in use within the health domain, specifically speaking the Electronic Patient Record (EPD), must be ensured and new registration of these citizens must be avoided.

Conclusion

We are very pleased to see that this subject has gained in importance and are hoping that we will have soon clarification on the way ahead.

We are part of the actors in the market, who have invested a lot in this topic in recent years → eID and EPD. Our expectation is that these efforts will be recognized and that companies, such as ours, will be considered and involved in the development of the new system as soon as possible. We believe a private-public partnership to be a good solution in this case! Thank you for your time and consideration.

Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössisches
Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Berne

Par email à :
rechtsinformatik@bj.admin.ch

Lausanne, 20 octobre 2022

CGR / SUTC

Loi Fédérale sur l'Identité Electronique et les Autres Identités Electroniques (E-ID-Gesetz, BGEID)

Prise de Position sur la Consultation V1.3

Madame la Conseillère fédérale Keller-Sutter
Mesdames et Messieurs

Résumé

Nous vous remercions de l'opportunité qui nous a été donnée de participer à cette consultation sur l'eID. En tant qu'ELCA Security - une filiale de l'entreprise privée de technologie de l'information ELCA Informatique en Suisse - nous considérons que notre responsabilité consiste moins à fournir une expertise politique qu'à nous concentrer pleinement sur notre expertise en matière de cybersécurité et de commerce. Nous sommes fiers de compter dans notre équipe certains des développeurs, ingénieurs, analystes et consultants en informatique les plus talentueux de Suisse et notre mission est de fournir à nos clients les meilleures solutions possibles sur le marché. C'est pourquoi nous sommes honorés de partager notre expertise avec vous.

Outre notre expertise pure en matière de cybersécurité, nous sommes également actifs en tant que fournisseur d'identité reconnu en Suisse. Depuis plus de trois

ans, nous sommes au service d'administrations publiques, de toutes les communautés de santé ainsi que d'entreprises privées. Ainsi, nous sommes convaincus que notre expertise et notre expérience du marché de l'identité électronique constituent un apport précieux pour cette consultation.

Nous souhaitons nous positionner sur les huit points suivants, sans ordre de priorité :

1. Sauvegarde et stockage des données critiques

En référence à l'article 21, un système de sauvegarde doit être fourni soit par la Confédération elle-même, soit par des prestataires certifiés, désignés par le gouvernement. Le stockage de ces données critiques doit être conforme aux normes de sécurité les plus élevées : des règles strictes - certifiées et contrôlées - sont nécessaires pour prévenir les violations de sécurité et les abus.

2. Sécurité et contrôles

La Confédération est responsable et doit garantir la conformité et l'authenticité ainsi que la sécurité des futurs wallets. Pourtant, selon l'article 14, la loi autoriserait en principe n'importe quelle application à stocker des données critiques. A notre avis, la loi doit définir clairement imposer une certification des applications et/ou des wallets. Autrement dit, les applications doivent être soumises à des mesures de sécurité spécifiques pour pouvoir être utilisées et installées. Cela peut être fait soit par le gouvernement, soit par des fournisseurs privés se conformant à des normes de sécurité, d'authentification et d'accréditation définies.

De plus, le gouvernement gèrera un registre public des fournisseurs accrédités. En outre, des mesures techniques devront être développées pour empêcher l'utilisation d'applications non sécurisées et non accréditées.

La déclaration suivante, telle que publiée dans un rapport de l'Agence de l'Union européenne pour la cybersécurité (ENISA) sur l'identité numérique, souligne :

"A wallet is the main component of the solution and is required to be certified as meeting the requirements of the regulation. A wallet is held and operated by the user. The user should be aware of downloads and use legitimate wallet applications that secure keys, identity, and identification processes. An unauthorized wallet can cause an actual security loss for the user, leading to risks that include a lack of confidentiality of their data and a possible key compromise."

3. Auditabilité

En raison de la nature décentralisée du système, il sera difficile de mener une enquête en cas de litige. Par conséquent, les services de police doivent être en mesure de savoir où et quand une SSI donnée a été utilisée (par exemple, dans le cadre d'une enquête sur un vol d'identité). Ceci est particulièrement important pour les émetteurs et les vérificateurs d'attributs.

4. Information et sensibilisation des citoyens

Le passé montre que les récentes initiatives concernant l'eID et le dossier électronique du patient (DEP) ont échoué en partie à cause d'un manque d'information pour les citoyens. La Confédération doit mettre en place des campagnes de communication régulières et - plus important encore - efficaces pour favoriser l'adoption par les citoyens.

En outre, comme nous passons à une approche plus décentralisée, la responsabilité se déplacera progressivement vers le citoyen lui-même. La population suisse doit donc être sensibilisée aux risques et aux responsabilités qu'implique cette évolution ! Cela doit se faire par le biais d'une communication efficace et de campagnes nationales de sensibilisation.

5. Maturité de la SSI

En tant que fournisseur de technologies et expert en cybersécurité, nous encourageons la décentralisation et la minimisation des données. Cependant, notre expérience montre que ces technologies sont à un stade très précoce et ne sont pas encore matures. C'est pourquoi nous soutenons les deux actions suivantes :

- a. Éviter tout détail lié à une technologie donnée dans le texte juridique ainsi que dans l'ordonnance (par exemple, mentionner une infrastructure SSI).
- b. Continuer les projets de recherche ayant pour but de vérifier la faisabilité de l'approche SSI.

En outre, nous tenons à souligner l'obligation de prendre en compte, dès le départ, de l'impact de cette décentralisation sur la sécurité.

6. Monétisation

Nous sommes d'accord, comme le souligne l'article 26, que l'eID doit être gratuite pour tous les citoyens et émetteurs. Une redevance doit être appliquée chaque fois qu'un attribut est émis ou consommé en retour.

Toutefois, il convient d'établir une distinction claire entre les attributs réglementés et non réglementés, comme le décrit également le "Règlement sur l'identité numérique européenne" :

"Avec un service distribué gratuitement et un marché libre et libéral, le risque est que le citoyen devienne l'otage de fournisseurs de technologie internationaux qui monétiseraient leurs données et violeraient la confidentialité de ces données". En effet, si c'est gratuit, l'utilisateur devient le produit. La Confédération doit mettre en place des mesures de contrôle pour éviter ce genre de développements.

7. Mode hors ligne

L'utilisation de l'eID et son processus de vérification de l'identification doivent fonctionner aussi bien en mode hors ligne qu'en mode en ligne : Dans un pays comme le nôtre, à la nature étendue et rude (Alpes), le système doit être pleinement opérationnel en mode hors ligne et ne doit en aucun cas dépendre de l'accès et de la disponibilité du réseau ! Ce point est particulièrement important car l'utilisation d'une carte d'identité électronique sera de plus en plus liée à des cas d'utilisation dans la vie réelle, où l'on ne peut pas attendre du citoyen qu'il ait accès à l'internet/au réseau.

8. Rétro-compatibilité et interopérabilité

En tant qu'IDP ayant une grande expérience en tant qu'émetteur d'identités, par exemple pour l'accès au dossier électronique du patient (EPR), nous demandons que la nouvelle loi sur l'eID prévoie et garantisse un accès continu aux identités vérifiées existantes, au moins pendant une certaine période : nous recommandons un minimum de 5 ans.

Aujourd'hui, de nombreux acteurs - comme les cantons - sont déjà des fournisseurs d'identité actifs. C'est pourquoi cette exigence est particulièrement importante, pour ne pas interrompre ou mettre en danger les efforts continus de numérisation. En outre, il n'y a et n'y aura aucune solution alternative disponible entre-temps et dans les années à venir ! Ces fournisseurs d'identité doivent être certains que le nouveau système sera interopérable. Une migration complète des identités électroniques existantes ne sera pas acceptable pour eux.

Plus important encore : il faut assurer la rétrocompatibilité avec les identités déjà certifiées utilisées dans le domaine de la santé, notamment dans le dossier électronique du patient (DEP), et éviter un nouvel enregistrement de ces citoyens.

Conclusion

Nous sommes très heureux de constater que ce sujet a gagné en importance et nous espérons que nous aurons bientôt des éclaircissements sur la voie à suivre. Nous faisons partie des acteurs du marché qui ont beaucoup investi dans ce sujet ces dernières années → eID et DEP. Nous espérons que ces efforts seront reconnus et que des entreprises comme la nôtre seront prises en compte et impliquées dans le développement du nouveau système dès que possible. Nous pensons qu'un partenariat privé-public est une bonne solution dans ce cas ! Nous vous remercions de votre temps et de votre attention.

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundeshaus West

CH-3003 Bern

Per Email an

rechtsinformatik@bj.admin.ch

Zürich-Flughafen, 20. Oktober 2022

Vernehmlassung über den Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise – Stellungnahme Flughafen Zürich AG

Sehr geehrte Damen und Herren,

Mit Schreiben vom 29. Juni 2022 hat Frau Bundesrätin Karin Keller-Sutter die Flughafen Zürich AG zur Teilnahme an der erwähnten Vernehmlassung eingeladen. Wir danken für diese Einladung und schätzen sie sehr. Gerne nehmen wir die Gelegenheit wahr, unsere Anliegen zur Einführung eines E-ID-Gesetzes zu äussern. Die Flughafen Zürich AG ist Eigentümerin und Betreiberin des grössten Landesflughafens mit über 30 Millionen Passagieren im Jahr (vor der Pandemie) und rund 27'500 Angestellten bei über 300 Unternehmen.

Die Flughafen Zürich AG begrüsst den Entwurf des E-ID Gesetzes und sieht viele Vorteile im Einsatz eines elektronischen Identitätsnachweises. Eine E-ID, die das gesamte digitale Ökosystem umfasst und verschiedene Funktionalitäten mitbringt, die in unterschiedlichen Bereichen eingesetzt werden können, bietet viele Opportunitäten für Nutzer, Kunden und Unternehmen. Damit können innovative Lösungen erarbeitet und angeboten werden sowie aktuelle Prozesse effizienter und sicherer gestaltet werden.

Am Flughafen Zürich tragen mehr als 27'500 Angestellte einen Flughafenausweis im Sinne eines Mitarbeiterausweises, davon werden jährlich 5'000 – 7'000 Ausweise neu erstellt oder erneuert. Für die Ausstellung sind zum Teil vielfältige Sicherheitsüberprüfungen notwendig, darunter fallen können unter anderem die Identitätsprüfung, der Nachweis eines Führerausweises, der Ausbildungsnachweis sowie der Betreibungs- und Strafregistrauszug. Eine nationale Infrastruktur einer E-ID, die die benötigten Informationen digital zur Verfügung stellt, würde den administrativen Aufwand enorm reduzieren und die Fehlerquellen deutlich minimieren.

Die Verknüpfung der E-ID mit weiteren staatlich regulierten Nachweisdokumenten könnte insbesondere bei Bewerbungsprozessen, der Ausstellung von Flughafenausweisen sowie für digitale Unterschriften zur Anwendung kommen. Ebenfalls könnte eine E-ID im Rahmen des «seamless travel», d.h. des möglichst barriere- und dokumentenfreien Reisens, eingesetzt werden. Pre-Covid nutzten ca. 13 Millionen Passagiere mit Wohnsitz Schweiz den Flughafen Zürich als An- oder Abflugsort. Eine E-ID würde damit gegen 1 Million mal pro Monat am Flughafen Zürich genutzt werden, bei der Schaffung von verschiedenen Touchpoints während der Reise noch höher. Damit einher geht eine Effizienz- und Komfortsteigerung für Passagiere und beteiligte Unternehmen.

Im Speziellen begrüssenswert sind die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern). Daneben ist es zentral, dass hinsichtlich der «elektronischen Brieftasche» eine Koordination mit europäischem Recht erfolgt, wie es der erläuternde Bericht vorsieht. Damit kann sichergestellt werden, dass künftig nicht nur Reisen von Schweizerinnen und Schweizern, sondern auch von europäischen oder anderen internationalen Fluggästen möglichst effizient abgewickelt werden können. Gleiches gilt selbstverständlich gegenseitig: mit einer international abgestimmten schweizerischen E-ID können Schweizer und Schweizerinnen in Zukunft auch im Ausland reibungsloser reisen.

Art. 4: Ausstellung

Neben der gesetzlichen Grundlage für die Schaffung einer E-ID ist es wichtig, dass diese relativ einfach zu beantragen ist. Es besteht ein grosses Interesse an einer Förderung der Nutzung und Verbreitung der E-ID. Je einfacher dieser Prozess, desto höher dürften viele berechnigte Personen eine E-ID beantragen. Mit einem verbreiteten Einsatz der E-ID könnte der Austausch mit Behörden und Privaten vereinfacht, die Transformation in den digitalen Raum weiter beschleunigt und neue Angebote für Kundinnen und Kunden geschaffen werden. Es sollte daher sichergestellt werden, dass nicht nur die „interessierte Minderheit“ eine E-ID aktiv über das Fedpol beantragt, sondern auch der grosse Teil der Bevölkerung eine E-ID einfach beantragen kann. Idealerweise werden Personen im Rahmen der Ausstellung von Pass und/oder Identitätskarte auf die Möglichkeit einer E-ID aktiv und standardmässig hingewiesen und im Prozess unterstützt. In diesem Fall ist der Ausstellungsort auf weitere Amtsstellen wie die Einwohnerkontrolle einer Wohngemeinde oder ein kantonales Passbüro zu erweitern.

Antrag 1: Art. 4, Abs. 1 ist folgendermassen zu ergänzen:

¹ Wer eine E-ID will, muss deren Ausstellung dem Bundesamt für Polizei (fedpol) oder Amtsstellen, die eine Identitätskarte oder einen Pass ausstellen, beantragen.

Art. 6: Gültigkeitsdauer

Der aktuelle Entwurf sieht aus Sicherheitsgründen eine zeitlich befristete Gültigkeit einer E-ID vor. Idealerweise lehnt sich die Gültigkeitsdauer der E-ID an die Gültigkeit von Pass und/oder ID an. Damit

kann der Erneuerungsprozess für Nutzerinnen und Nutzern der E-ID vereinfacht werden. Sollte aus Sicherheitsgründen die Spanne von zehn Jahren zu lange sein, so sollte die Gültigkeit fünf Jahre betragen und Nutzerinnen und Nutzer aktiv auf die Verlängerung hingewiesen werden.

Art. 26 Gebühren

Gemäss erläuterndem Bericht will der Bund für die übrigen Dienstleistungen keine Gebühren erheben. So sollen die Ausstellung der E-ID, deren Nutzung und Überprüfung sowie die Verwendung der elektronischen Brieftasche, das Aufrufen des Basisregisters und die Verwendung des Mechanismus zur Bestätigung des Identifikators gebührenfrei sein. Durch diesen Verzicht soll die Nutzung und Verbreitung der E-ID gefördert werden. Sowohl Behörden als auch Private haben ein grosses Eigeninteresse an einem möglichst verbreiteten Einsatz der E-ID. Im Sinne einer schnellen Skalierung der E-ID wäre eine gebührenfreie Nutzung aller Dienstleistungen zumindest in den ersten zehn Jahren empfehlenswert. Dies würde auch die Gefahr beseitigen, dass heutige Prozesse weiterhin günstiger bleiben als bei einer Umstellung zur E-ID und damit die Transformation verlangsamt würde.

Antrag 2: Art. 26 ist folgendermassen zu ergänzen:

⁵ Die Gebühren gemäss Artikel 26 werden frühestens zehn Jahre nach dem Inkrafttreten dieses Gesetzes erhoben.

Neben der gesetzlichen Grundlage zur E-ID gilt es im Sinne der nächsten Schritte ein Ökosystem digitaler Beweise aufzubauen. Daraus könnten sich weitere Anwendungsmöglichkeiten wie ein komplettes digitales und vereinfachtes Reiseerlebnis auf der Basis eines Kundenprofils und biometrischer Daten ergeben. Dieses könnte von der Ticketbuchung, über das Einchecken, Boarding bis hin zur Einreise in ein Drittland digital basiert sein. Dank der Vernetzung der verschiedenen Systeme, insbesondere auch auf internationaler Ebene (z.B. Schengen-Raum), könnten physische Kontrollen grossmehrheitlich entfallen. Ein gutes Beispiel ist das Known Traveller Digital Identity Projekt des World Economic Forums. Eine weitere Variante könnte die Einführung eines Plattform-Konzepts sein, auf dem ein digitaler und physischer Marktplatz entstehen kann. Ebenfalls zu prüfen ist, wie der Einsatz von Zutrittstickets mittels QR-Code und Alterskontrolle gewährleistet werden kann.

Wir danken Ihnen für die Berücksichtigung unseres Anliegens und stehen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Michael Hofmeier
Leiter Information & Communication Technology

Andrew Karim
Stv. Leiter Public Affairs



SGB-FSS
Schweizerischer Gehörlosenbund
Fédération Suisse des Sourds
Federazione Svizzera dei Sordi

SGB-FSS — Räfelstrasse 24 — CH-8045 Zürich

EJPD
Bundesamt für Justiz

Bundesrain 20
CH-3003 Bern
Per E-Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 30.09.2022

Vernehmlassung zum E-ID Gesetz, BGEID

Stellungnahme Schweizerischer Gehörlosenbund SGB-FSS

Der SGB-FSS ist ein nationaler Dachverband, der sich dafür einsetzt, dass Zugangsbarrieren für Menschen mit einer Hör- und Hörsehbehinderung abgebaut, dass sie gleiche Rechte und Chancen erhalten und dass die drei Landes-Gebärdensprachen (Deutschschweizerische Gebärdensprache (DSGS), Französische Gebärdensprache (LSF) und Italienische Gebärdensprache (LIS)) in der Schweiz gesellschaftlich und rechtlich anerkannt werden. Damit verfolgt er die vollständige Gleichstellung und Nichtdiskriminierung von Menschen mit Hör- und Hörsehbehinderung und deren Inklusion. Er sorgt für ein professionelles Angebot von Leistungen für die Zielgruppe von Menschen mit einer Hör- und Hörsehbehinderung, und der Kollektivmitglieder. Der SGB-FSS setzt sich als Experte und Interessenvertreter für die konsequente Verbreitung des bilingualen (und multilingualen) Spracherwerbs (Gebärdensprache und gesprochene / geschriebene Sprache) als Voraussetzung für die volle Inklusion aller gehörlosen, hör- und hörsehbehinderten Menschen in der Schweiz ein. Er tritt dafür ein, dass die schweizerischen Gebärdensprachen in allen Lebensbereichen gleichwertig wie die offiziellen Landessprachen Deutsch, Französisch, Italienisch und Rätoromanisch behandelt werden.

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit zur Stellungnahme zum E-ID.

Der SGB-FSS begrüsst die angestrebte Entwicklung in Richtung Digitalisierung.

Digitale Informations- und Kommunikationstechniken ermöglichen insbesondere auch Menschen mit einer Hörbehinderung einen barrierefreien Zugang zu Dienstleistungen der Behörden.

Allgemeine Bemerkungen



Die Schweiz hat die UNO Konvention über die Rechte von Menschen mit Behinderungen (UNO-BRK) ratifiziert. Gemäss Art. 21 UNO-BRK treffen die Vertragsstaaten alle geeigneten Massnahmen, um zu gewährleisten, dass Menschen mit Behinderungen das Recht auf Zugang zu Information gleichberechtigt mit anderen und durch alle von ihnen gewählten Formen der Kommunikation ausüben können. Unter anderem müssen die Vertragsstaaten dafür sorgen, dass sie Menschen mit Behinderungen öffentliche Informationen rechtzeitig und ohne zusätzliche Kosten in zugänglichen Formaten und Technologien zur Verfügung stellen (lit. a). Im Umgang mit Behörden soll dabei insbesondere die Verwendung von Gebärdensprachen akzeptiert und erleichtert werden (lit. b).

Weiter hält Art. 14 Abs. 1 des Behindertengleichstellungsgesetzes (BehiG) fest, dass Bundesbehörden im Verkehr mit der Bevölkerung auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten Rücksicht nehmen müssen. Art. 14 Abs. 2 BehiG verweist dabei explizit auch auf Dienstleistungen, welche im Internet angeboten werden.

Die Ausgestaltung des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben muss im Einklang mit den erwähnten Rechtsgrundlagen erfolgen.

Zu den einzelnen Artikeln

Der SGB-FSS fordert folgende Änderungen des Entwurfs zum E-ID Gesetz, BGEID:

Art. 1 Abs. 2 lit. c.

zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik **und der Barrierefreiheit** entsprechen.

NEU: Art. 16bis Barrierefreiheit

Die elektronischen Nachweise müssen den Grundsatz der Barrierefreiheit entsprechen. Sämtliche Infrastrukturbetreibende, die Ausstellerinnen einer E-ID, Verifikatorinnen und weiteren Usergruppen müssen die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sicherstellen.

Zur laufenden Überprüfung der Barrierefreiheit ist eine unabhängige Stelle mit vertretenden von Betroffenen verantwortlich.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse
Ihr Schweizerischer Gehörlosenbund
Rechtsdienst

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz Bundesrain 20

3003 Bern

Per E-Mail an: rechtsinformatik@bj.admin.ch

Bern, den 19. Oktober 2022

Vernehmlassungsantwort BGEID: Stellungnahme zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter

Sehr geehrte Damen und Herren

Am 29. Juni 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID, Vernehmlassungsfrist 20. Oktober 2022). Gerne nehmen wir hiermit Stellung und folgen dabei integral den Feststellungen der Digitalen Gesellschaft.

grundrechte.ch ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Dabei verteidigen wir insbesondere das Recht auf Überwachungsfreiheit und das Recht auf informationelle Selbstbestimmung.

Grundsätzliches

Die Hauptkritikpunkte des Gesetzes im Rahmen des Referendums und der Volksabstimmung betrafen den Zweck und die Herausgeberschaft («staatlicher, elektronischer Ausweis» anstatt «privates Login») sowie den mangelnden Datenschutz (Datenschutz durch Technik/Privacy-by-Design und Datensparsamkeit/Privacy-by-Default). Dies waren dann auch die Gründe, weshalb das Gesetz mit grosser Mehrheit an der Urne abgelehnt wurde.

Wir begrüssen die Neuauflage des E-ID-Gesetzes und sind mit der Stossrichtung einverstanden. **Wir vertreten jedoch die Auffassung, dass der Schutz der Persönlichkeit und der Personendaten im vorliegenden Vorentwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise noch unzureichend umgesetzt sowie der Schutz vor Missbrauch der Daten noch unzureichend gewährleistet ist. Dies betrifft insbesondere die drohende «Überidentifikation».**

Bearbeitung von Personendaten

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht, abgeleitet von Art. 13 Abs. 2 der Bundesverfassung (BV). Ein elektronischer Nachweis ist ein Eingriff in dieses Grundrecht und hat gemäss Art. 36 BV verhältnismässig zu erfolgen; im Speziellen sollte die Grundrechtseinschränkung nicht weiter gehen, als notwendig und sachlich gerechtfertigt ist. Diesem Grundsatz ist im vorgeschlagenen Gesetz ungenügend Rechnung getragen. Wir vertreten die Auffassung, dass die gesetzlich vorgesehene Erhebung von Daten sowie ihre Bearbeitung auf das zu ihrem Zweck unbedingt Erforderliche reduziert werden muss, um den Gehalt von Art. 13 Abs. 2 BV zu wahren.

Personendaten, welche in Bezug auf einen elektronischen amtlichen Nachweis erhoben und verarbeitet werden, erfordern zudem einen höheren und spezifischeren Schutz, als es das (revidierte) Datenschutzgesetz (DSG) bietet – und demnach eine ungenügende Grundlage für den Schutz der Personendaten nach dem BGEID darstellt. Wir sind der Auffassung, dass amtlich erhobene, verwaltete und bereitgestellte Daten ein erhöhter Schutz beizumessen ist und dass dies im BGEID selbst vorzusehen ist.

Dass BGEID schafft eine neue Kategorie von Daten: Daten, die erstens besonders schutzwerten Charakter haben, zweitens auch behördlich verifiziert sind und drittens, für welche eine breite private Verwendung vorgesehen ist. Sie bilden eine neue Kategorie an Daten, welche durch das DSG nicht gedeckt sind. Das allgemein formulierte Datenschutzgesetz sowohl in der derzeitigen als auch in der künftigen, revidierten Fassung vermag nicht, einen adäquaten Schutz zu liefern, gerade betreffend der Überidentifizierung.

Nach dem DSG kann eine Datenbearbeitung erfolgen, sofern ein überwiegendes privates oder öffentliches Interesse eine solche rechtfertigt. Hier besteht ein erheblicher Interpretationsspielraum der Beteiligten und lässt in der Praxis auch zweckfremde Datenbearbeitungen zu, soweit sie etwa aufgrund eines wirtschaftlichen Interesses der Inhaberin oder des Inhabers der Datensammlung für verhältnismässig angesehen werden können (Beispiel: Online-Tracking, Kreditwürdigkeit). Meist wird zudem eine Einwilligung durch das Akzeptieren der Allgemeinen Geschäftsbedingungen (AGB) und/oder der Datenschutzerklärung eingeholt, ohne dass diesem Vorgang widersprochen werden könnte. Das DSG schafft auch keinen Anspruch auf ein Widerspruchsrecht, wonach der Bearbeitung – mindestens im Nachhinein – (einfach, also ohne Klage auf Persönlichkeitsverletzung) widersprochen werden könnte.

Das Schweizer DSG geht überdies betreffend Vorschriften hinsichtlich Identifikation und Tracking deutlich weniger weit als die EU-Richtlinie (DSGVO). Namentlich entfällt in der Schweiz das Kopplungsverbot, welches verhindert, dass eine Einwilligung in eine zweckfremde Datenbearbeitung über eine Kopplung an die Leistung selbst abgenötigt wird. Dies kann dazu führen, dass Private Daten sammeln und gebrauchen können, welche nicht für die Erbringung von Leistungen erforderlich sind und für welche keine eigentliche Freiwilligkeit besteht.

Damit verletzt nach unserer Ansicht die vorgeschlagene Fassung des BGEID sowohl den Grundsatz der Datensparsamkeit als auch der informationellen Selbstbestimmung. Neben der Verletzung der genannten Grundrechte und Grundsätze würde die drohende Überidentifikation das Vertrauen in die elektronische Identifikation schädigen. Die Akzeptanz würde darunter insgesamt stark leiden. Im BGEID sind deshalb ausgestaltete, konkrete

Bestimmung betreffend diesen Grundsätzen vorzusehen; Vorschläge zu diesen Bestimmungen werden weiter unten konkretisiert.

Rechtssystematisch stehen solche Bestimmungen ohne Kollision mit dem Datenschutzgesetz. Art. 4 DSG (Art. 6 nDSG) bestimmt, dass die Bearbeitung von Personendaten nur rechtmässig erfolgen darf, äussert sich zum rechtlichen Rahmen aber nicht. Damit besteht Gestaltungsspielraum des rechtlichen Rahmens durch das BGEID, wobei zu betonen ist, dass im heutigen rechtlichen Rahmen die konkrete Ausgestaltung des rechtlichen Rahmens einer Datenbearbeitung spezialgesetzlich, und nicht durch das DSG, vorgenommen wird.

Diskriminierungsfreier Zugang zu Leistungen

Unter mehreren Gesichtspunkten erweist sich als problematisch, wenn der Erhalt von Leistungen vom Besitz einer E-ID abhängig gemacht wird. Damit werden einerseits Menschen ausgeschlossen, welche nach geltender Gesetzgebung kein Anrecht auf eine E-ID haben, andererseits aber auch solche, welche nicht über die technischen Kenntnisse oder die Mittel verfügen, eine E-ID zu beantragen, oder dies aus persönlichen Gründen ablehnen. Unter Hinweis auf das Diskriminierungsverbot (Art. 8 BV) ist ein diskriminierungsfreier Zugang zu Leistungen deshalb gesetzlich zu gewährleisten.

Hierzu sei noch angemerkt, dass nach den vorgeschlagenen Bestimmungen nur Menschen Anrecht auf eine E-ID haben, welche in der Schweiz über eine Aufenthaltsbewilligung verfügen. Dies schliesst alle Menschen aus, welche über eine solche nicht verfügen und sich unter einem anderen Titel als einer ordentlichen Aufenthaltsbewilligung in der (digitalen) Schweiz aufhalten. Das Gesetz könnte eine Möglichkeit vorsehen, dass bei genügender Identifikation (etwa über einen ausländischen Pass) eine elektronische ID ausgestellt werden kann, wobei bei unsicherer Identifikation diesem Umstand mit einer Anmerkung Rechnung getragen werden könnte.

Durchsetzbarkeit

Damit Gesetzesbestimmungen wirksam sind, müssen sie durchsetzbar sein. Das vorgeschlagene Gesetz verzichtet vollständig auf spezifische Bestimmungen, um Bestimmungen durchzusetzen und Verletzungen beheben zu können. Wir sehen es als wichtig an, dass juristische und natürliche Anbieterinnen (Ausstellerinnen, Verifikatorinnen), welche Bestimmungen verletzen, einer Strafbestimmung unterliegen, und dass ein vereinfachter und kostenfreier Zugang zu Verfahren zur Behebung von Verletzung sowohl für die Subjekte des elektronischen Identitätsnachweises als auch für Verbände, die sich im Bereich Daten- und Persönlichkeitsschutz engagieren, im Gesetz geschaffen werden.

Erster Abschnitt

Art. 1: Art. 1 Abs. 2 BGEID hält als Ziel des Gesetzes fest, den Schutz der Persönlichkeit und der Grundrechte im Zusammenhang mit der Verwendung der E-ID zu gewährleisten. Diese explizite Zweckbindung halten wir für unabdingbar.

Wie nachfolgend erläutert, tragen verschiedene Bestimmungen des Gesetzes dem in Art. 1 Abs. 2 BGEID beschriebenen Grundsatz ungenügend Rechnung, namentlich betreffend der Datensparsamkeit.

Zweiter Abschnitt

Art. 2 Abs. 3

Die AHV-Nummer, die Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde, und die Angaben zum Ausstellungsprozess sind für die Ausstellung und Verwendung der E-ID nicht erforderlich und stellen damit Daten dar, die nicht Teil der E-ID sein sollten; darüber ist darauf hinzuweisen, dass die AHV-Nummer auch üblicherweise auf amtlichen Ausweisen nicht ersichtlich ist. Sollte die AHV-Nummer auf der E-ID enthalten sein, sollte eine Verwendung auf Vorgänge beschränkt sein, bei welchen die AHV-Nummer gesetzlich vorgesehen ist.

Art. 4 Abs. 4

Der Ausstellungsprozess ist im erläuternden Bericht nicht genauer beschrieben. Art. 4 Abs. 4 lässt jedoch vermuten, dass die Verifikation der antragstellenden Person und die Ausstellung der E-ID online und komplett automatisch vonstattengehen soll – und kein Besuch auf der Gemeinde oder im Passbüro vorgesehen ist. Wie eine aktuelle Untersuchung des deutschen Chaos Computer Club (CCC) zeigt, weisen sämtliche gängigen Systeme zur «Video-Identifikation» Schwachstellen auf, die einen Identitätsdiebstahl möglich machen. Auf die Technik der «Video-Identifikation» und vergleichbare Verfahren ist daher zu verzichten. Auch wenn ein Identitätsdiebstahl durch einen «Deep-Fake» in Verbindung mit dem Abgleich des Gesichtsbild aus dem ISA oder dem ZEMIS allenfalls schwieriger durchzuführen ist, wäre eine erfolgreiche Demonstration eines Identitätsdiebstahls verheerend für das Vertrauen und die Akzeptanz der E-ID.

Ein Vergleich der Bilder mit den Datenbanken ZEMIS und ISA sehen wir als überflüssig an, weil er für den Ausstellungsprozess nicht unbedingt erforderlich ist. Auf jeden Fall – und unabhängig vom gewählten Verfahren – müssen allfällig erhobene biometrische Daten unmittelbar im Anschluss an die Ausstellung (und der Übertragung der Daten in die E-ID nach Art. 2 Abs. 2 lit. g.) vernichtet werden.

Art. 10

Wir schlagen die Streichung des letzten Satzes («sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können») vor, da ein nicht-elektronischer amtlicher Ausweis dieses Kriterium ohnehin erfüllen sollte und ein diskriminierungsfreier Zugang für Personen ohne E-ID gewährleistet sein soll.

Art. 11 Abs. 3

Ein Abgleich mit den Datenbanken ISA und ZEMIS sowie dem Versichertenregister halten wir, wir bereits ausgeführt, für nicht notwendig.

Vierter Abschnitt

Den vierten Abschnitt sehen wir als stark ergänzungsbedürftig an.

Art. 1 Abs. 2 lit. b des Vorschlags zum BGEID setzt als Ziel des Gesetzes fest, dass der Schutz der Persönlichkeit und der Grundrechte der Personen, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, gewahrt werden solle. In dieser Hinsicht ist aber die momentane Fassung des Art. 16 des Vorschlags, welche festlegt, dass die Inhaberin oder der Inhaber frei darüber entscheiden kann, welche Bestandteile des Nachweises sie bekanntgibt, ungenügend. Es droht eine Überidentifikation.

Es ist für den Persönlichkeitsschutz essentiell, dass die Verifikatorin nicht frei über die Erfordernis des elektronischen Nachweises und deren Umfang bestimmen kann, sondern diese gesetzlich auf das unbedingt Erforderliche beschränkt wird, und dass andernfalls eine informierte und explizite Zustimmung stattfindet. Betreffend Einschränkung der Datenmenge auf das Notwendige lässt der Vorentwurf zum BGEID zu, dass mehr Daten als notwendig verarbeitet werden, und damit mehr Möglichkeit für deren Missbrauch eröffnet werden. Um den geforderten Prinzipien «privacy by design» und Datensparsamkeit gerecht zu werden, ist eine Ergänzung notwendig.

Ergänzungsvorschlag zu Art. 16

Es werden zwei neue Gesetzesbestimmung in Ergänzung zu Art. 16 vorgeschlagen.

Art. 16^{bis} bestimmt, dass Umfang und Erfordernis von Seiten der Verifikatorin auf das unbedingt Erforderliche beschränkt wird. Er enthält auch eine Bestimmung des diskriminierungsfreien Zugangs zu Leistungen für Menschen ohne E-ID, welches vor allem Personen ohne Wohnsitz und Aufenthaltsbewilligung in der Schweiz sowie Menschen ohne Zugang zu technischen Mitteln betrifft. Der Absatz ist auch daraufhin ausgerichtet, dass sichergestellt ist, dass die Ausweiserfordernis von Privaten und Behörden nur dann besteht, wenn es die Umstände rechtfertigen.

Art. 16^{ter} verankert das Informations-, Zustimmungs- und Widerrufbarkeitsprinzip, namentlich beim Gebrauch der Daten über ihren gesetzlichen und unbedingt erforderlichen Zweck hinaus. Dem Umstand, dass ein Ausweisen verschiedene Zwecke erfüllen kann, wird mit der Bestimmung Rechnung getragen, dass die Zustimmung und Widerrufung auf jeden einzelnen Zweck anwendbar ist.

Gesetzestext

Art. 16^{bis} Einschränkung der Datenbearbeitung auf das unbedingt Erforderliche; diskriminierungsfreier Zugang

¹ Die Erfordernis eines elektronischen Nachweises darf von Behörden und Privaten als Voraussetzung für die Erbringung einer Leistung oder Gewährung eines Zugangs nur insoweit gestellt werden als sie für die Erbringung der Leistung oder der Gewährung des Zugangs unbedingt erforderlich ist.

² Falls die Übermittlung von Bestandteilen eines elektronischen Nachweises oder davon abgeleiteten Informationen unbedingt erforderlich ist, so ist stets die Möglichkeit vorzusehen, diese Bestandteile und Informationen ohne vermeidbare Nachteile auf andere Weise zu übermitteln.

Art. 16^{ter} Informations- und Zustimmungspflicht; Widerrufsrecht

Für Datenbearbeitungen, welche für die Erbringung der Leistung oder die Gewährung des Zugangs nicht unbedingt erforderlich sind, gelten nachfolgende Bestimmungen:

a Die Verifikatorin informiert die Inhaberin oder den Inhaber des Ausweises über Art, Zweck und Umfang der Datenbearbeitung.

b Die Datenbearbeitung bedarf der expliziten und jederzeit widerrufbaren Zustimmungen der Inhaberin und des Inhabers.

c Erfüllt die Bearbeitung verschiedene Zwecke, so hat die Inhaberin oder der Inhaber die Zustimmung zu jedem dieser Zwecke einzeln zu erteilen.

d Die Inhaberin oder der Inhaber kann die Zustimmung jederzeit und einzeln widerrufen.

Art. 16 Abs. 3

Streichen von «möglichst», da eine Vermeidung der Kenntnisaufnahme, beispielsweise durch Einsatz eines Proxys, technisch möglich ist.

Fünfter Abschnitt

Art. 20

Die Fakultativbestimmung sollte mit einer obligatorischen Bestimmung ersetzt werden. Der Bund sollte die Infrastruktur und alle benötigten Anwendungen (als Beispielapplikation) zur Verfügung stellen, damit ein vielfältiges Ökosystem und das nötige Vertrauen entstehen können.

Art. 21 Abs. 2

Aus der Bestimmung ergibt sich noch nicht eindeutig, dass der Zugriff auf die Sicherheitskopien durch andere Personen nicht möglich sein darf; dies ist entsprechend zu ergänzen. (Die benötigten Keys oder Informationen sind bei den Inhaberinnen; zur Not könnten Nachweise auch neu ausgestellt werden.)

Art. 25

Art. 25 BGEID kann dahingehend interpretiert werden, dass sie dem Bundesrat eine Gesetzgebungskompetenz delegiert. Mit Hinweis darauf ist es problematisch, wenn der Bundesrat selbständig Erweiterungen vornehmen kann, insbesondere weil der Rechtsweg betreffend Bundesratserlasse üblicherweise ausgeschlossen oder schwierig wahrzunehmen ist. Um die Möglichkeit unvorhergesehener technische Erneuerungen zu berücksichtigen, sei deshalb eine Methode vorzuschlagen, bei welcher die gerichtliche Überprüfung sowohl der Notwendigkeit als auch der Verhältnismässigkeit möglich ist.

Sechster Abschnitt

Art. 26

Es sei die Kostenlosigkeit aller Handlungen vorzusehen, welche die Zustimmung oder den Widerruf einer bestimmten Datenbearbeitung durch die Inhaberin oder den Inhaber eines elektronischen Ausweises erwirkt.

Mit freundlichen Grüßen



Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD Bundeshaus West
CH-3003 Bern

Einreichung per Mail an: rechtsinformatik@bj.admin.ch

Wallisellen, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zum neuen Vorschlag für ein E-ID-Gesetz äussern zu können, welche wir hiermit gerne wahrnehmen. Einleitend möchten wir dem EJPD für den partizipativen Prozess der Erarbeitung des BG E-ID danken, den wir als mustergültig und nachahmenswert erachten.

Grundsätzlich sind wir der Überzeugung, dass der Vorschlag für das E-ID-Gesetz eine sehr gute Basis darstellt und den Rahmen für eine Vertrauensinfrastruktur setzt, in dem eine staatlich herausgegebene E-ID das Kernelement darstellt. Wir begrüssen den Paradigma-Wechsel im Umgang mit personenbezogenen Daten und die Schaffung eines Rechtsrahmens für eine Vertrauensinfrastruktur.

Eine verlässliche Vertrauensinfrastruktur hat für das Gesundheitswesen und dessen Digitalisierung eine zentrale Bedeutung. Wir erachten es als äusserst wichtig, dass die Vertrauensinfrastruktur offen, sicher und verlässlich gestaltet ist und diese von allen Marktteilnehmern gleichermassen genutzt werden kann. Zudem sollte sie auch regelmässig von einer unabhängigen Instanz überprüft werden. Die E-ID soll sich darin als zentraler Nachweis der Identität von Personen verstehen und für die verschiedensten sektorspezifischen Anwendungen eingesetzt werden können. Grosse Wichtigkeit wird auch der zeitnahen Anpassung der Gesetze zugeschrieben, welche die Verwendung von elektronischen Identitäten definieren. Insbesondere sollte das Bundesgesetz über das elektronische Patientendossier EPDG entsprechend angepasst werden. Gemäss EPDG zertifizierte Identity Provider IDP sind per Inkraftsetzung des BG E-ID von Zertifizierungspflichten des EPDGs zu entbinden.

Spezifisch sehen wir folgende Punkte, die im Gesetzesentwurf präzisiert werden müssen:

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung definieren muss. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art 15 Übertragbarkeit von elektronischen Nachweisen

Entwurf Bundesrat	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. ...
Änderungsvorschlag	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. <u>1^{bis (neu)} Der Bundesrat sieht Ausnahmen für die Vormundschaft gemäss Art. 327a ff. ZGB für Minderjährige und die umfassende Beistandschaft gemäss Art. 388 ff. ZGB von Erwachsenen vor.</u> ...
Begründung	Es braucht eine Ausnahmeregelung für die Vormundschaft für Minderjährige und die umfassende Beistandschaft bei Erwachsenen mit einer entsprechenden Referenzierung der relevanten ZGB-Artikel.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat sieht vor kann vorsehen , dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss eine die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

	Ein konkretes Beispiel: die Erteilung von Facharzttiteln durch das Schweizerische Institut für ärztliche Weiter- und Fortbildung SIWF.
--	--

Art. 24^{bis} (neu) Überprüfung der Vertrauensinfrastruktur

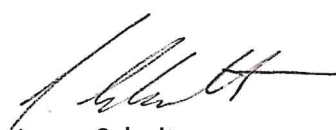
Entwurf Bundesrat	-
Änderungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bitten den Bundesrat, Experten der Zivilgesellschaft, der Wissenschaft und der Wirtschaft für die Ausarbeitung der entsprechenden Verordnung und Ausführungsbestimmung beizuziehen.

Wir sind davon überzeugt, dass mit einer speditiven Implementierung der Vertrauensinfrastruktur in der Schweiz der Digitalisierung in den verschiedenen Bereichen eine signifikante Weiterentwicklung ermöglicht wird.

Freundliche Grüsse

HEALTH INFO NET AG



Lucas Schult
Geschäftsführer (CEO)



Peer Hostettler
Leiter Vertrieb

IG eHealth, Amthausgasse 18 3011 Bern

Per Mail an: rechtsinformatik@bj.admin.ch

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements
EJPD Bundeshaus West
3003 Bern

Bern, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Die IG eHealth bedankt sich beim eidgenössischen Justiz- und Polizeidepartement EJPD und beim Bundesamt für Justiz BJ für den partizipativen Prozess bei der Erarbeitung des Entwurfs des E-ID-Gesetzes, den wir als mustergültig und nachahmenswert erachten. Wir bedanken uns auch für die rasche Ausarbeitung der Vernehmlassungsvorlage, die wir insgesamt als sehr gelungen und praxistauglich einschätzen.

Für das Gesundheitswesen ist ein elektronischer Identitätsnachweis (E-ID) eine zentrale Voraussetzung für die Nutzung von digitalen Dienstleistungen und eine vertrauenswürdige Kommunikation zwischen Gesundheitsfachpersonen und PatientInnen. Insofern wünschen wir eine zeitnahe Verabschiedung und Überweisung der Botschaft und des Gesetzesentwurfs ans Parlament.

Gemäss dem Gesetzesentwurf ist die Ausstellung und die Verwendung der neuen E-ID freiwillig. Wir begrüssen es, dass die Bevölkerung und die Gesundheitsfachpersonen die Wahl haben, wie sie auf das EPD zugreifen wollen. Die E-ID gemäss vorliegendem Gesetzesentwurf ist ein digitales Pendant zum physischen Pass oder zur Identitätskarte. Es ist kein «Login» im Sinne einer Authentifikation. Zu prüfen ist, ob dieser Punkt im Gesetz aufzunehmen ist.

Wir möchten einen Punkt zu Art. 16 Abs 1 Vorweisen von elektronischen Nachweisen anfügen. Der Artikel ist gut formuliert, wir erachten aber die Erläuterungen als unpräzise. Gemäss des Gesetzesartikels bestimmt die InhaberIn der E-ID, welche Bestandteile vom Verifikator geprüft werden. In den Erläuterungen steht unserer Meinung nach fälschlicherweise, dass dies der Verifikator bestimmt. Die Verifikatorin darf im Sinne der Datensparsamkeit nicht mehr Inhalte verlangen als absolut notwendig sind.

Nachfolgend gehen wir auf ausgewählte Elemente im Gesetzesentwurf ein, die aus unserer Sicht zu präzisieren sind:

Artikel 1

Entwurf Bundesrat	<p>2 Es hat zum Zweck:</p> <p>a. die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten;</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, 2. Datensicherheit, 3. Datensparsamkeit, und 4. dezentrale Datenspeicherung; <p>c. zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen;</p> <p>d. die Standardisierung der E-ID sowie die Sicherheit der Infrastruktur und der Ausstellung und Überprüfung der elektronischen Nachweise zu gewährleisten, ohne die technische Entwicklung unnötig einzuschränken.</p>
Änderungsvorschlag	<p>...</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, <u>2. Datenschutz durch datenschutzfreundliche Voreinstellungen</u> <u>3.</u> Datensicherheit, <u>4.</u> Datensparsamkeit, und <u>5.</u> dezentrale Datenspeicherung; <p>...</p>
Begründung	<p>Das revidierte Datenschutzgesetz verankert die Prinzipien «Privacy by Design» (Datenschutz durch Technik) sowie «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen). Im E-ID-Gesetz wird nur das Prinzip «Datenschutz durch Technik» explizit erwähnt. Aus unserer Sicht ist ebenfalls der «Datenschutz durch datenschutzfreundliche Voreinstellungen» aufzunehmen. Somit kann sichergestellt werden, dass beispielsweise die Voreinstellungen von Apps, die digitale Nachweise speichern, auf das nötige Mindestmass beschränkt werden.</p>

Art. 8 Anlaufstellen der Kantone

Entwurf Bundesrat	Die Kantone bezeichnen die Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Änderungsvorschlag	Die Kantone bezeichnen die <u>öffentlichen oder privaten</u> Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Begründung	Der Gesetzesartikel ist so zu präzisieren, dass die Kantone öffentliche und private Stellen für die Unterstützung bezeichnen können.

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung zu definieren hat. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art. 16 Abs 3 Vorweisen von elektronischen Nachweisen

Entwurf Bundesrat	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann möglichst keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen.
Änderungsvorschlag	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann <u>möglichst darf</u> keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen <u>können</u> .
Begründung	Die E-ID muss technisch so ausgestaltet sein, dass keine Rückschlüsse möglich sind. Ansonsten würde das das Prinzip «privacy by default» verletzt.

Art. 17 Basisregister

Entwurf Bundesrat	3 Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.
Änderungsvorschlag	3 Der Bundesrat regelt, welche Daten die Ausstellerinnen und Verifikatorinnen in das Basisregister einstellen dürfen.
Begründung	Gemäss dem Artikel müssen Ausstellerinnen und Verifikatorinnen ihre Daten in das Basisregister eintragen. Eine Eintragung ohne vorgängige Prüfung durch die entsprechende Stelle des Bundes öffnet dem Identitätsdiebstahl Tür und Tor. Es dürfte dem Vertrauen in das Basisregister schaden, wenn Einträge von Ausstellerinnen und Verifikatorinnen widerrufen werden müssen. Es ist eine Delegationsnorm zu schaffen, damit der Prozess der Überprüfung auf Verordnungsstufe präzisiert werden kann.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat <u>sieht vor</u> kann vorsehen , dass der Bund die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

Art. 24bis (neu) Überprüfung der Vertrauensinfrastruktur

Entwurf Bundesrat	-
Ergänzungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bedanken uns für die Prüfung und ggf. Berücksichtigung unserer Eingabe im Rahmen der Erarbeitung der Botschaft des Bundesrats und des Gesetzesentwurfs, der zu Händen des Parlaments verabschiedet wird.

Freundliche Grüsse
Im Namen des Vorstands

Anna Winter
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Vorsteherin des Eidgenössischen
Justiz- und Polizeidepartements EJPD

Per E-Mail an: rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

VERNEHMLASSUNGSANTWORT

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Inclusion Handicap vertritt als Dachverband der Behindertenorganisationen die Interessen der rund 1,8 Mio. Menschen mit Behinderungen in der Schweiz.¹ Die Abteilung Gleichstellung von Inclusion Handicap hat die Aufgabe, die **Umsetzung und Weiterentwicklung des Behindertengleichstellungsrechts** zu fördern und dadurch die **autonome Lebensführung von Menschen mit Behinderungen in allen Aspekten des täglichen Lebens** zu unterstützen.

Die Bundesverfassung (BV)² verbietet in Art. 8 Abs. 2 Diskriminierungen wegen einer körperlichen, geistigen oder psychischen Behinderung. Art. 8 Abs. 4 BV verpflichtet den Gesetzgeber, **Massnahmen zur Beseitigung der Benachteiligung von Menschen mit Behinderungen** zu ergreifen. Demnach müssen die in Erarbeitung stehenden oder einer Revision unterliegenden Gesetze sowie Verordnungen immer auch unter dem Aspekt der Gleichstellung von Menschen mit Behinderungen überprüft werden. Führen sie zu einer direkten oder indirekten Diskriminierung, sind sie mit Art. 8 Abs. 2 BV nicht vereinbar. Den Auftrag von Art. 8 Abs. 4 BV hat der Bundesgesetzgeber bis jetzt hauptsächlich durch den Erlass des Behindertengleichstellungsgesetzes

¹ [Bundesamt für Statistik BFS, Anzahl Menschen mit Behinderungen](#).

² [Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 \(BV; SR 101\)](#).



(BehiG)³ wahrgenommen, aber auch durch die Verankerung von behindertengleichstellungsrechtlicher Vorschriften in der Spezialgesetzgebung.

Zudem verpflichtet die UNO-Konvention über die Rechte von Menschen mit Behinderungen (BRK)⁴ die Schweiz seit Mai 2014 zur Berücksichtigung derer Anliegen, insbesondere auch im Gesetzgebungsverfahren (Art. 4 Abs. 1 lit. a und b BRK). Weiter hat der Staat bei der Ausarbeitung von Rechtsvorschriften, die Menschen mit Behinderungen betreffen, Behindertenorganisationen aktiv miteinzubeziehen (Art. 4 Abs. 3 BRK).

1. Behindertengleichstellungsrechtliche Grundlagen

1.1 Recht auf Autonomie von Menschen mit Behinderungen

Das Recht von Menschen mit Behinderungen, **autonom** am gesellschaftlichen Leben teilzuhaben, steht im Zentrum des Behindertengleichstellungsrechts sowohl auf der Ebene des Völkerrechts als auch auf der Ebene des Verfassungs- und Gesetzesrechts. Die BRK garantiert u.a. das **Recht auf ein unabhängiges und selbstbestimmtes Leben**⁵ und verankert die Achtung der individuellen Autonomie, einschliesslich der Freiheit, eigene Entscheidungen zu treffen, sowie der Unabhängigkeit als allgemeinen Grundsatz (Art. 3 lit. a BRK). Die Gewährleistung der **Möglichkeit einer autonomen Lebensführung** von Menschen mit Behinderungen stellt auch einen zentralen Teilgehalt des Diskriminierungsverbotes von Art. 8 Abs. 2 BV dar.⁶

Zum Recht auf Autonomie gehört insbesondere auch das **Recht auf autonomen Zugang zu Information und Kommunikation, einschliesslich Informations- und Kommunikationstechnologien und -systeme**, und damit u.a. das Recht, Informations- und Kommunikationstechnologien und -systeme grundsätzlich **ohne fremde Hilfe** zu benutzen. Wenn Informations- und Kommunikationstechnologien und -systeme für Menschen mit Behinderungen nur mit Hilfe Dritter zugänglich sind, ist ihr unabhängiges und selbstbestimmtes Handeln in einem Bereich, der für eine autonome Lebensführung von zentraler Bedeutung ist, nicht gewährleistet. Dadurch werden Menschen mit Behinderungen gegenüber Menschen ohne Behinderungen benachteiligt.

1.2 Pflicht zur Gewährleistung der Zugänglichkeit (Barrierefreiheit)

Art. 9 Abs. 1 BRK verpflichtet die Schweiz, geeignete Massnahmen zu treffen, um Menschen mit Behinderungen den **gleichberechtigten Zugang zu Information und**

³ [Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen vom 13. Dezember 2013 \(Behindertengleichstellungsgesetz, BehiG; SR 151.3\).](#)

⁴ [Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13. Dezember 2006, in Kraft getreten für die Schweiz am 15. Mai 2014 \(BRK; SR 0.109\).](#)

⁵ [Botschaft zur Genehmigung des Übereinkommens vom 13. Dezember 2006 über die Rechte von Menschen mit Behinderungen vom 19. Dezember 2012, BBl 2013 661, S. 665.](#)

⁶ MARKUS SCHEFER/CAROLINE HESS-KLEIN, Behindertengleichstellungsrecht, Bern 2014, S. 181.



Kommunikation, einschliesslich Informations- und Kommunikationstechnologien und -systeme, zu gewährleisten. Dieser Zugang soll Menschen mit Behinderungen deren **unabhängige Lebensführung** und die **volle Teilhabe in allen Lebensbereichen** ermöglichen. Zugänglichkeit i.S.v. Art. 9 BRK, insbesondere auch zu Information und Kommunikation, ist wesentliche Voraussetzung dafür, dass Menschen mit Behinderungen unabhängig leben, voll und gleichberechtigt an der Gesellschaft teilhaben und in den **uneingeschränkten Genuss aller ihrer Menschen- und Grundrechte** kommen, und zwar gleichberechtigt mit anderen.⁷ Sie ist für die Inklusion von zentraler Bedeutung.

Dabei ist zu unterscheiden zwischen der Zugänglichkeit, die sich auf Gruppen bezieht, und angemessenen Vorkehrungen, die sich auf Einzelpersonen beziehen. Die **Pflicht zur Gewährleistung der Zugänglichkeit (Barrierefreiheit)** ist **bedingungslos** und eine **Pflicht ex ante**: Die Zugänglichkeit (Barrierefreiheit) ist bereits vor und unabhängig von individuellen Rechten und Anträgen zu gewährleisten, z.B. durch universelles Design (*design for all*). Für Menschen mit Behinderungen, für die trotz dieser Zugänglichkeit der Zugang nicht gewährleistet ist, müssen zusätzlich angemessene Vorkehrungen i.S.v. Art. 2 BRK getroffen werden, es sei denn, dies wäre unverhältnismässig. Dabei handelt es sich um eine Pflicht *ex nunc*.⁸ Die Verweigerung des Zugangs, insbesondere auch zu Information und Kommunikation und den entsprechenden Technologien und Systemen, stellt eine Diskriminierung aufgrund von Behinderung i.S.v. Art. 5 BRK dar.⁹

Nach Art. 9 BRK¹⁰ müssen auch bei der Entwicklung von Informations- und Kommunikationstechnologien und -systemen, einschliesslich des Internets und digitalen Dienstleistungen, die Bedürfnisse von Menschen mit Behinderungen berücksichtigt werden. Die Schweiz ist somit verpflichtet, zur Sicherstellung des **Zugangs von Menschen mit Behinderungen zu digitalen Dienstleistungen** die **nötigen Massnahmen** zu ergreifen. Dabei hat sie nach Art. 9 Abs. 2 lit. b BRK insbesondere auch sicherzustellen, dass private Rechtsträger, die öffentlich-zugängliche Dienste anbieten, alle Aspekte der Zugänglichkeit für Menschen mit Behinderungen berücksichtigen. Art. 14 Abs. 1 BehiG hält zudem fest, dass Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Menschen mit Sprach-, Hör- oder Sehbehinderungen nehmen müssen. Soweit Behörden ihre Dienstleistungen online anbieten, müssen diese gemäss Art. 14 Abs. 2 BehiG für Menschen mit Sehbehinderungen ohne erschwerende Bedingungen zugänglich sein. Die Schweiz ist somit rechtlich verpflichtet,

⁷ [United Nations, Committee on the Rights of Persons with Disabilities CRPD, General comment No. 2 \(2014\), 22 May 2014, CRPD/C/GC/2](#), p. 4, para. 14.

⁸ [United Nations, Committee on the Rights of Persons with Disabilities CRPD, General comment No. 2 \(2014\), 22 May 2014, CRPD/C/GC/2](#), p. 7 f., para. 25 f.

⁹ [United Nations, Committee on the Rights of Persons with Disabilities CRPD, General comment No. 2 \(2014\), 22 May 2014, CRPD/C/GC/2](#), p. 10, para. 34.

¹⁰ Vgl. insbesondere Art. 9 Abs. 1 lit. b und Abs. 2 lit. a, b, f und g BRK.



die **barrierefreie Nutzung sowohl staatlicher elektronischer Dienste als auch privater elektronischer Dienste** sicherzustellen (**E-Accessibility**).

2. Anwendung auf das E-ID-Gesetz

2.1 Ausdrückliche Verankerung der Zugänglichkeit (Barrierefreiheit)

Vor diesem Hintergrund ist für Inclusion Handicap **nicht nachvollziehbar**, dass die **Zugänglichkeit (Barrierefreiheit)** des elektronischen Identitätsnachweises und der anderen elektronischen Nachweise sowie der damit einhergehenden Infrastruktur für Menschen mit Behinderungen **in der Vorlage nicht enthalten** ist. Weder im Vorentwurf für das E-ID-Gesetz noch im Erläuternden Bericht wird auf das entsprechende Recht von Menschen mit Behinderungen und die entsprechende rechtliche Pflicht der Behörden eingegangen.

Relevant im Zusammenhang mit dem Vorentwurf des E-ID-Gesetzes ist insbesondere Art. 9 BRK¹¹ als allgemeine Klausel zur Gewährleistung der Zugänglichkeit. Um Benachteiligungen von Menschen mit Behinderungen zu verhindern, welche die Dienstleistungen gemäss dem Vorentwurf zum E-ID-Gesetz – die Ausstellung und die Nutzung einer E-ID und weiterer elektronischer Nachweise sowie die Installation und Nutzung einer Briefftasche – in Anspruch nehmen, **müssen diese Dienstleistungen** demzufolge **nach dem design for all ausgestaltet** sein (Art. 2 Abs. 5 BRK). Im vorliegenden Zusammenhang von Bedeutung ist auch Art. 5 Abs. 2 BRK, der ein Verbot der Diskriminierung wegen einer Behinderung beinhaltet. Schliesslich hat sich die Schweiz als Folge von Art. 4 Abs. 1 lit. e BRK ausdrücklich dazu verpflichtet, alle geeigneten Massnahmen zur Beseitigung der Diskriminierung aufgrund von Behinderung zu ergreifen.

Eine Umsetzung der Verpflichtungen aus der BRK hat im vorliegenden Vorentwurf zum E-ID-Gesetz offensichtlich erneut nicht stattgefunden; dies war bereits beim am 7. März 2021 abgelehnten Vorentwurf zum E-ID-Gesetz der Fall. Um sicherzustellen, dass Menschen mit Behinderungen aus den Möglichkeiten gesellschaftlicher Teilhabe, die durch die Nutzung einer E-ID und weiterer elektronischer Nachweise eröffnet werden, nicht ausgeschlossen werden, fordert Inclusion Handicap, die **Anforderungen an die hindernisfreie Ausgestaltung ausdrücklich im Rahmen verschiedener Bestimmungen des E-ID-Gesetzes sowie der Ausführungsbestimmungen zu verankern**. Ohne Gewährleistung der E-Accessibility sind Menschen mit Behinderungen, insbesondere Menschen mit Sehbehinderungen, vom staatlichen Angebot einer E-ID,

¹¹ Zur Tragweite von Art. 9 BRK siehe aus der Lehre PETER TRENK-HINTERBERGER, Zugänglichkeit, Art. 9, in: Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter (Hrsg.), Die UNO-Behindertenrechtskonvention in der Praxis, Köln 2013, S. 130 ff. sowie ANTJE WELTI, Zugänglichkeit, Art. 9, in: Welke Antje (Hrsg.), UN-Behindertenrechtskonvention mit rechtlichen Erläuterungen, Ettenheim 2012, S. 127 ff.



weiteren staatlichen Angeboten elektronischer Nachweise und privaten elektronischen Nachweisen sowie einer elektronischen Briefftasche ausgeschlossen.

Diese Benachteiligung gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen **detailliert geregelt** wird, wie die **digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt** wird. In der Entwicklung sind u.a. sämtliche Umsetzungsschritte im Hinblick auf die jeweils aktuelle Version des Standards eCH-0059 (aktuell: Version 3.0) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG (aktuell: Version 2.1) des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, die von der E-Accessibility-Richtlinie der EU inspiriert sind. Zu denken ist ferner z.B. auch an **Leichte Sprache**. Wir ersuchen Sie zudem, zwecks Überprüfung der Vereinbarkeit des Gesetzesentwurfs mit BRK, BV und BehiG sowie der Formulierung von konkreten Gesetzesbestimmungen mit dem **Eidgenössischen Büro für die Gleichstellung von Menschen mit Behinderungen (EBGB)** und den **Behindertenorganisationen** Kontakt aufzunehmen und diese **beizuziehen**.

2.2 Laufende Prüfung der Zugänglichkeit (Barrierefreiheit)

Weiter muss **vor jeder Publikation** eines webbasierten Produkts und auch **vor jedem Update geprüft** werden, **ob diese barrierefrei zugänglich sind**. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das Prinzip des *design for all* zur Anwendung kommen, analog zum europäischen Recht. Dabei ist neben **E-Accessibility** u.a. auch an **Leichte Sprache** zu denken.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die **Zugänglichkeit (Barrierefreiheit) durch entsprechende Tests sicherzustellen**. Wir verweisen diesbezüglich auch auf die Antwort des Bundesrates auf die Frage 22.7406 von Nationalrätin Franziska Ryser, in der er ausführt, dass der **standardmässige Einsatz von Usability-Tests** im Rahmen der Weiterentwicklung der Instrumente zur Gewährleistung der Barrierefreiheit geprüft wird.¹² Die Freigabe bzw. Lancierung der E-ID und weiterer elektronischer Nachweise darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet, wie aktuelle Beispiele beim Bund (z.B. beim elektronischen Patientendossier, beim elektronischen Einreiseformular oder beim Covid-Zertifikat) oder in den Kantonen (kantonale eID+ Schaffhausen) zeigen.

¹² [Bundesrat, Antwort vom 7. Juni 2022 auf die Frage 22.7406 «Digitale Exklusion – Einsatz von Usability-Tests» von Nationalrätin Franziska Ryser vom 1. Juni 2022.](#)



3. Anträge von Inclusion Handicap

Aus diesen Gründen stellen wir folgende Anträge:

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein eigener **Artikel «Barrierefreiheit»** aufzunehmen. Darin ist der **Grundsatz der barrierefreien Nutzbarkeit** festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen, die von Antragstellenden, Inhaber:innen, Aussteller:innen, Verifikator:innen und weiteren Usergruppen genutzt oder betrieben werden können.
2. In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein eigenes **Kapitel zur Barrierefreiheit** aufzunehmen. In diesem Kapitel sei detailliert zu beschreiben, wie die **Zugänglichkeit (Barrierefreiheit)** des elektronischen Identitätsausweises und anderer elektronischer Nachweise für Menschen mit Behinderungen **sichergestellt** wird.
3. Zur **Kontrolle der Zugänglichkeit (Barrierefreiheit)** sei ein **Auftrag an eine anerkannte Fachinstitution** zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Bis heute sind die Grundlagen des Behindertengleichstellungsrechts im Dienstleistungsbereich und insbesondere im Bereich der E-Accessibility in der Praxis wenig bekannt. Sogar in der Bundesverwaltung sind sich viele Behörden ihrer Verpflichtungen immer noch zu wenig bewusst. Eine **klare Verankerung und Konkretisierung** der behindertengleichstellungsrechtlichen Anforderungen **in der jeweils relevanten Spezialgesetzgebung** kann dies ändern und zur konsequenten Umsetzung der Rechte von Menschen mit Behinderungen beitragen.

Wir danken Ihnen im Voraus für die Berücksichtigung unserer Stellungnahme. Gerne stehen wir Ihnen für Rückfragen zur Verfügung.

Freundliche Grüsse

Inclusion Handicap

Dr. iur. Caroline Hess-Klein
Leiterin Abt. Gleichstellung

lic. iur. Nuria Frei, Rechtsanwältin
Fachmitarbeiterin Abt. Gleichstellung



STELLUNGNAHME insieme SCHWEIZ

insieme – gemeinsam mit und für Menschen mit geistiger Behinderung

insieme Schweiz ist die Dachorganisation der Elternvereine für Menschen mit einer geistigen Behinderung. Sie unterstützt rund 50 regionale und kantonale Unterorganisationen in der ganzen Schweiz. Sie engagiert sich für und zusammen mit Menschen mit einer geistigen Behinderung für eine inklusive Gesellschaft, in der die Menschenrechte respektiert werden. Die Prinzipien, die im Übereinkommen über die Rechte von Menschen mit Behinderung (UN-BRK) formuliert wurden, leiten Vision und Engagement von **insieme**.

insieme Schweiz nimmt Stellung zur Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

insieme Schweiz begrüsst die Einführung eines staatlichen elektronischen Identitätsnachweises grundsätzlich. In dieser Stellungnahme beschränkt sich **insieme** Schweiz auf den Aspekt der Barrierefreiheit, der beim vorliegenden Gesetzesvorhaben von grosser Bedeutung ist.

E-Accessibility fehlt

insieme Schweiz ist überrascht, dass der Aspekt der E-Accessibility in der Vorlage keine Erwägung findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt wird. Dabei sind sowohl die Bedürfnisse von Menschen mit Sprach-, Hör- und Sehbehinderungen, wobei **insieme** Schweiz auf die Stellungnahme des Schweizerischen Blinden- und Sehbehindertenverbands SBV-FSA verweist, wie auch der Menschen mit kognitiver Beeinträchtigung zu beachten.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK, Übereinkommen über die Rechte von Menschen mit Behinderungen) unterzeichnet. Artikel 9 der UN-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies schliesst auch die Information und Kommunikation, einschliesslich der entsprechenden Technologien und Systeme ein. Die Schweiz ist also vertraglich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Zugang für Menschen mit kognitiver Beeinträchtigung

Für einen Grossteil der Menschen mit einer kognitiven Beeinträchtigung stellt die Digitalisierung eine Chance für einen breiteren Zugang zu Dienstleistungen aller Art dar. Sie sind dabei aber darauf angewiesen, dass die digitalen Kommunikationskanäle in Leichter Sprache zur Verfügung stehen und die Web-basierten Produkte einfach verständlich und zugänglich sind. Es muss vor jeder Publikation von Web-basierten Produkten geprüft werden, ob der Zugang für Menschen mit kognitiver Beeinträchtigung barrierefrei möglich ist, und zwar durch Menschen mit kognitiver Beeinträchtigung.

Weiter wird es aber auch immer Menschen mit kognitiver Beeinträchtigung geben, welche solche Web-basierten Produkte nicht ohne Unterstützung nutzen können und es auch nicht erlernen können. Es ist ein zentrales Anliegen von **insieme** Schweiz, dass es auch für Menschen mit starker Beeinträchtigung Wahlmöglichkeiten gibt und sie nicht im Vorhinein vom Ausstellen und Nutzen einer E-ID ausgeschlossen werden.

insieme Schweiz fordert daher:

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei Art. 1 Abs.2 um einen Buchstaben e. zu ergänzen: «zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur für Menschen mit Beeinträchtigung barrierefrei zugänglich sind;»
2. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein eigener Artikel «Barrierefreiheit» aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen die von Antragstellenden, Inhaber:innen einer E-ID, Aussteller:innen, Verifikator:innen und weiteren Usergruppen genutzt oder betrieben werden können. Der Zugang für Menschen mit einer schweren Beeinträchtigung soll auch in diesem Artikel sichergestellt werden.
3. In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein eigenes Kapitel zur Barrierefreiheit aufzunehmen. Dieses beschreibt detailliert, wie der Zugang des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
4. Zur Kontrolle der Barrierefreiheit sei ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Freundliche Grüsse,

Jan Habegger
Stv. Geschäftsführer



Bern, 13. Oktober 2022

Bundesamt für Justiz
Direktionsbereich Zentrale Dienste
Fachbereich Rechtsinformatik
3003 Bern

Bern, den 20.10.2022

Vernehmlassung ISSS zum neuen E-ID Gesetz BGEID

Sehr geehrte Damen und Herren

Gerne nehmen wir Stellung zum zweiten Vorschlag der Bundesverwaltung (Bundesamt für Justiz) über das E-ID Gesetz (BGEID).

Vorstellung Taskforce E-ID ISSS

Die Information Security Society Switzerland (ISSS) <http://www.issss.ch> ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1'100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander.

ISSS wurde 1993 als Verein gegründet und ist Mitglied von Digitalswitzerland sowie offizieller Security Fachpartner von SwissICT und ASUT. Mit unseren Mitgliedern arbeiten wir in Taskforces, um Fachexpertise gezielt abzuholen und der Öffentlichkeit zur Verfügung zu stellen. Auch vorliegende Stellungnahme wurde in einer Taskforce erarbeitet:

Taskforce Lead ISSS

Walder, Dario
Beranek Zanon, Nicole

- Team Leader Redguard, Vizepräsident ISSS
- Juristin HÄRTING Rechtsanwälte AG, ISSS-Vorstand

Juristen

Lehmann, Beat
Talleri, Rocco
Zbinden, Reto

- Jurist, ISSS-Vorstand
- Jurist Spezialgebiet Cyber Security, Talleri Law Studio legale
- Jurist, Swiss Infosec

Organisationen & Fachexperten

Laube, Annett
Monika Stucki
Rickenbacher, Fridel

- Dozentin, Berner Fachhochschule
- Senior Consultant, Redguard AG
- Senior Consultant / Investor, Swiss IT Security AG

Nachdem das Volk den ersten Gesetzesentwurf zur E-ID am 07.03.2021 deutlich abgelehnt hat, sind wir grundsätzlich erfreut zu hören, dass sich mit dem neuen Entwurf zum Bundesgesetz zur E-ID einiges zum Positiven hinbewegt hat. So nehmen wir beispielsweise mit Freude zur Kenntnis, dass die Infrastruktur neu durch das Bundesamt für Justiz (staatliche Vertrauensinfrastruktur) sichergestellt wird. Ausserdem bekennt sich der Bundesrat mit dem neuen BGEID zu drei wichtigen Grundsätzen zum Schutz der Persönlichkeit und der Grundrechte von Personen (Schutzes der Privatsphäre durch Technik «privacy by design», der Datensparsamkeit und der dezentralen Datenspeicherung). Auch freuen wir uns,

dass bei der Erstellung des neuen Gesetzesentwurfs ein partizipativer Ansatz verfolgt wird, durch den die Mitarbeit durch regelmässige Informationssitzungen¹ und auch ein entsprechendes Gitlab-Projekt² sichergestellt werden.

Trotzdem möchten wir auf weitere wichtige Security- und Privacy-Aspekte hinweisen, die aus unserer Sicht bei der Umsetzung der E-ID mitberücksichtigt werden sollen.³ Dabei möchten wir an dieser Stelle insbesondere auf die Arbeiten im Rahmen der EU verweisen.⁴ Aus unserer Sicht ist anzustreben, dass das BGEID heute oder in Zukunft dem harmonisierten Recht der digitalen Identität im EWR so weit als möglich entspricht: Es sollte die auch im Kommissionsvorschlag erwähnte "Äquivalenz" mit dem harmonisierten europäischen Recht der Digitalen Identität angestrebt werden - wie das im bisherigen und neuen Datenschutzrecht, oder der Übernahme der Regelung der EU über Produkthaftung erreicht wurde.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anregungen.

Stellungnahme zum neuen BGEID

- Art. 1 Abs. 2c beschreibt den Zweck des BGEID, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen. Wir verstehen darunter auch, dass die Vertrauensinfrastruktur regelmässigen Sicherheitsprüfungen (Audit und/oder Pentest, inkl. allenfalls auch Second und Third Opinion) unterzogen werden muss zugunsten einer maximierten Angriffs- und Betriebs-Sicherheit in der immer dynamischer werdenden Bedrohungslage. Dies sollte bereits hier im Gesetz stehen (z.B. security & privacy by design, zero trust principle, need to know) und nicht erst nachträglich und zu einem späteren Zeitpunkt adressiert werden.
- Auch sehen wir es als notwendig, dass neben regelmässigen Sicherheitsprüfung die Vertrauensinfrastruktur Sicherheitszertifiziert wird (z.B. ISO 27001, NIST, COBIT, ITIL, ISACA). Mit auch entsprechendem Business Continuity Planning, Incident Response Planning zur Optimierung der Resilienz.
- Im Rahmen von nationalen Kampagnen und auch den Tätigkeiten im Zentrum NCSC wäre die weitere bzw. weitergehende Cybersecurity Sensibilisierung der Bevölkerung bzw. der Anwender der E-ID eine flankierend sinnvolle Massnahme im Umgang mit der digitalen Identität.
- Alle an der E-ID involvierten Akteure sollen entsprechend der Verordnung über die Datenschutzzertifizierungen (VDSZ⁵) zertifiziert sein. Als Beispiel dient hier Art. 59a 832.102, Verordnung über die Krankenversicherung (KVV): "Jeder Versicherer muss über eine Datenannahmestelle verfügen. Diese muss nach Artikel 11 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz zertifiziert sein."
- Art. 18 Abs. 2,3 stellt die Rolle des Bundes und Bundesrates betreffend Zurverfügungstellung von Systemen, Bestätigungen und Abfragen im System dar. Wir beurteilen es als notwendig, dass hier keine "kann-Formulierungen" sondern eine "muss-Formulierung" verwendet wird:
 - o ² Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.

¹ Swiss E-ID Ecosystem - <https://github.com/e-id-admin> (Stand 03.09.2022)

² Website des Bundesamts für Justiz – Partizipationsmöglichkeiten rund um die E-ID - <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/partizipationsmoeglichkeiten.html> (Stand 03.09.2022)

³ <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-85476.html>

⁴ E-IDAs Verordnung (EU) Nr. 910/2014) <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX%3A32014R0910&from=BG> sowie COM(2021)281 final vom 3.6.2021 <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0281&from=DE>

⁵ der Verordnung über die Datenschutzzertifizierungen (VDSZ) <https://www.fedlex.admin.ch/eli/cc/2007/701/de> (Stand 23.09.2022)

- ³ Alle Behörden und Privaten ~~können~~ müssen die Zuordnungen durch Abfragen im System überprüfen.
-
- Gleiches gilt auch für Art., 20
 - Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund eine Anwendung zur Verfügung stellt, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können.
-
- Gleiches gilt auch für Art. 21 Abs. 1
 - Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund ein System zur Verfügung stellt, dem die Inhaberinnen und Inhaber Sicherheitskopien ihrer elektronischen Nachweise zur Aufbewahrung übergeben können.
- Art. 25. Abs. 2 E-ID-Gesetz verursacht einerseits eine Normenkollision mit der Datenschutzgesetzgebung (im Rahmen von Bst. c), indem bis zum „Inkrafttreten der gesetzlichen Grundlage“ eine rein materiellrechtliche Grundlage auch bei Bearbeitung besonders schützenswerter Personendaten ohne Weiteres genügen soll (ohne dass somit bis dann die für eine materielle Rechtsgrundlage geltenden Einschränkungen gelten, nämlich dass die Bearbeitung für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich zu sein hat oder der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken zu bergen hat (Art. 34 Abs. 3 nDSG)). Ein Widerspruch mit der Datenschutzgesetzgebung und eine Aufweichung der Grundrechte der betroffenen Personen ist zu vermeiden und verträgt sich ausserdem schlecht mit dem programmatischen Bekenntnis im E-ID-Gesetz selbst zur Datensparsamkeit (Art. 1 Abs. 2 E-ID-Gesetz).
- Weiter ist Art. 25. Abs. 2 E-ID-Gesetz potenziell verfassungswidrig: Nach Art. 36 Abs. 1 BV müssen schwerwiegende Einschränkungen von Grundrechten im (formellen) Gesetz selbst vorgesehen sein. Ausgenommen sind nur Fälle ernster, unmittelbarer und nicht anders abwendbarer Gefahr.
- Art. 25. Abs. 2 E-ID-Gesetz schafft ausserdem mehrfach unnötige Rechtsunsicherheit: Die Bestimmung enthält lediglich eine Aussage dazu, wann zusätzliche Vorgaben des Bundesrates zur Anpassung der Vertrauensinfrastruktur ausser Kraft treten sollen, nämlich dann, wenn eine rechtstaatlich solidere Rechtsgrundlage erreicht ist. Ihrem Wortlaut nach kann der Bestimmung aber nicht entnommen werden, dass entsprechende Vorgaben des Bundesrates Vorrang haben sollen gegenüber Art. 34 nDSG. Art. 25 Abs. 2 Bst. c E-ID-Gesetz lässt mit der Erwähnung der „gesetzlichen Grundlage“ ausserdem offen, ob damit wirklich eine formellrechtliche (von der Legislative verabschiedete Vorgaben) verlangt wird oder eine materiellrechtliche Grundlage letztlich genügend könnte, was wiederum aus grundrechtlicher Perspektive äusserst bedenklich wäre und noch dazu im diametralen Widerspruch zur Datenschutzgebung.
- Schliesslich halten wir die Regelung in Art. 25. Abs. 2 E-ID-Gesetz für verzichtbar, weil die Datenschutzgesetzgebung auf Bundesebene bereits Bestimmungen enthält zur automatisierten Datenbearbeitung mit besonders schützenswerten Personendaten im Rahmen von Pilotversuchen (Art. 35 nDSG)
- Aus all diesen Gründen regen wir die ersatzlose Streichung von Art. 25. Abs. 2 E-ID-Gesetz an. Dies nicht zuletzt auch deshalb, um damit nicht die gesamte Vorlage einem erhöhten Risiko auszusetzen, im Rahmen der parlamentarischen Beratungen Schiffbruch zu erleiden.

Datenschutz:

- Der Vorschlag, die AHV-Nummer als integrierten Bestandteil der Digitalen Identität aufzunehmen,

kann einen Verstoß gegen elementare Grundsätze des Datenschutzes darstellen. Denn damit droht durch die Spur, die jeder Einsatz der E-ID durch den Benutzer notwendigerweise hinterlässt, die Gefahr einer Kontrolle seines Verhaltens und bewirkt ein verpöntes Profiling im Sinne von Art. 5 Bst. f) und g) revDSG 2020.

- Die Verknüpfung der E-ID mit einem universellen Mitteln zur Identifikation von Personen ist im harmonisierten europäischen Recht verboten, denn es schafft die Grundlage für die umfassende Kontrolle des Verhaltens von Personen, wie dies heute in technologisch weit entwickelten autoritären Staaten (z.B. China) realisiert ist.
- Im Weiteren stellt die Beschränkung des BGEID auf bestimmte Kategorien amtlich registrierter natürlicher Personen, möglicherweise eine Verletzung von Art. 6 der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen dar und weicht ebenfalls vom harmonisierten europäischen Recht ab.

Inputs zum erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens

- Art 14 - Hier wird erwähnt, dass man die E-ID nur auf einem einzigen Gerät installieren kann. Das wäre eine Einschränkung der Verwendung (was genau wären die Probleme damit?).
- Art. 15 Abs. 1 Hier soll geregelt werden, wie im Delegationsfall (z.B. bei Ausnahmefällen / Notfällen – siehe z.B. auch beim ePD-Notfall-Zugang) vorgegangen werden soll. Genau da muss man ja, die E-ID einer Drittperson überlassen.
- Art. 15 Abs. 2 Ein grundsätzliches Problem ist die Wiederherstellung von privaten Schlüsseln (Key Recovery), die es ja nur einmal geben darf und damit Sicherheitskopien und das Wiederherstellung eigentlich verunmöglichen. (siehe auch Art 21)
- Art. 17 und 18 es ist nicht klar, warum Aussteller und Verifikationen ihre Identifikatoren erst selbst in Basisregister eintragen können und dann ein System zur Bestätigung der Identifikatoren gebaut wird. Hier wird auch im Gegensatz zum Rest der Dokumente auf sehr tiefem technischen Niveau argumentiert
- Art. 17 Abs. 4: «Das Basisregister enthält keine Daten über die einzelnen elektronischen Nachweise mit Ausnahme über deren Widerruf.» Das könnte Auswirkungen auf die Privacy des Holders haben, in den Fällen, wenn allein der Besitz oder die Revokation eines Nachweises eine sensible Information darstellt, z.B. Mitgliedschaft in einer religiösen Gemeinschaft. Hier muss man sehr sorgfältig schauen, wie ein einzelner Nachweis referenziert wird.

Mit freundlichen Grüßen



ARIÉ MALZ
CO-PRÄSIDENT



DARIO WALDER
VIZE-PRÄSIDENT

Information Security Society Switzerland (ISSS)

Zentweg 13, 3006 Bern

E-Mail: president@isss.ch

E-Mail: vicepresident@isss.ch

BUNDESGESETZ ÜBER DEN ELEKTRONISCHEN IDENTITÄTSNACHWEIS UND ANDERE ELEKTRONI- SCHE NACHWEISE (EID-GESETZ, BGEID)

VERNEHMLASSUNGSANTWORT

Verfasser

Dr. Bruno Wildhaber

Version

1.0

Datum

2022—10—09

Zum krm:

DAS KRM (Kompetenzzentrum Records Management AG) IST EIN UNABHÄNGIGES BERATUNGSHAUS auf den Gebieten des Datenmanagements und der Informationssicherheit

Das krm kombiniert interdisziplinäre Kompetenz und langjährige Erfahrung im Daten- und Informationsmanagement zum Nutzen des Kunden. Der Fokus liegt auf der Beherrschung der Datenflut und den Anforderungen der Cybersecurity. Das Unternehmen bietet nebst Beratung und Schulungen verschiedene Lösungen und ist Kompetenzpartner einiger führender Lösungsanbieter. Dabei setzt das krm auf eigene Methoden bei der Umsetzung von Projekten in allen Industriezweigen und der Verwaltung.

Das krm verfügt über jahrzehntelange Erfahrung in der Konzeption und Gestaltung von rechtskonformen Identitätssystemen und -verfahren. Experten des krm waren u. a. bei der Erstellung der Signaturgesetze in D und CH tätig. Das krm und seine Partner haben mehrere Fachbücher zu diesen Themen verfasst und wir dozieren regelmässig an nationalen und internationalen Hochschulen.

Kompetenzzentrum Records Management AG Hegnastr. 60 6802 Wangen
Tel. +41 44 888 10 11 Info@krm.swiss www@krm.swiss

ZUSAMMENFASSUNG EXECUTIVE SUMMARY

Die Ausgabe eines einfachen digitalen Ausweises (eID) ist so rasch als möglich umzusetzen.

Bevor über Ökosysteme nachgedacht werden soll, muss mit höchster Dringlichkeit diese EINE eID SOFORT umgesetzt werden (nutzbar für Bund und Kantone). Wir finden es unnötig, dass der vorliegende Vorentwurf bzw. die vorgesehene Infrastruktur unterschiedliche elektronische Nachweise vorsieht und ein umfangreiches Ökosystem gemäss Ambitionsniveau 3 beschreibt. Letzteres führt zu einer Verzettlung der Kräfte und wird die Einführung der dringend benötigten eID unnötig verzögern. Eine Beschränkung auf das Wesentliche bildet den Schlüssel zum Erfolg.

Ohne massive Vereinfachung droht der eID das Schicksal des ePD (el. Patientendossier).

Die Erfüllung von Sicherheitsanforderungen und Datenschutzanliegen sind zwar wichtig, stehen aber klar hinter der Einfachheit und offenen Anwendbarkeit der eID.

Die Drittnutzung der Infrastruktur erzeugt unbekannte Risiken.

Die Nutzung der Infrastruktur für andere elektronische Nachweise ausserhalb der eID ist zu überdenken. Die damit verbundenen Risiken sind nicht zu unterschätzen und können für den Bund nicht abschätzbare Folgen haben. Das schliesst nicht aus, dass unterliegende ID-Aussteller die eID nutzen können (im Vordergrund stehen z.B. die Kantone), sie sind dann aber lediglich Konsumenten und haben keinen Einfluss auf die Sicherheit des Gesamtsystems. Ob im Einzelfall andere Anwender die eID nutzen können, müsste im Einzelfall rigorosen Risikobeurteilungen unterliegen (ins Gesetz aufzunehmen).

Der Grundsatz der Technologieneutralität wurde gut berücksichtigt.

Die Technologieneutralität ist im Entwurf gut umgesetzt und sollte nicht verwässert werden. Insbesondere ist auf eine detaillierte Beschreibung der technischen Verfahren und Systeme bei den Endbenutzern zu verzichten.

Nutzen, was bereits existiert: Für die eID-Infrastruktur existiert bereits ein Gesetz!

Völlig übersehen wurde offenbar, dass für die Umsetzung der Infrastruktur in Kapitel 5 bereits Gesetze existieren, nämlich die ZertES und die VZertEs. Wir empfehlen dringend, diese Gesetze zu harmonisieren. Die ZertEs enthält 80–90 % der im eID-Entwurf beschriebenen Verfahren: Kapitel 5 aus dem Gesetz streichen und ein separates Infrastrukturgesetz erlassen bzw. besser

die ZertES anpassen. Das eID-Gesetz sollte sich auf die Verfahren zur Umsetzung der «Root»-Identität (=eID) beschränken.

Keine Anwendungsfälle ins Gesetz

Wir begrüßen, dass darauf verzichtet wurde, konkrete Anwendungsfälle ins Gesetz aufzunehmen. Diese gehören nicht ins BGEID.

ERLÄUTERUNGEN UND KOMMENTARE

Welches sind die drei wichtigsten Anforderungen an eine staatliche eID als digitaler Ausweis?

Absolut vordringlich und vor allen anderen Überlegungen muss der Entscheid zur sofortigen Umsetzung einer elektronischen Identität fallen. Die Schweiz hat den Zug für die Umsetzung der elektronischen Identität schon lange verpasst. Bereits 1996 fanden unsererseits Besprechungen mit dem EJPD statt, um abzuklären, wann man mit der Einführung einer elektronischen Identität rechnen dürfe. In der aktuellen Situation kann es nur noch um Schadensbegrenzung gehen. Das zu schaffende Gesetz muss möglichst schlank und ohne unnötige Detailregelungen entworfen und im Eilverfahren umgesetzt werden.

Die digitale Identität muss durch den Staat herausgegeben und finanziert werden. Sie ist der «Trust Anchor» und das hochwertigste Identifikationsmittel des Bürgers. Kein System kann eine vergleichbare Vertrauensbasis schaffen (das gilt im Speziellen auch nicht für DLT-basierte Systeme). Aber: Es gibt keine kommerziellen Business Cases, die für die Finanzierung herangezogen werden können. Es handelt sich hierbei um eine Basis-Infrastruktur. Niemand hat sich bei der Einführung des physischen Passes oder der Identitätskarte gefragt, wie häufig man diese werde nutzen können. Noch weniger, ob derjenige, der sich darauf verlässt, daraus einen Business Case ableiten kann. Diese illusionäre Annahme hat unter anderem dazu geführt, dass die Abstimmung zum eID-Gesetz verlorengegangen ist.

Die Umsetzung der digitalen Identität muss möglichst einfach und auf etablierten Technologien erfolgen. Dazu am besten geeignet und praxisbewährt sind Public-Key-Infrastrukturen, welche ohne grossen Aufwand implementiert werden können. Alle anderen Lösungsansätze sind entweder noch nicht reif oder basieren im Kern auch auf PKI- und DLT-Technologie.

Welche Anwendungsfälle der eID stehen im Vordergrund?

Im beleuchtenden Bericht wurde wiederholt von Privacy und Sicherheit gesprochen. Mit kaum einem Wort werden jedoch die wirklich wichtigen Anforderungen angesprochen: Interoperabilität (ausdrücklich gemäss nationaler Datenbewirtschaftung, NaDB) und Einfachheit. Diesen Aspekten wurde zu wenig Augenmerk verliehen.

Wir sind seit 30 Jahren im Geschäftsfeld digitaler Identitäten, Trust Center und digitaler Signaturen tätig. Wir haben viele gute Lösungen kommen und vor allem gehen sehen. Diese sind schlicht daran gescheitert, dass die Benutzerakzeptanz fehlte. Erfolgsfaktoren bei der Umsetzung sind (in dieser Reihenfolge):

1. Zuerst kommt die «Usability», d. h. die möglichst einfache und simple Anwendbarkeit, dann die
2. Kosten: Vergleichbare Kosten wie bei einer traditionellen ID/einem Pass, die

3. Interoperabilität, die Nutzung der ID für Behördengänge (Bund, Kanton), die
4. Sicherheit und ganz zuletzt
5. der Datenschutz.

Selbst wenn man alles perfekt macht, wird die Hemmschwelle nach wie vor sehr hoch sein. Themen wie Datensparsamkeit sind für den Normalbenutzer irrelevant, wenn das System nicht funktioniert. Auch bei der Sicherheit gilt: Im Zweifelsfall wird unverschlüsselt kommuniziert, Verfügbarkeit kommt immer vor Vertraulichkeit. Dieses Verhalten wird sich durch die eID NICHT ändern.

Schlägt man den vorgesehenen Weg ein, riskiert man das Schicksal des ePD: Unendlich hohe Kosten und keine realisierbaren Lösungen. Der Gesetzesentwurf weist in die richtige Richtung. Man hat es vermieden, die übertriebenen und kaum realisierbaren Anforderungen der IT-Lobbyisten zu bedienen. Wir lehnen den SSI-Ansatz derzeit ab (unausgegoren, zu komplex, auf wackligem Grund). Eine Beschränkung auf das Wesentliche bildet den Schlüssel zum Erfolg.

Das fehlgeleitete Dogma: Der Bund muss ein Ökosystem für die Nutzung der eID liefern.

Wie oben bereits erfasst, geht es bei der Schaffung der EID nicht um deren Anwendung. Es ist nicht Aufgabe des Staates, dafür zu sorgen, dass die digitale Identität eingesetzt werden kann (ausser natürlich für seine eigenen Verfahren). Ebenso wenig, wie der Staat Autos gebaut hat, um Autobahnen zu nutzen, muss er Anwendungen für die EID liefern. Sobald eine vertrauenswürdige Identitätsinfrastruktur steht, werden sich sofort Anwendungen anbieten, welche heute entweder bereits in Betrieb sind oder in kurzer Frist in Betrieb genommen werden können.

Die alleinige Kernaufgabe des Staates damit des Bundes ist es, den digitalen Ausweis zu erstellen.

Wichtig ist jedoch, dass die Anzahl staatlicher Identitäten zwingend auf 1 (= eine) eingeschränkt wird! Es kann nicht sein, dass Verwaltungseinheiten oder Kantone zusätzliche Identitäten und Infrastrukturen aufbauen. Dies wäre ein Föderalismus, welcher die EID verunmöglichen würde. Wie erwähnt, die EID soll das Pendant zum physischen Identifikationsdokument sein. Andere Nutzer sollen darauf aufbauen können, aber auf keinen Fall Parallelösungen bauen.

Sobald eine digitale Identität für eine Anwendung genutzt werden soll, gibt es hierzu verschiedene Möglichkeiten für die Umsetzung. Hier darf und soll sich der Herausgeber der EID nicht einmischen. Über die Zeit werden heute isolierte Lösungen die EID als Identifikationsanker nutzen, weil der Aufwand für die Weiterführung eigener Identifikationslösungen zu gross werden wird.

Gefahren der Komplexität und fehlender Akzeptanz

Die im Vorfeld durchgeführten Abklärungen, in welche Richtung die Umsetzung der eID gehen soll, sind fehlgeleitet. Das von der IT-Industrie und den Digitalverbänden geliebte Ambitionsniveau 3 ist ein Irrweg. Statt sich auf das Wesentliche zu beschränken, wird versucht, möglichst viel in das Gesetz zu packen. Das wird nicht funktionieren. Wir haben bereits beim ePD gesehen, dass zu viele Sicherheitsvorgaben zum Scheitern führen. Der SSI-Ansatz ist dabei ein interessanter Versuch, man sollte ihn aber als das behandeln, was er ist: Eine Sammlung von Ideen und ersten Gehversuchen auf einem weitgehend unpräparierten Terrain.

Für die Infrastruktur existiert bereits ein Gesetz

Mit Erstaunen stellen wir fest, dass dasjenige Gesetz, welches bereits 90 % der Infrastrukturfragen regelt, nicht einmal zitiert wurde. Es handelt sich dabei um das ZertES, es regelt bereits umfassend die wichtigsten Strukturen und Verfahren. Dessen Titel lautet:

943.03: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)

Konkret werden eIDs in Form digitaler Zertifikate herausgegeben werden. Eine eID ist in einem digitalen Zertifikat verkörpert. Damit können diese unter dieses Gesetz fallen. Es erübrigt sich, die Trust-Infrastruktur im BGEID neu zu regeln. Ggf. kann man die Regelungen auf die eID-spezifischen Verfahren und Systeme reduzieren.

Was uns im Detail aufgefallen ist

Die Verfahren in Kapitel 5 sind zumindest noch im Anfangsstadium. Wie erwähnt kann man sich hier an der ZertES orientieren.

Die Verfahren sind sicher noch nicht zu Ende gedacht: So widerspricht der Ablauf in Art. 17 Abs. 3 fundamentalen Sicherheitsprinzipien als auch dem Gebot der Datensparsamkeit. Würde dieses Verfahren so etabliert, ist mit einer sehr hohen Fehlerquote zu rechnen. Zudem lassen sich solche Einträge, wenn das System sauber aufgesetzt wurde, kaum mehr entfernen. Passende Verfahren aufzusetzen ist mit sehr hohen Anforderungen verbunden und man muss mit Sicherheitskompromissen, also Risiken, rechnen.



Stiftung für Konsumentenschutz
Nordring 4
Postfach
3001 Bern

Frau Bundesrätin
Karin Keller-Sutter
Eidgenössisches Justiz- und
Polizeidepartement (EJPD)
Per E-Mail:
rechtsinformatik@bj.admin.ch

Rückfragen:

Lucien Jucker, Leiter Datenschutz / Digitalisierung / IT
l.jucker@konsumentenschutz.ch

Bern, 18. Oktober 2022

Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Vielen Dank für die Möglichkeit, an der Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz) teilzunehmen.

Die Stiftung für Konsumentenschutz ist eine Nichtregierungs-Organisation, die sich seit 1964 für die Rechte und Interessen von Konsumentinnen und Konsumenten einsetzt.

Der Konsumentenschutz nimmt zum Vorentwurf des BGEID wie folgt Stellung:

Die Richtung des E-ID-Gesetzes und den Einbezug interessierter Kreise auf dem Weg zum Vorentwurf begrüssen wir sehr. Der offene Austausch über Partizipationsmeetings war der richtige Weg – es wäre wünschenswert, wenn ein solches Vorgehen auch für zukünftige Gesetzgebungsprozesse öfters gewählt würde.

Die wichtigsten drei Anforderungen, die der Konsumentenschutz in der öffentlichen Konsultation geäußert hat, werden durch den Vorentwurf erfüllt.

Wir freuen uns besonders darüber, dass der Datenschutz durch Technik und die Datensparsamkeit im Vorentwurf in Art. 1 Abs. 2 lit. b Ziff. 1 und 3 BGEID explizit als Gesetzeszweck aufgeführt wurden. Damit nimmt das E-ID-Gesetz Bezug zu Art. 7 des neuen Datenschutzgesetzes, das im September 2023 in Kraft tritt.

Leider wird – wie beim nDSG – auch im E-ID-Gesetz zu wenig für die Einhaltung dieser Prinzipien getan: Es gibt keine Gesetzesnorm, die Verifikatorinnen unter Strafandrohung dazu verpflichtet, nur die für den Zweck unbedingt erforderlichen Daten zu erheben. Folglich kann ein Sammeln von nicht unbedingt erforderlichen Daten nicht sanktioniert werden. Auch das nDSG kennt keine Sanktionen für einen Verstoß gegen das Prinzip der Datensparsamkeit. Das Sammeln von nicht unbedingt erforderlichen Daten wird also weder nach BGEID noch nach nDSG mit rechtlichen Konsequenzen bewehrt. Folglich haben Verifikatoren, die nicht unbedingt erforderliche Daten verlangen, höchstens einen Reputationsschaden zu befürchten. Immerhin kann nach Art. 16 BGEID letztendlich die Inhaberin der E-ID entscheiden, ob sie alle angeforderten Daten übertragen möchte. De facto werden die E-ID-Inhaber aber – wie im digitalen Raum leider üblich – in der schwächeren, abhängigen Position sein. Die E-ID-Inhaberinnen können nur wählen, ob sie sämtliche Daten übertragen wollen, oder auf die Erbringung der Leistung verzichten. Aufgrund dieses Machtgefälles und weil die hinterlegten Daten eine besonders hohe Qualität aufweisen, ist die Widerspruchslösung als einziges Mittel gegen eine solche drohende Überidentifikation nicht ausreichend.

Der Konsumentenschutz befürchtet, dass einzelne Unternehmen die staatlich verifizierten Daten straflos horten und für eigene Zwecke missbrauchen. Deshalb fordert er eine Sanktionsmöglichkeit für Unternehmen und Behörden, die sich nicht an den Grundsatz der Datensparsamkeit halten.

Das Erstellen einer Wallet-App zur Aufbewahrung und Vorweisung von elektronischen Nachweisen durch den Bund nach Art. 19 BGEID erscheint uns sinnvoll. Es erschliesst sich uns aber nicht, wieso Art. 20 BGEID keine Pflicht zur Erstellung einer Prüfungs-App für elektronische Nachweise vorsieht. Die Voraussetzung, dass der Bevölkerung ermöglicht werden soll, die Authentizität einer E-ID zu überprüfen, hat der Konsumentenschutz bereits in der öffentlichen Konsultation geäußert. Dafür ist eine Prüfungs-App unerlässlich, weshalb der Bund eine solche App zur Verfügung stellen muss. Falls die Integration einer Prüffunktion in der Wallet-App technisch möglich ist, wäre das einer Lösung mit zwei unterschiedlichen Apps vorzuziehen.

Wir danken Ihnen für die Kenntnisnahme unserer Antwort und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Sig. Sara Stalder
Geschäftsleiterin

Sig. Lucien Jucker
Leiter Datenschutz /
Digitalisierung / IT



Stellungnahme der Piratenpartei Schweiz zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 29.06.2022 nehmen wir gerne Stellung.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Gerne nehmen wir wie folgt Stellung:

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Die Piratenpartei ist erfreut, darüber, dass der Bund den Ball aufgenommen hat und deutliche Schritte in Richtung Wahrung der Digitalen Integrität macht. Leider beinhaltet der aktuelle Vorschlag Punkte, welche mit dieser nicht vereinbar sind und deshalb ist auch die in diesem Gesetz geplante E-ID in der jetzigen Form abzulehnen. Zwar wird im Gesetz ausdrücklich Datenschutz durch Technik, Datensicherheit und Datensparsamkeit als verbindlich erklärt, jedoch wird es im Detail diesen Anforderungen nicht gerecht.



Unbedingt korrigiert werden müssen:

Art. 4 Keine Ausstellung per Liveness-Check (Gesichtsvideo) und besonders keine Speicherung der Daten auf viele Jahre (Art. 11)

Art. 4 Analoge Ausstellungsmöglichkeit

Art. 10 Einsatz nur, wenn der Gesetzgeber eine Ausweispflicht vorsieht

Art. 2 Selbstbestimmte Auswahl der Daten, die in der E-ID gespeichert werden

Unsere Stellungnahme zu den einzelnen Artikeln:

Art. 2 Form und Inhalt

Abs. 2

Forderung:

Abs. 2 neu: Sie kann die folgenden Personenidentifizierungsdaten enthalten:

Die Absätze 2 und 3 enthalten eine lange Auflistung aller Daten, die bei Ausstellung zwangsweise in der E-ID hinterlegt werden. Für die Identifikation mit der E-ID mag dies insbesondere für die Behörden angenehm sein, widerspricht allerdings der Datensparsamkeit (Art. 1 Abs. 2 Ziff. 3) gänzlich.

Aus Gründen der Datensparsamkeit, -sicherheit und Selbstbestimmung des Bürgers muss dieser entsprechend selbst auswählen können, welche Daten er überhaupt auf seiner E-ID gespeichert haben möchte. So lange er beispielsweise mit der E-ID nur online Alkohol kaufen möchte, sollte es reichen auf der E-ID abzuspeichern, ob die Person das 18. Lebensjahr vollendet hat.

Abs. 3

Forderung:

Streichung lit a. AHV-Nummer

Der dritte Absatz unterscheidet sich vom zweiten theoretisch darin, dass die aufgezählten Daten keine "Personenidentifizierungsdaten" sein sollten. Dieser Punkt wird im Moment der Zusammenführung jedoch gänzlich hinfällig. Bei gesetzlicher Nutzung der E-ID ist die Illusion, dass die Daten in Abs. 3 nicht zur Identifizierung genutzt werden



können, schon schwierig aufrechtzuerhalten. Aber bei einmaligem widerrechtlichem Auslesen der E-ID sind mehrere Daten in Absatz 3 alles andere als harmlose "zusätzliche Informationen". So wird insbesondere die AHV-Nummer einmalig ausgestellt und bleibt ein Leben lang unverändert. Was Personendaten angeht, gibt es nur wenig Wertvolleres.

Eine Verknüpfung widerspricht auch generell dem Konzept der AHV-N13, denn "die 13-stellige AHV-Nummer ist völlig anonym, zufällig generiert und nicht sprechend. Sie wird nur einmal vergeben und bleibt ein Leben lang unverändert, auch wenn der Zivilstand, etwa durch Heirat, ändert." [1] Ferner ist die AHV-Nummer auf anderen amtlichen Ausweisen nicht gespeichert.

Nicht zuletzt verspricht der Bund, es darf erneut erwähnt werden, die E-ID datenspar-sam umzusetzen (Art. 1 Abs. 2 Ziff. 3), was mit der Speicherung der AHV-Nummer sicher nicht eingehalten wird.

Eine Verknüpfung der E-ID mit der AHV-Nummer ist entsprechend vollumfänglich auszuschliessen.

Art. 4 Ausstellung

Liveness-Check

Forderung:

1. Auf unsichere Methoden und die darauffolgende Datenspeicherung ist zu verzichten.
2. Explizites Anbieten einer E-ID-Erstellung ohne Liveness-Check

Bei der Eröffnung des Vernehmlassungsverfahrens hat Michael Schöll (Direktor BJ) den Ausstellungsprozess der E-ID nach Art. 4 genauer beschrieben und dabei einen "Liveness-Check", ein Videogesichtsbild, als Grundkomponente hervorgehoben (Abs. 4) [2]. Auf Nachfrage wurde bestätigt, dass eine Software den Abgleich mit den hinterlegten Gesichtsbildern vornehmen wird. Nicht nur Menschen, sondern auch Maschinen lassen sich allerdings von Deep-Fakes und anderen technischen Umgehungsversuchen nachweisbar täuschen. So gibt der Bund faktisch selbst zu, dass der Liveness-Check nicht sicher ist, indem das fedpol die Gesichtsvideos bis 5 Jahre nach Gültigkeit zur Missbrauchsverhinderung/-analyse speichern darf (siehe Art. 11 Abs. 2b), um bei Verdacht die Daten erneut kontrollieren zu können.

Aus Datenschutzgründen ist es äusserst problematisch vom Antragstellenden ein Gesichtsvideo zu fordern. Zum einen können daraus detaillierte 3D-Gesichtsmodelle aller



erstellt werden, was beispielsweise für die Identifikation bei Videoüberwachung genutzt werden kann. Zum anderen werden diese Daten jahrelang zentral gespeichert werden, was diese Daten wiederum selbst zu einem lukrativen Ziel für Cyberangriffe macht. Sämtliche Daten in Bezug auf die E-ID sind besonders wertvoll und da inzwischen andauernd über Hacks, auch gegenüber staatlichen Stellen, berichtet (oder auch verschwiegen) wird, muss davon ausgegangen werden, dass mittel- bis langfristig eine sichere Datenhaltung nicht garantiert werden kann.

Viele Menschen werden aus oben genannten Gründen eine E-ID auf dem Weg des Liveness-Checks nicht beantragen. Wir halten es für zwingend notwendig, dass gleichwertig eine E-ID-Erstellung auch bei einer staatlichen Stelle wie dem Passbüro oder Gemeindeverwaltung ermöglicht wird. Eine solche analoge Option hätte die oben genannten Probleme des Liveness-Checks nicht und wäre eine zweckdienliche Alternative.

Art. 10 Vorweisen einer E-ID

Forderung:

1. Abs. 1 neu: Das Vorweisen der E-ID darf nur verlangt werden, wenn die Ausweispflicht in einem Gesetz vorgesehen ist.
2. Streichung des letzten Teilsatzes

Der Artikel wird mit "Vorweisen einer E-ID" betitelt, bietet inhaltlich aber nur eine unvollständige Regelung, unter welchen Umständen die E-ID statt anderen Ausweismöglichkeiten vorgewiesen werden muss. Es fehlt somit im ganzen Gesetz ein konkreter Grundsatz zur Vorweisung. Der Artikel sollte entsprechend einen neuen ersten Absatz erhalten, der die Vorweisung generell regelt und gleichzeitig einer inflationären Ausweispflicht vorbeugt.

Deswegen neu Abs. 1: Das Vorweisen der E-ID darf nur verlangt werden, wenn die Ausweispflicht in einem Gesetz vorgesehen ist.

Der Artikel, wie er im Entwurf steht, sieht vor, dass grundsätzlich andere Ausweismöglichkeiten weiterhin gleichwertig benutzbar bleiben sollen. Der letzte Teilsatz des Artikels relativiert aber alles Vorhergehende mit einem schwammigen Verweis auf "Anforderungen insbesondere an die Sicherheit des Prozesses". Wenn die Ausweise vor der Einführung der E-ID den Anforderungen genügt haben, sollte man davon ausgehen,



dass dies danach auch noch so sein sollte. In jedem Fall ist der Verweis auf "Anforderungen insbesondere an die Sicherheit des Prozesses" zu nichtssagend und offen, um als Grund herzuhalten.

Art. 11 Informationssystem zur Ausstellung und zum Widerruf der E-ID

Forderung:

1. Keine Speicherung der Daten aus dem Verifikationsprozess (Streichung von Abs. 2 lit. b).
2. Senkung der Aufbewahrungsfrist

Abs. 2

Der Artikel bestimmt, dass das fedpol ein "Informationssystem zur Ausstellung und zum Widerruf der E-ID" betreibt.

Abs. 2 legt sodann fest, welche Daten darin festgehalten werden. Darunter fallen unter anderem "die Daten zum Ausstellungsprozess" (lit. b). Wie in unserer Stellungnahme zu Artikel 4 ausgeführt, werden die Daten aus dem Verifikationsprozess selbst zu einem möglichen Ziel für Cyberkriminalität.

Abs. 5

Eine Aufbewahrungsfrist von fünf Jahren erscheint exzessiv. Sie sollte auf ein deutlich tieferes Minimum begrenzt werden.

Art. 16 Vorweisen von elektronischen Nachweisen

Forderung:

Der Verifikator darf nur die minimal nötigen Daten abfragen, muss diese beim ersten möglichen Zeitpunkt wieder löschen und darf diese, unter Strafe, nicht anderweitig bearbeiten.

Verwendung von Zero-Knowledge Proofs

Abs. 1 bestimmt, dass der Inhaber oder die Inhaberin des Nachweises bestimmt, welche Daten an die Verifikatorin übertragen werden. Auch wenn dieser Ansatz grundsätzlich gut ist, ignoriert er ein mögliches Machtgefälle zwischen den Parteien. Der Inhaber kann so u.U. dazu gedrängt oder getäuscht werden, mehr Daten herauszugeben, als tatsächlich nötig wären.



Um der Datensparsamkeit (Art. 1 Abs. 2 lit. b) und dem Datenschutz durch Technik (Art. 1 Abs. 2 lit. a) zu genügen, sollte ausserdem, wo immer möglich, auf Zero-Knowledge Proofs gesetzt werden. Dies bedeutet, dass auch die vorhandenen Informationen nicht übergeben werden, wenn der Nachweis durch anonymere Angaben erreicht werden kann. Beispielsweise genügt es bei Alkoholkaufr der Verifikatorin ein "erlaubt/volljährig" anzuzeigen, statt das Geburtsdatum selbst.

Art. 17 Basisregister

Forderung:

Entzug der Gültigkeit des Nachweises statt Widerruf

Der Bund führt ein Basisregister, um u.a. die Echtheit der Nachweise zu bestätigen. Nach Abs. 1 lit. c bzw. Abs. 2 lit. d wird auch der Widerruf von elektronischen Nachweisen festgehalten. Aus dem erläuternden Bericht ist leider nicht ersichtlich, wieso nicht stattdessen schlicht die Gültigkeit entzogen werden kann. Wenn ein Nachweis mit Widerruf markiert ist, lässt dies immer noch darauf schliessen, dass die Daten vermutlich echt waren, was den Wert von diesen für Cyberkriminelle (oder Datenkraken) erhöht.

Der erläuternde Bericht erwähnt ausserdem die Verwendung von Blockchain als mögliche Grundlage für das Basisregister. Einerseits sind Blockchains lange nicht so manipulationssicher, wie häufig dargelegt. Andererseits gibt es bis jetzt keinen Anwendungsfall, den die Blockchain-Technologie besser löst als herkömmliche Alternativen. Auf eine Blockchain ist entsprechend zu verzichten, insoweit es hier nur aus modischen Gründen Erwähnung fand.

Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Forderung:

1. Die Anwendung muss hohen Sicherheitsstandards genügen.
2. Das Anbieten einer externen Speicherung der Daten sollte angeboten werden.

Der Bund sieht eine sogenannte Wallet-App vor, um die elektronischen Nachweise aufzubewahren. Hierbei vermissen wir die Anerkennung des Schutzbedürfnisses der Daten, welche insbesondere gegenüber Malware und physischem Verlust zu schützen sind.

Durch unterschiedliche Sicherheitslevels von Handys, veralteten Systemen oder schlicht



durch die durchgehende Verfügbarkeit auf einem ständig vernetzten Gerät ist es aus unserer Sicht fragwürdig, ob genügend sichergestellt werden kann, dass die Daten auch sicher bleiben. Es sollte deshalb die Möglichkeit geboten werden, die Daten auf einem Offline-Speicher, wie einer verschlüsselten NFC-Chipkarte, getrennt aufzubewahren.

Art. 20 Anwendung zur Prüfung von elektronischen Nachweisen

Forderung: Der Bund stellt in jedem Falle eine solche Anwendung zur Verfügung. Die optionale Formulierung ist durch eine obligatorische zu ersetzen.

Art. 21 System für Sicherungskopien

Abs. 2

Forderung:

E2E Verschlüsselung der Sicherungskopien

Die Sicherungskopien der E-ID müssen aus Sicherheitsgründen explizit mit einer Ende-zu-Ende-Verschlüsselung geschützt werden, sodass nur die Inhaberin oder Inhaber.

Art. 22 Missbrauch

Forderung:

Der Bund informiert nicht nur über (Verdachts-)Missbrauch der Vertrauensinfrastruktur, sondern über sämtliche Fälle im Ökosystem E-ID.

Nur mit Transparenz kann Vertrauen geschaffen werden. Und der Steuerzahler/Nutzer hat ein Recht darüber informiert zu werden, ob es in diesem sensiblen Bereich zu einem Datenreichtum oder Manipulation gekommen ist.

Art. 26 Gebühren

Abs.2

Forderung:

Keine Gebühren für Sicherungskopien

Der Absatz sieht Gebühren für Sicherungskopien vor. Die Datenmenge ist überschaubar und eine Sicherung der E-ID sollte kostenfrei sein, da allein schon der administrative Aufwand des Inkassos in keinem Verhältnis zu den eigentlichen Kosten steht.



Darüber hinaus:

Dem E-ID-Gesetz sollte ein neuer Absatz über Strafbestimmungen hinzugefügt werden, der Strafandrohungen bei Missbrauch der Daten vorsieht (vgl. z.B. Art. 16). Das Datenschutzgesetz alleine reicht nicht aus.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:

[1] www.bsv.admin.ch/bsv/de/home/sozialversicherungen/ahv/grundlagen-gesetze/ahv-nummer.html

[2] <https://www.youtube.com/watch?v=epW4xEqr3mw&t=689s>

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 17. Oktober 2022



Die Schweizerische Post AG
Stab CEO
Wankdorfallee 4
3030 Bern

Telefon +41 58 341 15 64
www.post.ch

Stab CEO, Wankdorfallee 4, 3030 Bern

Bundesrätin Karin Keller-Sutter
Eidgenössisches Justiz- und Polizeidepartement
EJPD
Bundeshaus West
3033 Bern

Als PDF/Word an: rechtsinformatik@bj.admin.ch

Datum 14. Oktober 2022
Ihre Nachricht
Kontaktperson Franziska Heer
E-Mail franziska.heer@post.ch
Direktwahl +41 58 341 15 64

Stellungnahme der Schweizerischen Post zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung nehmen zu können.

1. Betroffenheit der Schweizerischen Post

Die Schweizerische Post sieht in der digitalen Transformation eine Notwendigkeit für die Schweiz und fördert sie mit ihren Kompetenzen. Als bundesnahe Unternehmen und Bindeglied zwischen Bund, Kantonen und Wirtschaft will die Post aktiv beim Aufbau des E-ID Ökosystems mitwirken und Verantwortung übernehmen. Mit ihrem schweizweiten Netz an Zugangspunkten bietet die Post eine ideale Voraussetzung als mögliche Anlaufstelle für die Bevölkerung im Zusammenhang mit der Ausstellung und dem Einsatz der E-ID. Schon heute bieten die Filialen der Post der Bevölkerung allgemeine Unterstützung bei verschiedenen E-Government-Anwendungen.

Eine sichere Identität für Akteure im digitalen Raum ist ein Schlüsselement für den Erfolg der notwendigen digitalen Transformation der Schweiz und wir messen ihr daher eine hohe Priorität bei. Sichere digitale Systeme sind seit Langem Teil des Postalltags: sie schaffen die Voraussetzung dafür, dass die Post ihre Kernkompetenz, sensible Informationen sicher und vertrauensvoll zu transportieren, im physischen Kerngeschäft wie auch in der virtuellen Welt umsetzen kann. Die Post hat in den letzten Jahren ihre Kompetenzen und Ressourcen in der Informations- und Verschlüsselungstechnologie ausgebaut und bietet heute digitale Lösungen für Behörden, Geschäfts- und Privatkunden an.

Unsere Tochtergesellschaft SwissSign bietet digitale Dienstleistungen an, etwa die SwissID und Zertifikats- und Signaturlösungen. Die SwissID ist eine digitale Identität, welche einen einfachen und sicheren Zugang zur Onlinewelt ermöglicht. Sie ist bereits heute den Zugang für rund 200 Online Services von Schweizer Firmen. So hat die SwissID erfolgreich das Zertifizierungsverfahren für die sichere

Identifizierung im elektronischen Patientendossier (EPD) durchlaufen. Zudem hat sie ein Onlineverfahren zur Identitätsüberprüfung eingeführt (Videoidentifikation).

Die selbst verwaltete Identität, die sogenannte Self Sovereign Identity (SSI), ist das Kernelement eines auf SSI basierenden E-ID-Ökosystems. Die Post baut mit der Durchführung von Pilotprojekten wie der elektronischen Wohnsitzbestätigung sowie dem digitalen Anstellungsprozess in diesem Bereich ein fundiertes Know-How auf und teilt dieses mit der Fach-Community.

2. Grundsätzliches zum Entwurf

Das Gesetz sieht die Einführung eines staatlichen elektronischen Identitätsnachweises vor für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises. Es setzt den Rahmen für eine Vertrauensinfrastruktur, deren Kernelemente eine staatliche E-ID ist. Die Post fordert schon länger eine solche elektronische Identität. Wir begrüssen daher, dass das EJPD in kurzer Zeit eine Vernehmlassungsvorlage ausgearbeitet hat. Wir sind der Ansicht, dass der vorliegende Gesetzesentwurf den politischen Auftrag gut umsetzt und die zentralen Grundsätze «privacy by design», «Datensparsamkeit» und «dezentrale Datenspeicherung» angemessen berücksichtigt.

Für die Post ist die elektronische Identität in vielerlei Hinsicht von zentraler Bedeutung. Infolgedessen möchten wir die folgenden Punkte besonders hervorheben und Sie bitten, diese zu berücksichtigen:

Ambitionsniveau 3 (Ökosystem) muss zügig erreicht werden

Ein rein staatlich genutzter, digitaler Ausweis erscheint uns nicht zweckdienlich und wird nicht ausreichen, um die Digitalisierung in der Schweiz entscheidend voranzutreiben. Dass der vorliegende Gesetzesentwurf bzw. die vorgesehene Infrastruktur unterschiedliche elektronische Nachweise vorsieht und damit Richtung Ambitionsniveau 3 als offenes Ökosystem abzielt, begrüssen wir. Der Ausbau dieses Ökosystems muss schrittweise, aber zielstrebig und zügig erfolgen. Wir sind der Meinung, nur ein Ökosystem, in dem es eine Vielzahl unterschiedlichster Ausstellerinnen und Verifikatorinnen gibt, kann der Bevölkerung den Mehrwert der digitalen Identität bieten. Die Post ist bereit, mit ihren Dienstleistungen einen aktiven Beitrag zu leisten, um das Erreichen des Ambitionsniveaus 3 voranzutreiben.

Klarere Abgrenzung der E-ID als Identifikationsmittel von Authentifikationsmittel

Die Ausstellung und die Verwendung der E-ID sind gemäss Vorentwurf freiwillig. Wir begrüssen dies ausdrücklich. Die Bevölkerung soll künftig weiterhin die Wahl haben, wie auf das persönliche elektronische Patientendossier (EPD) zugegriffen werden kann. SwissSign und aktuell zwei weitere Unternehmen sowie zwei Kantone sind gemäss Bundesgesetz über das elektronische Patientendossier (EPDG) zertifiziert und bieten eine sichere Login-Lösung an. Im Sinne der Freiwilligkeit, des Wettbewerbs und nicht zuletzt auch vor dem Hintergrund der getätigten Investitionen sollten neben der staatlichen E-ID weiterhin z.B. gemäss EPDG zertifizierte Lösungen möglich bleiben. Dafür ist eine klare Abgrenzung zwischen Identifikationsmittel und Authentifikationsmittel vorzusehen. Die E-ID gemäss vorliegendem Gesetzesentwurf ist ein digitaler Identitätsnachweis im Sinne eines digitalen Pendant zum Pass oder zur Identitätskarte. Sie sollte kein «Login» im Sinne eines Zugangsmittels zu digitalen Diensten (Authentifikationsfunktion) sein. Diese Unterscheidung wird im Vorentwurf aus unserer Sicht zu wenig deutlich gemacht. Wird diese Unterscheidung explizit vorgenommen, werden bestehende und künftige, private und öffentliche Angebote von elektronischen Authentifizierungsdiensten nicht benachteiligt und wäre dies unserer Meinung nach ein wesentlicher Treiber für das angestrebte Ökosystem.

Gleichberechtigte Angebote von privaten Dritten ermöglichen

Es erscheint uns essenziell, dass es im Sinne des angestrebten E-ID-Ökosystems auch Akteuren des privaten Sektors möglich ist, separate, nichtstaatliche Lösungen und Mechanismen bereitzustellen. Aus dem vorliegenden Gesetzesentwurf ist nicht gänzlich ersichtlich, welche Rollen Private bei der Entwicklung und Einführung des angestrebten Ökosystems einnehmen können und dürfen.

Im Gesetz nicht geregelt – und daher implizit erlaubt – ist die Verwendung von elektronischen Brief-taschen (Wallets), die von privaten Akteuren ausgestellt werden. Es ist vorgesehen, dass Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden können. Wichtig scheint uns daher, dass auch diese privaten Anwendungen an die Vertrauensinfrastruktur des Bundes und insbesondere an das Informationssystem des fedpol beim Ausstellprozess angebunden werden können – im Sinne von gleich langen Spiessen für alle. Wir schlagen vor, dass die staatliche E-ID auch aus einer privaten Wallet hinaus beantragt werden kann.

Disruptive Prozesse und Nutzung der E-ID in der physischen Welt

Die E-ID ermöglicht den Inhaberinnen und Inhabern, sich bei Geschäftsprozessen in der digitalen Welt einfacher zu identifizieren. So können die bestehenden (Online)-Identifizierungsprozesse ersetzt werden, die heute viel komplexer sind. Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden (analog zu einem COVID Zertifikat). Damit kann die E-ID auch in der physischen Welt wie ein Papierausweis genutzt werden. Die Post sieht in dieser Möglichkeit einen klaren Mehrwert für die E-ID. Aus unserer Sicht ist dabei zentral, dass die E-ID und das E-ID Ökosystem symbiotisch und aufeinander abgestimmt wachsen und die Schnittstellen klar definiert werden. Aus unserer Sicht werden diese Grundsätze und Prozesse der Verwendung der E-ID in der physischen Welt noch zu wenig klar beschrieben. Es besteht aktuell ein hoher Interpretations-spielraum (beispielsweise die Nutzung und Validierung eines COVID Zertifikats mit einem gültigen digitalen Ausweis als Zutrittskontrolle oder bei der Einreise in die Schweiz).

Kantonale Anlaufstellen (Artikel 8 des BGEID)

PostNetz stellt den Kantonen die rund 800 eigenbetriebenen Filialen als physische Anlaufstellen zur Verfügung. Täglich verzeichnen die Filialen der Post mehr als 9 Mio. Passantinnen und Passanten und dabei über 320'000 Kundengeschäfte. Das Filialnetz der Post bietet in der ganzen Schweiz – sowohl in urbanen als auch in ländlichen Regionen – niederschweligen Zugang zu Dienstleistungen und dadurch Nähe zu Bürgerinnen und Bürgern. Ergänzend zum Support des fedpol bei der Ausstellung oder dem Widerruf der E-ID, kann die Post der Bevölkerung daher in ihren Filialen allgemeine Unter-stützung anbieten in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID. Das breite Post-filialnetz kann als wichtiger Multikanal fungieren und neben der Unterstützung in den digitalen Pro- zessen (Fernidentifizierung) auch im physischen Prozess in der E-ID Ausstellung unterstützend wir- ken. Dadurch kann die Post einen wesentlichen Beitrag für die Verbreitung der E-ID in der Bevölke- rung leisten.

3. Im Einzelnen

Bezogen auf unsere Tätigkeiten und Visionen möchten wir zu den folgenden Artikeln aus Sicht der Schweizerischen Post ergänzend zu den eingangs gemachten Erläuterungen im Detail Stellung bezie- hen.

Art. 1 VE E-ID-Gesetz: Gegenstand und Zweck

- Abs. 1

Die Erweiterung des E-ID Gesetzes auf «andere elektronische Nachweise» und das dadurch entste- hende Ökosystem haben enorme Bedeutung weit über das E-ID Thema hinaus. Da eine für Private zur Nutzung offenstehende staatliche Infrastruktur geschaffen werden soll, muss die Gleichbehand- lung mit ähnlichen privaten Infrastrukturen im Gesetz geregelt werden.

Um dies klar zum Ausdruck zu bringen, schlagen wir in Absatz 1 folgende Änderung vor:

d. die Förderung neuer digitaler Geschäftsmodelle, die mit dieser Vertrauensinfrastruktur verbundenen sind.

Konkretisiert wird das Förderungsziel durch den neuen Art. 25^{bis} Finanzhilfen (s.u.).

- **Abs. 1^{bis} (neu)**

Das BGEID basiert auf dem Grundverständnis, dass die E-ID ein digitaler Identitätsnachweis im Sinne eines digitalen Pendants zum Pass oder zur Identitätskarte ist und nicht ein «Login» im Sinne eines Zugangsmittels zu digitalen Diensten (Authentifikationsfunktion). Dies muss im BGEID klar zum Ausdruck kommen, damit bestehende und künftige, private und öffentliche Angebote von elektronischen Authentifizierungsdiensten, namentlich föderierte Dienste im angestrebten E-ID-Ökosystem nicht benachteiligt werden. Wir schlagen deshalb eine entsprechende Abgrenzung in einem neuen Absatz 1^{bis} in Artikel 1 vor:

Das Gesetz regelt nicht die Anforderungen an mit der E-ID verbundenen, öffentlichen oder privaten elektronischen Authentifizierungsdienste.

Art. 8 VE E-ID-Gesetz: Anlaufstellen der Kantone

Mit privaten, vertrauenswürdigen Unterstützungsangeboten können Bürgerinnen und Bürger dort und dann erreicht werden, wenn sie konkreten Bedarf haben. Die Post hat schweizweit bereits Infrastrukturen und Prozesse zur Identitätsprüfung im Einsatz. Sie kann als Anlaufstelle für Bürgerinnen und Bürger einen wesentlichen Beitrag leisten und z.B. im Auftrag der Kantone Unterstützung für die E-ID anbieten. Privaten Unterstützungsangeboten ist gleichberechtigt zu öffentlichen Angeboten ein Platz einzuräumen. Wir schlagen deshalb in Artikel 8 folgende Änderung vor:

Die Kantone bezeichnen die öffentlichen oder privaten Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.

(neu) Art. 25^{bis} VE E-ID-Gesetz: Finanzhilfen

Um den angestrebten Nutzen aus der E-ID und der Infrastruktur für andere elektronische Nachweise ziehen zu können, ist es notwendig im E-ID Ökosystem das Ambitionsniveau 3 zügig erreichen zu können. Finanzhilfen sind ein wichtiges Mittel dazu. Wir schlagen die Verankerung von Finanzhilfen im BGEID vor, sofern dies nicht bereits durch das geplante EMBaG abgedeckt ist.

Der Bund richtet Finanzhilfen für die Umsetzung des E-ID-Gesetzes aus. Der Bund hält sich dabei an die Anforderungen von Art. 8 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBaG) und fördert dabei gezielt neue digitale Geschäftsmodelle, die mit der E-ID Vertrauensinfrastruktur verbunden sind.

4. Schlussbemerkungen

Wir bedanken uns für Ihre Kenntnisnahme und die Berücksichtigung unserer Ausführungen in ihren weiteren Arbeiten betreffend das E-ID Gesetz.

Sehr gerne partizipieren unsere Spezialistinnen und Spezialisten weiterhin im Projektraum des Bundesamts für Justiz zu den Themen E-ID und digitale Vertrauensinfrastruktur in der Schweiz und tauschen sich dazu mit den Fachstellen des BJ aus. Sie stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Die Schweizerische Post AG



Katrin Nussbaumer
Co-Leiterin Stab



Nicole Burth
Leiterin Kommunikations-Services

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail:
rechtsinformatik@bj.admin.ch

Bern, 12. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Vorentwurf für ein E-ID-Gesetz (VE-BGEID) Stellung nehmen zu können. Aus datenschutzrechtlicher Sicht ergeben sich folgende Hinweise:

1. Allgemeine Bemerkungen

Wir begrüssen die neue Initiative zur Einführung eines elektronischen Identitätsnachweises (E-ID) auf der Basis einer staatlich betriebenen Infrastruktur und den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung.

2. Bemerkungen zu den einzelnen Artikeln des VE-BGEID

Art. 2 Abs. 2 Bst. b – Gesichtsbild

In Art. 4 Abs. 4 VE-BGEID und den zugehörigen Erläuterungen wird der Bedarf nach einem biometrischen Gesichtsbild nur für den Ausstellungsprozess begründet. Demgegenüber wird der Bedarf nach einem biometrischen Gesichtsbild in der E-ID selbst weder in den Erläuterungen zu Art. 2 Abs. 2 Bst. g – der auf die Informationssysteme nach dem Ausweisgesetz (AwG) und dem Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) verweist, die beide biometrische Gesichtsbilder enthalten können (vgl. Art. 11 i. V. m. Art. 2^{bis} AwG und Art. 1 i. V. m. Art. 4 Abs. 1 Bst. a^{bis} BGIAA) – noch anderswo erklärt. Es bleibt deshalb nicht nachvollziehbar, weshalb auf einer ID für den Einsatz in der digitalen Welt ein biometrisches Gesichtsbild enthalten sein soll. Dafür ist entweder eine zwingende Begründung zu liefern oder es ist darauf zu verzichten.

Art. 2 Abs. 3 Bst. a – Verwendung der AHV-Nummer

Der Vernehmlassungsentwurf sieht vor, dass die E-ID auch die AHV-Nummer enthalten soll (Art. 2 Abs. 3 Bst. a VE-BGEID). In den Erläuterungen wird nicht ersichtlich, weswegen die AHV-Nummer enthalten sein muss. Der Zweck des Gesetzes in Art. 1 Abs. 2 Bst. a VE-BGEID, die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten, kann auch ohne die AHV-Nummer erreicht werden. In diesem Sinne genügt die Verwendung der AHV-Nummer dem im Gesetz selbst verankerten Grundsatz der Datensparsamkeit nicht (Art. 1 Abs. 2 Bst. b Ziff. 3 VE-BGEID). Auf die Verwendung der AHV-Nummer in der E-ID ist zu verzichten. Wenn die AHV-Nummer nicht systematisch verwendet werden darf, muss das anwendbare Recht dies gemäss Art. 153c Abs. 2 AHVG explizit ausschliessen. Eine entsprechende Bestimmung ist in das Gesetz aufzunehmen.

Art. 3 und Art. 4 – Prüfung der Identität bei der Ausstellung der E-ID

Die Erläuterungen zu den persönlichen Voraussetzungen für die E-ID (Art. 3 VE-BGEID) und der Ausstellung der E-ID (Art. 4 VE-BGEID) besagen, dass bei der Ausstellung der E-ID auf eine erneute Prüfung der Identität der antragstellenden Person aufgrund der Kosten, Benutzerfreundlichkeit und Geschwindigkeit verzichtet wird. Vorgesehen sei lediglich eine Verifikation der Identität anhand der eingereichten Informationen und der Gesichtsbildverifikation. Gemäss Art. 6 Abs. 5 des neuen Datenschutzgesetzes (nDSG) muss, wer Personendaten bearbeitet, sich über deren Richtigkeit vergewissern. Dieselbe Bestimmung verlangt, dass die Angemessenheit der Massnahmen von der Art und dem Umfang der Bearbeitung sowie vom Risiko abhängt, das die Bearbeitung für die Grundrechte der betroffenen Personen mit sich bringt. Eine nicht korrekt ausgestellte E-ID bringt ein erhebliches Risiko für die Grundrechte der betroffenen Person mit sich (Identitätsdiebstahl). Entsprechend müssen die Massnahmen zur Verhinderung dieses Risikos tief greifen. Kosten, Benutzerfreundlichkeit und Geschwindigkeit sind keine Argumente, um ein solches Risiko für die Grundrechte nicht angemessen zu adressieren. Die entsprechenden Ausführungen in den Erläuterungen sind zu streichen. Das Risiko muss mit gesetzlich festgehaltenen Massnahmen reduziert werden. Sollte auf Stufe des formellen Gesetzes auf zusätzliche Massnahmen verzichtet werden, dann ist die Delegationsnorm in Art. 4 Abs. 5 VE-BGEID dahingehend zu konkretisieren, dass der Bundesrat Massnahmen zur korrekten Feststellung der Identität erlässt.

Art. 7 und Art. 8 – Sorgfaltspflicht und Unterstützung durch die Kantone

Die Verankerung der Sorgfaltspflichten bei der Inhaberin oder beim Inhaber der E-ID nach Art. 7 VE-BGEID muss mit Massnahmen begleitet werden, welche die Inhaberinnen und Inhaber der E-ID bei der Wahrnehmung der Sorgfaltspflichten unterstützen. Die Pflicht für die Kantone in Art. 8 VE-BGEID, Anlaufstellen zur Unterstützung bei der Ausstellung und dem Einsatz der E-ID einzurichten, erachten wir als sinnvoll aufgrund der Nähe der kantonalen Behörden zu den Bürgerinnen und Bürger. Zusätzlich möchten wir anregen, Massnahmen zur Wahrnehmung der Sorgfaltspflichten übersichtlich und gut zugänglich in der Applikation mit der E-ID darzustellen.

Art. 10 – Wahlfreiheit

Wir begrüssen die in Art. 10 VE-BGEID festgehaltene Wahlfreiheit zwischen E-ID und einem anderen Ausweisdokument und den damit einhergehenden Grundsatz der Nichtdiskriminierung zwischen Personen, die eine E-ID nutzen wollen, und Personen, die keine E-ID nutzen wollen.

Art. 10 und Art. 16 – Umsetzung der Datensparsamkeit auf Seite Verifikatorin

Bei der Verwendung von elektronischen Identitätsnachweisen stellt die Überidentifikation ein Problem dar. Der Begriff Überidentifikation bezeichnet die Bearbeitung zu vieler Personendaten bei der Identifikation einer Person für einen bestimmten Zweck. Die Überidentifikation steht im Widerspruch zum Grundsatz der Datensparsamkeit. Das Vorweisen einer E-ID und das Vorweisen von (anderen) elektronischen Nachweisen ist in zwei Bestimmungen der Vorlage geregelt (Art. 10 und Art. 16 VE-BGEID). Hinsichtlich der Überidentifikation erwähnt Art. 10 VE-BGEID zwar die Möglichkeit die E-ID *oder Teile davon* vorzuweisen, der eigentliche Regelungsgegenstand von Art. 10 VE-BGEID ist aber die Pflicht zur Akzeptanz von physischen Ausweisdokumenten. In Art. 16 Abs. 1 VE-BGEID wird geregelt, dass die Inhaberin oder der Inhaber eines elektronischen Nachweises (also auch der E-ID) bestimmt, welche Bestandteile des Nachweises oder davon abgeleiteten Informationen an die Verifikatorin übermittelt werden. Jedoch wird dies in den Erläuterungen von Art. 16 VE-BGEID dahingehend relativiert, dass die Verifikatorin festlegt, welche Daten für den Zugang zu ihren Diensten erforderlich sind und dass dies den Handlungsspielraum der Inhaberin oder des Inhabers begrenzt. Die Erläuterungen bringen klar zum Ausdruck, dass ein Dienst nicht genutzt werden kann, wenn die Inhaberin oder ein Inhaber beschliesst, die von der Verifikatorin verlangten Elemente nicht zu übermitteln. Zwar wird in den Erläuterungen auf den «Grundsatz der Beschränkung der Datenbearbeitung auf das strikte Minimum» (Datenvermeidung und Datensparsamkeit) verwiesen. Weil es sich dabei um einen allgemeinen Grundsatz zum Schutz von Personendaten handle, müsse er im Gesetz nicht erwähnt werden.

Gemäss den Erläuterungen besteht keine Absicht, das Verhalten der Verifikatorin im VE-BGEID weiter zu regulieren. Das Verhalten der Verifikatorin ist datenschutzrechtlich einzig den Regeln des nDSG unterstellt. Dabei öffnet sich allerdings ein Widerspruch zum Zweck des VE-BGEID. Gemäss Art. 1 Abs. 2 Bst. b Ziff. 3 VE-BGEID hat das Gesetz zum Zweck, die Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden und soll dies durch die *Umsetzung des Grundsatzes der Datensparsamkeit* tun. Das Gesetz selbst sieht also vor, dass der Grundsatz der Datensparsamkeit umgesetzt werden muss, wenn bei der Verwendung der E-ID Personendaten bearbeitet werden. Der Zweck in Art. 1 VE-BGEID beschränkt sich dabei nicht auf die Datensparsamkeit auf Seite der Ausstellerin. Zudem braucht es Regeln zur Einhaltung der Datensparsamkeit durch die Verifikatorin. Ein Verweis in den Erläuterungen reicht nicht aus. Es braucht unter Art. 10 VE-BGEID weitere Regeln für das Vorweisen der E-ID: Einerseits soll die Verifikatorin verpflichtet sein, die E-ID nur dann zu verlangen, wenn dies absolut notwendig ist, und andererseits soll die Verifikatorin verpflichtet sein, nur diejenigen Teile der E-ID abzufragen, auf die sie nicht verzichten kann. Die Konkretisierung von datenschutzrechtlichen Grundsätzen im VE-BGEID ist gerechtfertigt, weil die Möglichkeit zur einfachen Identifikation auf elektronischem Weg einen Anreiz für neue und unnötige Identifikationspflichten und Datensammlungen setzt, welche bei der analogen Identifikation gar nicht aufgekommen wären. Zusätzlich soll die Verifikatorin verpflichtet sein, die Daten der Identifikation weder zu speichern noch weiterzugeben noch sonst wie zu bearbeiten, ausser eine anderweitige Pflicht verlangt dies. Eine zusätzliche Sammlung der Daten durch die Verifikatorin zu anderen Zwecken als der Identifikation basierend auf der datenschutzrechtlichen Grundlage der Einwilligung einer Person im privatrechtlichen Kontext wäre in einem zweiten, separaten Schritt nach der Identifikation immer noch möglich. Diese Einwilligung müsste dann in der Form einer freiwilligen Willensäusserung ausserhalb des Identifikationsvorgangs eingeholt werden.

Art. 11 Abs. 4 – Keine Aufbewahrung der über Schnittstellen abgerufenen Daten

Das Informationssystem zur Ausstellung und zum Widerruf der E-ID verfügt zum Bezug der Personenidentifizierungsdaten nach Art. 2 Abs. 2 VE-BGEID über Schnittstellen zu verschiedenen Informationssystemen (Art. 11 Abs. 3 VE-BGEID). Die Erläuterungen halten fest, dass die aufgerufenen Daten weder dupliziert noch im Informationssystem des Fedpols gespeichert werden. Dies geht aus dem Normtext nur implizit hervor, weil die Aufzählung der im Informationssystem zur Ausstellung und zum Widerruf der E-ID enthaltenen Daten die Personenidentifizierungsdaten nach Art. 2 Abs. 2 VE-BGEID nicht enthält (Art. 11 Abs. 2 VE-BGEID). Es ist wünschenswert, wenn dieser essentielle Punkt, dass die abgerufenen Daten nicht aufbewahrt werden im Informationssystem zur Ausstellung und zum Widerruf der E-ID, im Normtext explizit zum Ausdruck kommt. Dazu könnte Art. 11 Abs. 4 VE-BGEID ergänzt werden: Die via Schnittstellen bezogenen Daten werden ausschliesslich zum Zweck der Ausstellung der E-ID bearbeitet und nicht im Informationssystem aufbewahrt. Diese Ergänzung würde die Umsetzung des Prinzips der dezentralen Datenhaltung rechtlich klar verankern.

Art. 16 Abs. 3 – Keine Datenspur bei der Prüfung durch die Verifikatorin im System zur Bestätigung von Identifikatoren

Die Prüfung der E-ID oder anderer elektronischer Nachweise durch die Verifikatorin im System zur Bestätigung von Identifikatoren in Art. 18 VE-BGEID darf keine Personendaten hinterlassen. Es darf nicht ersichtlich sein, wann, wo und für was eine Nutzerin oder ein Nutzer der E-ID oder eines anderen elektronischen Nachweises ihre E-ID oder ihren elektronischen Nachweis eingesetzt hat. Art. 16 Abs. 3 VE-BGEID hält fest, dass die Betreiberin der Systeme keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise hat und möglichst keine Rückschlüsse auf deren Verwendung und die Beteiligten ziehen kann. Es ist nicht klar, warum die Systeme nicht so gestaltet werden müssen, dass gar keine Rückschlüsse gezogen werden können. Auf das Wort «möglichst» ist im Text von Art. 16 Abs. 3 VE-BGEID zu verzichten. Falls aus technischen oder rechtlichen Gründen nicht darauf verzichtet werden kann, ist in den Erläuterungen klar darzulegen, warum eine Ausgestaltung eines Systems, dass keine Rückschlüsse über die Verwendung der E-ID oder anderer elektronischer Nachweise zulässt, nicht möglich ist.

Art. 17 Abs. 3, Art. 18 Abs. 2 und Art. 22 – Verifizierung der Identität von privaten Ausstellerinnen und Verifikatorinnen

Die Öffnung des Systems zur Bestätigung von Identifikatoren für die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bedingt begleitende Massnahmen. Insbesondere ist eine Verifizierung der Identität der privaten Ausstellerinnen und Verifikatorinnen vorzusehen. Entsprechend ist Art. 17 Abs. 3 VE-BGEID zu ändern, dass die Ausstellerinnen und Verifikatorinnen ihre Daten nicht ohne Verifikation selbst in das Basisregister eintragen können. In den Erläuterungen wird das Risiko ausgewiesen, dass Ausstellerinnen oder Verifikatorinnen mit vorgetäuschter Identität elektronische Beweismittel ausstellen könnten. Weil jedoch ein Zulassungsverfahren ressourcenintensiv wäre und zu einem teuren und unnötigen Flaschenhals führen würde, soll auf eine Verifikation verzichtet werden. Art. 22 VE-BGEID sieht vor, dass der Bund öffentlich über Fälle von begründetem Verdacht auf Missbrauch der Vertrauensinfrastruktur informiert. Die Erläuterungen nennen dies als risikomindernde Massnahme. Ein nachträglicher Kommunikationsweg ausserhalb der Systeme der VE-BGEID erscheint jedoch ungenügend, dem benannten Risiko zu begegnen. Die hohen Kosten des Zulassungsprozesses dürfen zudem kein Argument sein, die Risiken des Missbrauchs der Vertrauensinfrastruktur zu erhöhen. Von einer Vertrauensinfrastruktur kann zudem nur gesprochen werden, wenn die Risiken

des Missbrauchs mit allen möglichen Mitteln reduziert werden. Deswegen ist ein Verifizierungsprozess bei der Öffnung für Private vorzusehen.

Art. 23 – Open Source Software

Wir unterstützen die Veröffentlichung des Quellcodes der vom Bund zur Verfügung gestellten Elemente der Vertrauensinfrastruktur zur Umsetzung der E-ID in Art. 23 VE-BGEID. Open Source Software und die damit einhergehende Transparenz trägt zum Vertrauen in technische Lösungen bei, was gerade im sensiblen Bereich des Nachweises der Identität von natürlichen Personen essentiell ist.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim



EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern
rechtsinformatik@bj.admin.ch

Kontakt Anna Pestalozzi
Funktion Stv. Leiterin Sozialpolitik
Tel. direkt 062 206 88 97
E-Mail anna.pestalozzi@procap.ch
Datum 11. Oktober 2022

E-ID-Gesetz, BGEID, Vernehmlassung

Sehr geehrte Damen und Herren

Wir bedanken uns für die Vorlage und den erläuternden Bericht zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Procap begrüsst die Einführung eines staatlichen elektronischen Identitätsnachweises grundsätzlich. In unserer Stellungnahme beschränken wir uns auf den Aspekt der Barrierefreiheit, der beim hier vorliegenden Gesetzesvorhaben von grosser Bedeutung ist.

Grundsätzliche Erwägungen

Procap ist überrascht, dass der Aspekt der E-Accessibility keine Erwähnung in der Vorlage findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt wird. In der Entwicklung sind sämtliche Umsetzungsschritte im Hinblick auf den Standard eCH-0059 Version 3.0 (oder spätere Versionen) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG 2.1 des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, welche von der E-Accessibility-Richtlinie der EU inspiriert sind.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK, Übereinkommen über die Rechte von Menschen mit Behinderungen) unterzeichnet. Artikel 9 der UNO-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen.

Dies schliesst auch die Information und Kommunikation, einschliesslich der entsprechenden Technologien und -systeme ein. Das Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen, kurz BehiG, schreibt in Art. 14 vor, dass die Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten nehmen müssen. Ohne Garantierung der E-Accessibility wären Menschen mit Sehbeeinträchtigung vom staatlichen Angebot in Form eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Brieftasche ausgeschlossen.

Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Praktische Überlegungen

Für Menschen mit Sehbeeinträchtigung stellt die Digitalisierung eine Chance dar zu einem breiteren Zugang zu Dienstleistungen aller Art. Die digitalen Kommunikationskanäle sind das eigentliche Tor zu den Informationen für Menschen mit einer Sehbehinderung. **Zwingende Voraussetzung für die Nutzbarkeit der digitalen Angebote ist aber, dass diese barrierefrei zur Verfügung stehen.** Deshalb muss vor jeder Publikation eines Web-basierten Produkts und auch vor jedem Update geprüft werden, ob dieses barrierefrei zugänglich ist. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das design-for-all-Prinzip zur Anwendung kommen, analog dem europäischen Recht.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Wir verweisen diesbezüglich auch auf die Antwort des Bundesrates auf die Frage [22.7406](#) von Nationalrätin Franziska Ryser, in der er ausführt, dass der standardmässige Einsatz von Usability-Tests im Rahmen der Weiterentwicklung der Instrumente zur Gewährleistung der Barrierefreiheit geprüft wird. Die Freigabe bzw. Lancierung der E-ID darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet, wie aktuelle Beispiele beim Bund (z.B. beim elektronischen Patientendossier, beim elektronischen Einreiseformular oder beim Covid-Zertifikat) oder in den Kantonen (kantonale e-ID Schaffhausen) zeigen.

Anträge

1. Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein eigener Artikel «Barrierefreiheit» aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen die von Antragstellenden, Inhaber:innen einer E-ID, Aussteller:innen, Verifikator:innen und weiteren Usergruppen genutzt oder betrieben werden können.
2. In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein eigenes Kapitel zur Barrierefreiheit aufzunehmen. Dieses beschreibt detailliert, wie die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
3. Zur Kontrolle der Barrierefreiheit sei ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Wir danken Ihnen für die Möglichkeit einer Stellungnahme und bitten Sie höflich um eine wohlwollende Prüfung unserer Anliegen.

Freundliche Grüsse



Martin Boltshauser
Leiter Rechtsdienst
Mitglied der Geschäftsleitung



Anna Pestalozzi
Stv. Leiterin Sozialpolitik

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 11. Oktober 2022

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Einladung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung zu nehmen.

Allgemeine Einschätzung

Der veröffentlichte Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise umfasst nicht nur eine Regelung der nationalen E-ID, sondern integriert auch weitere digitale Nachweise und Akteure (Aussteller und Verifikatoren) sowohl aus dem öffentlichen als auch privaten Sektor in die bundesbetriebene Vertrauensinfrastruktur, was Procivis sehr begrüsst. Dies erlaubt es, in der Schweiz ein E-ID Ökosystem für verschiedenste digitale Nachweise aufzubauen und somit die Durchdringung und ganzheitliche Digitalisierung konsequent zu erzielen.

Voraussetzung dafür ist die Konkretisierung sowie frühzeitige und verlässliche Zurverfügungstellung der Vertrauensinfrastruktur auch an Dritte, um den Auf- und Ausbau, wenn allenfalls auch schrittweise, zu ermöglichen. Zwar ist die technologieneutrale Formulierung der Gesetzgebung gutzuheissen, allerdings sehen wir hier den Bedarf, den Gesetzesentwurf resp. die dazugehörigen Verordnungen und die Erläuterungen aus dem Bericht baldmöglichst weiter zu konkretisieren und die initiale technologische Umsetzung detaillierter zu deklarieren, damit sich alle betroffenen Staatsebenen und Behörden sowie die Privatwirtschaft entsprechend darauf vorbereiten können. Dies wird auch unerlässlich sein, um eine technische Akzeptanz der E-ID bei deren Einführung seitens der Kantone und Gemeinden sowie in der Privatwirtschaft zu gewährleisten und eine schnelle Verbreitung der nationalen E-ID zu ermöglichen.

In diesem Zusammenhang wird im erläuternden Bericht eine Zeitabgabe von 24 bis 36 Monaten zwischen der Lancierung bis zur Inbetriebnahme der Vertrauensinfrastruktur angegeben. Neben der zeitnahen Klärung der erwähnten technologischen Details einer solchen Vertrauensinfrastruktur wäre es für alle Akteure des Schweizer E-ID Ökosystems sehr wichtig zu verstehen, ab welchem Zeitpunkt diese 24 bis 36 Monate anfangen zu laufen - ab dem Moment, wenn von den Bundesbehörden eine erste Testinfrastruktur aufgebaut wird (sprich ab 2022) oder ab dem Moment, wenn das Gesetz vom Parlament verabschiedet und eine allfällige Referendumsfrist verstrichen ist (voraussichtlich nicht vor Ende 2024). Letztere Variante würde bedeuten, dass die produktive Einführung einer nationalen E-ID frühestens ab dem Jahr 2027 möglich wäre. Aus unserer Erfahrung würde das weiter bedeuten, dass eine bereite Durchdringung der Schweizer E-ID wohl nicht vor dem Jahr 2030 zu erwarten wäre.

Weiter bedarf es baldmöglichst genauerer Angaben zum Thema Gouvernanz der Vertrauensinfrastruktur, konkret zu Fragen, ob beliebige Systeme (Wallets, Software zur Ausstellung und Prüfung von Nachweisen) auf die Vertrauensinfrastruktur zugreifen dürfen und ob spezifische Zulassungen dafür vorgesehen sind, welche nicht explizit gesetzlich festgehalten wurden.

Gemäss Gesetzestext baut der Bund einen Ausstellungsprozess für die E-ID auf, bei dem die Daten auf der physischen ID gescannt, mit den Daten vom fedpol gegengeprüft, und ein Abgleich des Gesichts vorgenommen wird. Wird dieser Prozess Teil der Bundeswallet sein und/oder können private Wallets diesen Prozess (vom Bund verarbeitet) einbinden?

Weiter ist unklar, welche Konditionen für die Kantone und Behörden bezüglich der Akzeptanzpflicht der E-ID als Identifikation gelten: Gibt es hier Übergangsfristen beziehungsweise fixe Fristen? Wird die Einführung dieses neuen Identifikationsmittel und die Neuschaffung von Anlaufstellen zur Unterstützung der Ausstellung und dem Einsatz der E-ID personell und/oder finanziell vom Bund (vorab) unterstützt oder müssen die Mittel von den Kantonen sichergestellt werden? Selbstverständlich führen wir unsere Fragen in einem Gespräch weiter aus.

Procivis engagiert sich für Identitäts- und Nachweislösungen unter dem Grundsatz der Datenminimierung, Privacy-by-Design und Dezentralisierung und begrüsst und unterstützt daher grundsätzlich den konsistenten Vorentwurf in diesem Zusammenhang.

Bemerkungen zu einzelnen Bestimmungen

Art. 13

Bei der Widerrufsfrist wird eine Berücksichtigung wie kritisch der entsprechende Nachweis ist, empfohlen, da ein „unverzüglicher“ Widerruf bei niederschweligen Nachweisen wie beispielsweise einer Mitgliederkarte für ein Fitnesscenter o.Ä. nicht verhältnismässig erscheint.

Art. 18

Eine obligatorische Bestätigung ist gemäss Gesetzestext lediglich für Bundes-, Kantons- und Gemeindebehörden vorgesehen. Jedoch wird eine Prüfung von privaten Ausstellerinnen und Verifikatorinnen durch den Bund für einen Aufbau eines Ökosystems als essenziell betrachtet. Durch die Entrichtung von Gebühren (nach Art. 26 Abs. 1) wird bereits eine Registration der entsprechenden Akteure vorgenommen und eine Prüfung könnte im gleichen Prozess erfolgen. Damit Private das Ausstellen eigener Nachweise oder die Prüfung von Nachweisen über die Vertrauensinfrastruktur im Voraus evaluieren und vorbereiten können, sollte transparent vorgelegt werden, ob und unter welchen Bedingungen eine Organisation zur Teilnahme zugelassen ist.

Art. 19

Gemäss Art. 14 kann die Inhaberin oder der Inhaber das technische Mittel zur Aufbewahrung der elektronischen Nachweise selbst wählen. Unter Art. 19 ist festgehalten, dass der Bund den Bürgern ein eigenes Wallet zur Verfügung stellen wird. Im erläuternden Bericht wird jedoch erwähnt, dass auch von Privaten ausgestellte Wallets für die Aufbewahrung und Vorweisung erlaubt sind. Idealerweise sollte dies im Gesetzestext erläutert werden, um die mögliche Anbindung privater Wallets an die Vertrauensstruktur explizit zu erlauben.

Die Herausgeber einer solchen elektronischen Brieftasche können jedoch nach Art. 13 nDSG einem Bewertungs- und Zertifizierungsprozess unterstellt werden. Dieser Prozess würde sich demnach jedoch lediglich obligatorisch und auf Verlangen etablieren und keine mögliche Zertifizierungspflicht zulassen. Zudem werden durch die Softwarekomponenten der Wallet keine Personendaten verarbeitet, sondern dies geschieht durch die Nutzerin oder den Nutzer auf dem Smartphone selbst. Aufgrund der sensiblen Daten, dem kritischen Missbrauchspotential und der heterogenen Bevölkerung in Hinblick auf den Umgang mit digitalen Medien, empfiehlt Procivis eine klare Zertifizierungspflicht gesetzlich für elektronische Brieftaschen einzuführen.

Art. 20

Die freie Nutzung des Bundeswallet ist im Gesetz verankert. Die Auflagen zur Nutzung der Anwendung zur Prüfung von elektronischen Nachweisen wiederum werden offengelassen. Lediglich eine gebührenfreie Nutzung ist nach Art. 26 definiert. Sollen keine genaueren Angaben zu der Offenheit der Vertrauensinfrastruktur gemacht werden, wie dies in der Einleitung angefragt ist, so müssten die Auflagen vorab kommuniziert werden, um den Ausstellern und Prüfern eine vorzeitige Einschätzung der Teilnahme am Ökosystem zu ermöglichen.

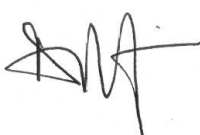
Art. 21

Wie bereits im erläuternden Bericht festgehalten, ist der Bedarf eines Backup-Systems aufgrund eines Verlusts oder Wechsels des Geräts (z.B. Smartphone) naheliegend. Eine Lösung angeboten vom Bund ist lediglich optional festgehalten. Um diesem Bedarf zu entsprechen, sollte auch die explizite Erlaubnis privater Anbieter eines Backup-Systems evaluiert werden. Ein fehlendes Backup-System würde sowohl beim Inhaber als auch bei den privaten Ausstellern und den Behörden einen erheblichen Aufwand und eine Zeitverzögerung bedeuten. Wird beispielsweise die durchschnittliche Nutzungsdauer eines Smartphones betrachtet, fällt diese deutlich kürzer aus als die Gültigkeit der physischen ID. Unter anderem wird daher die Zulassung von privaten Backup-Lösungen empfohlen, falls keine Bundeslösung angeboten wird.

Procivis begrüsst den Vorentwurf grundsätzlich und schätzt insbesondere die Wahrung der Privatsphäre der Nachweisinhaber, die Datenminimierung sowie die Inkludierung weiterer Nachweise des Schweizer Marktes. Eine entsprechende, transparente Kommunikation der Meilensteine in der Entwicklung der Vertrauensinfrastruktur und frühzeitige Beteiligung von Behörden und Privaten wird für eine erfolgreiche Einführung der neuen Infrastruktur und Digitalisierung der Schweiz entscheidend sein. Wir danken für die Berücksichtigung unserer Feedbacks und freuen uns ebenfalls in den weiteren Etappen der Ausarbeitung und Umsetzung des neuen E-ID Gesetzes unseren Beitrag zu leisten. Für weitere Erläuterungen unserer Inputs stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Daniel Gasteiger



CEO und Mitgründer Procivis AG

Pro Senectute Schweiz
Lavaterstrasse 60 · Postfach · 8027 Zürich

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 20. Oktober 2022

Direktion · Alain Huber
Telefon +41 44 283 89 95 · E-Mail alain.huber@prosenectute.ch

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Pro Senectute begleitet Seniorinnen und Senioren beim Einstieg in die digitale Welt. Die kantonalen und interkantonalen Pro Senectute Organisationen befähigen Seniorinnen und Senioren dazu, neue Informationstechnologien zu nutzen und unterstützen sie im Umgang mit der Digitalisierung. Gleichzeitig ist Pro Senectute auch den «Offlinern» behilflich, damit sie vom gesellschaftlichen Leben nicht ausgegrenzt werden.

Gerne nehmen wir die Möglichkeit wahr, im Rahmen des Vernehmlassungsverfahrens zum «Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)» Stellung zu nehmen.

Grundsätzliche Überlegungen

Die Digitalisierung betrifft alle Bevölkerungsgruppen und eröffnet in vielen Lebensbereichen neue Wege. Die Möglichkeit einer sicheren, verlässlichen und eindeutigen elektronischen Identifikation von natürlichen Personen ist ein wesentlicher Punkt dieser Veränderung und gleichzeitig eine Grundvoraussetzung für die weitere Entwicklung.

Der Vorschlag für das neue Bundesgesetz setzt den Rahmen für eine Vertrauensinfrastruktur, deren Kernelement eine staatlich herausgegebene E-ID ist. Es wird angestrebt, dass sich Nutzerinnen und Nutzer künftig sicher, schnell und unkompliziert digital ausweisen können. Pro Senectute ist der Auffassung, dass mit der neu erarbeiteten Gesetzesvorlage die wichtigsten Kritikpunkte, welche in der Abstimmung vom März 2021 zur Ablehnung geführt haben, aufgenommen und gelöst worden sind.

Gemäss der Studie «Digitale Senioren 2020» von Pro Senectute Schweiz, kann die Mehrheit der Seniorinnen und Senioren heute mit digitalen Technologien bestens umgehen. Bei der Einführung von neuen digitalen Produkten, Geräten usw. sehen sich ältere Menschen unterdessen mit weitgehend gleichen Vor- und Nachteilen wie jüngere Personen konfrontiert. Dies gilt auch für die Einführung und Nutzung der E-ID in der Schweiz.

Mit dem freiwilligen Charakter des Bezuges sowie der Verwendung der neuen elektronischen Identität bzw. dank dem Umstand, dass bei einer Annahme der Vorlage die herkömmlichen analogen Registrierungsmöglichkeiten nach wie vor zur Verfügung stehen, ist aus der Sicht von Pro Senectute Schweiz sichergestellt,

Pro Senectute Schweiz

Lavaterstrasse 60 · Postfach · 8027 Zürich · Telefon 044 283 89 89
Fax 044 283 89 80 · info@prosenectute.ch · prosenectute.ch

Postkonto 87-500301-3
IBAN CH91 0900 0000 8750 0301 3



dass «Offliner» nicht ausgeschlossen werden. Zudem ist zu begrüßen, dass beim Einsatz der E-ID für die sie nutzenden, natürlichen Personen keine Gebühr anfällt, was die Nutzung auch für Menschen mit geringen finanziellen Mitteln sicherstellt.

Kompatibilität mit Vorsorgedokumenten

Heutzutage müssen die meisten offiziellen Dokumente handschriftlich unterschrieben werden, um als rechtsgültig zu gelten. Hier bietet die E-ID eine Vielfalt von neuen Möglichkeiten. In diesem Zusammenhang ist aus der Sicht von Pro Senectute Schweiz die Einführung der neuen E-ID insbesondere im Hinblick auf mögliche Entwicklungen hinsichtlich der Erstellung der Vorsorgedokumente bzw. deren Rechtsgültigkeit ausdrücklich zu begrüßen.

Gerade im Bereich der Patientenverfügung, bei welcher eine zeitnahe Auffindbarkeit von entscheidender Bedeutung für die Umsetzung des Patientenwillens ist, wäre eine vollständig digitale Lösung nicht zuletzt auch für deren Nutzung mittels Notfallzugang in einem elektronischen Safe oder im Elektronischen Patientendossier (EPD) zwingend notwendig.

Die aktuell geltenden rechtlichen Rahmenbedingungen verhindern eine vollständig digitale Abwicklung der Vorsorgedokumente. So kann die Patientenverfügung zwar digital ausgefüllt werden, muss aber nach wie vor ausgedruckt und eigenhändig unterschrieben werden (Art. 371 ZGB). Das Verfahren beim Vorsorgeauftrag ist noch komplizierter und vollständig «analog». Es bestehen dabei zwei rechtsgültige Formen (Art. 361 ZGB): Der eigenhändige Vorsorgeauftrag ist gemäss Gesetz von Anfang bis Ende von Hand zu verfassen, zu datieren und eigenhändig zu unterzeichnen. Der öffentlich beurkundete Vorsorgeauftrag wird gemeinsam mit einem Notar oder einer Urkundsperson erstellt und am Schluss von dieser beurkundet.

Mit der Einführung einer E-ID ist daher darauf zu achten, dass auch solche bestehenden Hürden zur Rechtsgültigkeit eines Vorsorgeauftrages und einer Patientenverfügung entfallen. Indem man sich einfach elektronisch sicher und eindeutig identifiziert und sicher signieren kann, könnten in naher Zukunft alle Vorsorgedokumente digital umgesetzt und es könnte auf sämtliche analoge Prozesse verzichtet werden. Die Verwendung der E-ID würde einen klaren Vorteil gegenüber der heutigen Situation schaffen, wo eine komplette Abwicklung der Erstellung von Vorsorgedokumenten aufgrund der aktuell geltenden rechtlichen Hürden leider nicht möglich ist und letztlich deren Auffindbarkeit erschwert. Um die Wirksamkeit der E-ID sowie deren Mehrwert in allen Bereichen sicherzustellen, müssen aus der Sicht von Pro Senectute die Kompatibilität der E-ID mit der Erstellung und Hinterlegung von Vorsorgedokumenten garantiert sowie die derzeit geltenden rechtlichen Formvorschriften in den Artikeln 361 und 371 ZGB entsprechend angepasst werden.

Für die Berücksichtigung unserer Stellungnahme bei der Überarbeitung des Entwurfs sowie des erläutern- den Berichts danken wir Ihnen.

Freundliche Grüsse
Pro Senectute Schweiz



Eveline Widmer-Schlumpf
Präsidentin des Stiftungsrates



Alain Huber
Direktor

Public Affairs und Regulation · Hilfikerstrasse 1 · CH-3000 Bern 65

Bundesamt für Justiz
3003 Bern

Per E-Mail an: E-ID@bj.admin.ch

Bern, 19. Oktober 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz): Stellungnahme SBB.

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme. Die Stossrichtungen der Vorlage sind für die SBB sowohl als Mobilitätsanbieter als auch als Industrieunternehmen von zentraler Bedeutung. Vor allem aber eröffnet die Gesetzesvorlage hohe Nutzenpotentiale für unsere Kundinnen und Kunden.

Mit dem E-ID-Gesetz wird eine Basisinfrastruktur geschaffen, die es der Bevölkerung in der Schweiz erlaubt, jegliche Art von Nachweisen, Zugangsschlüsseln und anderen Berechtigungen aus einer digitalen Briertasche heraus selbstbestimmt und datenschutzkonform verwalten zu können. Zudem schafft es die Voraussetzung, dass organisationsübergreifende Nachweisprozesse medienbruchfrei und damit effizienter als heute gestaltet werden können. Die SBB begrüsst und unterstützt deshalb den Vorentwurf des E-ID-Gesetzes als wichtigen Beitrag zur Digitalisierung der Schweiz.

Die Verbreitung einer E-ID wird massgeblich von den alltäglichen Anwendungen in einem Ökosystem digitaler Nachweise beeinflusst werden. Die E-ID und das Ökosystem müssen deshalb aufeinander abgestimmt wachsen. Der Mehrwert einer künftigen E-ID wird sich für die Bevölkerung schliesslich nur in einem Ökosystem mit mehreren unterschiedlichen Ausstellern bzw. Prüfstellen von digitalen Nachweisen entfalten. Im vorliegenden Gesetzesentwurf erkennen wir noch ein zu starkes Gewicht auf der eigentlichen E-ID und zu wenig Fokus auf dem Ökosystem, in welches die künftige E-ID eingebettet sein muss. Es gilt deshalb auf der Zielebene des E-ID-Gesetzes zu verankern, dass eine Anbindung anderer elektronischer Nachweise, deren Ausstellung und Überprüfung, gewährleistet werden soll.

SBB AG
Public Affairs und Regulation
Hilfikerstrasse 1 · 3000 Bern 65 · Schweiz
luca.arnold@sbb.ch / www.sbb.ch

Der Aufbau eines gemeinsamen Vertrauensnetzwerks für das gesamte Ökosystem muss dabei sichergestellt sein.

Die SBB ist bereit gemeinsam mit ihren Partnern im Bereich der Mobilität ihrer Kundinnen und Kunden auf dem Weg in das neue Ökosystem aktiv zu begleiten und zu unterstützen, damit sich die grossen Nutzenpotenziale eines E-ID-Ökosystems für die Schweiz erschliessen lassen. Gerne bringen wir uns mit unseren digitalen Anwendungen in die Diskussion ein, um einen konkreten Beitrag zur Entwicklung des E-ID-Ökosystems zu leisten.

Für Fragen sowie für eine Kontaktaufnahme für die weiteren Diskussionen auf Fachebene steht Ihnen Vitus Ammann (vitus.ammann@sbb.ch) zur Verfügung.

Freundliche Grüsse

Jochen Decker
Mitglied der Konzernleitung
Chief Information Officer

Luca Arnold
Leiter Regulation und Internationales

Kopie an:

- Gery Balmer, Vizedirektor, Abteilungschef Politik, BAV

Réponse à la consultation

Groupe de travail TIC du CSA

Loi sur l'e-ID : prise de position du Conseil Suisse des Aînés

Le Conseil Suisse des Aînés - CSA a pris position dans le cadre de la consultation organisée par la Confédération sur la future loi sur l'e-ID, établissant les bases légales nécessaires à la mise en place et l'utilisation d'une identité électronique reconnue par les administrations suisses.

Fondamentalement, le CSA salue la rapidité avec laquelle le Conseil fédéral a su réagir après l'échec de la votation populaire de mars 2021 à laquelle le CSA avait manifesté son opposition, s'agissant d'un élément important d'accès aux prestations publiques numériques.

Le CSA salue notamment les choix effectués pour cette nouvelle mouture, à savoir une approche de l'identité auto-souveraine (*self sovereign identity*), une infrastructure de confiance gérée directement par la Confédération, le respect de la vie privée dès la conception (*privacy by design*), la volonté de limitation des flux de données nécessaires (principe d'économie des données) une protection des données personnelles et un enregistrement décentralisé des données. Des éléments qui tiennent compte des craintes exprimées en mars 2021 par les seniors et rentiers AVS représentés par le CSA.

Enfin, le CSA relève en particulier le souci d'interconnexion avec les systèmes des pays européens voisins, éléments importants au regard des seniors faisant partie pour nombre d'entre eux des voyageurs de ce pays.

Toutefois, il s'agira de porter une attention particulière sur un certain nombre de points essentiels pour les seniors, plus particulièrement de celles et ceux qui ne sont pas familiarisés avec les technologies modernes du monde virtuel et pour lesquels la digitalisation représente un handicap majeur.

Il s'agira également de tenir compte de cette frange de la population de seniors résidents qui résident sans papier, des touristes de longues durées et des seniors dans des situations précaires.

En conclusion, le Conseil Suisse des Aînés est favorable et soutient la nouvelle proposition de la loi sur l'e-ID du Conseil fédéral.

Le Conseil Suisse des Aînés
La Coprésidence



Bea Heim
079 790 52 03



Roland Grunder
079 669 98 02

e-ID IN SWITZERLAND

PUBLIC CONSULTATION ON THE e-ID LAW, LeID

SICPA's response

October 2022

Présented by:
SICPA SA
AV DE FLORISSANT 41,
1008 PRILLY
Suisse



Enabling trust

table of contents

1	CONTEXT & OBJECTIVES OF DOCUMENT.....	3
2	PROPOSAL FOR CHANGES.....	4
2.1	ACCESSIBILITY FOR ALL	4
2.2	IDENTIFICATION (ART1).....	4
2.3	IDENTIFIER CONFIRMATION SYSTEM (ART18 AL1 ET AL2).....	5
2.4	SOURCE CODES (ART23)	5
3	QUESTIONS.....	6
3.1	PHOTOGRAPHS (ART2 ET ART4 AL4).....	6
3.2	REVOCATION IN THE EVENT OF DEATH	6
3.3	PHYSICAL-DIGITAL EQUIVALENCE (ART9).....	6
3.4	UNIQUENESS OF E-ID (ART5 E).....	7
3.5	MANDATE (ART 15 AL1).....	7
3.6	IDENTITY OF ORGANISATIONS (ART15 AL2)	7
3.7	IDENTITY OF ISSUERS AND VERIFIERS (ART17 AL3).....	8
3.8	VERIFICATION WITHOUT INTERNET ACCESS (OUT OF BAND)	8
3.9	WALLET ACCESS (ART19)	8
3.10	SERVICE PROVIDER (ART19).....	9
4	CONCLUSION	9

1 CONTEXT & OBJECTIVES OF DOCUMENT

At its June 29, 2002, meeting, the Federal Council sent out for consultation a draft federal law on electronic identity and other electronic means of proof (LeID).

The objective of this document is to propose some modification to the draft law and to raise some questions concerning its implementation, the aim being to inform the various stakeholders who are evaluating the impacts on existing digital identity systems and processes.

2 PROPOSAL FOR CHANGES

The draft bill on the e-ID (LeID) provides details of the applications, the need for interoperability with European neighbours (Art19 and Art27) and the division of roles and responsibilities of the Confederation, Fedpol and the Cantons (Art4 and Art8). It is important that the law remains technologically neutral (Art25) to allow for future developments. In our view, the current draft satisfies the legislative requirements that would allow the harmonious introduction of digital identity in Switzerland.

Nevertheless, we would like to raise the following points for further consideration.

2.1 ACCESSIBILITY FOR ALL

The first point, which is related to the very definition of e-ID, is accessibility of tools for every citizen, regardless of age and in the case of disability (societal inclusion). The technologies put in place should benefit everyone and it is important that usability aspects are taken into account by technology and service providers right from the design stage. For example, on 28 May 2019, the government of Luxembourg decided to enshrine such a principle in law¹.

The Federal Office of Justice (FOJ) could guarantee accessibility for all by specifying this principle in the law, which would oblige the various providers to comply with relevant current standards in Switzerland and use all available tools, for example those offered by providers of mobile phone operating systems, to make life easier for people with disabilities. It is also important to consider technological inclusion for people who do not have a mobile phone or smartphone.

2.2 IDENTIFICATION (ART1)

Art. 1, para. 2a states:

"Aims to ensure secure identification, by means of an e-ID, between private persons and between private persons and authorities;"

In order to meet ambition level 3, why not also include legal entities? The e-ID would be a very useful means for companies to securely identify their customers or business partners, for example.

PROPOSAL

a. "Aims to ensure secure identification, by means of an e-ID, between private persons and between private persons and authorities or legal entities;"

¹ <https://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a373/jo>

2.3 IDENTIFIER CONFIRMATION SYSTEM (ART18 AL1 ET AL2)

According to Article 18(1): *"From the outset, the Confederation is delegated the competence to confirm the identity of federal, cantonal and communal authorities that act as issuers and verifiers. It entrusts an entity within the federal administration with the management and maintenance of the identifier confirmation system. This entity maintains a list of authorities acting as issuers and verifiers which it publishes on its website and updates regularly."* In 2022, Switzerland has 2,145 municipalities², more than 570,000 companies and many cantonal services and registers. Within the framework of federalism, decentralisation of the management of issuers and verifiers to the cantons should therefore be considered. Indeed, complete centralisation of this function risks being very cumbersome to manage by the designated administration. It could instead be based on existing systems such as cantonal commercial registers or relevant umbrella associations (banks, insurance companies, etc.). It would also be good to clarify what the conditions are, in particular the financial conditions (Art. 26), to be part of the identifier confirmation system (Art. 28 d).

PROPOSAL

Add to Art. 18, para. 2: *"The Confederation may set up a system for delegating the confirmation of issuers and verifiers to public and private bodies. These delegations shall be secured by an associated electronic evidence system"*.

2.4 SOURCE CODES (ART23)

Art23 states that the Confederation will publish the source code of the components of the trust infrastructure that it makes available. In its current form, it seems to make the publication of the source codes of all components mandatory, which could in some cases prove problematic in terms of implementation, licensing or security.

In the draft Federal Act on the Use of Electronic Means for the Execution of Tasks of the Authorities (LMETA)³, Article 9 para. 1 resolves this uncertainty by formulating this point as follows:

"Insofar as this is possible and sensible and provided that the rights of third parties are preserved, the federal authorities subject to this Act shall publish the source code of the software they develop or have developed for the performance of their tasks."

PROPOSAL

In order to remove any legal ambiguity on this point and to be in line with the draft LMETA, it is proposed, for example, to complete Article 23 in the following way (using the terms of Art 9.1 of the LMETA):

"The Confederation shall publish the source code of the elements of the trust infrastructure which it makes available, insofar as this is possible and sensible and provided that the rights of third parties are preserved."

² <https://www.agychapp.bfs.admin.ch/fr/state/results?SnapshotDate=01.05.2022>

³ <https://www.news.admin.ch/newsd/message/attachments/70501.pdf>

3 QUESTIONS

In addition to the points raised in chapter 2 of this document, SICPA has identified some questions related to the practical side of the implementation of digital identity. These questions will no doubt be answered in more specific technical orders. However, they may also influence certain articles of the draft LeID law. A list of these questions is provided below:

3.1 PHOTOGRAPHS (ART2 ET ART4 AL4)

Is a photograph considered as "personal data" according to art. 5.a of the Data Protection Act (DPA)⁴ in the same way as a name and surname, or should it be considered as biometric data and therefore sensitive according to art. 5.c.4 of the DPA? If it is considered as biometric data, this would require special treatment in terms of encryption and security. According to art. 5.c.4 of the DPA, biometric data allow a natural person to be uniquely identified and the photo could be considered as such. As a reminder, the photograph is displayed on the personal information page of the passport and identity card in the same way as the surname or first name and in contrast to biometric data which are only accessible by the issuing authority. This is important insofar as the passport photograph, being part of the attributes of the e-ID, would not require any particular cryptographic processing and would therefore be at the same level of protection as the surname, the first name or the date of birth.

As an identity photograph can be exchanged as an attribute and be visible for the purpose of identification during a face-to-face check, in the same way as the name and surname, it seems that this attribute of the e-ID should not be considered as a sensitive element in the same way as biometric data. Also, if compromised, a passport photograph can easily be replaced by another photograph of the holder, whereas biometric data in principle and by definition do not change. It would be advisable to clarify this ambiguity in art. 2 of the LeID.

3.2 REVOCATION IN THE EVENT OF DEATH

Article 5 defines that Fedpol is responsible for revoking the e-ID upon knowledge of the death of the holder. It would be advisable to clarify the process of transmitting the death notification from end to end (e.g. via the AVS number).

3.3 PHYSICAL-DIGITAL EQUIVALENCE (ART9)

The draft law establishes legal equivalence of a state-issued electronic identity and a recognised identity document such as an ID card or passport (Art9) which would cover ambition level 1. This would allow, for example, FINMA to adapt the regulations relating to knowledge of bank account holders in Switzerland and to simplify the processes and user experience in the banking sector. However, this draft only covers the equivalence of the identity document and not all other certificates issued by federal, cantonal or communal authorities to cover level of ambition 2. This may considerably slow down the adoption of electronic identity as it would probably require a change of law for each document. According to Art. 9: *"Any authority or service that performs public tasks must accept the e-ID when it uses electronic identification"*. Similarly, all electronic certificates issued by federal, cantonal or municipal authorities should have legal value and should also be accepted as such.

⁴ <https://www.fedlex.admin.ch/eli/fga/2020/1998/fr>

In Luxembourg, for example, the only document that has a physical-digital legal equivalence is the certificate of residence⁵. Only this document can be recognised and used by banks in its digital form, which limits the transition to a digital society. The EU eIDAS regulation is being adapted to address this problem by providing a framework of trust and legal validity of digital identity allowing equivalence of all certificates issued by member states within and across borders⁶. This new regulation would thus avoid the need for all Member States to adapt their legislation to cover the equivalence of all state-issued certificates. As Switzerland is not part of the European Union, this new regulation will not benefit the Swiss legislative framework. The objectives of the LMETA seem to cover part of these needs and it would be wise for this law to be a legal basis for adapting federal and cantonal regulations quickly after the introduction of the LeID.

Furthermore, Art. 1 para. 2.d mentions the standardisation of the e-ID. It would also be necessary to standardise all certificates issued by the state, such as certificates of residence issued by the communes, birth certificates or driving licences. It would be sensible for the definition of these certificates to be regulated by a body at federal level in order to guarantee inter-cantonal and inter-municipal interoperability and equivalence.

3.4 UNIQUENESS OF E-ID (ART5 E)

Article 5e appears to indicate that a person can only have one e-ID. While it is obvious that a person has only one identity, in the physical world it is common for a person to have several variations of identity, such as passport and ID card. It is also not uncommon for a person to have more than one mobile phone. Could each device have a wallet that contains a version of the e-ID?

An important question for technical implementation is what the issued eID credential will be linked to (the mobile phone (e.g. IMEI number), other ...)?

3.5 MANDATE (ART 15 AL1)

A related issue is the question of the mandate (Art4 para 2 and Art15). In many cases a natural person may be called upon to act on behalf of another natural or legal person and would need either to hold an electronic certificate belonging to that other person in his portfolio, or at least to have access to the portfolio. This includes the case of parents and their children (<14 or even <18), legal representatives in the event of bereavement or incapacity of any kind, or representatives of a legal person. It is a question of clarifying from the point of view of the law the principle and, if possible, the processes that would govern such cases so that technology providers can respond adequately to this problem. In particular, is it possible for the legal representative (e.g. parent) to hold the eID in their wallet? If so, in the case of parents for example, can this eID be stored with two different people (e.g. father and mother)? Or does the child have to have his or her own phone and wallet, which raises the problem of access to the wallet (Art14)?

3.6 IDENTITY OF ORGANISATIONS (ART15 AL2)

At the same time as the e-ID for citizens, an identity for organisations (legal entities) should be considered. The European Commission is working on this matter because the two concepts of identity are linked, particularly in the case of mandates where a natural person (company representative)

⁵ <https://legilux.public.lu/eli/etat/leg/rgd/2016/03/29/n2/jo>

⁶ <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

represents a legal person for legal or financial transactions, for example. It is in Switzerland's interest to establish an identity system for organisations in parallel with an e-ID for citizens that is compatible with the schemes set up by the European Commission. In particular, it is necessary to clarify the conditions for using the e-ID in the context of a mandate and to clarify the decentralised role of the cantonal commercial registers in this process.

3.7 IDENTITY OF ISSUERS AND VERIFIERS (ART17 AL3)

According to Article 17(3): "Verification of the identity of issuers or verifiers is not required before they can use the base register. This would imply a resource-intensive authorisation procedure, which would inevitably lead to an expensive and unnecessary bottleneck. Of course, there is a risk that issuers or verifiers could issue electronic evidence by impersonating them. However, this risk is mitigated by the publication of information on cases of well-founded suspicion of misuse of the trust infrastructure in accordance with Article 22 and excluded by the system of confirmation of identifiers provided for in Article 18. The exclusion of registered issuers or verifiers is not technically possible in the base register, but it is possible in the system for confirming identifiers in accordance with Article 18."

On the other hand, Article 7 Paragraph 1 describes the duty of care of an e-ID holder: *"He must take the necessary measures that are reasonably required under the circumstances to prevent any misuse of his eID."*

The article (Art17 AL3) may prove problematic for citizen trust. Relying solely on the citizen's duty of care (Art 7 para 1) while leaving the door open to identity theft by excluding bad issuers/verifiers only after the fact may hinder adoption of the system by citizens. It is therefore essential that during the verification process, the citizen has a clear and easy way to identify the verifier who is making the request to share wallet attributes. The citizen must be able to easily know whether the verifier is part of the identifier confirmation register and if not, a warning notice must appear. This way the citizen can be sure that he or she is only sharing data with legitimate verifiers.

3.8 VERIFICATION WITHOUT INTERNET ACCESS (OUT OF BAND) (ART18 AL3 ET ART20)

In the real world, i.e. during face-to-face verification, should e-ID attributes and issuers/verifiers be verifiable without an internet network (technological inclusion) knowing that technological solutions make this possible?

3.9 WALLET ACCESS (ART19)

Does the Confederation intend to provide the necessary tools to restrict access to the wallet (e.g. Biometrics, Login/Password, ...)? Following people's response to the Federal Act on eID it would seem appropriate for the Confederation to take on this responsibility and to not use similar functions made available by phone manufacturers or their operating systems, in order to have end-to-end control over security (e.g. via the use of biometric templates).

3.10 SERVICE PROVIDER (ART19)

Will the service provider keep the flexibility to delegate, when this is required, the operation of some parts of the infrastructure to a third party, while ensuring that this third party remains under full control of the federal authorities?

4 CONCLUSION

The Self-Sovereign Identity (SSI) approach has been recognised by many public and private stakeholders as the approach of choice for the transition to digital identity of the future. In view of the market trends mentioned above, the expectations of the Swiss population and the technical constraints, SSI appears to be the most suitable approach to ensure a high level of adoption of eID in Switzerland. Even though it is a new approach and a number of questions remain open, there is a good chance that it will become the next generation Internet identity system. As other countries such as Canada and the United States, and the European Union, are currently conducting similar pilot projects to assess the impact on their existing infrastructure and processes, Switzerland could also be among the SSI pioneers shaping the digital transactions of tomorrow.

The draft LeID law submitted for consultation by the Federal Office of Justice (FOJ) lays the foundation for an SSI-based implementation of digital identity in Switzerland. This draft allows the various state and private sector actors to prepare for the adaptation and migration of existing processes and technologies. SICPA has raised a number of issues that could be critical to the implementation and operational management of this platform in Switzerland. We hope that we can initiate open discussions on these issues and contribute to a successful and smooth implementation of digital identity in Switzerland.

We remain at your disposal to share our experience and vision in this field or for any additional information.



SICPA SA
Headquarters
Av de Florissant 41
1008 Prilly
Switzerland

Tel +41 21 627 55 55
Fax +41 21 627 57 27
www.sicpa.com/contact
www.sicpa.com

e-ID en SUISSE

CONSULTATION PUBLIQUE SUR LA LOI SUR l'e-ID, LeID

Réponse de SICPA

Octobre 2022

Présenté par:
SICPA SA
AV DE FLORISSANT 41,
1008 PRILLY
Suisse



Enabling trust

TABLE DES MATIÈRES

1	LE CONTEXTE & OBJECTIFS DU DOCUMENT	3
2	PROPOSITIONS DE MODIFICATION	4
2.1	ACCESSIBILITÉ POUR TOUS	4
2.2	IDENTIFICATION (ART1)	4
2.3	SYSTEME DE CONFIRMATION DES IDENTIFIANTS (ART18 AL1 ET AL2)	5
2.4	CODES SOURCE (ART23)	5
3	QUESTIONS.....	6
3.1	PHOTOGRAPHIE (ART2 ET ART4 AL4)	6
3.2	REVOCATION EN CAS DE DECES (ART5).....	6
3.3	EQUIVALENCE PHYSIQUE-NUMÉRIQUE (ART9).....	6
3.4	UNICITE DE L'EID (ART5 E).....	7
3.5	MANDAT (ART 15 AL1).....	7
3.6	IDENTITÉ D'ORGANISATIONS (ART15 AL2).....	8
3.7	IDENTIFICATION DES EMETTEURS ET DES VERIFICATEURS (ART17 AL3)	8
3.8	VÉRIFICATION SANS RÉSEAU INTERNET (OUT OF BAND) (ART18 AL3 ET ART20	
3.9	ACCÈS AU PORTEFEUILLE (ART19).....	9
4	CONCLUSION	10

1 LE CONTEXTE & OBJECTIFS DU DOCUMENT

Lors de sa séance du 29 juin 2022, le Conseil fédéral a envoyé en consultation un avant-projet de loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID).

L'objectif de ce document est d'apporter des propositions de modification de cet avant-projet et de poser quelques questions concernant la mise en œuvre de ce dernier afin d'éclairer les différents intervenants qui évaluent les impacts sur les systèmes d'identité digitale et les processus existants.

2 PROPOSITIONS DE MODIFICATION

L'avant-projet de loi sur l'e-ID (LeID) détaille bien les aspects applicatifs, les besoins d'interopérabilité avec nos voisins européens (Art19 et Art27) et la répartition des rôles et responsabilités de la Confédération, de la Fedpol et des Cantons (Art4 et Art8). Il est important qu'il reste neutre technologiquement parlant (Art25) afin de garantir les possibles évolutions en la matière. Par conséquent, de notre point de vue, cet avant-projet sous sa forme actuelle satisfait aux besoins législatifs qui permettraient une introduction harmonieuse de l'identité numérique dans notre pays.

Néanmoins, nous souhaitons soulever les points ci-dessous, qui méritent d'être approfondis.

2.1 ACCESSIBILITÉ POUR TOUS

Le premier point qui vient à l'esprit dans la définition même de l'e-ID est la question de l'accessibilité de ces outils pour chaque citoyen, quel que soit leur âge ou leur situation de handicap (inclusion sociétale). Les technologies mis en place devraient bénéficier à chacun et il semble important que les aspects d'ergonomie soient pris en compte par les fournisseurs de technologie et de service dès la conception. Par exemple, le 28 mai 2019, le gouvernement du Luxembourg a décidé d'inscrire dans la loi un tel principe¹.

L'OFJ pourrait garantir l'accessibilité pour tous en spécifiant ce principe dans le cadre de cette loi, ce qui obligerait les différents prestataires à se conformer aux normes existantes aujourd'hui en Suisse en la matière et à utiliser tous les outils mis à disposition par exemple par les fournisseurs de systèmes d'exploitation des téléphones portables pour faciliter la vie aux personnes en situation de handicap. Il est de plus également important de prendre en considération l'inclusion technologique, pour les personnes ne possédant pas de téléphone portable ou de Smartphone.

2.2 IDENTIFICATION (ART1)

L'Art. 1, Al2a stipule :

"Elle vise à garantir une identification sûre, à l'aide d'une e-ID, entre personnes privées et entre personnes privées et autorités ;"

En vue de satisfaire le niveau d'ambition 3, pourquoi ne pas inclure également les personnes morales ? En effet, l'e-ID sera un moyen très utile pour les entreprises pour identifier de manière sûre leurs clients ou leurs partenaires commerciaux par exemple.

PROPOSITION

- a. *" Elle vise à garantir une identification sûre, à l'aide d'une e-ID, entre personnes privées et autorités et entre personnes privées ou morales ;"*

¹ <https://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a373/jo>

2.3 SYSTEME DE CONFIRMATION DES IDENTIFIANTS (ART18 AL1 ET AL2)

Selon l'article 18 Al1, « dès le début, la Confédération se voit déléguer la compétence de confirmer l'identité des autorités fédérales, cantonales et communales qui agissent en tant qu'émetteurs et vérificateurs. Elle charge une entité au sein de l'administration fédérale de gérer et d'entretenir le système de confirmation d'identité. Cette entité maintient une liste d'autorités agissant en tant qu'émetteurs et vérificateurs qu'elle publie sur son site et la met régulièrement à jour ».

En 2022, la Suisse compte 2'145² communes, plus de 570'000 sociétés et beaucoup de services et de registres cantonaux. Dans le cadre du fédéralisme, une décentralisation au niveau des cantons de la gestion des émetteurs et vérificateurs serait donc à étudier. En effet, une centralisation complète de cette fonction risque d'être très lourde à gérer par l'administration désignée alors qu'elle pourrait s'appuyer sur des systèmes existants comme les registres du commerce cantonaux ou des associations faitière par branche économique (banques, assurances, ...). Il serait bien également de clarifier quelles sont les conditions, notamment financières (Art26), pour faire partie de ce système de confirmation des identifiants (Art28 d).

PROPOSITION

Ajouter à l'Art 18. al 2. "La Confédération pourra mettre en place un système de délégation de ces confirmations d'émetteurs et de vérificateurs auprès d'instances publiques et privées. Ces délégations seront sécurisées par un système de preuves électroniques associé".

2.4 CODES SOURCE (ART23)

L'Art23 mentionne que la Confédération publiera le code source des composants de l'infrastructure de confiance qu'elle met à disposition. Sous sa forme actuelle, il semble rendre obligatoire la publication des codes source de tous les éléments, ce qui pourrait dans certains cas se révéler problématique au niveau de l'implémentation, de licences ou au niveau de la sécurité.

Dans le projet de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA)³, l'article 9 Al.1 résout cette incertitude en formulant ce point de la manière suivante : " Dans la mesure où cela est possible et judicieux et pour autant que les droits des tiers soient préservés, les autorités fédérales soumises à la présente loi publient le code source des logiciels qu'elles développent ou font développer pour l'exécution de leurs tâches."

PROPOSITION

Afin de lever toute ambiguïté juridique quand à ce point et être aligné par rapport au projet de la LMETA, il est proposé par exemple de compléter l'Article 23 de la manière suivante (reprenant les termes de l'Art 9.1 de la LMETA) :

"La Confédération publie le code source des éléments de l'infrastructure de confiance qu'elle met à disposition, dans la mesure où cela est possible et judicieux et pour autant que les droits des tiers soient préservés."

² <https://www.agychapp.bfs.admin.ch/fr/state/results?SnapshotDate=01.05.2022>

³ <https://www.news.admin.ch/news/message/attachments/70501.pdf>

3 QUESTIONS

En complément des points soulevés au chapitre 2 de ce document, SICPA a identifié quelques questions liées au côtés pratiques de l'implémentation de l'identité numérique. Ces questions trouveront certainement des réponses dans des ordonnance spécifiques à ces aspects plus techniques. Cependant, elles peuvent également conditionner certains articles de l'avant-projet de loi LeID. Vous trouverez donc ci-dessous une liste de ces questions :

3.1 PHOTOGRAPHIE (ART2 ET ART4 AL4)

Est-ce que la photographie est considérée comme « donnée personnelle » selon l'art5.a de la loi sur la protection des données (LPD)⁴ au même titre que le nom et le prénom, ou est-ce qu'elle doit être considérée comme donnée biométrique et donc sensible selon l'art5.c.4 de la LPD ? En effet, si elle est considérée comme donnée biométrique ce qui nécessiterait un traitement particulier en termes de cryptographie et de sécurité. En effet, selon l'art5.c.4 de la LPD, une donnée biométrique permet d'identifier une personne physique de manière univoque et la photo pourrait être considérée comme tel. Pour rappel, la photographie est exposée sur la page de personnalisation du passeport et de la carte d'identité au même titre que le nom ou le prénom et à contrario des données biométriques qui ne sont accessibles que par l'autorité émettrice dans le passeport. Ceci est important dans la mesure où la photographie d'identité faisant partie des attributs de l'e-ID ne nécessiterait pas de traitement cryptographique particulier et serait ainsi au même niveau de protection que le nom, le prénom ou la date de naissance.

Comme une photographie d'identité peut être échangée comme attribut et visible pour permettre une identification lors d'un contrôle en présentiel, au même titre que le nom et le prénom, il semble que cet attribut de l'e-ID ne doit pas être considéré comme élément sensible au même titre que des données biométriques. Également, si compromise, une photographie d'identité peut être facilement remplacée par une autre photographie du détenteur, alors que les données biométriques sont en principe et par définition invariants. Il serait judicieux de clarifier cette ambiguïté à l'art2 de la LeID.

3.2 REVOCATION EN CAS DE DECES (ART5)

L'article 5 définit que Fedpol est responsable de révoquer l'e-ID s'il prend connaissance du décès de son titulaire. Il serait judicieux de pouvoir clarifier le processus de transmission de la notification de décès de bout en bout (p.ex via le numero AVS).

3.3 EQUIVALENCE PHYSIQUE-NUMÉRIQUE (ART9)

Cet avant-projet établi une équivalence légale d'une identité électronique fourni par l'état et d'un document d'identité reconnu comme la carte d'identité ou le passeport (Art9) ce qui couvrirait le niveau d'ambition 1. Ceci permettrait par exemple à la FINMA d'adapter les règlements relatifs à la connaissance des titulaires de comptes bancaires en Suisse et de simplifier les processus et l'expérience utilisateur dans le domaine bancaire. Cependant, cet avant-projet ne couvre que l'équivalence du document d'identité et pas tous les autres certificats émis par les autorités fédérales, cantonales ou communales pour couvrir le niveau d'ambition 2. Ceci risque de ralentir considérablement l'adoption de l'identité électronique car cela nécessiterait probablement une modification de loi pour chaque

⁴ <https://www.fedlex.admin.ch/eli/fga/2020/1998/fr>

document. Selon l'art9, « toute autorité ou tout service qui accomplit des tâches publiques doit accepter l'e-ID lorsqu'il recourt à l'identification électronique ». De même, il faudrait que tous certificats électroniques émis par les autorités fédérales, cantonales ou communales ait valeur légale et doive également être accepté en tant que tel.

Au Luxembourg par exemple, le seul document qui bénéficie d'une équivalence légale physique-numérique est le certificat de résidence⁵. Seul ce document peut être reconnu et utilisé par les banques sous sa forme numérique ce qui limite la transition vers une digitalisation de la société. Le règlement européen eIDAS est en train d'être adapté pour palier à ce problème en fournissant un cadre de confiance et une validité légale de l'identité numérique permettant l'équivalence de tous les certificats émis par les états membres à l'intérieur et au-delà des frontières⁶. Ce nouveau règlement éviterait ainsi à tous les états membres de devoir adapter leur législation pour couvrir l'équivalence de tous les certificats émis par l'état. La Suisse ne faisant pas partie de l'union européenne, ce nouveau règlement ne bénéficiera pas au cadre législatif Suisse. Les objectifs de la LMETA semblent couvrir une partie de ces besoins et il serait judicieux que cette loi puisse être une base légale pour adapter les règlements fédéraux et cantonaux rapidement après l'introduction de la LeID.

Par ailleurs, l'art1 al2.d fait mention de normalisation de l'e-ID. De même, il serait nécessaire que toutes les attestations émises par l'état comme par exemple les attestations de domicile émises par les communes, les certificats de naissance ou les permis de conduire soient normalisés. Il serait judicieux que la définition de ces attestations soit réglementée par un organisme au niveau fédéral afin de garantir une interopérabilité et une équivalence intercantonale et intercommunale.

3.4 UNICITE DE L'EID (ART5 E)

L'Article 5e semble indiquer qu'une personne ne peut avoir qu'une seule e-ID. S'il est évident qu'une personne n'a qu'une seule identité, on constate dans le monde physique que cette personne peut posséder plusieurs déclinaisons de son identité, comme son passeport et sa carte d'identité. De même, il arrive fréquemment qu'une personne possède également plusieurs téléphones portables. Est-ce que chaque appareil pourrait avoir un portefeuille/wallet qui contiendrait une version (ou instance) de l'e-ID ?

Une question qui concerne l'implémentation technique de manière importante est de savoir à quoi sera lié le credential eID émis (au téléphone portable (eg IMEI number), autres ...) ?

3.5 MANDAT (ART 15 AL1)

Une question liée au point précédent est la question du mandat (Art4 Al2 et Art15). En effet, dans plusieurs cas de figure une personne physique peut être appelé à agir au nom d'une autre personne physique ou morale et aurait besoin soit de détenir une attestation électronique appartenant à cette autre personne dans son portefeuille ou tout du moins d'avoir accès à son portefeuille. Il s'agit notamment des cas de parents et de leurs enfants (<14 ou même <18), de représentants légaux en cas de deuil ou d'incapacité de tout type ou représentant d'une personne morale. Il s'agit de clarifier du point de vue de la loi le principe et si possible les processus qui pourraient régir de tels cas de figure afin que les fournisseurs technologiques puissent répondre de manière adéquate à cette problématique. Notamment, est-il envisageable pour le représentant légal (p.ex des parents) d'avoir l'eID dans leur

⁵ <https://legilux.public.lu/eli/etat/leg/rgd/2016/03/29/n2/jo>

⁶ <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

portefeuille ? Si oui, dans le cas des parents par exemple, est-ce que cette eID peut être stockée chez deux personnes différentes (p. ex père et mère) ? Où est-ce que l'enfant doit avoir son propre téléphone et son propre portefeuille, ce qui pose le problème de l'accès au portefeuille) (Art14)?

3.6 IDENTITÉ D'ORGANISATIONS (ART15 AL2)

En même temps que l'e-ID pour les citoyens, une identité pour organisations (personnes morales) serait à envisager. En effet, la commission européenne travaille sur ce sujet car les deux concepts d'identité sont liés notamment dans le cas de mandat où une personne physique (référént d'une entreprise) représente une personne morale pour des transactions légales ou financières par exemple. La Suisse a tout intérêt à mettre en place une identité pour organisation en parallèle d'un e-ID pour citoyens qui soit compatible avec les schémas mis en place par la commission européenne. Il s'agit notamment de clarifier les conditions d'utilisation de l'e-ID dans le cadre d'un mandat et de clarifier le rôle décentralisé des registres du commerce cantonaux dans ce processus.

3.7 IDENTIFICATION DES EMETTEURS ET DES VERIFICATEURS (ART17 AL3)

Selon l'article 17 Al3, « la vérification de l'identité des émetteurs ou des vérificateurs n'est pas nécessaire avant qu'ils ne puissent utiliser le registre de base. Cela impliquerait une procédure d'autorisation nécessitant des ressources importantes, ce qui conduirait inévitablement à un goulot d'étranglement coûteux et inutile. Certes, il existe un risque que des émetteurs ou des vérificateurs puissent délivrer des preuves électroniques en usurpant leur identité. Ce risque est toutefois atténué par la publication d'informations sur les cas de soupçons fondés d'utilisation abusive de l'infrastructure de confiance, conformément à l'art. 22, et exclu par le système de confirmation des identifiants prévu à l'art. 18. L'exclusion d'émetteurs ou de vérificateurs enregistrés n'est techniquement pas possible dans le registre de base, mais elle l'est dans le système de confirmation des identifiants selon l'art. 18 ».

D'autre part, l'article 7 Al1 décrit le devoir de diligence d'un titulaire d'une e-ID. « Il doit prendre les mesures nécessaires et raisonnablement exigibles au vu des circonstances pour empêcher toute utilisation abusive de son e-ID. »

L'article (Art17 AL3) peut se révéler problématique pour la confiance du citoyen. En effet, compter que sur le devoir de diligence du citoyen (Art 7 Al1) tout en laissant la porte ouverte à l'usurpation d'identité en excluant les mauvais émetteurs/vérificateurs qu'à posteriori risque de freiner l'adoption du système par le citoyen. Il est donc essentiel que lors de toute vérification, le citoyen ait à disposition dans son portefeuille un moyen clair et facile d'identification du vérificateur qui lui demande le partage de certains attributs. Il doit pouvoir savoir sans effort si ce vérificateur fait bien partie du registre de confirmation des identifiants et que dans le cas contraire, une notice d'avertissement apparaisse. Ainsi le citoyen pourra avoir la certitude de partager ses données qu'à des vérificateurs légitimes.

3.8 VÉRIFICATION SANS RÉSEAU INTERNET (OUT OF BAND) (ART18 AL3 ET ART20)

Dans le monde réel, c'est-à-dire lors d'une vérification d'attestation en présentiel, est-ce que les attributs e-ID et les émetteurs/vérificateurs doivent pouvoir être vérifiables sans réseau internet (inclusion technologique) sachant que des solutions technologiques rendent cela possible ?

3.9 ACCÈS AU PORTEFEUILLE (ART19)

Est-ce que la Confédération pense fournir les outils nécessaires à la restriction d'accès au portefeuille (eg Biométrie, Login/Password, ...)? Suivant la réponse du peuple concernant la LSIE, il semble opportun que la Confédération prenne cette responsabilité et n'utilise pas les fonctions similaires mises à disposition par les fabricants de téléphones ou les systèmes d'exploitation de ces derniers afin d'avoir le contrôle de bout en bout sur les aspects liés à la sécurité (exemple via utilisation des templates biométriques).

3.10 PRESTATAIRE DE SERVICE (ART24)

Est-ce que ce prestataire de services gardera la flexibilité de pouvoir déléguer, quand cela est nécessaire, l'exploitation d'une partie de l'infrastructure à un tiers, tout en garantissant que ce tiers opère sous le contrôle total de la Confédération ?

4 CONCLUSION

L'approche dite « Self-sovereign Identity » (SSI) a été reconnue par de nombreux protagonistes publics et privés comme étant l'approche de choix pour une transition vers l'identité digitale du futur. Au vu des tendances de marché évoquées ci-dessus, des attentes de la population suisse et des contraintes techniques, l'approche dite « Self-sovereign Identity » (SSI) semble l'approche la plus adaptée pour garantir un taux d'adoption élevé de l'eID en Suisse. Même s'il s'agit d'une nouvelle approche et qu'un certain nombre de questions restent ouvertes, il y a de fortes chances qu'il devienne le système d'identité de la prochaine génération d'Internet. Comme d'autres pays comme le Canada, les États-Unis ou l'Union Européenne mènent actuellement des projets pilotes similaires pour évaluer les impacts sur leurs infrastructures et leurs processus existants, la Suisse pourrait également faire partie des pionniers du SSI qui façonnent les transactions numériques de demain.

L'avant-projet de la loi LeID soumis à consultation par l'Office Fédéral de la Justice (OFJ) permet de jeter les bases d'une implémentation d'identité numérique en Suisse basée sur le SSI. Cet avant-projet permet aux différents acteurs étatiques et du secteur privé de se préparer à l'adaptation et à la migration des processus et technologies existants. SICPA a soulevé quelques points qui pourraient se révéler critiques lors de la mise en place et pour la gestion opérationnelle de cette plateforme en Suisse. Nous espérons par cette démarche pouvoir initier des discussions ouvertes sur ces thèmes et pouvoir contribuer à une mise en œuvre réussie et harmonieuse de l'identité numérique en Suisse.

Nous restons volontiers à votre disposition pour partager notre expérience et vision dans le domaine ou toute information complémentaire.



SICPA SA
Headquarters
Av de Florissant 41
1008 Prilly
Switzerland

Tel +41 21 627 55 55
Fax +41 21 627 57 27
www.sicpa.com/contact
www.sicpa.com

Eidgenössisches Justiz- und
Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter

Ausschliesslich per E-Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 20. Oktober 2022

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID), Vorentwurf: Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin Keller-Sutter,
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese gerne innerhalb der angesetzten Frist wahr.

Swico ist der Wirtschaftsverband der Digitalisierer und vertritt die Interessen etablierter Unternehmen sowie auch Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 700 Mitglieder aus der ICT- und Online-Branche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken. Neben Interessenvertretung betreibt Swico das nationale Rücknahmesystem «Swico Recycling» für Elektronik-Altgeräte.

1. Allgemeine Bemerkungen

Swico begrüsst die Stossrichtung des Vorentwurfes. Aus unserer Sicht setzt dieser den politischen Auftrag gut um, und die **zentralen Grundsätze** «Privacy by Design», «Datensparsamkeit» und «dezentrale Datenspeicherung» werden angemessen berücksichtigt. Das Gesetz setzt einen geeigneten Rahmen für eine **Vertrauensinfrastruktur** als Kernelement einer staatlich herausgegebenen E-ID.

Der Vorentwurf regelt die Eckpunkte der E-ID sowie der Vertrauensinfrastruktur und verweist an zahlreichen Stellen auf den Bundesrat, der für den Erlass der Ausführungsbestimmungen in Form von **Verordnungsrecht** zuständig ist. Das technologieneutrale Gesetz ist grundsätzlich begrüssenswert. Es ermöglicht eine dynamische Weiterentwicklung der Vertrauensinfrastruktur und deren Anpassung an den jeweiligen Stand der Technik. Es ist darauf zu achten, dass die Akteure rechtzeitig über die massgeblichen Eckpunkte informiert werden, damit die konkrete Planung von potenziellen Diensten und

Dienstleistungsangeboten, welche auf der künftigen E-ID basieren, rechtzeitig angegangen werden können. Wir wünschen uns deshalb, dass auch die Verordnung zur E-ID zur Vernehmlassung gebracht wird. In jedem Fall ist frühzeitig Klarheit zu schaffen in Punkten, welche für Entscheide privater Akteure massgeblich sind (insb. Abschnitt 5).

Das Ziel muss ein **umfangreiches Ökosystem (Ambitionsniveau 3)** von elektronischen Nachweisen sein, wobei solche durch staatliche und private Stellen ausgestellt werden können und ein etappenweises Vorgehen möglich ist. Ein rein staatlich genutzter, digitaler Ausweis erscheint uns nicht zweckdienlich und wird nicht ausreichen, um die Digitalisierung in der Schweiz entscheidend voranzutreiben. Wir begrüssen daher, dass der vorliegende Vorentwurf, bzw. die vorgesehene Infrastruktur, unterschiedliche elektronische Nachweise ermöglicht und der Weg zu einem umfangreichen Ökosystem gemäss Ambitionsniveau 3 offensteht.

Somit müssen **Angebote von privaten Dritten** gleichberechtigt zulässig sein. Der vorliegende Gesetzesentwurf ist zum jetzigen Zeitpunkt noch nicht klar betreffend die Rollen, welche Private bei der Entwicklung und Einführung des angestrebten Ökosystems einnehmen können und sollen. Der Beitrag von Privaten ist indes entscheidend für das Gelingen des Vorhabens.

Schliesslich sollte die E-ID nicht als **Identifikationsmittel zweiter Klasse** definiert werden, welches vom zu Grunde liegenden Papier oder Plastikdokument abhängig ist, wie dies an mehreren Stellen im vorliegenden Vorentwurf suggeriert wird. Vielmehr soll die E-ID als eigenständiges Identifikationsmittel breit für behördliche und nicht behördliche Dienstleistungen in Anspruch genommen werden können.

2. Einzelne Gesetzesbestimmungen gemäss Vorentwurf (VE-E-ID)

- **Art. 1 Abs. 1 Erweiterung des Gegenstandes**

Die Erweiterung des E-ID Gesetzes auf «andere elektronische Nachweise», und das dadurch entstehende Ökosystem, haben weit über das E-ID Thema hinaus Bedeutung. Da eine staatliche Infrastruktur geschaffen werden soll, die für Private zur Nutzung offensteht, muss die Gleichbehandlung mit ähnlichen privaten Infrastrukturen im Gegenstand des Gesetzes geregelt werden. Dies ist mittels folgender Ergänzung möglich:

Art. 1 Abs. 1 lit. d (neu): die Förderung neuer digitaler Geschäftsmodelle, die mit dieser Vertrauensinfrastruktur verbundenen sind.

- **Art. 1 Abs. 2 lit. c: Erweiterung des Zweckartikels**

Diese Bestimmung beschreibt den Zweck des Gesetzes, eine sichere, staatliche E-ID einzuführen, die unter Privaten und Behörden verwendet werden kann. In Abs. 2 lit. c wird dabei die Vertrauensinfrastruktur genannt, die dem aktuellen Stand der Technik entsprechen soll. Aus unserer Sicht fehlt an dieser Stelle die Forderung nach einer kontinuierlichen Weiterentwicklung der Vertrauensinfrastruktur. Dies wird auch nicht im erläuternden Bericht

klargestellt. Im Gegenteil: Er macht diese Forderung optional, indem von «fördern» die Rede ist. Wir empfehlen deshalb die folgende Anpassung:

Art. 1 Abs. 2 lit. c: Zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen, kontinuierlich gepflegt und weiterentwickelt werden;

- **Art. 2 Abs. 2: Ergänzungen bzw. Anpassungen am E-ID Inhalt**

Der Einbezug von Rufnamen, unter den Inhalt der E-ID, könnte die Akzeptanz des Gesetzes und die User Experience fördern (entspricht eCH 0011 und eCH 0201).

Art. 2 Abs. 2 lit. h (neu): Rufname

In Art. 2 Abs. 2 lit. d müsste aus unserer Sicht zudem klargestellt werden, welches Geschlecht gemeint ist, das biologische oder das wahrgenommene Geschlecht.

Art. 2 Abs. 3 lit. a: Wir gehen davon aus, dass die AHV-Nummer vor allem für öffentliche Anwendungsfälle als häufiger Identifier verwendet wird. Die Motivation des Gesetzgebers für den Einbezug der AHV-Nummer sollte aus unserer Sicht aus Akzeptanzgründen in den begleitenden Materialien präzisiert werden.

- **Art. 3: Gleichstellung des Ausstellungsprozesses der E-ID mit amtlichem Ausweis**

Vorliegend wird impliziert, dass die E-ID nicht einem amtlichen Ausweis gleichgestellt, sondern von einem amtlichen Ausweis abhängig ist. Es sollte ein Prozess implementiert werden, bei dem die E-ID ohne oder gleichzeitig mit einem anderen amtlichen Dokument (Pass, ID etc.) ausgegeben werden kann.

Zudem ist die vorgeschlagene Formulierung in diesem Artikel aus unserer Sicht nicht optimal, da sie nicht zwischen Besitz und Eigentum unterscheidet. Hält man am bestehenden Ausstellungsprozess fest, so schlagen wir eine Terminologie vor, die dem Ausweisgesetz folgt:

Art. 3: Die persönlichen Voraussetzungen zum Erhalt einer E-ID erfüllt, wer zum Zeitpunkt der Ausstellung der E-ID ~~einen der folgenden Ausweise besitzt~~ Inhaber eines der folgenden Ausweise ist:

- **Art. 4 Abs. 1: Konkretisierung des Ausstellungsprozesses und Anmerkungen zum Fedpol als ausstellende Stelle**

Der Ausstellungsprozess der E-ID sollte dahingehend konkretisiert werden, dass dieser ausschliesslich digital und vollautomatisiert zu erfolgen hat. Für Personen mit Einschränkungen im elektronischen Bereich müssen Ausnahmen vorgesehen werden.

Es kann diskutiert werden, ob neben dem Fedpol auch weitere Stellen (z.B. Passbüro, Gemeinden) zur Ausstellung der E-ID legitimiert werden sollen. So könnte eine E-ID gleichzeitig mit dem Pass beantragt werden, was die Attraktivität steigern würde. Soll der Lead beim Fedpol belassen werden, so ist es möglich, den Ausstellungsprozess durch weitere Stellen unter der Schirmkontrolle des Fedpol zuzulassen.

- **Art. 4 Abs. 2 Notwendigkeit der Altersbegrenzung fraglich**

Analog der Diskussion zum elektronischen Patientendossier, könnte sich die vorliegende Altersbegrenzung längerfristig als überflüssig erweisen. Die Mehrheit der Impfungen wird beispielsweise direkt nach der Geburt verabreicht. Diese Daten sollten somit ab Geburt digital dokumentiert und abgerufen werden können. Allenfalls sprechen Datenschutz-rechtliche Gründe für die Beibehaltung dieser Formulierung. Gemäss erläuterndem Bericht ist die vorliegende Altersbegrenzung aus EU-Kompatibilitätsgedanken nicht notwendig.

- **Art. 5 Bereinigung von Unklarheiten in Zusammenhang mit dem Widerruf**

Lit. c. dieser Bestimmung über den Widerruf der E-ID lässt offen, was ein «begründeter Verdacht» auf Missbrauch bedeutet. Hier wären aus unserer Sicht konkretisierende Hinweise in den erläuternden Materialien hilfreich. Von einer abschliessenden Liste von Missbrauchsfällen sollte jedoch abgesehen werden. Dies würde sich hinderlich auf die Missbrauchsbekämpfung auswirken. Gemäss lit. d Ziff. 1 ist unklar, wie «Ausweis entzogen» auszulegen ist. Insbesondere wird der Fall der Ungültigkeit eines Ausweises nicht geregelt. Handelt es sich bei der Begrifflichkeit «Ausweis entzogen» um eine Analogie zu Art. 7 Ausweisgesetz, so sollte dies in den Materialien konkretisiert werden. Die Bestimmung in lit. e verunmöglicht schliesslich, dass Bürgerinnen und Bürger sowohl auf dem alten als auch auf dem neuen Mobiltelefon eine E-ID gespeichert haben. Dies wäre jedoch als Schutz vor Verlust der E-ID sinnvoll. Zu klären bleibt, wie Personen identifiziert werden, die den Widerruf verlangen oder Missbrauch melden bzw. ob diese physisch vorstellig werden müssen.

- **Art. 9 Ausweitung der Pflicht zur Akzeptanz der E-ID auf den physischen Bereich**

Die Freiwilligkeit der Wahl des Mittels (z.B. Vorzeigen der Plastikkarte oder einer E-ID bei der Polizeikontrolle) sollte beim Bürger liegen und nicht beim Staat. Es fehlt bei dieser Bestimmung grundsätzlich an der Akzeptanz der elektronischen Identifizierung auch im physischen Bereich. Da die E-ID auf einem Smartphone installiert werden kann, liegt der Einsatz in der physischen Welt nahe, beispielsweise analog einem Covid-Zertifikat. Die Verwendung auch im physischen Bereich dürfte einen grossen Mehrwert darstellen. Dazu sollten die E-ID und das E-ID Ökosystem aufeinander abgestimmt wachsen und die Schnittstellen definiert werden.

Zudem sollte die Möglichkeit für Kantone, bestehende E-ID Lösungen nicht akzeptieren zu müssen, zeitlich beschränkt werden.

- **Art. 10 Vorweisen einer E-ID: Präzisierung der Aussage zur Sicherheit**

Diese Bestimmung äussert sich zum Prozess des Vorweisens einer E-ID. Sie ist aber dabei unklar im Punkt «...sofern die Anforderungen insbesondere an die Sicherheit des Prozesses auch auf diese Weise erfüllt werden können». Die Aussage kann fälschlicherweise so verstanden werden, dass die E-ID inhärent weniger sicher ist als die physischen Ausweise.

Eine Gleichstellung ist wünschenswert.

- **Art. 11 Abs. 1 Informationssystem zur Ausstellung und zum Widerruf der E-ID**

Diese Bestimmung bezeichnet das Fedpol als zuständige Stelle für den Betrieb des Informationssystems zur Ausstellung und zum Widerruf der E-ID. Aus unserer Sicht sollte die Delegation an Dritte möglich sein, solange der Bund in der Verantwortung bleibt und eine Delegation nicht gegen die Prinzipien nach Art. 2 verstösst. Die Delegationsmöglichkeit kann mittels folgender Änderung vorgesehen werden:

Art. 11 Abs. 1: Das Fedpol ~~betreibt~~ führt ein Informationssystem zur Ausstellung und zum Widerruf der E-ID.

- **Art. 12 Abs. 2 Ausstellung von anderen elektronischen Nachweisen**

Dieser Absatz ist aus unserer Sicht unvollständig in Bezug auf die Referenz zum Inhaber. Dies sollte in den Materialien entsprechend ergänzt werden: Die anderen elektronischen Nachweise müssen ermöglichen, dass der Inhaber des Nachweises beweisen kann, dass die vom Aussteller im Nachweis dokumentierten Inhalte unter seiner alleinigen Kontrolle sind.

- **Art. 13 Widerruf: Harmonisierung mit Art. 5**

In unserem Verständnis handelt es sich bei Art. 5 um den Widerruf der E-ID, während Art. 13 den Widerruf anderer elektronischer Nachweise regelt. Die beiden Bestimmungen müssen inhaltlich harmonisiert werden.

Wenn Daten im VC, welche der Aussteller verantwortet (autoritative Quelle), nicht mehr korrekt sind, müssen diese VCs revoziert werden. Dies kann am Beispiel eines Diploms veranschaulicht werden: Die Schule ist für die Erteilung eines Titels verantwortlich, aber nicht für den Namen der Person. Ein Verlust des Titels muss zur Revokation führen, ein Wechsel des Namens nicht.

- **Art. 15 Abs. 2 Übertragung von elektronischen Ausweisen**

Gemäss dieser Bestimmung kann der Bundesrat die Übertragung von elektronischen Ausweisen, welche nicht auf eine natürliche Person ausgestellt sind, zulassen. Der erläuternde Bericht impliziert, dass ein Kopieren von privaten Schlüsseln zwischen Geräten möglich sein soll. Dieser Ansatz birgt diverse, hohe Sicherheitsrisiken. Die Limitation der Übertragung von

«nicht persönlichen» VCs scheint technisch kaum möglich. Zudem schränkt das den Nutzen der Übertragung ein.

- **Art. 16 Vorweisen von elektronischen Nachweisen und Einhaltung des Datenschutzes**

Gemäss dieser Norm bestimmt die Inhaberin oder der Inhaber eines elektronischen Nachweises, welche Bestandteile des Nachweises, oder davon abgeleitete Informationen, übermittelt werden an die Behörde oder den Privaten, die den elektronischen Nachweis überprüfen. Der datenschutzrechtliche Grundsatz der Datenminimierung verlangt, dass potenziellen Verifikatoren Schranken bei der Wahl gesetzt werden, welche Nachweise sie für den Zugang zu ihren Diensten voraussetzen dürfen. Diese Schranke wird in Art. 16 nicht explizit genannt. Dies ist auch nicht zwingend notwendig, da die allgemeinen Grundsätze zum Schutz von Personendaten gelten. Die Akzeptanz der Vorlage könnte jedoch erhöht werden, wenn in Art. 16 explizit festgehalten wird, dass Verifikatoren für den Zugang von Diensten nur jene Nachweise verlangen dürfen, die aus explizit zu nennenden Gründen erforderlich sind. Konsumentinnen und Konsumenten könnten andernfalls mit dem Umstand konfrontiert werden, dass sie Datenschutzerklärungen annehmen müssen, die sie nicht wollen, um einen Dienst nutzen zu können.

Die Bestimmung legt nicht fest, was mit den von den Konsumentinnen und Konsumenten erhaltenen Inhalten geschieht. Es können unter anderem wertvolle Datensätze entstehen, wo das Missbrauchsverbot nach revidiertem Datenschutzgesetz greift. Allenfalls macht es Sinn, Konsumentenschutzorganisationen in diese Diskussionen miteinzubeziehen.

- **Art. 18 System zur Bestätigung von Identifikatoren**

Art. 17 benennt das Basisregister eindeutig. Für das Trustregister nach Art. 18 wird auf eine Benennung ohne ersichtlichen Grund verzichtet. Wir empfehlen deshalb, dass in Absatz 1 dieser Bestimmung auch das Trustregister einen einprägsamen und selbsterklärenden Namen erhalten soll.

In den erläuternden Materialien sollte unserer Ansicht nach festgehalten werden, dass jeder Betreiber einen Trustregister festlegt, wer und nach welchen Regeln sich im Register registrieren lassen kann. Ziel der Regelung sollte ein klares Verständnis über Inhalt und Betrieb des Trustregisters sein.

- **Art. 19 Aufnahme von privaten Anwendungen zur Aufbewahrung und Vorweisung von elektronischen Nachweisen**

Die Erläuterungen zu diesem Artikel halten fest, dass neben der staatlichen elektronischen Briefftasche, Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden können. Die Verwendung von elektronischen Briefftaschen, welche von privaten Akteuren angeboten werden, sollten unserer Ansicht nach explizit im Gesetz genannt werden. Das zeigt die Gleichwertigkeit und Interoperabilität solcher Lösungen auf und fördert deren Akzeptanz.

- **Art. 21 Abs. 3 Sicherheitskopien nach Ableben einer Person**

Aus unserer Sicht ist nicht geklärt, was mit Sicherungskopien nach Ableben einer Person geschieht.

Wir bedanken uns für die Kenntnisnahme und Berücksichtigung unserer Anliegen und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse



Ivette Djonova
Head Legal & Public Affairs



Adrian Müller
Präsident

Würenlos, 20.10.2022

Einschreiben

Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Vorab per Mail: rechtsinformatik@bj.admin.ch, rolf.rauschenbach@bj.admin.ch, info@bj.admin.ch

Vernehmlassung bzw. Stellungnahme zum:

- **Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise;**
- **bzw. (E-ID-Gesetz, BGEID).**

Sehr geehrte Frau Bundesrätin
Sehr geehrter Herr Rauschenbach
Sehr geehrte Damen und Herren

Gestützt auf das Vernehmlassungsgesetz (VLG) und die Vernehmlassungsverordnung (VIV) wie auch unseren gesammelten Praxiserfahrungen gerade im Zusammenhang mit dem Datenschutz ersuchen wir Sie im Rahmen des vorbezeichneten Vernehmlassungsverfahrens bzw. -prozesses als Zugehörige der interessierten Kreise höflich um Ihre überaus geschätzte Kenntnisnahme und wohlwollende Berücksichtigung der folgenden Ausführungen, wobei die jeweiligen *rechtlichen Bestimmungen kursiv und darin weiter angebrachte Änderungswünsche **fett** oder ~~durchgestrichen~~* sowie nachfolgend zugehörige Kommentare "normal", also ohne Schriftauszeichnung, erscheinen.

Art. 1 Abs. 2 lit. b Ziff. 5

Förderung des gleichberechtigten Datenzugangs.

Mit Einführen der E-ID besteht darüber hinaus die Chance, für berechtigte Personen den Datenzugang mit einem Höchstmass an Sicherheit nicht nur überaus effizient sondern auch für die E-ID-Inhaber in gleichberechtigter Form nachhaltig zu gestalten, so dass individuelle Interessen oder gar persönliche Präferenzen bestimmter "Datenwächter oder Zugangsentscheider" gegenüber objektiven Kriterien und Rechtsansprüchen definitiv zurücktreten.

Für die Aufnahme eines solchen Zusatzes bzw. einer solchen Grundsatzregelung sprechen insbesondere:
Art. 2 Abs. 3 BV, Art. 8 BV und Art. 29 BV.

Art. 1 Abs. 2 lit. c

zu gewährleisten, dass die E-ID und die ~~Vertrauens~~ **diesbezüglich zu sichernde bzw. sicherzustellende** Infrastruktur dem aktuellen Stand der **Wissenschaft und Technik** entsprechen;

Die Präsenz des Standes der Wissenschaft stellt gegenüber der Technik in nahezu jedem erdenklichen Fall ein anzustrebendes deutlich höheres Mass an Sicherheit dar und bereitet aufgrund der quasi überall uneingeschränkten Verfügbarkeit keine zusätzlichen Hemmnisse. Im Übrigen gehört der Stand der Wissenschaft im Qualitätswesen und der Produkthaftung seit mehreren Jahrzehnten zum allseits bewährten und geschätzten Standard. Warum sollte er dann bei solch wichtigen Themen wie der Personenidentifizierung und dem Datenschutz fehlen?

Bei Rückgriff auf hochgesteckte bzw. moralisch arg strapazierte Begriffe wie Vertrauen und Vertrauensinfrastruktur innerhalb von Gesetzestexten bedarf es zwingend genauer Auslegungsnormen, ähnlich dem fest verankerten Gebot der vertrauensvollen Zusammenarbeit im Personalrecht einiger europäischer Mitgliedstaaten, um ein konstruktives und ziel- wie ergebnisorientiertes Vorgehen zu forcieren und nicht wie immer wieder an andersartig skandalösen Fällen zu beobachten, unter Verwendung bzw. dem Anschein von "Vertrauen" genau das Gegenteil erwirkt und den über Generationen geprägten und nur zu häufig stets bestätigten Erfahrungssatz, "Vertrauen ist gut, Kontrolle ist besser!", leidigerweise mehr als vernachlässigt zu sehen. Hier, also zur rechtsverständlichen wie -sicheren begrifflichen Manifestierung einer Vertrauensinfrastruktur, reichen von daher keinesfalls die Bezüge auf Art. 81 BV und die unter Abschnitt 5 gefassten Ausführungen aus.

Art. 2 Abs. 1

~~Die E-ID wird mittels der Infrastruktur nach dem 5. Abschnitt als elektronischer Nachweis ausgestellt.~~

Die E-ID **zählt zu den** elektronischen Nachweisen, die mittels der Infrastruktur und **den Bestimmungen** nach Abschnitt 5 **Ausfertigung bzw. Ausstellung erlangen.**

Art. 2 Abs. 2 lit. g

~~Gesichtsbild~~ **amtliche und personenspezifische Ergänzungen**

Für die digitale Personenidentifizierung bedarf es nach derzeitigem Verständnis nicht notwendiger Weise ein Gesichtsbild, dessen Verwendung zudem den Grundsätzen der Datensparsamkeit und elementarer Persönlichkeitsrechte, wie dem Recht am eigenen Bild, entgegensteht und darüber hinaus vermehrt zu Missbrauch Anlass gibt. Von daher gilt es diesen Punkt vollständig zu streichen und ggf. durch amtliche sowie personenspezifische Ergänzungen zu ersetzen, wie beispielsweise Künstlername oder gar lebensrettende bzw. überlebenswichtige Informationen etc.

Sofern sich in naher Zukunft oder aus anderweitig zwingend erforderlichen Gründen ein Bezug zum Gesichtsbild nicht vollständig vermeiden lässt, so gilt es in den Personenidentifizierungsdaten allenfalls eine Prüfsumme der Bilddatei des Gesichtsbildes zu vermerken.

Art. 2 Abs. 3 lit. f

~~Angaben zum Ausstellungsprozess.~~

Ersatzlos streichen, da Angaben zum Ausstellungsprozess für den E-ID-Inhaber kein erkennbaren Zweck und Nutzen besitzen und eine solche Erhebung auch nicht dem sparsamen Umgang mit Daten entspricht.

Art. 3 lit. c

oder ohne gültige Ausweisapapiere ein Sonderbewilligungsverfahren bei einer dafür legitimierten Institution erfolgreich durchläuft.

Diese Regelung hilft auch Personen und Fälle zu berücksichtigen, die aus welcherlei Gründen auch immer über keine Ausweisapapiere verfügen, deren Identität und Integrität aber keinerlei Anlass für eine Ausgrenzung von einer E-ID-Inhaberschaft bietet. Die dafür zu legitimierenden Institutionen gilt es durch eine gesonderte Verordnung zu erfassen und mit entsprechenden Rechtspflichten wie Befugnissen auszustatten.

Art. 4 Abs. 4

~~*Zum Zweck der Gesichtsbildverifikation der antragstellenden Person können während dem Ausstellungsprozess biometrische Daten erhoben und mit dem Gesichtsbild aus dem ISA oder dem ZEMIS verglichen werden.*~~

Für das komplette Streichen dieses Absatzes sprechen nicht nur die bereits unter Art. 2 Abs. 2 lit. g vermerkten Gründe, wie Datensparsamkeit etc., sondern insbesondere die ausgeprägte bevölkerungsweite Skepsis gegenüber dem Erheben biometrischer Daten, was letztlich sogar eine schwerwiegende Gefahr für das Gelingen des gesamten E-ID-Projektes darstellt speziell durch zu befürchtende Zurückhaltung oder noch schlimmer vollständige Abkehr des überwiegenden Teils potentieller Nutzerinnen und Nutzer, also letztlich ein grossmehrheitliches Akzeptanzproblem verursacht. Hinzu kommt, dass der Einsatz der E-ID in absehbarer Zeit analog zu den qualifiziert elektronischen Signaturen allein auf nationale Ebene nicht zuletzt bedingt durch die Abschnitt 5 erklärte Infrastruktur beschränkt bleibt und insofern keinem internationalen Erfordernis biometrischer Datenerhebung unterliegt.

Sofern sich in naher Zukunft oder aus anderweitig zwingend erforderlichen Gründen ein Bezug zum Gesichtsbild oder biometrischer Daten nicht vollständig vermeiden lässt, so gilt es dieses allenfalls über Prüfsummenvergleiche zu den mit den Ausweisapapieren verbundenen Bild- und Biometriedateien sicherzustellen und zugleich die E-IDs bzw. deren Inhabern gänzlich vor der Gefahr zu bewahren, sich der direkten Les- wie Bearbeitbarkeit einschliesslich technisch leicht möglicher Bevorratung solchen Bild- und Biometriematerials gegenüber bekannten oder unbekannten Dritten ausgesetzt zu sehen.

Art. 6 Gültigkeitsdauer

E-IDs sind befristet gültig. Der Bundesrat regelt ihre Gültigkeitsdauer **einschliesslich diesbezüglicher Übergangs- und Nachfolgeregelungen.**

Nach Ablauf der E-ID-Gültigkeit bedarf es Regelungen zur ggf. erforderlichen bzw. notgedrungenen Weiterverwendung, wenn es aus welcherlei Gründen auch immer nicht gelingt, die jeweilige E-ID bzw. dessen Gültigkeit zu aktualisieren.

Art. 7 Sorgfaltspflichten

Statt eines evtl. direkt PIN-basierten Zuganges zur E-ID bieten hier beispielsweise Zwei-Faktor-Authentisierungen u.a. mittels Mobilgeräte, wie Mobiltelefone und Smartphones, ein deutliches Mehr an Sicherheit und kommen somit dem erleichterten Erfüllen der nach Art. 7 unbedingt einzuhaltenden Sorgfaltspflichten ein grosses Stück näher. Dazu braucht es auch keinesfalls biometrischer Charakteristika, die sich zudem auf vielen im Handel befindlichen Geräten gar nicht erst erfassen lassen.

Darüber hinaus besteht noch weitgehend Unklarheit über schadensersatz- und haftpflichtrechtlicher Regelungen in Missbrauchfällen.

Art. 9 Pflicht zur Akzeptanz der E-ID

Jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, muss die E-ID **zur Personenidentifikation** akzeptieren, ~~wenn sie eine elektronische Identifizierung vornimmt~~ und zugleich neben Nachweisausstellungen anbieten, weitere Vorgänge, wie in jedem Fall Kommunikation und Dateneditionsverfahren etc., sofern technisch irgendsmöglich auf rein elektronischem Wege insbesondere über **anerkannt sichere Zustellplattformen** zu erledigen.

Der deutliche Nutzen der E-ID ergibt sich unmittelbar aus den grundsätzlichen Einsatzmöglichkeiten in all den Bereichen, wo es um den Aus- wie Nachweis der Identität von natürlichen Personen und um Wahrung derer Rechte geht. Jeder diesbezüglich indentifizierende Vorgang, der kontaktlos auf digitalem Wege geschieht, bedeutet in letzter Konsequenz unabhängig der damit sowieso in Coronazeiten einhergehenden Vorteile neben erheblich höherer Be- und Verarbeitungsgeschwindigkeit bei gleichzeitiger Schonung von Personal, Material und Umwelt einen beachtlichen Gewinn an Rechtssicherheit sowie Transparenz auch und gerade hinsichtlich des Datenschutzes und der informationellen Selbstbestimmung einschliesslich deren Weitung, also genau das Gegenteil, was Digitalisierungsgegner und gewisse Teile der Bevölkerung vorschnell zum Vorwurf erheben und durchaus bei unklarer oder nicht angepasster Gesetzeslage gerade im Bereich nicht verfolgbarer oder unsanktionierbar bleibenden Datenschutzverletzungen tatsächlich Berechtigung erlangt bis hin zum Eintritt schwerwiegender Folgen wie nicht wiedergutzumachender Schädigungen.

Von daher gilt es auf jeden Fall gerade diesen Art. 9 zu begrüßen, der jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, anweist, die E-ID zu akzeptieren. Die konsequente Ausgestaltung dieser Bestimmung verlangt darüber hinaus die Ergänzung, nach Akzeptanz der E-ID anzubieten, neben Nachweisausstellungen weitere Vorgänge, wie in jedem Fall Kommunikation und Dateneditionsverfahren etc., sofern technisch irgendsmöglich auf rein elektronischem Wege insbesondere über **anerkannt sichere Zustellplattformen** zu erledigen.

5. Abschnitt: ~~Vertrauensinfrastruktur~~ **E-ID-Bundesinfrastruktur**

Statt der Verwendung des bereits unter Art. 1 Abs. 2 lit. c für eher unglücklich gehaltenen Begriffes "Vertrauensinfrastruktur" bietet sich beispielsweise der weit treffendere bzw. aussagekräftigere Terminus "E-ID-Bundesinfrastruktur" an.

Zur Infrastruktur dürfte zudem ganz im Sinne des Datenschutzes und der informationellen Selbstbestimmung bzw. des Öffentlichkeitsgesetzes, BGÖ, und Einhaltung des Legalitätsprinzipes gehören, als Inhaber einer E-ID oder Nachweisausteller sich jederzeit Kenntnis mittels einer präzis abgefassten lückenlosen Dokumentation, namentlich Aufstellung, der kontinuierlich bzw. chronologisch durchnummerierenden vollzogenen Prozessvorgänge verschaffen zu können, also welche Handlungen [Prozess-Schritt] auf Veranlassung bzw. Bearbeitung von wem [Frau/Herr/Code] zu welchem Zeitpunkt [Datum/Zeit] nach welcher gesetzlichen Vorgabe [rechtlichen Bestimmung] zu welchem Zweck [zwecks] unter welchen Massgaben und Folgerungen [Bemerkungen] stattfanden, etwa nach dem Schema:

Prozess-Schritt	ggf. bearbeitet von	am	zwecks	Folgerungen
	Frau/Herr/Code	Datum/Zeit	rechtlicher Bestimmung	Bemerkungen

Allenfalls gilt es durch einen zusätzlich einzufügenden Sonderartikel mit Verweis auf das Öffentlichkeitsprinzip nochmals auf diesen überaus wichtigen Umstand aufmerksam zu machen, wobei selbstverständlich davon der Nichtzugriff gegenüber Dritten unberührt bleibt.

Swiss Data Alliance
Schiffbaustrasse 10
Postfach
8031 Zürich
info@swissdataalliance.ch

Zürich, 18. Oktober 2022

Stellungnahme der Swiss Data Alliance zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Die Swiss Data Alliance bedankt sich für die Möglichkeit, zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung nehmen zu dürfen.

Die Swiss Data Alliance ist ein überparteilicher Zusammenschluss von Unternehmen, Wirtschaftsverbänden, zivilgesellschaftlichen Organisationen, Forschungsinstitutionen und Einzelpersonen mit dem Ziel, eine zukunftsorientierte Datenpolitik in der Schweiz zu etablieren.

Aus diesem Grunde hat die Swiss Data Alliance schon immer die Wichtigkeit einer digitalen Identität für die Schweiz betont und sich aktiv in die Diskussion um die E-ID eingebracht. Wir unterstützen deshalb alle Bestrebungen für die rasche Einführung einer E-ID und danken für das konstruktive und zielgerichtete Vorgehen des Bundesamts für Justiz.

Wir halten fest, dass wir auf Grund unserer Mitarbeit die Stellungnahme von Swico zu den einzelnen Gesetzesartikeln vollständig unterstützen. Wir verzichten darauf, die Stellungnahme an dieser Stelle nochmals aufzuführen.

Die Swiss Data Alliance begrüsst die Stossrichtung des Gesetzentwurfs. Aus unserer Sicht setzt dieser den politischen Auftrag gut um und die zentralen Grundsätze «Privacy by Design», «Datensparsamkeit» und «dezentrale Datenspeicherung» werden angemessen berücksichtigt. Das Gesetz setzt einen geeigneten Rahmen für eine Vertrauensinfrastruktur als Kernelement einer staatlich herausgegebenen E-ID.

Der Gesetzesentwurf regelt die Eckpunkte der E-ID sowie der Vertrauensinfrastruktur und verweist an zahlreichen Stellen auf den Bundesrat, der für den Erlass der Ausführungsbestimmungen in Form von Verordnungsrecht zuständig ist. Das technologieneutrale Gesetz ist grundsätzlich begrüßenswert, um eine dynamische Weiterentwicklung der Vertrauensinfrastruktur und deren Anpassung an den jeweiligen Stand der Technik zu ermöglichen. Es ist darauf zu achten, dass die Akteure rechtzeitig über die massgeblichen Eckpunkte informiert werden, damit die konkrete Planung von potenziellen Diensten und Dienstleistungsangeboten, welche auf der künftigen E-ID basieren werden, rechtzeitig angegangen werden können. Wir wünschen uns deshalb, dass auch die Verordnung zur E-ID zur Vernehmlassung gebracht wird.



Langfristiges Ziel muss ein umfangreiches Ökosystem von elektronischen Nachweisen sein, wobei solche durch staatliche und private Stellen ausgestellt werden können und ein etappenweises Vorgehen möglich ist. Ein rein staatlich genutzter, digitaler Ausweis erscheint uns nicht zweckdienlich und wird nicht ausreichen, um die Digitalisierung in der Schweiz entscheidend voranzutreiben. Wir begrüssen daher, dass der vorliegende Vorentwurf bzw. die vorgesehene Infrastruktur unterschiedliche elektronische Nachweise vorsieht und der Weg zu einem umfangreichen Ökosystem gemäss Ambitionsniveau 3 offensteht.

Schliesslich sollte die E-ID nicht als Identifikationsmittel zweiter Klasse definiert werden, welches vom zu Grunde liegenden Papier oder Plastikdokument abhängig ist, wie dies an mehreren Stellen im vorliegenden Vorentwurf suggeriert wird. Vielmehr soll die E-ID als eigenständiges Identifikationsmittel breit für behördliche und nicht behördliche Dienstleistungen in Anspruch genommen werden können.

Die Swiss Data Alliance möchte noch einmal betonen, dass wir eine staatliche E-ID und deren rasche Einführung sehr unterstützen. Die Schweiz braucht, um weiter wettbewerbsfähig und zukunftsorientiert zu bleiben, eine breit abgestützte und weit verbreitete digitale Identität. Deshalb stellen wir auch die Freiwilligkeit einer staatlichen E-ID in Frage. Unserer Meinung nach muss jede Bürgerin und jeder Bürger der Schweiz eine elektronische Identität besitzen. Nur so ist es zeitnah möglich, von einem Digital first- auf ein Digital only-Prinzip umzustellen und rascher eine digitale Nation mit einer effizienten und digitalisierten Verwaltung zu werden.

Wir sind gerne bereit, uns in der öffentlichen Diskussion mit unseren Experten und unserem Netzwerk jederzeit einzubringen und bedanken uns noch einmal für die Möglichkeit, uns an dieser Vernehmlassung beteiligen zu dürfen.

Freundliche Grüsse

André Gollietz, Präsident

Dr. Alain Gut, Vorstandsmitglied

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern

Per Mail zugestellt an: E-ID@bj.admin.ch und rechtsinformatik@bj.admin.ch

Zürich, 20. Oktober 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID Gesetz, BGEID) – Stellungnahme SFTI

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 29. Juni 2022 publizierte Vernehmlassung und bedanken uns für die Möglichkeit, auf diesem Wege unsere Anregungen zum Vorschlag für das auch aus unserer Sicht sehr wichtige E-ID Gesetz einbringen zu können.

Der Verband **Swiss Fintech Innovations** (SFTI, www.swissfintechinnovations.ch) vertritt die Interessen seiner Mitglieder (hauptsächlich Schweizer Banken und Versicherungen) im Bereich der Digitalisierung und Innovation in der Finanz- und Versicherungsindustrie.

Der vorgelegte VE-BGEID wird von SFTI ausdrücklich begrüsst. Namentlich schafft der Vorentwurf den rechtlichen Rahmen für die elektronischen Nachweise in der Schweiz, einschliesslich des staatlichen elektronischen Identitätsnachweises. Er beabsichtigt zudem die Regelung der Anforderungen an die Vertrauensinfrastruktur, die zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen erfüllt werden muss. Dies umfasst alle wesentlichen Kernbereiche und ist zu begrüssen. Ebenso positiv sehen wir, dass der Vorentwurf die Rollen und Kompetenzen für den Betrieb der Vertrauensinfrastruktur für einen elektronischen Identitätsnachweis (E-ID) regelt, welcher nicht nur im Verkehr mit Behörden, sondern auch unter Privaten verwendet werden kann.

Aus parlamentarischer Perspektive unterstützt bzw. ermöglicht die Schaffung einer E-ID beispielsweise die Umsetzung folgender Motionen:

- a) [Motion 20.223643 Für digitale Identitätsausweise; Motion NR Philippe Nantermod \(FDP.Die Liberalen\) vom 15.06.2022](#)
- b) [Motion 21.3180 Vollständig digitale Unternehmensgründung sicherstellen, von NR Andri Silberschmidt \(FDP, Zürich\) vom 16.3.2021](#)
- c) [Motion 20.4356 Digitaler Fahrzeug- und Führerausweis, von NR Franz Grüter \(SVP, Luzern\), vom 30.11.2020](#)

Gleichwohl sind nach unserer Einschätzung noch Präzisierungen angezeigt, um bei Wirtschaft und Gesellschaft das notwendige Vertrauen in die technische Lösung weiter zu stärken, gleichzeitig die Attraktivität für die künftige Nutzung der neuen Infrastruktur zu optimieren und damit insgesamt auch die Innovationskraft und die Attraktivität des Wirtschaftsstandorts Schweiz zu fördern.

Nachstehend formulieren wir vorab die Hauptpunkte, bei welchen aus unserer Sicht auf Gesetzesstufe noch Optimierungsbedarf besteht und begründen unsere Haltung anschliessend im Detail.

1. **Abbildung von Vertretungsrechten an juristischen Personen:** Natürliche Personen und durch diese vertretene Unternehmen müssen sich gestützt auf die E-ID eindeutig, sicher und benutzerfreundlich digital ausweisen können. Obwohl die E-ID richtigerweise nur für natürliche Personen konzipiert ist, muss es dennoch möglich sein, auch allfällige Vertretungsrechte dieser natürlichen Personen an juristischen Personen auf der E-ID (der natürlichen Person) abzubilden, indem das Basisregister nicht nur mit den Datenbanken der Fedpol, sondern auch mit dem Handelsregister bzw. dem SHAB verbunden wird. Damit würden im Geschäftsverkehr enorme Effizienzgewinne ermöglicht.
2. **Internationale Interoperabilität:** Vergleichbare ausländische E-IDs sollen in der Schweiz explizit anerkannt werden. In einer international verwobenen Wirtschaft ist es unabdingbar, dass die Prozesse auch in diesem Bereich durch technische Lösungen vereinfacht werden.
3. **Rechtssicherheit und Verantwortlichkeit:** Die Folgen des Missbrauchs der E-ID sowie weiterer elektronischer Nachweise sind im Gesetz nur marginal geregelt. Vor diesem Hintergrund schlagen wir vor, im Gesetz eine Haftungsnorm aufzunehmen. Zudem soll auch über die privaten Identifikatoren und Nachweise eine gewisse Kontrolle bestehen, weshalb dies im Gesetz besser reflektiert werden sollte.
4. **Förderung der Anwendung**
 - 4.1. Hoher Datenschutz und hohe Datensicherheit sind grundlegende Voraussetzungen.
 - 4.2. Die regulatorischen Zwecke der Weiterentwicklung und Akzeptanz der E-ID sowie der Förderung von digitalen Geschäftsmodellen, namentlich auch der Privatwirtschaft, sind ausdrücklich im BGEID zu verankern.
 - 4.3. Das BGEID muss mit einem breiten Feld zulässiger Anwendungsmöglichkeiten sowie attraktiven Einsatzbedingungen und Preismodellen Anreize schaffen, dass sowohl Wirtschaft als auch Nutzerinnen und Nutzer von der E-ID tatsächlich Gebrauch machen.
5. **Abstimmung mit ZertES und GwG:** Die Voraussetzungen zur Erlangung einer E-ID und einer QES müssen aufeinander abgestimmt werden, wobei klarzustellen ist, dass auf jeden Fall die Einhaltung der GwG-rechtlichen Anforderungen einer Video- oder Onlineidentifikation genügt. Um der E-ID von Beginn weg genügend Anwendungsbereich zu geben, sollte die Vorlage der E-ID darüber hinaus der persönlichen Vorsprache gleichgestellt sein bzw. der GwG-rechtlichen Identifikationspflicht Genüge tun.
6. **Technologieneutralität und technische Umsetzung:** Für die technische Umsetzung sind Experten beizuziehen.
7. **Periodische Überprüfung:** Trotz technologieneutralem Ansatz des VE-BGEID muss eine periodische Überprüfung etabliert werden, welche dauernd sowohl nach "state of the art"-Ansatz die technische Funktionsfähigkeit wie auch die Cybersicherheit gewährleistet.
8. **Gültigkeitsdauer der E-ID:** Die Gültigkeitsdauer der E-ID darf jene des Identitäts- oder Legitimationsdokuments, welches im Rahmen der Ausstellung der E-ID verwendet wurde, nicht überschreiten. Zudem sollte die zeitliche Kontinuität der Gültigkeit einer E-ID gewährleistet werden, d.h. ein zu einem bestimmten Zeitpunkt überprüft und zertifizierter Ausweis soll beispielsweise auch 10 Jahre später als überprüft und zertifiziert gelten.

1 Abbildung von Vertretungsrechten an juristischen Personen

Die digitale Abbildung der Vertretungsrechte für eine juristische Person entspricht einem grossen Bedürfnis der Wirtschaft. Während eine E-ID für juristische Personen kaum zu realisieren ist, wäre es dennoch möglich und sinnvoll, solche Vertretungsrechte auf der E-ID für *natürliche* Personen abzubilden und entsprechend im Basisregister als Nachweis einzutragen. Vorstellbar wäre dabei, das Basisregister mit HR und SHAB zu verbinden, damit die entsprechenden Identifikatoren im Register abgebildet werden können. Eine solche Lösung würde den Schweizer Standort bezüglich Digitalisierung wesentlich stärken und wäre zudem auch im Interesse der Verbreitung der E-ID, da man diese nicht nur für private, sondern auch für kommerzielle Zwecke einsetzen könnte.

Art. 1

¹ Dieses Gesetz regelt:

d. den Nachweis der Vertretungsrechte an juristischen Personen.

Art. 12^{bis}

Vertretungsrechte an juristischen Personen können als Nachweise auf der E-ID geführt werden. Der Bundesrat regelt die Einzelheiten, insbesondere den dafür notwendigen Datenaustausch zwischen den Handelsregistern und dem Basisregister gemäss diesem Gesetz.

2 Internationale Interoperabilität

Die Interoperabilität mit vergleichbaren ausländischen E-ID Lösungen ist für die international stark verwobene Schweizer Wirtschaft wichtig. Damit könnten die ohnehin schon komplexen grenzüberschreitenden Wirtschaftsprozesse zumindest in diesem Bereich vereinfacht werden. In Frage für eine Anerkennung kämen dabei insbesondere die nach der eIDAS ausgestellten Identitäten in der EU.

Wir schlagen daher vor, die Anerkennung und Herstellung von Interoperabilität mit vergleichbaren ausländischen E-ID Systeme bereits bei der Zielsetzung des Gesetzes aufzunehmen und Art. 1 BGEID entsprechend zu ergänzen.

Art. 1

² Es hat zum Zweck:

e. Interoperabilität und Anerkennung mit vergleichbaren ausländischen Identitätsnachweisen sicherzustellen;

Aus unserer Sicht käme zudem auch eine einseitige Anerkennung durch die Schweiz in Frage (vgl. Art. 27 VE-BGEID). Das könnte relativ unkompliziert geschehen. Vor allem wäre dazu kein Staatsvertrag notwendig. Art. 27 VE-BGEID müsste daher entsprechend erweitert werden und dem Bundesrat die Kompetenz einer einseitigen Anerkennung einräumen.

7. Abschnitt: Internationale ~~Abkommen~~ Anerkennung

Art. 27

¹ Der Bundesrat kann vergleichbare ausländische E-ID anerkennen.

3 Rechtssicherheit und Verantwortlichkeit

Das Basisregister wird durch den Bund geführt und muss daher gewissen inhaltlichen Anforderungen genügen. Das gilt sowohl für die öffentlichen als auch für die privaten Identifikatoren und Nachweise, die im Register enthalten sind. Klar ist auch, dass der Bund selber nicht absolute Richtigkeit garantieren kann, er muss aber ein Prüfmechanismus einführen, um zumindest Missbrauch zu vermeiden und eine hohe Qualität des Registers zu gewährleisten. Wird das Vertrauen in das Basisregister öfters enttäuscht, wird es letztlich auch nicht benützt werden. Es ist daher im Interesse der E-ID als solche, dass die Qualität des Registers stimmt.

Vor diesem Hintergrund schlagen wir vor, die «kann» Vorschrift in Art. 18 als Pflicht vorzusehen.

Art. 18 System zur Bestätigung von Identifikatoren

² Der Bundesrat regelt das Verfahren, wonach kann-vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.

Aus Gründen der Rechts(-verkehrs)sicherheit und auch eines sinnvollen Anwendungsbereichs für die E-ID ist im Gesetz eine Haftungsklausel aufzunehmen.

Art. 18^{bis} Haftung

Wenn ein Schaden entsteht, haftet dafür jene Partei, die die inhaltlich falsche Information eingeliefert hat.

4 Förderung der Anwendung

4.1 Hoher Datenschutz und hohe Cybersicherheit

Als vertrauensbildende Massnahme müssen die Vorkehrungen zur Cybersicherheit von Anfang an berücksichtigt und gesetzlich verankert werden. Die Sicherheit vieler Anmeldeverfahren wird oftmals reduziert, indem Passwörter z.B. mehrfach verwendet oder sogar aufgeschrieben werden. Mit einer digitalen Infrastruktur könnten die Schweizer Bevölkerung alle persönlichen Unterlagen in einem einzigen digitalen Wallet speichern und dieses jederzeit auf Abruf vorweisen oder übermitteln. Um Innovation und Wettbewerb zu fördern, sollten aber verschiedene digitale Wallets zugelassen werden. Die Kundenbeziehungen könnten so einfacher überprüft und abgeschlossen werden. Essenziell bleibt, dass bei jeder Verwendung die Wahl bestehen muss, welche Informationen der Gegenpartei zur Verfügung gestellt werden sollen und welche nicht. Somit wird der elektronische Geschäftsverkehr sicherer und die Privatsphäre jedes Einzelnen besser gewahrt. Dafür ist es notwendig, verschiedenste digitale Nachweise sicher speichern und teilen zu können. Vielfältige Anwendungsmöglichkeiten im Privatsektor stellen die Relevanz der E-ID sicher. Die nationale Infrastruktur kann darüber hinaus die Basis dafür bilden, dass sich jeder Mensch und jedes Unternehmen europaweit online und offline ausweisen kann und bestimmte persönliche Informationen nachgewiesen werden können, wenn die Interoperabilität mit entsprechenden EU-Lösungen gesichert ist.

Im VE-BGEID werden zwei Systeme beschrieben, nämlich das Fedpol-System zur Ausstellung von E-IDs (gemäss 2. Abschnitt, Art. 2 ff. VE-BGEID) und die Vertrauensinfrastruktur (gemäss 5. Abschnitt, Art. 17 ff. VE-BGEID). Namentlich muss sichergestellt sein, dass bei Verwendung der E-ID, z.B. bei Abschluss eines Vertrages, zur Eröffnung einer Geschäftsbeziehung oder zur Inanspruchnahme einer Dienstleistung, keine unnötigen digitalen Spuren hinterlassen werden. Insbesondere dürfen sich in der Vertrauensinfrastruktur tatsächlich keinerlei Daten befinden, was

bei korrekter Implementierung der Fall sein sollte (vgl. Art. 17 Abs. 4 u. Art. 25 Abs. 2 VE-BGEID). Auch sollte technisch ausgeschlossen sein, dass seitens staatlicher Stellen oder Privater wie z.B. Verifikator:innen Daten tracken bzw. speichern kann. Das alles ist wegen der gesetzlichen Anforderung dezentraler Datenhaltung zur Sicherstellung eines hohen Datenschutzes notwendig (Art. 1 Abs. 2 Bst. b Ziff. 1 u. 4 VE-BGEID). Aus Bankensicht gelten diese Anforderungen überdies gemäss Bankkundschaftsgeheimnis (Art. 47 BankG).

Entgegen diesen zwingenden Anforderungen wird gemäss Wortlaut von Art. 16 Abs. 3 VE-BGEID lediglich angeordnet, dass Betreiber:innen der Systeme nach dem 5. Abschnitt keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise haben und "möglichst" keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen können dürfen.

Die Einschränkung "möglichst" keine Kenntnisse wird den Anforderungen nicht gerecht, zumal sich diese wie dargelegt teilweise aus anderen Gesetzen wie namentlich DSG und BankG ergeben. Die Einschränkung "möglichst" ist deshalb ersatzlos zu streichen und es ist klarzustellen, dass die Betreiberin diese zwingende Anforderung mit geeigneten technischen und organisatorischen Massnahmen sicherzustellen hat. Art. 16 Abs. 3 VE-BGEID ist demzufolge wie folgt anzupassen:

Art. 16 Vorweisen von elektronischen Nachweisen

³ Die Betreiberin der Systeme nach dem 5. Abschnitt hat aufgrund technischer und organisatorischer Massnahmen keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann möglichst keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen

Der Widerruf nach Art. 5 VE-BGEID (Widerruf der E-ID) und Art. 13 VE-BGEID (Widerruf anderer elektronischer Nachweise) sollte ebenfalls möglich sein bei betrügerischer Erlangung der E-ID resp. des elektronischen Nachweises und nicht nur bei Missbrauch der E-ID resp. des elektronischen Nachweises). Eine betrügerische erlangte E-ID rechtfertigt auf jeden Fall deren Widerruf ebenso wie deren Missbrauch.

Die Bestimmungen sind entsprechend anzupassen.

Art. 5 Widerruf

Das fedpol widerruft die E-ID unverzüglich, wenn:

- f. der begründete Verdacht besteht, dass die E-ID betrügerisch erlangt wurde.

Art. 13 Widerruf

² Sie widerrufen diese unverzüglich, wenn

- d. der begründete Verdacht besteht, dass der elektronische Nachweis betrügerisch erlangt wurde.

4.2 Weiterentwicklung und Akzeptanz

Der Bund muss mit geeigneter Information und Kommunikation für **Transparenz und Verständnis** der Materie sorgen. Nur so kann in diesem Ökosystem mit einer Vielzahl von Ausstellern und Verifikatoren das notwendige **Vertrauen** der Bevölkerung in die neuartige Identifikationsmöglichkeit entstehen. Und erst wenn dieses Vertrauen geschaffen ist, kann der mit der E-ID bezweckte Nutzen

zum Tragen kommen. Zu dieser Information und Kommunikation gehört auch, die verschiedenen und vielfältigen Rollen von Staat und Wirtschaft innerhalb des "Systems" einer E-ID darzustellen, ebenso wie die Tatsache, dass solche verschiedenen Rollen für das Funktionieren des Gesamtsystems notwendig sind. Die Vorteile der E-ID sowie deren Funktionsweise müssen verständlich aufgezeigt werden. Allfälligen Ängsten der Bevölkerung, dass eine elektronische Identität nicht sicher sei oder in Richtung eines digitalen Überwachungsstaates gehe, muss von Anfang an proaktiv mit aufklärender Kommunikation begegnet werden. Dazu gehört die Schlüsselaussage, dass ein wiederverwendbarer digitaler Identitätsservice nicht möglich ist ohne das klare Verständnis, Vertrauen und Engagement eines jeden Benutzers. Nur so kann ein funktionierendes System entstehen, welches zutreffend "Vertrauensinfrastruktur" genannt wird (vgl. Art. 17 ff. VE-BGEID; Erläuterungsbericht BGEID, insb. S. 5 oben Ziff. 3.1. u. unten Ziff. 4, ferner S. 13 f. Ziff. 5). SFTI wird diesen Transparenz und Vertrauen schaffenden Prozess nach Kräften aktiv mitunterstützen.

Entsprechend ist die Bestimmung von Art. 1 Abs. 2 VE-BGEID zur Förderung des Vertrauens im digitalen Raum mit dem zusätzlichen **Zweck zu ergänzen, die Weiterentwicklung der E-ID und deren Akzeptanz zu fördern.**

Sodann schlagen wir vor, die Bestimmung von Art. 1 Abs. 2 VE-BGEID mit der zusätzlichen Zweckbestimmung zu ergänzen, die Entwicklung und Zulassung neuer digitaler Geschäftsmodelle zu fördern. Dabei muss es namentlich auch um neue Geschäftsmodelle gehen, welche von privaten Strukturen entwickelt werden. Zu denken ist etwa an neue Identifizierungslösungen zur KYC ("Know Your Customer")-Thematik. Ein Anbieter könnte solche neuen technischen Lösungen z.B. an Banken und/oder Versicherungen verkaufen. Gestützt darauf könnten diese Institute die Effizienz ihrer internen Prozesse bei der Abwicklung von Geschäftsvorgängen steigern. Dies wiederum würde die Gesamtkosten der Institute trotz Kauf der neuen technischen Lösung sogar reduzieren und die Kundenbindung verbessern. Durch solche Möglichkeiten der indirekten „Monetarisierung“ der E-ID wird wiederum der Anreiz für Anbieter aus der Privatwirtschaft gefördert, E-ID Lösungen weiterzuentwickeln und neue Anwendungsfälle zu finden. Hierdurch könnte die E-ID zu einem wirklich innovativen Baustein in der Wirtschaft werden. Beispiele dieser Art sind zwecks Förderung des Verständnisses in die künftige Botschaft zum neuen VE-BGEID aufzunehmen.

Demnach ist Art. 1 Abs. 2 VE-BGEID, ergänzend zu dem im Kapitel 2 vorgeschlagenen Bst. e, noch mit den zwei zusätzlichen Bst. f und g wie folgt zu ergänzen:

Art. 1

² Es hat zum Zweck:

- f. die Förderung der E-ID und deren Akzeptanz,
- g. die Förderung neuer digitaler Geschäftsmodelle.

Der VE-BGEID hält nicht klar fest, ob die E-ID "nur" als elektronisches Identifikationsmittel in der virtuellen Welt ausgestaltet werden soll (Gegenstück zu ID/Pass in der physischen Welt) oder auch in der physischen Welt einsetzbar sein soll (E-ID als umfassendes Identifikationsmittel für physische und virtuelle Welt; vgl. bspw. Bericht zu Art. 1 Abs. 2 Bst. a "Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden" und Bericht zu Art. 9 "...die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet ..."). Eine Verwendung der E-ID auch in der physischen Welt wäre wünschenswert und würde nicht zuletzt auch zu deren Verbreitung beitragen. Entsprechend wäre auch die Pflicht zur Akzeptanz der E-ID nicht an eine elektronische Identifizierung zu koppeln (vgl. Art. 9 VE-BGEID).

Art. 9 Pflicht zur Akzeptanz der E-ID

Jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, muss die E-ID akzeptieren, wenn sie eine **elektronische** Identifizierung vornimmt.

4.3 Attraktive Einsatzbedingungen und Preismodelle

Die Möglichkeit kostengünstiger Lösungen fördert bei den Unternehmen der Wirtschaft Innovation und die Schaffung neuer Geschäftsmodelle mit immer breiteren Paletten von Anwendungsmöglichkeiten. Damit einhergehend wächst auf Seiten der Nutzer und Nutzerinnen der Anreiz, die gesetzlich geregelte E-ID zu benutzen. Auf diese Weise wird das System der gesetzlich geregelten E-ID "monetarisiert", dies im positiven Sinne durch Schaffung einer immer breiteren Palette von Angeboten mit immer attraktiveren Preisen.

Die Kosten und Preise für Aussteller:innen und Verifikator:innen werden direkten Einfluss auf den Erfolg des Gesamtprojektes zur Implementierung einer gesetzlichen E-ID haben. Kommerzielle Überlegungen sind hochrelevant für Firmen, welche ihre Nachweise mit der E-ID verbinden und somit einen wesentlichen Teil des anzustrebenden E-ID Ökosystem ausmachen.

5 Abstimmung mit ZertES und GwG

Die Voraussetzungen zur Erlangung einer E-ID und einer QES müssen aufeinander abgestimmt werden, wobei klarzustellen ist, dass auf jeden Fall die Einhaltung der GwG-rechtlichen Anforderungen einer Video- oder Onlineidentifikation genügt.

Wichtig ist zudem, dass klar festgehalten wird, dass mit einer Identifizierung mittels E-ID die Anforderungen an die Ausstellung einer QES erfüllt werden (vgl. Bericht, S. 7: "So können die bestehenden (Online)-Identifizierungsprozesse, die viel komplexer sind, ersetzt werden. Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden.").

Die Anpassung von Art. 9 ZertES (vgl. Bericht, S. 20) sollte entsprechend klar formuliert werden:

Änderung anderer Erlasse:

ZertES Art. 9 Ausstellung geregelter Zertifikate

¹ Die anerkannten Anbieterinnen von Zertifizierungsdiensten müssen von den Personen, die einen Antrag auf Ausstellung eines geregelten Zertifikats stellen, verlangen:

- a. bei natürlichen Personen: dass sie persönlich erscheinen ~~und~~ oder durch eine E-ID gemäss BGEID den Nachweis ihrer Identität erbringen;

Im Bereich des Finanzmarktrechts könnten mit der Einführung der E-ID wesentliche Effizienzgewinne resultieren. Das GwG geht in Art. 3 immer noch von einer Identifikation durch beweiskräftige Dokumente aus. Es stellt sich daher die Frage, ob die E-ID als solches Dokument gilt. Wir schlagen aber vor hier Klarheit zu schaffen und die Identifikation durch die E-ID ausdrücklich vorzusehen. Damit hätte diese Art der Identifikation ihre Grundlage auf der richtigen Stufe, d.h. im formellen Gesetz.

Änderung anderer Erlasse:

GwG Art. 3 Identifizierung der Vertragspartei

¹ Der Finanzintermediär muss bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines beweiskräftigen Dokumentes oder einer E-ID gemäss BGEID identifizieren. Handelt es sich bei der Vertragspartei um eine juristische Person, so muss der Finanzintermediär die Bevollmächtigungsbestimmungen der Vertragspartei zur Kenntnis nehmen und die Identität der Personen überprüfen, die im Namen der juristischen Person die Geschäftsbeziehung aufnehmen.

6 Technologieneutralität und technische Umsetzung

Die technische Umsetzung darf nicht auf Gesetzesstufe erfolgen. Dies ist bereits notwendige Folge davon, dass der VE-BGEID nach bewährter Schweizer Gesetzgebungstradition nicht nur prinzipien- und risikobasiert, sondern auch wettbewerbs- und technologieneutral ausgestaltet ist. Damit wird das Regulierungsziel festgelegt, der Weg ins Ziel muss aber offenbleiben. Aber auch aufgrund des raschen technischen Fortschritts soll und muss der Bund die Kompetenz haben, auf Verordnungsstufe einen Technologie-Kontext zu wählen, welcher im Zeitpunkt der Einführung dem Zweck des Gesetzes und den Anforderungen – wie z.B. Datenschutz durch Technik, Datensicherheit, Datensparsamkeit und dezentrale Datenspeicherung - am besten gerecht wird. Deshalb ist die Bundeskompetenz gemäss Art. 25 VE-BGEID zu begrüssen.

Messlatte der technischen Umsetzung muss sein, dass der Erfolg der Vertrauensinfrastruktur davon abhängt, wie konsequent und überzeugend das Gesetz aus der Perspektive der Nutzer und Nutzerinnen zu Ende gedacht und umgesetzt wird (z.B. "elektronische Briefftasche", System für Sicherungskopien, etc.). Die technologische Gesetzesumsetzung beinhaltet sowohl die User Experience (UX) im Generellen wie auch matchentscheidende 'Momente' in der Customer Journey, besonders weil SSI die Verantwortung der Identität dem User überträgt. Das Spannungsfeld zwischen Sicherheit, User Experience und dem dezentralen Ansatz ist noch nicht abschliessend geklärt. Gerade weil die Mehrheit solcher Fragen im Zusammenhang mit der technologischen Umsetzung nicht auf Gesetzesstufe zu regeln ist, erwarten wir eine Plattform für Privatwirtschaft und die Wissenschaft, welche es erlaubt, Diskussionsbeiträge beizusteuern und somit die Umsetzung – innerhalb des erwähnten Spannungsfeldes – für den Bund zu erleichtern bzw. allfällige Blindspots zu vermeiden. Dies sollte in Form einer gemischten Arbeitsgruppe geschehen. Dies entspricht jedenfalls dem bewährten Regulierungsansatz der Bundesverwaltung, zumindest bei besonders vielfältigen und entsprechend komplexen Themen, wie sie vorliegend sicher gegeben sind, gemischte Arbeitsgruppen einzusetzen.

Dementsprechend schlagen wir eine entsprechende Ausführungsbestimmung als neuen Absatz 2 von Art. 28 VE-BGEID vor:

Art. 28 Ausführungsbestimmungen

¹ Der Bundesrat erlässt ... [unverändert]

² Der Bundesrat zieht bei Erarbeitung der Ausführungsbestimmungen Experten der Privatwirtschaft und der Wissenschaft bei.

7 Periodische Überprüfung

Zudem schlagen wir vor, das BGEID und die darauf basierenden technischen Infrastrukturen einer periodischen Überprüfung zu unterziehen. Diese soll klären, ob die technische Funktionalitäten zur Sicherstellung von Datenschutz (inkl. Bankkundengeheimnis) und Cybersecurity jeweils dem aktuellen Stand der Technik entsprechen und somit "state of the art" sind (Art. 1 Abs. 2 Bst. c VE-BGEID) und die E-ID ihren Zweck zur Förderung digitaler Geschäftsmodelle erfüllen kann.

8 Gültigkeitsdauer der E-ID

Schliesslich erscheint aus unserer Sicht sehr wichtig, dass die Gültigkeitsdauer der E-ID gemäss Art. 6 VE-BGEID die Gültigkeitsdauer des Identitäts- oder Legitimationsdokuments, das im Rahmen der Ausstellung/Erstellung der E-ID verwendet wurde, nicht überschreiten darf.

Zudem ist sicherzustellen, dass auch die zeitliche Kontinuität der Gültigkeit einer E-ID gewährleistet werden kann, das heisst, dass ein zu einem bestimmten Zeitpunkt überprüfter und zertifizierter Ausweis auch zum Beispiel 10 Jahre später als überprüft und zertifiziert gilt. Es sollte eine Vorgabe bestehen, dass ein entsprechendes technisches Verfahren vorhanden sein muss, analog zur heutigen Long Term Validation (LTV) im Bereich der elektronischen Signaturen.

Abschliessend danken wir Ihnen bestens für die Berücksichtigung unserer Anliegen. Für eine vertiefte Diskussion und für die weitere Zusammenarbeit stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Sig. Werner W. Wyss

Leiter SFTI-Arbeitsgruppe Regulations

Sig. Prof. Dr. Cornelia Stengel

Co-SFTI- Director/Mitglied Arbeitsgruppe Regulations

Per E-Mail an:
rechtsinformatik@bj.admin.ch

Zu Handen:
Frau Bundesrätin Keller-Sutter
Eidgenössisches Justiz- und
Polizeidepartement EJPD

Datum	12.10.2022
Ihr Kontakt	Raffael Knecht / 058 221 61 01 / raffael.knecht@swisscom.com
Thema	Stellungnahme zum Vorentwurf des E-ID-Gesetzes

Seite
1 von 5

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Vielen Dank für Ihre Einladung vom 29. Juni 2022 und die Möglichkeit, im Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung zu nehmen.

Auch für Swisscom ist die digitale Identität ein wichtiges Thema. Denn beim heutigen Stand der Digitalisierung ist es ein dringendes Anliegen, ein elektronisches Identifikationsverfahren mit breiter Akzeptanz einsetzen zu können. Swisscom ist überzeugt, dass der Erfolg der staatlichen elektronischen Identität (E-ID) sowie dem damit zusammenhängenden Vertrauensökosystem von drei Faktoren abhängt:

- die Handhabung der E-ID sowie der anderen elektronischen Nachweise muss benutzerfreundlich ausgestaltet sein;
- die Verwendung der E-ID muss bei wenigen, jedoch weit verbreiteten Services aktiv gefördert werden und
- die Umsetzung muss schliesslich schnell erfolgen.

1. Grundsätzliches

Gleich wie in der physischen Welt erfordert die Abwicklung bestimmter Dienstleistungen oder Behördengeschäfte auch in der digitalen Welt die Identifikation der beteiligten Nutzerinnen und Nutzer.

In vielen Anwendungsfällen genügt jedoch bereits der Nachweis eines bestimmten Merkmals, wie beispielsweise das Erreichen des erforderlichen Mindestalters beim Kauf von Gütern, die einer Altersbeschränkung unterliegen.

Überall dort, wo keine spezifischen Regelungen gelten und ein Geschäftsvorfall mit einer unmittelbaren Zahlung abgeschlossen werden kann, ist üblicherweise kein weiterer Nachweis zur Abwicklung einer Transaktion erforderlich.

In diesem Spannungsfeld zielen Konzepte wie namentlich „Self-Sovereign Identity“ (SSI) darauf ab, datenschutzrechtlichen Anliegen wie dem Prinzip der Datenminimierung mittels selbstverwalteter Identitäten und Attributen bestmöglich zu entsprechen. Gleichermassen sollen auch die weiteren Ansprüche der handelnden Akteure, allen voran an die Benutzerfreundlichkeit, berücksichtigt werden, indem konzeptionell an altbekannte Abläufe aus der physischen Welt angeknüpft wird.

Ein derart ausgestaltetes Vertrauensökosystem bildet schliesslich die Basisinfrastruktur für eine digitale Landschaft, auf deren Grundlage sich bereits bestehende Anwendungen überhaupt erst in der Breite etablieren und neue Anwendungen gedeihen können. Viel diskutierte Beispiele hierfür sind E-Collecting und -Voting-Systeme, die Bestellung von Registerauszügen aller Art sowie in übergeordneter Weise die digitale Willenskundgabe mittels der elektronischen Signatur.

Gerade beim digitalen Gegenstück zur handschriftlichen Unterschrift, der qualifizierten elektronischen Signatur (QES) nach dem Bundesgesetz über die elektronische Signatur (ZertES), verunmöglichte das Fehlen niederschwelliger Identifikationsverfahren in der Vergangenheit deren Verbreitung in der Schweiz. Swisscom befürwortet deshalb die Regelung, wonach der Identitätsnachweis bei der Registrierung für die QES durch einen elektronischen Identitätsnachweis nach dem BGEID wird erbracht werden können. Wir gehen davon aus, dass die für den Privatrechtsverkehr anerkannten Anbieterinnen von Zertifizierungsdiensten von dieser Möglichkeit Gebrauch machen werden und die Verwendung der elektronischen Signatur in der breiten Bevölkerung dadurch weiter gefördert wird.

Vor diesem Hintergrund begrüsst Swisscom den Vorentwurf grundsätzlich, regt aber an, nachfolgende Punkte in den weiteren Arbeiten zu berücksichtigen.

2. Risiken und Verbesserungsvorschläge aus Sicht Swisscom

a) Balanceakt zwischen technologieneutraler Regulierung und Wahrung der Investitionssicherheit privater Akteure

Der Vorentwurf regelt die Eckpunkte der E-ID sowie der darunterliegenden Vertrauensinfrastruktur und verweist an zahlreichen Stellen auf die Möglichkeit oder die Pflicht des Bundesrates, auf Verordnungsstufe Ausführungsbestimmungen zu erlassen.

Ein technologieneutraler Rechtsrahmen ist grundsätzlich begrüssungswert, um eine dynamische Weiterentwicklung der Vertrauensinfrastruktur und deren Anpassung an den jeweiligen Stand der Technik zu ermöglichen.

Bevor allerdings die Grundzüge der Ausgestaltung der Vertrauensinfrastruktur sowie die konkrete Rollenverteilung zwischen Staat und privaten Akteuren nicht hinreichend konkret sind, können potenzielle Technologielieferanten und Dienstleistungserbringer ihre Geschäftsmodelle nur ungenügend ausarbeiten. Dadurch wird auch die Planung von potenziellen E-ID-verwendenden Diensten und Dienstleistungsangeboten im Bereich der digitalen Nachweise erschwert. Dies birgt das Risiko, dass zwischen Inkrafttreten des Gesetzes und der Etablierung eines Vertrauensökosystems, das den Benutzerinnen und Benutzern Anwendungsmöglichkeiten der E-ID und anderer elektronischer Nachweise bietet, unnötig viel Zeit verstreicht, was im schlimmsten Fall die Adaption der Lösung verhindert. Deshalb ist es aus Sicht Swisscom wichtig, frühzeitig Klarheit zu schaffen in Punkten, die geschäftsstrategische Entscheide privater Akteure massgeblich beeinflussen könnten. Insbesondere betrifft dies Aspekte zur Ausgestaltung der Vertrauensinfrastruktur und deren vielfältigen Schnittstellen. Diesbezüglich erscheinen

uns die Ausführungen im 5. Abschnitt zur Vertrauensinfrastruktur in grundlegender Weise zu abstrakt, um konkrete Handlungsempfehlungen daraus ableiten zu können.

b) Vertrauen schaffen durch explizite Regelung des Schutzes der Privatsphäre und Abwehrrecht auf freien Zugang zum Internet

Der datenschutzrechtliche Grundsatz der Datenminimierung verlangt, dass die Bearbeitung von Personendaten dem Zweck angemessen und auf das für die Zwecke der Bearbeitung notwendige Mass beschränkt sein muss. Demnach setzt das Datenschutzrecht potenziellen Verifikatoren Schranken bei der Wahl, welche Nachweise sie für den Zugang zu ihren Diensten voraussetzen dürfen.

Der einschlägige Art. 16 Abs. 1 des Vorentwurfs betreffend das Vorweisen von elektronischen Nachweisen nennt diese Schranke nicht explizit, auch andernorts wird darauf abgestellt, dass allgemeine Grundsätze zum Schutz von Personendaten im BGEID nicht wiederholt werden müssen, um Geltung zu behalten. Aus rechtssystematischer Sicht ist dies selbstredend zu begrüssen.

Hingegen könnte es die Akzeptanz der Vorlage fördern, wenn im BGEID, konkret in dessen Art. 16, explizit verankert wird, dass Verifikatoren für den Zugang von Diensten nur jene Nachweise verlangen dürfen, die aus explizit zu nennenden Gründen erforderlich sind. KonsumentInnen könnten andernfalls mit allgemeinen Geschäftsbedingungen (AGB) und Datenschutzerklärungen konfrontiert werden, die sie eigentlich gar nicht akzeptieren wollen, aber faktisch nicht ablehnen können, wenn sie einen entsprechenden Dienst in Anspruch nehmen möchten.

In grundlegender Weise bildet schliesslich der Zugang zum Internet sowie zu zentralen digitalen Basisdiensten beim heutigen Stand der Digitalisierung gar die Voraussetzung für die wirksame umfassende Wahrnehmung praktisch aller Grundrechte. Thematisch spiegelbildlich zur Materie der digitalen Nachweise möchten wir deshalb anregen, die Einführung eines Abwehrrechts auf freien Zugang zum Internet, verstanden als die Summe essenzieller digitaler Dienste, zu prüfen. Als Leuchtturm könnte hier das Bayerische Digitalgesetz (vgl. BayDiG: Art. 8 Freier Zugang zum Internet) dienen, das seinen Rechtsunterworfenen einen freien Zugang zum Internet garantiert.

Sowohl die explizite Nennung des obgenannten datenschutzrechtlichen Grundsatzes zum Einsatz digitaler Nachweise als auch ein Abwehrrecht auf freien Zugang zum Internet könnten Bedenken hinsichtlich des Schutzes der Privatsphäre und ungerechtfertigter Zutrittsschranken im digitalen Raum in grundlegender Weise Rechnung tragen und so das Vertrauen in die künftige digitale Infrastruktur der Schweiz stärken.

c) Einführung eines standardisierten Identifikationsverfahrens für Personen ohne E-ID

Gemäss Vorentwurf ist die E-ID erhältlich für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises. Falls zu einem späteren Zeitpunkt politisch gewollt, kann die Schweizer E-ID dank grenzüberschreitender Interoperabilität internationale Anerkennung erlangen und umgekehrt können ausländische E-ID in der Schweiz zugelassen werden. Zur Umsetzung wären jedoch bilaterale Abkommen mit den jeweiligen Staaten erforderlich.

Vor diesem Hintergrund ist davon auszugehen, dass es gerade im stark international geprägten Schweizer Wirtschaftsverkehr noch lange Personen geben wird, die keine Möglichkeit haben, sich eine kompatible E-ID zu beschaffen.

Damit diese Lücke geschlossen werden kann, regen wir an, ein standardisiertes Identifikationsverfahren zu bezeichnen, dass ebenbürtig zur E-ID zur Anwendung gebracht werden kann. Damit könnten namentlich digitale Angebote der Privatwirtschaft, die eine Identifikation erfordern (z.B. die Eröffnung eines Bankkontos), von hierfür zugelassenen Akteuren mittels eines standardisierten Verfahrens erbracht werden, welches Personen ohne E-ID zur Verfügung gestellt werden kann, sodass diese nicht von entsprechenden

digitalen Angeboten ausgeschlossen werden oder E-ID-verwendende Angebote aufgrund einer zu niedrigen Verbreitung der E-ID in der einschlägigen Population gar nicht erst geschaffen werden.

Eine derartige Regelung hätte schliesslich den Vorteil einer gesetzesübergreifenden Standardisierung der digitalen Identifikationsverfahren, welche sich heute in unterschiedlichster Ausprägung an verschiedenen Stellen der Rechtsordnung wiederfinden.

3. Einzelpunkte aus dem Vorentwurf

a) Zu Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Neben der staatlichen elektronischen Briefftasche können gemäss Erläuterungen zu Art. 19 die Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden. Wir regen in diesem Zusammenhang an, die Verwendung von elektronischen Briefftaschen, die von privaten Akteuren angeboten werden, ebenfalls im Gesetz zu nennen, um die Gleichwertigkeit entsprechender Lösungen auszuweisen und damit deren Akzeptanz zu fördern.

b) Zu Art. 9 Abs. 4^{bis} des Bundesgesetzes vom 18. März 2016 über die elektronische Signatur

Wie einleitend erwähnt, begrüsst Swisscom die Regelung, wonach der Identitätsnachweis bei der Registrierung für die QES durch einen elektronischen Identitätsnachweis nach dem BGEID wird erbracht werden können. Wir gehen davon aus, dass dies die Verwendung der elektronischen Signatur in der breiten Bevölkerung weiter fördern wird.

Entgegen dessen Wortlaut ist Abs. 4 von Art. 9 jedoch nicht ganz, sondern nur im zweiten Satz aufzuheben.

Zusammengefasst begrüsst Swisscom den Vorentwurf grundsätzlich, sieht aber gleichzeitig Verbesserungsbedarf in einigen Punkten. Der Erfolg der E-ID wird aber schliesslich vom zeitnahen Aufbau des notwendigen Vertrauensökosystems abhängen, weshalb wir dringend anregen, regulatorische und projektspezifische Arbeiten möglichst zu parallelisieren. Weiter sollte ein umsetzungsorientierter Umgang mit Abhängigkeiten zu gleichlaufenden, ausländischen Vorhaben gefunden werden. Denn die berechnete Forderung nach internationaler Interoperabilität der E-ID-Systeme darf nicht zu Verzögerungen bei der nationalen Umsetzung führen.

Gerne stehen wir Ihnen zur Erläuterung unserer Sichtweise zur Verfügung. Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

Swisscom (Schweiz) AG

Raffael Knecht
FinTech & Digital Trust

Stéphane Vaucher
Senior Counsel

Schweizerische Eidgenossenschaft
Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter

Per E-Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 20. Oktober 2022

Stellungnahme zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter
sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zur Stellungnahme zum Vorentwurf des E-ID-Gesetzes und nehmen diese gerne mit der folgenden Stellungnahme wahr.

SWITCH wurde 1987 als privatrechtliche Stiftung vom Bund und den damals acht Hochschulkantonen gegründet. Die Stiftung unterstützt Hochschulen und weitere Partner innerhalb und ausserhalb der akademischen Welt dabei, die Möglichkeiten der Digitalisierung effektiv und effizient zu nutzen. Dabei verfolgt SWITCH das Ziel, die gemeinsame Innovationskraft zu stärken und mitzuhelfen, die Wettbewerbsfähigkeit der Schweiz nachhaltig auszubauen.

Die Stiftung betreibt und koordiniert seit bald 20 Jahren die digitalen Identitäten der schweizerischen Hochschullandschaft. Die nach nutzerzentrischen Prinzipien aufgebaute SWITCH edu-ID hat sich dabei als die Identitäts-Lösung für den gesamten tertiären Bildungsbereich mit aktuell mehr als 750'000 Nutzenden etabliert und bedient über 1'500 Dienste im BFI-Ökosystem (Bildung, Forschung, Innovation).

Unterstützung der Stossrichtung des Gesetzes

SWITCH unterstützt die Stossrichtungen des BGEID und bestärkt den Bund, diese beiden neuen zentralen, jedoch recht unterschiedlichen Aufgaben anzugehen:

1. Die Bereitstellung einer sicheren und nutzerfreundlichen E-ID auf einer staatlich betriebenen Infrastruktur, die von staatlichen Akteuren konzipiert, umgesetzt und betrieben werden muss.
2. Die Förderung eines Ökosystems digitaler Nachweise durch die Schaffung eines attraktiven Umfelds für vielfältigste Anwendungen.

SWITCH ist der Ansicht, dass beide Aufgaben parallel und mit gleicher Aufmerksamkeit angegangen werden müssen, damit das Ziel, ein funktionierendes und gut genutztes soziotechnisches System elektronischer Nachweise verwirklicht werden kann. Dadurch können Abhängigkeiten zwischen den beiden zentralen Aufgaben frühzeitig erkannt und berücksichtigt werden.

Einbezug von Fachgruppen

Der Schweiz fehlen, im Gegensatz zu vielen anderen Staaten, Jahre der betrieblichen Erfahrung mit staatlichen E-IDs. Das umfasst sowohl die Erfahrung des Staates als Betreiber, als auch diejenige der Bevölkerung als Nutzende. Um diesen Reifungsprozess zu beschleunigen, aber auch um den Nutzenden die Möglichkeiten aufzuzeigen, sind explorative Pilotprojekte des Bundes in Zusammenarbeit mit Stakeholdern aus dem privaten und öffentlichen Sektor von grosser Bedeutung. Damit kann das Ziel verfolgt werden, gemeinsam zu lernen, ohne die Wahl spezifischer Produkte bereits in dieser Phase zu präjudizieren.

Wir begrüssen die bereits aufgelegten Pilotprojekte des Bundes, wünschen uns aber eine verstärkte Durchführung von Pilotprojekten mit gemischter Beteiligung aus dem öffentlichen und privaten Sektor. Zudem regen wir an, dass auch bei der Umsetzung des Basisregisters die Möglichkeiten für eine operative Einbindung der Industrie unter der Führung des Bundes vorgesehen werden kann. Dadurch liessen sich möglicherweise die Betriebskosten des Bundes senken, die geforderte Dezentralität erhöhen, eine stärkere Verankerung in der Industrie erreichen und eine insgesamt erhöhte Resilienz des Registers gewinnen.

Wünschenswert wäre daher die Verankerung einer gemeinsamen Pilotierung mit gemischter Beteiligung aus öffentlichem und privatem Sektor an geeigneter Stelle im Gesetz oder auf Verordnungsstufe.

Als weitere Massnahme zur Beschleunigung der Adaption elektronischer Nachweise empfehlen wir Fachgruppen in die Steuerung der BGEID-Umsetzung einzubeziehen, die aus Vertretungen des Staates und des Privatsektors bestehen.

Datenschutz

Der Datenschutz ist bei der Ausgestaltung eines Systems elektronischer Nachweise ein zentrales Anliegen. Der Vorentwurf unterstreicht dieses Anliegen und setzt den politischen Auftrag gut um, indem es die zentralen Grundsätze Privacy by Design, Datensicherheit, Datensparsamkeit und dezentrale Datenspeicherung angemessen berücksichtigt.

Um den im Gesetz normierten Datenschutzgrundsätzen zum Durchbruch zu verhelfen, ist die datenschutzkonforme Ausgestaltung der Verordnung ebenfalls von grosser Wichtigkeit.

Freie Wahl betreffend Identifikationsmittel

Wer im Besitz einer E-ID ist, soll die freie Wahl haben, den Nachweis der eigenen Identität mit einem herkömmlich ausgesellten staatlichen Identifikationsmittel wie Reisepass oder Identitätskarte oder mit der staatlich ausgestalteten E-ID zu erbringen, sofern der Nachweis der Identität erforderlich ist. Diese Freiheit soll sowohl im physischen wie auch im virtuellen Verkehr mit der Trägerschaft öffentlicher Aufgaben gelten. Artikel 9 (Pflicht zu Akzeptanz) sowie Artikel 10 (Vorweisen einer E-ID) verankern den Grundsatz der freien Wahl nicht absolut.

Übertragung elektronischer Nachweise

Der Regelungsinhalt von Artikel 15 wirft einige Fragen auf. Grundsätzlich sollen bestimmte elektronische Nachweise, wie z.B. die E-ID, welche einer bestimmten natürlichen Person ausgestellt werden, nicht auf eine andere Person «übertragen» werden können. Es wird jedoch einerseits nicht genügend klar, was mit «Übertragung» gemeint ist, andererseits erschliesst sich uns die adressierte Person dieser Bestimmung nicht.

System zur Bestätigung von Identifikatoren

Wir erachten es als wichtig, dass die staatliche Infrastruktur auch zur Überprüfung der kryptografischen Schlüssel der im Basisregister eingetragenen privaten ausstellenden und verifizierenden Personen genutzt werden kann. Dies stärkt das Vertrauen in andere elektronische Nachweise und fördert zudem den Aufbau des langfristig anvisierten Ökosystems. Wie eingangs angemerkt, hoffen wir auf eine parallele Förderung der E-ID wie auch der anderen elektronischen Nachweise.

Internationale Interoperabilität

Im Bereich BFI (Bildung, Forschung, Innovation) ist internationale Interoperabilität von grösster Bedeutung, z.B. für die Forschungszusammenarbeit, für internationale Studierenden-Mobilität oder um Bildungsnachweise über Grenzen hinweg zu nutzen. Die internationale Interoperabilität – ohne «Swiss Finish» - soll als wichtige Anforderung berücksichtigt werden. Prioritär soll die Kompatibilität zu Ökosystemen digitaler Nachweise in Länder und Regionen hergestellt werden, mit denen die Schweiz regen Austausch pflegt, insbesondere zum EU-Raum. Dadurch werden zudem die Hürden für eine spätere Notifizierung reduziert.

Das vorliegende BGEID als pragmatischer erster Schritt

Das BGEID in der vorliegenden Form verfolgt einen pragmatischen Ansatz, der jedoch überprüft und nachgeführt werden muss. Wir regen an, dass Umsetzungsziele definiert, die Zielerreichung periodisch geprüft und Anpassungen am Gesetz als geplanter, iterativer Prozess vorgesehen wird (Horizont 3 bis 5 Jahre).

Gebühren

Eine weitere wichtige Steuerungsgrösse stellt die Preisgestaltung dar. Wir empfehlen eine sehr moderate Belastung für die Nutzung des Basisregisters und damit eine Förderung von Innovation und Wachstum im Bereich der elektronischen Nachweise.

Breite Abstützung

Wir regen an, dass künftige Umsetzungsschritte ebenfalls durch breit angelegte Vernehmlassungen abgestützt werden. Als potenziell nächste Kandidatin soll die Verordnung zum BGEID ebenfalls eine solche Vernehmlassung durchlaufen.

Wir bedanken uns für die Möglichkeit einer Stellungnahme und hoffen, dass unsere Anliegen so weit als möglich berücksichtigt werden.

Gerne bringt sich SWITCH auch in etwaigen Pilotprojekten und der Konzipierung im Rahmen des Systems elektronischer Nachweise ein und steht für weitere Erläuterungen selbstverständlich zur Verfügung.

Für weitere Auskünfte: Christoph Graf, Program Manager, +41 44 268 15 37, christoph.graf@switch.ch.

Freundliche Grüsse



Marco Dütsch
Head of Community Solution



Christoph Graf
Program Manager



Verband Schweizerischer Einwohnerdienste (VSED)
Association suisse des services des habitants (ASSH)
Associazione svizzera dei servizi agli abitanti (ASSA)
Associaziun svizra dals servetschs als abitants (ASSA)

Per E-Mail
rechtsinformatik@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD

Winterthur/Zofingen, 20. Oktober 2022

Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit zur Stellungnahme. Gerne machen wir davon Gebrauch und äussern uns wie folgt:

Aus Sicht des Verbandes Schweizerischer Einwohnerdienste (VSED) ist die Einführung der E-ID zu begrüßen. Die E-ID wird dank eindeutiger Personenidentifikation die Abwicklung elektronischer Dienstleistungen auch im Bereich der Einwohnerdienste beschleunigen und damit einen weiteren Beitrag zum Service Public leisten.

Als Voraussetzung für Synergieeffekte und gleichzeitig auch für eine erhöhte Sicherheit bezüglich der eindeutigen Personenidentifikation erscheint es dem VSED unerlässlich, dass kommunale webbasierte Anwendungen (bspw. Onlinemeldungen und -bestellungen) wie auch weitere damit zusammenhängende Applikationen von Beginn weg mit E-ID kommunizieren und funktionieren können. Aus Sicht der Einwohnerdienste besonders zentral erscheint in diesem Kontext ein frühzeitiger Miteinbezug von eOperationsCH respektive deren für die Bevölkerung mittlerweile fundamental wichtige Dienstleistung «eUmzugCH».

Für die Akzeptanz und Glaubwürdigkeit der E-ID begrüsst der VSED die anfängliche Personenidentifikation durch eine staatliche Stelle. Da eine Personenidentifikation respektive -verifikation für die Ausstellung einer E-ID mutmasslich auf rein elektronischem Weg und ohne persönliche Vorsprache auf einer lokalen Verwaltungsstelle erfolgen soll, erkennt der VSED darin ein potentiell Missbrauchsrisiko. Unabhängig wie die Personenidentifikation erfolgt, muss sichergestellt sein, dass solch potentielle Missbräuche mit entsprechenden technischen und/oder organisatorischen Massnahmen a priori verhindert werden können.

Im Sinne von kritischen Hinweisen möchten wir nachstehend auf einige Bestimmungen des Entwurfes eingehen:

Präsidium	Carmela Schürmann, Leiterin Einwohnerkontrolle Stadt Winterthur, Pionierstrasse 7, 8403 Winterthur, Tel. 052 267 57 54, carmela.schuermann@win.ch
Sekretariat	Corinne Schär, Leiterin Einwohnerdienste Zofingen, Kirchplatz 26, 4800 Zofingen Tel. 062 745 71 41, corinne.schaer@zofingen.ch

2. Abschnitt: E-ID

Art. 2 BGEID Form und Inhalt

Im Gesetzestext werden in Abs. 2 die einzelnen Personenidentifizierungsdaten aufgeführt. Besonders herausfordernd könnten sich die in den verschiedenen Registern unterschiedlich geführten Identifikationsmerkmale erweisen:

Unterschiedliche Namensführungen (insbesondere auch Sonderzeichen) in verschiedenen Registern sind ein altbekanntes Phänomen (beispielsweise bei ausländischen Staatsangehörigen im Zemis «Name nach Ausweisdokument» versus «Namensführung nach Zivilstandsregister» resp. nach Infostar im Anschluss an ein Zivilstandereignis). Neben der Namensführung, kann dies auch andere Merkmale betreffen, wie beispielsweise den Geburtsort, vereinzelt auch das Geschlecht oder das Geburtsdatum. Gemäss geltender Ausweisverordnung ist es beim Namen auf Reisedokumenten (Pass und Identitätskarte) zudem möglich, auch einen Allianznamen (Ledigname mit Bindestrich hinter Familienname) zu führen.

Der VSED kann sich demzufolge vorstellen, dass ein automatisches Weiterverwenden solcher Namensdaten oder weiterer Merkmale (sofern auch in der E-ID berücksichtigt) dann zu allfälligen Problemen in den lokalen Applikationen führen könnte – dies insbesondere in Anbetracht der sich ebenfalls in Vernehmlassung befindlichen Revision des Schweizerischen Zivilgesetzbuches zur Ermöglichung von Doppelnamen bei der Heirat, wo auch weiterhin die Verwendung eines Allianznamens nicht per se ausgeschlossen sein soll.

Bei der Umsetzung ist daher diesen beiden Aspekten die nötige Beachtung zu widmen.

In der Praxis hat sich gezeigt, dass mit der zunehmenden Vernetzung unterschiedlich geführte Daten zu Verwirrung, Ineffizienz und zu Missverständnissen führen. Insbesondere die Einwohnerdienste haben viel Abklärungs- und Datenbereinigungsaufwand, was die voneinander abweichenden Daten in den verschiedenen Registern anbelangen. Diese sind meist auf unterschiedliche rechtliche Grundlagen oder mangelnde harmonisierte Richtlinien zurückzuführen.

Art. 3 BGEID Persönliche Voraussetzungen

Als persönliche Voraussetzung wird entweder ein Ausweis nach AwG (bei Schweizer Bürger) oder - bei ausländischen Staatsangehörigen - ein gültiger Ausweis nach AIG verlangt. Das heisst, dass für die Identifizierung von ausländischen Staatsangehörigen eine gültige Bewilligung notwendig ist. Beim schweizerischen Ausländerausweis handelt es sich jedoch lediglich um ein Legitimationspapier. Wir regen daher an, diesen Aspekt zu berücksichtigen und zu prüfen, ob nicht auch bei ausländischen Personen ein gültiges heimatliches Reisedokument verlangt werden soll. Dieses ist gerade bei Personen mit Bewilligung L, B und C in aller Regel vorhanden.

Art. 10 BGEID Vorweisen einer E-ID

Je nach Kontext muss es zudem möglich bleiben, bei einer persönlichen Vorsprache ein physisches Ausweisdokument vorzulegen.

Präsidium	Carmela Schürmann, Leiterin Einwohnerkontrolle Stadt Winterthur, Pionierstrasse 7, 8403 Winterthur, Tel. 052 267 57 54, carmela.schuermann@win.ch
Sekretariat	Corinne Schär, Leiterin Einwohnerdienste Zofingen, Kirchplatz 26, 4800 Zofingen Tel. 062 745 71 41, corinne.schaer@zofingen.ch

3. Abschnitt: Andere elektronische Nachweise

Beim Widerruf von elektronischen Nachweisen fehlt unseres Erachtens allenfalls die Möglichkeit einen Nachweis zu revozieren, wenn dieser nicht mehr aktuell oder korrekt und somit nicht mehr gültig ist.

Art. 13 BGEID Widerruf (Ergänzungsvorschlag)

d. der elektronische Nachweis nicht mehr gültig ist.

Auswirkungen auf die Kantone und Gemeinden

Art. 8 BGEID Anlaufstellen der Kantone

Das Errichten von Anlaufstellen für die Bevölkerung begrüssen wir, wie auch das Errichten in der Nähe der Personen. Es ist naheliegend, dass die Einwohnerdienste, als meist erste Anlaufstelle der örtlichen Verwaltung, für diese Aufgabe prädestiniert sind. Dies wäre allerdings nicht ohne Mehraufwand zu bewältigen, der entsprechend zu entschädigen wäre, damit die personellen Ressourcen zur Verfügung gestellt werden können.

Aus diesem Grund beantragen wir eine Ergänzung in Art. 26 BGEID:

Art. 26 BGEID (Ergänzung)

Abs. 5 Der Bundesrat regelt die aufwandgerechte Entschädigung für die von den Kantonen bezeichneten Stellen, die im Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.

Laut erläuterndem Bericht greift das Fedpol für die Ausstellung auf die unter Art. 11 Abs. 3 verschiedenen erwähnten Register für die Ausstellung zu und könne seine Aufgabe bei der Ausstellung deshalb automatisiert erfüllen. Dies vermag vermutlich auf einen grossen Teil der Bevölkerung zutreffen. Die jahrelange Erfahrung der Einwohnerdienste mit der zunehmenden Vernetzung der Register zeigt allerdings, dass der Datenbereinigungs- und –abklärungsaufwand aufgrund unterschiedlich geführten Merkmalen bei den Einwohnerdiensten massiv zugenommen hat. Unterschiedlich geführte Merkmale könnte Einfluss auf diesen angedachten Ausstellungsprozess haben.

Das Registerharmonisierungsgesetz (RHG; SR 431.02) bezweckt zwar eine Harmonisierung von Merkmalen um den gesetzlich vorgesehenen Austausch von Personendaten zu vereinfachen. Die verschiedenen Register führen jedoch trotz dieser Bestrebung teilweise nach wie vor unterschiedliche Merkmale. Diese Tatsache hat im besonderen Masse immer wieder Auswirkungen auf die Einwohnerregister der Gemeinden, welche Einwohnerdaten an verschiedene Bundesregister liefern. Mit dem vorgesehenen E-ID-Ökosystem stehen deshalb Befürchtungen im Raum, dass weitere Datenabklärungsaufgaben den Einwohnerdiensten zufallen werden.

Angesichts dessen stellt sich die Frage, ob nach Art. 26 Abs. 1 BGEID die Gemeinden für die Nutzung des Basisregisters nicht von einer allfälligen Nutzungsgebühr entbunden werden müssten, um diesem Aspekt Rechnung zu tragen.

Präsidium Carmela Schürmann, Leiterin Einwohnerkontrolle Stadt Winterthur,
Pionierstrasse 7, 8403 Winterthur, Tel. 052 267 57 54, carmela.schuermann@win.ch

Sekretariat Corinne Schär, Leiterin Einwohnerdienste Zofingen, Kirchplatz 26, 4800 Zofingen
Tel. 062 745 71 41, corinne.schaer@zofingen.ch

Wir beantragen deshalb beispielsweise zusätzlich folgende Ergänzung:

Abs. 6 Der Bundesrat kann eine Entschädigung vorsehen für Datenbereinigungsaufgaben, die bei den Kantonen und den Gemeinden im Zusammenhang mit dem Ökosystem der E-ID entstehen. Er kann sie dabei auch von einer allfälligen Nutzungsgebühr bei der Nutzung des Basisregisters entbinden.

Ganz generell würde es der VSED begrüssen, wenn die weitere Harmonisierung der Register generell verstärkt durch den Bund gefördert werden würde, durch beispielsweise eine Anpassung des Registerharmonisierungsgesetzes. Dies würde die zukünftige Digitalisierung unterstützen und erleichtern.

Zusammenfassend halten wir fest, dass die eindeutige und sichere Identität einer Person sowie eine klare Regelung in Bezug auf die geführten Merkmale von höchster Wichtigkeit sind.

Unser Verband hat in den vergangenen Jahren immer wieder die Erfahrung gemacht, dass Bundesprojekte, bei welchen die involvierten Stellen im Vorfeld nicht einbezogen wurden, nach ihrer Umsetzung in der Praxis grosse Probleme verursacht haben. Wir danken Ihnen daher für die Gelegenheit uns bereits zum Vorentwurf einbringen zu können und stehen Ihnen weiterhin für Fragen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Einwohnerdienste



Carmela Schürmann
Präsidentin



Corinne Schär
Sekretärin

Kopie:

Schweizerischer Gemeindeverband
Schweizerischer Städteverband

Präsidium Carmela Schürmann, Leiterin Einwohnerkontrolle Stadt Winterthur,
Pionierstrasse 7, 8403 Winterthur, Tel. 052 267 57 54, carmela.schuermann@win.ch

Sekretariat Corinne Schär, Leiterin Einwohnerdienste Zofingen, Kirchplatz 26, 4800 Zofingen
Tel. 062 745 71 41, corinne.schaer@zofingen.ch



VSPB · FSFP

Verband Schweizerischer Polizei-Beamter
Fédération Suisse Fonctionnaires de Police
Federazione Svizzera Funzionari di Polizia

Geht an

Bundesamt für Justiz
rechtsinformatik@bj.admin.ch

Luzern, 29. August 2022

Vernehmlassungsantwort des Verbandes Schweizerischer Polizei-Beamter zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) – 2022/19

Sehr geehrter Herr Bundesrat

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum vorgeschlagenen Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise.

Der Verband Schweizerischer Polizei-Beamter VSPB vertritt 59 Sektionen mit insgesamt über 26'500 Mitglieder. Davon sind fast 20'000 im aktiven Polizeidienst für Gemeinden, Kantone und Bund, was zu einem Deckungsgrad des VSPB von 95% aller Polizistinnen und Polizisten führt.

Nach dem Scheitern der ersten Vorlage zum e-ID Gesetz, die auch dem VSPB nicht genehm war, wird nun ein neuer Text unterbreitet. Inhaltlich ist zu bemerken, dass der aus unserer Sicht grosse Stolperstein der Privatisierung einer solch wichtigen Aufgabe aus der Welt geschaffen wurde.

Der VSPB unterstützt demzufolge diese neue Vorlage und wird sich konsequent im Rahmen der eventuellen Kampagne dafür einsetzen.

Für die Aufnahme und Berücksichtigung unserer Position danken wir Ihnen bestens.

Freundliche Grüsse

Max Hofmann

Generalsekretär VSPB



ASSOCIATION DES SERVICES DES AUTOMOBILES
VEREINIGUNG DER STRASSENVERKEHRSÄMTER
ASSOCIAZIONE DEI SERVIZI DELLA CIRCOLAZIONE

Bundesamt für Justiz

Per E-Mail

rechtsinformatik@bj.admin.ch

Bern, 15. September 2022

Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Der Bundesrat hat mit dem Richtungsentscheid zur E-ID am 17.12.2021 den Aufbau eines Ökosystems für die E-ID beauftragt. Die asa und das ASTRA können mit dem Teilprojekt T1 (digitaler Führerausweis, mDL) ein Pilotprojekt im Rahmen des Vorhabens E-ID realisieren. Die Zusammenarbeit mit der Projektleitung E-ID verläuft sehr gut und zielführend. Wir bedanken uns, dass wir an diesem wegweisenden Digitalisierungsprojekt aktiv mitarbeiten und die Interessen der digitalen Ausweise im Strassenverkehr vertreten dürfen.

Die Vereinigung der Strassenverkehrsämter (asa) bedankt sich ebenfalls für die Möglichkeit, im vorliegenden Vernehmlassungsverfahren mitzuwirken.

Allgemeine Bemerkungen:

- Wir begrüssen die Einführung des elektronischen Identitätsnachweises E-ID sehr. Die E-ID schafft die Grundlage um in den Strassenverkehrsämtern in Zukunft viele Prozesse mit unseren Kunden vereinfacht zu digitalisieren.
- Zudem wird die auch von der E-ID genutzten Basisinfrastruktur die zeitnahe Einführung digitaler Ausweise der Verkehrszulassung (Lernfahrausweis – 300'000/Jahr; Führerausweis - 6.5 Mio.; Ausweis 95 / Chauffeurzulassung; Fahrzeugausweis - 6 Mio.; Schiffsführerausweis – 300'000 und Schiffsausweis – 100'000) ermöglichen.
- In der gewählten Technologie „Self-Sovereign Identity“ (SSI) besteht noch wenig praktische Erfahrung. Dadurch ist diese entsprechend risikobehaftet in Bezug auf die praktische Umsetzung und den Betrieb. Unseren Kunden ermöglicht diese jedoch einen zeitgemässen und selbstbestimmten Schutz der Privatsphäre bei der Nutzung der digitalen Ausweise, was wir sehr begrüssen.
- Wir begrüssen es, dass der Bund sich in der Verantwortung für die Basisinfrastruktur (Vertrauensinfrastruktur) sieht und hier die Führung übernommen hat.

Bemerkungen zu den einzelnen Gesetzesartikeln:

Art. 2 Form und Inhalt

- Mittelfristig wäre es zielführend, die Personenidentifizierungsdaten von ISA, ZEMIS und weiteren Umsystemen wie denen des Informationssystems (IVZ) des ASTRA zu harmonisieren.
- Das Ablaufdatum der E-ID darf keine Auswirkungen auf gültige digitale Ausweise (Credentials) haben, da z.B. der heutige Führerausweis unbefristet gültig ist. Auch andere Ausweise werden unterschiedliche Ablaufdaten haben. Eine Erneuerung der E-ID darf diesbezüglich keinen grossen Mehraufwand auf die vorhandenen Ausweise haben. Namentlich müssen die Kunden bei einer Erneuerung der E-ID einfach und rasch die fortbestehenden digitalen Ausweise wieder aktivieren können.

Art. 8 Anlaufstelle der Kantone

Der Bund (BIT) ist für die Basisinfrastruktur und somit auch für dessen Support zuständig. Kantonale Anlaufstellen können, wenn nötig, die Bundesstellen in dieser Aufgabe unterstützen.

Die unterschiedlichen Anbieter von digitalen Ausweisen (eLernfahrausweis, eFührerausweis, ePersonalausweis, eWohnsitzbestätigung, eStrafregisterauszug, usw.) sind hingegen für den jeweiligen Support zuständig. In der Einführungsphase ist eine direkte Absprache zwischen den unterschiedlichen Organisationen dringend notwendig.

Art. 15 Übertragbarkeit von elektronischen Nachweisen

Die Strassenverkehrsämter planen auch den Fahrzeugausweis (ca. 6 Mio.) als digitalen Ausweis abzugeben. Der Fahrzeugausweis verbleibt beim Halter eines Fahrzeuges. Der Halter hat jedoch die Möglichkeit, das Fahrzeug und damit den Fahrzeugausweis einer anderen Person für eine bestimmte Zeit «auszuleihen». Es muss deshalb die Möglichkeit bestehen, einen digitalen Ausweis zeitbefristet oder unbegrenzt «teilen» zu können, beispielsweise innerhalb der Familie.

Art. 26 Gebühren

Die Gebühren für den Eintrag im Basisregister müssen frühzeitig bekannt und angemessen sein. Im Kontext der Führerausweise wäre eine Gebühr in der Grössenordnung der Gestehungskosten heutiger physischer Ausweise wünschenswert. Ansonsten müssen die Kantone die Kosten durch höhere Gebühren für diese Produkte auf die Bürger abwälzen. Dies könnte zu Widerständen gegen die Digitalisierungsvorhaben führen.

Art. 27 Internationale Abkommen

Es muss unbedingt die Möglichkeit geschaffen werden, dass die unterschiedlichen digitalen Ausweise der Strassenverkehrsämter auch im EU-Raum genutzt werden können.

Art. 28 Ausführungsbestimmungen

Es muss die Möglichkeit geschaffen werden, dass gewisse digitale Ausweise (Beispiel eFahrzeugausweis, ca. 6 Mio.) mit anderen Personen «geteilt» werden können (Weitergabe eines Fahrzeugausweises für eine bestimmte oder unbestimmte Zeit bei der privaten oder kommerziellen Ausleihe). Siehe auch Bemerkung zu Art. 15. Wir schlagen daher vor, dass eine neue lit. e aufgenommen wird:

e. zu den Möglichkeiten einer temporären Verwendung von Nachweisen durch andere E-ID-Benutzer (Teilen).

Allgemeine Bemerkungen:

Die erwähnten Betriebskosten (jährlich CHF 15 – 20 Mio.), welche durch Gebühren bezahlt werden müssen, sind im Verhältnis zu den Projektkosten von ca. CHF 25 – 30 Mio. aus unserer Sicht viel zu hoch. Es darf nicht sein, dass der Bund die E-ID «gratis» zur Verfügung stellt und die Kantone, Gemeinden und Private bezahlen mit den Gebühren für ihre digitalen Ausweise die hohen Betriebskosten, welche dann in irgendeiner Form an die Kunden überwälzt werden müssen. Es besteht somit die Gefahr, dass digitale Ausweise von Kantonen und Dritten nicht über die Basisinfrastruktur und das zugehörige Bundeswallet des Bundes verteilt werden und sich alternative Kanäle etablieren.

Vielen Dank für die Kenntnisnahme und die weitere Prüfung.

Freundliche Grüsse



Andreas Vetsch
Präsident asa



Sven Britschgi
Geschäftsführer asa

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz-
und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern

Einreichung per Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 7. Oktober 2022

Betreff: Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

**Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren**

Wir danken Ihnen für die Gelegenheit, uns zum Vorentwurf des neuen E-ID-Gesetzes als langjähriger Dienstleistungspartner des Bundes äussern zu dürfen.

Als Experten im Bereich Identity und Access Management, Mitgründer des Vereins *cardossier*, aktives Mitglied des Vereins DIDAS und Co-Initiant der SSI-Initiative mit dem Kanton AG setzen wir uns seit mehreren Jahren in unterschiedlichen Projekten mit den Themen E-ID und Self-Sovereign Identity intensiv auseinander. In diesem Kontext pflegen wir einen regen Austausch mit Vertreterinnen und Vertretern der Wirtschaft, der IT-Branche sowie Non-Profit-Organisationen. Dabei stellen wir fest, dass der neue Vorschlag für das E-ID-Gesetz auf breite positive Resonanz stösst. Zudem werden die Geschwindigkeit und die Transparenz des Gesetzgebungsprozesses von allen Beteiligten sehr geschätzt. Da der Vorentwurf bereits eine sehr hohe Qualität aufweist, fokussiert sich unsere Stellungnahme mehrheitlich auf Empfehlungen für die Umsetzung. Die Kommentare zu einzelnen Artikeln finden Sie im Anhang.

Gestaltung des neuen E-ID-Ökosystems

Wir begrüssen es, dass Bürgerinnen und Bürger mit der neuen E-ID einen universell einsetzbaren Identitätsnachweis mit hohem Datenschutz erhalten sollen, der die Online-Anmeldungen und die Onboarding-Prozesse stark vereinfacht und sicherer macht.

Im Sinne einer ganzheitlichen digitalen Transformation sind wir jedoch der Meinung, dass die E-ID ihr volles Potenzial erst mit der Umsetzung eines umfangreichen E-ID-Ökosystems mit Einbezug aller Wirtschaftssektoren wie Bildung, Gesundheit, Finanz und Mobilität entfaltet. Wie wir in verschiedenen Umsetzungs-Projekten wie *cardossier* oder der *SSI-Initiative* mit dem Kanton AG aufzeigen konnten, ermöglicht das E-ID-Ökosystem nicht nur eine effizientere Ausstellung und Verifikation digitaler Nachweise,



sondern auch die Gestaltung neuer Arbeitsprozesse und allenfalls neuer Geschäftsmodelle. Richtig eingesetzt bringt das Ökosystem damit markante Vorteile für alle Akteure, also sowohl für die Wirtschaft und die Verwaltung als auch für Bürgerinnen und Bürger.

Für den Erfolg der E-ID ist es aus unserer Sicht deshalb zentral, dass bei der Gestaltung und Umsetzung des neuen Gesetzes dem E-ID-Ökosystem die gleiche Aufmerksamkeit geschenkt wird wie der E-ID selbst.

Verbindliche und ausgeglichene Governance

Ein wichtiger Erfolgsfaktor für einen hohen Nutzen der E-ID ist eine frühzeitige und ausbalancierte Regelung der Governance für die Nutzung der Vertrauensinfrastruktur. Sie definiert die Rollen der einzelnen Akteure und die Regeln. So wird zum Beispiel festgelegt, wie die Identität der Beteiligten verifiziert wird, wie die hoheitlichen Nachweise standardisiert werden, wie der Zugang zur Vertrauensinfrastruktur geregelt ist und wie die Gebührenstruktur für die Nutzung der Infrastruktur gestaltet wird. Diese Governance-Themen müssen frühzeitig geklärt werden, damit sich die verschiedenen Akteure auf die Nutzung der Vertrauensinfrastruktur vorbereiten sowie sinnvolle Anwendungen und allenfalls Produkte identifizieren und mit dem nötigen Investitionsschutz implementieren können. Dabei sollte sich der Bund an den bereits existierenden Rollen- und Verantwortungs-Modellen orientieren, die in den o.g. Wirtschaftssektoren bereits implementiert sind.

Bürgerinnen und Bürger im Zentrum

Ein weiteres Thema, das bei der Gestaltung und Umsetzung des neuen Gesetzes mit Priorität angegangen werden muss, ist die Akzeptanz in der Bevölkerung. Der Erfolg der E-ID hängt davon ab, wie konsequent und überzeugend das Gesetz aus der Perspektive der Nutzerinnen und Nutzer zu Ende gedacht und umgesetzt wird (z.B. praxisrelevante Anwendungsfälle, Benutzerfreundlichkeit der Wallets, breite Hardware-Kompatibilität, Delegation von Rechten, einfaches Backup und rasche Wiederherstellung bei Verlust etc.). Dies ist deshalb besonders wichtig, weil die Self-Sovereign-Identity die Verantwortung für die Verwaltung der Identität weitgehend an die Bürgerinnen und Bürger delegiert. Das Spannungsfeld zwischen Sicherheit, Kundenerfahrung und Betriebsorganisation muss deshalb aus der Optik der Nutzerbedürfnisse betrachtet und gelöst werden.

Vertrauen in die Technologie durch offene Standards und Referenzimplementierungen

Das Vertrauen in die eingesetzte Technologie bildet die Basis für den Erfolg der E-ID. Damit Bürgerinnen und Bürger der Technologie vertrauen, braucht es robuste offene Standards und solide Referenzimplementierungen. Abhängig von der Kritikalität der Anwendungsfälle und den rechtlichen Anforderungen müssen strenge Sicherheits- und Qualitätsanforderungen für kritische Architekturkomponenten der Vertrauensinfrastruktur und der Integrationskomponenten gelten, die durch Zertifizierung durchgesetzt werden.



Der Bund soll die Standards sowie die Zertifizierungsprozesse für die relevanten Komponenten des E-ID-Ökosystems definieren und verwalten (z. B. in Form von eCH-Standards, welche die W3C/DIF-Standards ergänzen und Anforderungen für Aussteller, Inhaber und Prüfer definieren). Diese Standards sollten sich an der internationalen Umsetzung (insbesondere eIDAS 2.0) orientieren.

Für spezifische Architekturkomponenten empfehlen wir, dass der Bund Referenzimplementierungen veröffentlicht. Dabei soll berücksichtigt werden, dass die Niveaus 2 und 3 des E-ID-Ökosystems auf eine einfache Integration in die Businessprozesse von Unternehmen und Verwaltungsprozesse der Kantone und Gemeinden angewiesen sind. Dies muss durch ein technologisch adaptives Konzept ermöglicht werden.

Enge Zusammenarbeit von Privatwirtschaft und Verwaltung

Die oben geschilderten Themen sind komplex und verlangen deshalb ein iteratives Vorgehen. Aus unserer Sicht ist es wünschenswert, die Privatwirtschaft zum Beispiel in Form von gemeinsamen Arbeitsgruppen, Studien und Pilotprojekten frühzeitig zu involvieren. So können wir gemeinsam innerhalb der erwähnten Spannungsfelder schnell die notwendigen Erkenntnisse gewinnen, um das E-ID-Ökosystem agil und gewinnbringend zu gestalten.

Fazit

Adnovum steht hinter dem neuen Gesetz, vor allem im Hinblick auf das E-ID-Ökosystem, das zusammen mit der E-ID einen markanten Digitalisierungs-Vorteil für alle Beteiligten bringt.

Aus unserer Sicht werden die E-ID und das E-ID-Ökosystem ein Erfolg sein, wenn man

- dem E-ID-Ökosystem die gleiche Aufmerksamkeit schenkt wie der E-ID selbst,
- die Governance frühzeitig und ausbalanciert definiert,
- die Nutzenden ins Zentrum stellt,
- das Vertrauen in die Technologie durch offene Standards und Referenzimplementierungen fördert,
- und die Erfahrungen der Privatwirtschaft von Beginn an einbindet.

Als langjähriger Vertrauens- und Umsetzungspartner des Bundes freuen wir uns, dieses Vorhaben zu unterstützen.

Freundliche Grüsse

Stefan Hediger
Managing Director Public Sector

Stéphane Mingot
Head of Adnovum Incubator

Anhang: Kommentare zu einzelnen Artikeln



Anhang: Kommentare zu einzelnen Artikeln

Referenz	Kommentar
Art. 5 e	<p><i>"Das fedpol widerruft die E-ID unverzüglich, wenn: e. für dieselbe Person eine neue E-ID ausgestellt wird."</i></p> <p>Dies impliziert, dass es pro Person nur eine E-ID ausgestellt werden kann. In der digitalen Welt könnte diese Einschränkung, die für physische Ausweise Sinn macht, negative Auswirkungen haben. Es kann durchaus sinnvoll und nötig sein, dass eine Person in mehreren Wallets eine E-ID besitzt. Insbesondere für Anwendungsfälle, in welchen eine Verifikatorin Daten von mehreren elektronischen Ausweisen verlangt. Der Inhaber kann für solche Fälle z.B. auf dem Firmentelefon Wallet die E-ID mit weiteren Nachweisen zu seiner Rolle in der Firma und auf dem privaten Telefon eine Wallet mit E-ID und weiteren Nachweisen aus seinem privaten Kontext verwalten. Daher empfehlen wir dies nicht im Gesetz auszuschliessen.</p>
Art. 12.1	<p><i>"1 Wer elektronische Nachweise ausstellen möchte, kann die Infrastruktur nach dem 5. Abschnitt nutzen."</i></p> <p>Dieser Artikel könnte restriktiver formuliert werden, so dass die Ausstellung eines Zertifikats nur unter Beachtung der Governance der vertrauenswürdigen Infrastruktur zulässig ist. Zum E-ID-Ökosystem gehören auch Richtlinien, Vorgaben, Rahmenbedingungen etc., welche vom Aussteller erfüllt werden müssen, um ausstellen zu dürfen.</p>
Art 13.2	<p><i>"1 Die Ausstellerinnen können die von ihnen ausgestellten elektronischen Nachweise widerrufen.</i></p> <p><i>2 Sie widerrufen diese unverzüglich, wenn:</i></p> <ul style="list-style-type: none"><i>a. die Inhaberin oder der Inhaber dies verlangt;</i><i>b. die gesetzliche Vertretung von Minderjährigen bis zum vollendeten vierzehnten Lebensjahr oder von Personen unter umfassender Beistandschaft dies verlangt;</i><i>c. der begründete Verdacht auf Missbrauch des elektronischen Nachweises besteht; "</i> <p>Dieser Artikel geht davon aus, dass alle Nachweise revozierbar sein müssen, und schliesst die Ausstellung und Nutzung von nicht-revozierbaren Nachweisen aus.</p> <p>Die Regel für die Erstellung, den Widerruf und die Verwendung privater Beweismittel muss nicht unbedingt im Gesetz verankert sein, sondern im Governance-Framework.</p>
Art. 15	<p><i>Übertragbarkeit von elektronischen Nachweisen</i></p> <p><i>1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden.</i></p> <p>Im Fall von Minderjährigen, falls eine Übertragbarkeit in das Wallet der Eltern nicht möglich ist, soll mindestens eine Art Delegation der Rechte für die Nutzung des E-ID des Minderjährigen möglich sein.</p>



Referenz	Kommentar
Art. 17.1	<p><i>"Der Bund stellt ein öffentlich zugängliches Register (Basisregister) zur Verfügung, das Daten enthält über:</i></p> <ul style="list-style-type: none"><i>a. die Ausstellerinnen elektronischer Nachweise;</i><i>b. die Verifikatorinnen;</i><i>c. den Widerruf von elektronischen Nachweisen."</i><p>Die Daten der Verifikatorinnen müssen nicht zwingend im Basisregister publiziert werden, sondern im separaten Vertrauensregister (Trust Registry).</p>
Art. 18.2	<p><i>"Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt".</i></p> <p>Aus unserer Sicht sind der Einbezug bzw. die Zulassung und Bestätigung von ausgewählten privaten Ausstellerinnen und Verifikatorinnen für einen erfolgreichen E-ID-Ökosystem zwingend notwendig. Dies sollte daher nicht nur als Möglichkeit formuliert, sondern als Tatsache.</p>
Art. 24	<p><i>"Der Betrieb der Elemente der Vertrauensinfrastruktur erfolgt durch eine Leistungserbringerin innerhalb der Bundesverwaltung."</i></p> <p>Im Sinne der Vertrauensbildung und der föderalen Struktur unseres Staates Rechnung tragend, könnten Elemente der Vertrauensinfrastruktur auch durch kantonale oder kommunale Leistungserbringer betrieben werden.</p>

Bundesrätin Karin Keller-Sutter
Eidgenössischen Justiz- und Polizeidepartements EJPD
Bundeshaus West
CH-3003 Bern

Einreichung per Mail an:
rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

Stellungnahme zum Vorentwurf des E-ID-Gesetzes

Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 29. Juni 2022 eröffnete Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) und übermitteln Ihnen fristgerecht die Einschätzung des Schweizerischen Verbandes der Telekommunikation (asut).

Für die Telekommunikations-Branche ist die Schaffung einer funktionierenden und allgemein akzeptierten E-ID ein Anliegen höchster Priorität. Ebenso begrüssen wir den richtungsweisenden Ansatz, mittels eines datensparsamen Konzepts wie "Self Sovereign Identity" (SSI) ein eigentliches Vertrauensökosystem für digitale Nachweise aller Art zu etablieren.

Denn eine solche Basisinfrastruktur bietet Gewähr für eine digitale Landschaft, auf deren Grundlage sich bereits bestehende Anwendungen überhaupt erst in der Breite etablieren und neue digitale Angebote ge-
deihen können.

Neben der technologieneutralen Regulierung sehen wir eine zeitnahe praktische Umsetzung als zentralen Erfolgsfaktor des Vorhabens.

Damit die Digitalisierung der Schweiz keine weitere Verzögerung erleidet, möchten wir daher eine überlap-
pende Vorgehensweise zwischen Rechtsetzung und technischer Umsetzung anregen, sodass der Aufbau des Vertrauensökosystems ab Inkrafttreten des vorliegenden Gesetzes starten kann. Mit Blick auf den hohen volkswirtschaftlichen Nutzen sowie die breit abgestützte, politische Akzeptanz des vorliegenden Vorhabens erscheint uns dieses gerechtfertigt.

Schliesslich muss der inklusive Charakter des Vorhabens auch konsequent in die Praxis überführt werden, so dass die für die Etablierung und Aufrechterhaltung des Ökosystems notwendigen Anreize an alle Akteure gesetzt und erhalten werden können.

Wir danken Ihnen für den Entwurf, den wir im vorstehenden Sinne begrüssen. Für die Berücksichtigung unserer Punkte danken wir Ihnen im Voraus.

Freundliche Grüsse

asut – Schweizerischer Verband der Telekommunikation



Peter Grütter, Präsident



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation - Rue des Chanoines 2, 1700 Fribourg

Office fédéral de la justice
Bundesrain 20
3003 Berne
rechtsinformatik@bj.admin.ch

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

La Commission

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm

Réf: 2022-PrD-242/2022-Trans-163/2022-Méd-34
Courriel: secretariatatprdm@fr.ch

Fribourg, le 5 octobre 2022

Avant-projet de la loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques (Loi sur l'e-ID, LeID)

Madame, Monsieur,

La Commission se prononce sur l'avant-projet de loi fédérale sur l'identité électronique et autres moyens de preuve électronique (LeID) mis en consultation par le Conseil fédéral lors de sa séance du 29 juin 2022.

La Commission en a traité lors de sa séance du 4 octobre 2022. Elle ne se prononce que sur les aspects relatifs à la protection des données, à la transparence et à la médiation administrative (art. 30a al. 1 let. b de la loi du 25 novembre 1994 sur la protection des données, LPrD ; RSF 17.1 ; art. 40 let. c de la loi du 9 septembre 2009 sur l'information et l'accès aux documents, LInf ; RSF 17.5 ; art. 6 al. 2 let. c de la loi du 25 juin 2015 sur la médiation administrative, LMéd ; RSF 181.1).

A toutes fins utiles, la Commission tient à relever que son examen se limite à vérifier la conformité des dispositions aux exigences des règles de protection des données, de transparence et de médiation administrative. Il ne lui appartient pas de rendre attentif sur les conséquences du respect des exigences, ni de vérifier si des traitements de données nécessitant une base légale auraient été oubliés.

I. Sous l'angle de la protection des données

1. Généralités

La Commission salue la création d'une base légale formelle tendant à créer une nouvelle identité électronique (e-ID) qui permettra de prouver son identité par des moyens numériques, de manière simple, sûre et rapide et dont l'émission et l'exploitation de l'infrastructure nécessaire seront du ressort de la Confédération. Elle se réfère à sa prise de position du 24 avril 2017 relative à la loi fédérale sur les moyens d'identification électronique reconnus, disponible sur le site Internet www.fr.ch/atprdm.ch, publications, consultations.

2. Remarques par articles – AP-LeID

- > **Ad article 2 alinéa 3 lettre a :** La Commission estime qu'il n'est pas nécessaire que l'e-ID contienne le numéro AVS pour atteindre le but visé à l'article 1 alinéa 2 lettre a AP-LeID, soit pour garantir une identification sûre entre personnes privées et entre personnes privées et autorité. Il sied de préciser qu'une utilisation systématique de ce dernier à des fins d'identification comporterait un grand risque d'interconnexions de données personnelles dans les différents systèmes et élargirait considérablement son utilisation, ce qui contreviendrait au but même recherché par le présent projet de loi. En effet, le numéro AVS a été initialement prévu pour être utilisé dans le domaine des assurances sociales et, en principe, son utilisation systématique devrait être autorisée uniquement aux organes et services chargés des tâches dans ce domaine.

Dans l'hypothèse où le numéro AVS serait malgré tout utilisé, la Commission propose qu'une disposition soit ajoutée à la loi, selon laquelle des mesures techniques rendraient l'utilisation systématique du numéro AVS possible uniquement pour les vérificateurs prévus selon ladite loi. Ceci afin d'éviter que des vérificateurs privés qui utilisent l'e-ID n'y aient accès:

- > **Articles. 3 et 4 :** L'article 6 alinéa 5 nLPD dispose que « *[c]elui qui traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment du type de traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées* ». Et plus l'atteinte aux droits fondamentaux peut être grave, plus la base légale doit être précise.

En l'occurrence, une e-ID émise qui contiendrait des données incorrectes engendrerait un risque important sous l'angle des droits fondamentaux de la personne concernée et notamment la question de l'usurpation d'identité. Par conséquent, des mesures qui permettraient d'atténuer de tels risques doivent, soit figurer dans le présent projet, soit être concrétisées dans la procédure d'émission réglée par le Conseil fédéral par le biais de l'article 4 alinéa 5. De même, et au vu de l'importance de ces risques, il convient de supprimer le dernier paragraphe de la page 9 du Rapport explicatif de ladite loi se rapportant à l'article 3 exposant que la possibilité de procéder à une nouvelle vérification de l'identité du requérant, autre que le fait de présenter une preuve d'identité suisse valide, « *a été abandonné pour des raisons de coûts, de convivialité et de rapidité. En effet, cette démarche aurait été plus coûteuse que l'obtention d'un document d'identité* ».

- > **Ad Article 7 et 8 :** Ces dispositions, en particulier celle qui prévoit des bureaux cantonaux, semblent judicieuses compte tenu de la proximité des autorités cantonales avec les citoyens. La Commission propose que des mesures d'accompagnement en lien avec le devoir de diligence soient prévues, qui accompagnent les détenteurs de l'e-ID. Ces mesures pourraient figurer clairement et de manière aisément accessible dans l'application avec l'e-ID.

- > **Ad Article 10 :** La Commission salue la possibilité d'offrir le choix de présenter une e-ID ou un autre document d'identification, afin de garantir la non-discrimination entre personnes qui souhaitent utiliser l'e-ID, et celles qui ne le souhaitent pas.
- > **Ad Article 10 et 16 en lien avec la minimisation des données de la part du vérificateur :** Il s'agit ici de veiller à ce qu'il n'y ait pas surabondance de données personnelles lors de l'identification. La forme et l'utilisation de preuves électroniques sont réglées aux articles 10 et 16 AP-LeID. Selon l'article 16 alinéa 1 AP-LeID, c'est le titulaire du moyen de preuve électronique qui détermine quels éléments de ce moyen de preuve sont transmis au vérificateur. Mais l'explication relative à cet article 16 AP-LeID dans le Rapport explicatif (page 13) est en contradiction avec l'article 16 AP-LeID, puisqu'il figure dans le Rapport explicatif que c'est au vérificateur de définir les données requises en l'occurrence, ce qui limite la marge de manœuvre du titulaire. Il en résulte que si le titulaire refuse de communiquer les données demandées par le vérificateur, il ne pourra pas utiliser le service concerné.

Par ailleurs, une mention explicite des principes de protection des données dans ledit avant-projet nous semble justifiée en raison du fait qu'une possibilité d'identification simple par voie électronique entraîne de nouvelles obligations d'identification et des collectes de données inutiles qui n'auraient pas été nécessaires en cas d'identification analogique.

Enfin, le vérificateur devrait être tenu de ne pas enregistrer ou transmettre les données d'identification ou de les traiter autrement, sauf si une obligation le requiert. Une collecte de données supplémentaires sur la base du consentement, sous la forme d'une manifestation de volonté en dehors du processus de vérification, d'une personne dans un contexte de droit privé serait possible dans une seconde étape distincte après l'identification.

- > **Ad Article 11 :** Le système prévoit différents interfaçages avec d'autres systèmes d'informations (alinéa 3). A la page 11 du Rapport explicatif pour l'ouverture de la procédure de consultation de l'AP-LeID, il est mentionné que « *[l]es données consultées ne sont ni dupliquées ni sauvegardées dans le système d'information de fedpol* ». Cela devrait être explicitement exprimé dans le texte de la loi afin d'ancrer juridiquement la mise en œuvre du principe de stockage décentralisé des données. L'alinéa 4 pourrait être complété en indiquant que les données obtenues au travers de ces interfaces sont traitées exclusivement dans le but d'émettre l'e-ID, et qu'elles ne sont pas conservées dans le système d'information.
- > **Ad Section 3 concernant les autres moyens de preuve électroniques :** La Commission relève que la durée de conservation des autres moyens de preuve électroniques n'est pas traitée dans le présent avant-projet.
- > **Ad Article 12 :** Cette disposition mentionne que quiconque peut émettre des moyens de preuve électroniques au moyen de l'infrastructure prévue à la section 5. Le Rapport explicatif précise qu'il peut s'agir de personnes privées. Or, rien dans cet avant-projet ne mentionne les mesures à prendre en cas de faillite ou de cessation d'activité de l'émetteur comme personne

privée, ce qui ne remplit pas les exigences de la protection des données. En effet, cela pourrait amener indirectement à une commercialisation des données personnelles.

- > **Ad Article 16 al. 3 :** La partie de phrase « *dans toute la mesure du possible* » devrait à notre sens être supprimée. Selon cet article, l'exploitant des systèmes n'a pas connaissance du contenu des moyens de preuve électronique présentés. S'il n'est pas possible de ne pas tirer de conclusions sur son utilisation et sur les autorités et personnes privées impliquées pour des raisons techniques ou juridiques, ces raisons doivent être clairement expliquées.
- > **Ad Article 17 :** Cette disposition prévoit de manière générale que « *[l]a Confédération met à disposition un registre accessible au public (registre de base) où sont stockées des données* ». Le Rapport explicatif mentionne à la page 13 qu'« *[i]l n'est pas encore déterminé quels services de l'administration fédérale seront responsables de la mise en place et de l'exploitation des différents éléments de l'infrastructure de confiance. C'est pourquoi la section 5 parle encore de manière générale de « Confédération* ». Sur la base des expériences faites avec les projets pilotes, cette question devra être clarifiée et fixée lors de l'élaboration du message ». Or, la disposition légale doit indiquer quel organe fédéral est responsable de la sécurité du système et de la légalité du traitement de données afin que la personne concernée puisse savoir auprès de quelle autorité elle peut faire valoir ses droits et en particulier son droit d'accès. Cette indication devrait figurer dans l'AP-LeID.
- > **Article 17 al. 3, Article 18 al. 2 et Article 22 :** L'article 17 alinéa 3 AP-LeID devrait à notre sens être modifié de manière à prévoir la vérification de l'identité des émetteurs et vérificateurs privés.

Le Rapport explicatif expose à la page 14 qu'« *il existe un risque que des émetteurs ou des vérificateurs puissent délivrer des preuves électroniques en usurpant leur identité* ». Toutefois, afin de ne pas mobiliser des ressources importantes pour parer à un goulot d'étranglement coûteux et inutile, le Rapport explicatif indique qu'il y a lieu de renoncer à la vérification de l'identité des émetteurs et vérificateurs privés. Ainsi, il est à prévoir que les émetteurs et les vérificateurs ne puissent pas inscrire eux-mêmes leurs données dans le registre de base sans vérification, par exemple, à travers une communication hors des systèmes de la LeID.

- > **Ad Article 23 :** La Commission salue cet article car il contribue à donner confiance dans les solutions techniques du domaine traité par l'AP-LeID.

II. Sous l'angle de la transparence

La Commission n'a aucune remarque à formuler concernant cette thématique.



III. Sous l'angle de la médiation administrative

La Commission n'a aucune remarque à formuler concernant cette thématique.

Tout en vous souhaitant bonne réception de la présente, nous vous prions de recevoir, Madame, Monsieur, nos salutations les meilleures.



Laurent Schneuwly
Président

Copie à :

—

Chancellerie d'Etat, Madame D. Gagnaux-Morel, Chancelière d'Etat, Rue des Chanoines 17, Céans

Épalinges, le 14 octobre 2022

Dossier traité par :
Daniel Rohrer, 078 739 88 20
daniel.rohrer@cara.ch

Office fédéral de la justice
M. Rolf Rauschenbach
Bundesrain 20
3003 Berne

Prise de position sur l'avant-projet de Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques

Monsieur,

Nous avons pris connaissance avec intérêt de l'avant-projet de Loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID). Nous vous faisons parvenir ci-après nos commentaires.

- En tant que communauté au sens de la LDEP constituée et financée par des cantons, CARA soutient l'implication directe de la Confédération pour l'identité électronique. Nous pensons en effet qu'elle seule dispose de la légitimité suffisante et peut fournir les garanties nécessaires à l'établissement d'une identité électronique sûre et largement diffusée.
- Avec l'utilisation du dossier électronique du patient (DEP), des dizaines de milliers de citoyennes et de citoyens auront déjà une identité certifiée selon la LDEP. Le processus d'obtention, pour des raisons de sécurité, est complexe. Il est donc impératif que ces citoyens puissent conserver leur identité lors de l'arrivée de la nouvelle eID et ne doivent pas passer par une nouvelle procédure de vérification.
- De notre expérience dans le cadre du DEP, nous constatons tous les jours le besoin important en termes d'assistance aux utilisatrices et utilisateurs, en particulier en ce qui concerne l'obtention et l'usage d'une identité électronique. Il est donc capital que la Confédération fournisse un service d'assistance doté des ressources suffisantes et facilement joignable. Il s'agira de disposer d'un véritable centre d'appel qui puisse accompagner et dépanner les utilisateurs.
- Il sera très utile de prévoir la possibilité de « porter » l'identité électronique d'une personne mineure ou sous curatelle. Un parent pourra ainsi « porter » l'identité de son enfant comme il porte actuellement sa carte d'identité physique.

Nous vous remercions de votre attention et restons, Monsieur, à votre disposition pour toute question ou pour une rencontre afin de vous faire bénéficier de notre expérience en matière d'utilisation des identités électroniques par le public du dossier électronique du patient.


CARA
Patrice Hof, secrétaire général

Madame la Conseillère fédérale
Karin Keller-Sutter
Cheffe du Département fédéral de
justice et police
3003 Berne

Par courrier électronique :
rechtsinformatik@bj.admin.ch

Paudex, le 30 septembre 2022
GDO

**Procédure de consultation : loi fédérale sur l'identité électronique et les autres
moyens de preuve électroniques (loi sur l'e-ID, LeID)**

Madame la Conseillère fédérale,

Nous avons pris connaissance du projet cité en titre, mis en consultation par vos services et qui a retenu toute notre attention. Nous prenons ainsi la liberté de vous adresser notre position.

Généralités

Après le rejet par le peuple de la loi fédérale sur les services d'identification électronique le 7 mars 2021, le Conseil fédéral, le Département fédéral de justice et police, la Chancellerie fédérale et le Département fédéral des finances ont su réagir rapidement. Par ailleurs, les Chambres fédérales ont approuvé six motions allant dans ce sens, émanant de tous les groupes parlementaires, et demandant la mise en place d'un système géré par la Confédération sans passer par un intermédiaire privé.

L'évolution rapide et constante du numérique et son installation dans l'immense majorité de nos activités poussent au développement de son utilisation dans le rapport qu'exercent les citoyens suisses avec la Confédération. Il est nécessaire que la Confédération développe ses activités digitales tant dans son infrastructure interne que dans ses rapports externes. L'élaboration d'une identité électronique qui permet aux citoyens de s'identifier de façon sûre, simple et rapide tant numériquement que dans le monde réel tout en minimisant les obstacles administratifs est une avancée hautement désirable.

Nous soutenons ainsi le projet mis en consultation.

Remarques particulières

Contrairement à la loi rejetée en votation, c'est désormais la Confédération qui émettra les e-IDs et exploitera l'infrastructure nécessaire dite « infrastructure de confiance ».

Nous jugeons positivement que les données soient stockées de manière décentralisée sur un support déterminé par le titulaire de l'e-ID, et que ledit titulaire en garde ainsi le contrôle. Le concept d'auto-souveraineté impliquant un détachement des données par la Confédération et un contrôle total par l'individu est dans ce sens souhaitable.

Il est ainsi nécessaire que la Confédération n'ait de facto pas d'accès aux données des citoyens dépassant ce qui est prévu par la loi. Il en va de la protection de la sphère privée.

Par ailleurs, il est appréciable que l'art. 10 prévoie que quiconque offre la possibilité de présenter une e-ID ou une partie d'une e-ID, doive laisser au citoyen le choix alternatif de s'identifier au moyen d'un document d'identité au sens de la LDI. Nous restons ainsi libres d'utiliser un moyen d'identification physique, l'e-ID n'étant pas une solution imposée mais proposée aux citoyens.

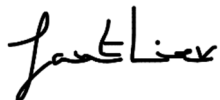
Il est important que la Confédération fasse ses preuves en matière de numérique. Il faut que la solution proposée soit digne de confiance, sûre en matière de sécurité des données et simple d'utilisation. L'application de l'e-ID doit par son utilisation offrir une valeur ajoutée pour la population et l'économie.

Finalement, l'e-ID est conçue dans le projet comme neutre technologiquement et nous en soulignons l'importance. Cette neutralité permet une certaine agilité quant à l'adaptation aux nouvelles réalités technologiques.

En conclusion, nous approuvons le projet mis en consultation, tout en faisant remarquer l'importance de la protection de la sphère privée, de la liberté d'utilisation, de l'efficacité et de l'efficience de l'e-ID.

Nous vous remercions de l'attention que vous porterez à ce qui précède et vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre haute considération.

Centre Patronal



Gauthier Dorthe

Per Mail an: rechtsinformatik@bj.admin.ch

Bundesrätin Karin Keller-Suter
Vorsteherin des Eidgenössischen
Justiz- und Polizeidepartements
EJPD Bundeshaus West
3003 Bern

Bern, 20. Oktober 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Bundesrätin, sehr geehrte Damen und Herren

ChiroSuisse bedankt sich für die Gelegenheit zur Stellungnahme.

Die Schaffung einer gesetzlichen Grundlage für einen elektronischen Identitätsnachweises erachten wir als dringend notwendig, die vorgeschlagene Umsetzung als weitgehend gelungen.

Im Übrigen schliessen wir uns den Stellungnahmen der IG ehealth und von HIN an.

Freundliche Grüsse

ChiroSuisse



Mireille Schläppi
Vorstand ChiroSuisse
Departement Digitalisierung



Sabine Schläppi
CEO

IG eHealth, Amthausgasse 18 3011 Bern

Per Mail an: rechtsinformatik@bj.admin.ch

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements
EJPD Bundeshaus West
3003 Bern

Bern, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Die IG eHealth bedankt sich beim eidgenössischen Justiz- und Polizeidepartement EJPD und beim Bundesamt für Justiz BJ für den partizipativen Prozess bei der Erarbeitung des Entwurfs des E-ID-Gesetzes, den wir als mustergültig und nachahmenswert erachten. Wir bedanken uns auch für die rasche Ausarbeitung der Vernehmlassungsvorlage, die wir insgesamt als sehr gelungen und praxistauglich einschätzen.

Für das Gesundheitswesen ist ein elektronischer Identitätsnachweis (E-ID) eine zentrale Voraussetzung für die Nutzung von digitalen Dienstleistungen und eine vertrauenswürdige Kommunikation zwischen Gesundheitsfachpersonen und PatientInnen. Insofern wünschen wir eine zeitnahe Verabschiedung und Überweisung der Botschaft und des Gesetzesentwurfs ans Parlament.

Gemäss dem Gesetzesentwurf ist die Ausstellung und die Verwendung der neuen E-ID freiwillig. Wir begrüssen es, dass die Bevölkerung und die Gesundheitsfachpersonen die Wahl haben, wie sie auf das EPD zugreifen wollen. Die E-ID gemäss vorliegendem Gesetzesentwurf ist ein digitales Pendant zum physischen Pass oder zur Identitätskarte. Es ist kein «Login» im Sinne einer Authentifikation. Zu prüfen ist, ob dieser Punkt im Gesetz aufzunehmen ist.

Wir möchten einen Punkt zu Art. 16 Abs 1 Vorweisen von elektronischen Nachweisen anfügen. Der Artikel ist gut formuliert, wir erachten aber die Erläuterungen als unpräzise. Gemäss des Gesetzesartikels bestimmt die InhaberIn der E-ID, welche Bestandteile vom Verifikator geprüft werden. In den Erläuterungen steht unserer Meinung nach fälschlicherweise, dass dies der Verifikator bestimmt. Die Verifikatorin darf im Sinne der Datensparsamkeit nicht mehr Inhalte verlangen als absolut notwendig sind.

Nachfolgend gehen wir auf ausgewählte Elemente im Gesetzesentwurf ein, die aus unserer Sicht zu präzisieren sind:

Artikel 1

Entwurf Bundesrat	<p>2 Es hat zum Zweck:</p> <p>a. die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten;</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, 2. Datensicherheit, 3. Datensparsamkeit, und 4. dezentrale Datenspeicherung; <p>c. zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen;</p> <p>d. die Standardisierung der E-ID sowie die Sicherheit der Infrastruktur und der Ausstellung und Überprüfung der elektronischen Nachweise zu gewährleisten, ohne die technische Entwicklung unnötig einzuschränken.</p>
Änderungsvorschlag	<p>...</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, <u>2. Datenschutz durch datenschutzfreundliche Voreinstellungen</u> <u>3.</u> Datensicherheit, <u>4.</u> Datensparsamkeit, und <u>5.</u> dezentrale Datenspeicherung; <p>...</p>
Begründung	<p>Das revidierte Datenschutzgesetz verankert die Prinzipien «Privacy by Design» (Datenschutz durch Technik) sowie «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen). Im E-ID-Gesetz wird nur das Prinzip «Datenschutz durch Technik» explizit erwähnt. Aus unserer Sicht ist ebenfalls der «Datenschutz durch datenschutzfreundliche Voreinstellungen» aufzunehmen. Somit kann sichergestellt werden, dass beispielsweise die Voreinstellungen von Apps, die digitale Nachweise speichern, auf das nötige Mindestmass beschränkt werden.</p>

Art. 8 Anlaufstellen der Kantone

Entwurf Bundesrat	Die Kantone bezeichnen die Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Änderungsvorschlag	Die Kantone bezeichnen die <u>öffentlichen oder privaten</u> Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Begründung	Der Gesetzesartikel ist so zu präzisieren, dass die Kantone öffentliche und private Stellen für die Unterstützung bezeichnen können.

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung zu definieren hat. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art. 16 Abs 3 Vorweisen von elektronischen Nachweisen

Entwurf Bundesrat	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann möglichst keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen.
Änderungsvorschlag	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann <u>möglichst darf</u> keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen <u>können</u> .
Begründung	Die E-ID muss technisch so ausgestaltet sein, dass keine Rückschlüsse möglich sind. Ansonsten würde das das Prinzip «privacy by default» verletzt.

Art. 17 Basisregister

Entwurf Bundesrat	3 Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.
Änderungsvorschlag	3 Der Bundesrat regelt, welche Daten die Ausstellerinnen und Verifikatorinnen in das Basisregister einstellen dürfen.
Begründung	Gemäss dem Artikel müssen Ausstellerinnen und Verifikatorinnen ihre Daten in das Basisregister eintragen. Eine Eintragung ohne vorgängige Prüfung durch die entsprechende Stelle des Bundes öffnet dem Identitätsdiebstahl Tür und Tor. Es dürfte dem Vertrauen in das Basisregister schaden, wenn Einträge von Ausstellerinnen und Verifikatorinnen widerrufen werden müssen. Es ist eine Delegationsnorm zu schaffen, damit der Prozess der Überprüfung auf Verordnungsstufe präzisiert werden kann.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat <u>sieht vor</u> kann vorsehen , dass der Bund die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

Art. 24bis (neu) Überprüfung der Vertrauensinfrastruktur

Entwurf Bundesrat	-
Ergänzungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bedanken uns für die Prüfung und ggf. Berücksichtigung unserer Eingabe im Rahmen der Erarbeitung der Botschaft des Bundesrats und des Gesetzesentwurfs, der zu Händen des Parlaments verabschiedet wird.

Freundliche Grüsse
Im Namen des Vorstands

Anna Winter
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD Bundeshaus West
CH-3003 Bern

Einreichung per Mail an: rechtsinformatik@bj.admin.ch

Wallisellen, 17. Oktober 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zum neuen Vorschlag für ein E-ID-Gesetz äussern zu können, welche wir hiermit gerne wahrnehmen. Einleitend möchten wir dem EJPD für den partizipativen Prozess der Erarbeitung des BG E-ID danken, den wir als mustergültig und nachahmenswert erachten.

Grundsätzlich sind wir der Überzeugung, dass der Vorschlag für das E-ID-Gesetz eine sehr gute Basis darstellt und den Rahmen für eine Vertrauensinfrastruktur setzt, in dem eine staatlich herausgegebene E-ID das Kernelement darstellt. Wir begrüssen den Paradigma-Wechsel im Umgang mit personenbezogenen Daten und die Schaffung eines Rechtsrahmens für eine Vertrauensinfrastruktur.

Eine verlässliche Vertrauensinfrastruktur hat für das Gesundheitswesen und dessen Digitalisierung eine zentrale Bedeutung. Wir erachten es als äusserst wichtig, dass die Vertrauensinfrastruktur offen, sicher und verlässlich gestaltet ist und diese von allen Marktteilnehmern gleichermassen genutzt werden kann. Zudem sollte sie auch regelmässig von einer unabhängigen Instanz überprüft werden. Die E-ID soll sich darin als zentraler Nachweis der Identität von Personen verstehen und für die verschiedensten sektorspezifischen Anwendungen eingesetzt werden können. Grosse Wichtigkeit wird auch der zeitnahen Anpassung der Gesetze zugeschrieben, welche die Verwendung von elektronischen Identitäten definieren. Insbesondere sollte das Bundesgesetz über das elektronische Patientendossier EPDG entsprechend angepasst werden. Gemäss EPDG zertifizierte Identity Provider IDP sind per Inkraftsetzung des BG E-ID von Zertifizierungspflichten des EPDGs zu entbinden.

Spezifisch sehen wir folgende Punkte, die im Gesetzesentwurf präzisiert werden müssen:

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung definieren muss. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art 15 Übertragbarkeit von elektronischen Nachweisen

Entwurf Bundesrat	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. ...
Änderungsvorschlag	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. <u>1^{bis (neu)} Der Bundesrat sieht Ausnahmen für die Vormundschaft gemäss Art. 327a ff. ZGB für Minderjährige und die umfassende Beistandschaft gemäss Art. 388 ff. ZGB von Erwachsenen vor.</u> ...
Begründung	Es braucht eine Ausnahmeregelung für die Vormundschaft für Minderjährige und die umfassende Beistandschaft bei Erwachsenen mit einer entsprechenden Referenzierung der relevanten ZGB-Artikel.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat <u>sieht vor</u> kann vorsehen , dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss eine die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

	Ein konkretes Beispiel: die Erteilung von Facharzttiteln durch das Schweizerische Institut für ärztliche Weiter- und Fortbildung SIWF.
--	--

Art. 24^{bis (neu)} Überprüfung der Vertrauensinfrastruktur

Entwurf Bundesrat	-
Änderungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bitten den Bundesrat, Experten der Zivilgesellschaft, der Wissenschaft und der Wirtschaft für die Ausarbeitung der entsprechenden Verordnung und Ausführungsbestimmung beizuziehen.

Wir sind davon überzeugt, dass mit einer speditiven Implementierung der Vertrauensinfrastruktur in der Schweiz der Digitalisierung in den verschiedenen Bereichen eine signifikante Weiterentwicklung ermöglicht wird.

Freundliche Grüsse

HEALTH INFO NET AG

Lucas Schult
Geschäftsführer (CEO)

Peer Hostettler
Leiter Vertrieb



Eidgenössisches Justiz- und Polizeidepartement EJPD

Frau Bundesrätin Karin Keller-Sutter

3003 Bern

per E-Mail an rechtsinformatik@bj.admin.ch

Lausanne, 20. Oktober 2022

Vernehmlassungsantwort zum Entwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Mit grossem Interesse haben wir die Vernehmlassung zum BGEID zur Kenntnis genommen. Unsere Organisation CH++ widmet sich unabhängig einer nachhaltigen, wohlhabenden und handlungsfähigen Schweiz durch Wissenschaft und Technologie. Das Thema E-Id verfolgen wir seit der Neulancierung entsprechend intensiv und haben uns verschiedentlich bereits direkt wie indirekt eingebracht.

CH++ unterstützt das aktuelle Vorgehen in weiten Teilen, insbesondere den aktiven Einbezug der Community aus Wissenschaft und Technologie. Eine gute, vertrauenswürdige E-Id ist für uns **datensparsam, dezentral und open source** — und wird agil, nutzerzentriert und inklusiv entwickelt. Wo diese Grundsätze mit dem Entwurf noch in Konflikt stehen, erlauben wir uns im Folgenden eine knappe, unterstützende Rückmeldung.

Wir bedanken uns für Ihr Interesse und stehen Ihnen für weiteren Dialog stets gerne zur Verfügung.

Hannes Gassert, Präsidium

Marcel Salathé, Präsidium

Olga Baranova, Geschäftsleitung

Allgemeine Würdigung

CH++ hat sich bereits in der Vergangenheit positiv zum Ansatz der Self Sovereign Identity geäußert, ebenso zur Idee eines Ökosystems von digitaler Infrastruktur. Im jetzt vorliegenden Entwurf des E-ID-Gesetzes sehen wir eine deutliche Verbesserung im Vergleich zur in der Volksabstimmung abgelehnten Vorlage. Unabhängig vom Gesetzgebungsprozess wollen wir Sie dazu ermutigen, weiter und in grossem Tempo die konkrete, prototypische Entwicklung und Erprobung der E-ID voranzutreiben, mitunter als Pilotversuch unter Art. 15 EMBAG — und Erkenntnisse daraus laufend einfließen zu lassen in die Entwürfe des Gesetzes und sodann der Verordnung.

Artikel 1

Nach Ansicht von CH++ ist der Zweckabschnitt gut gelungen, in seiner Breite schafft er einen grossen Raum an Möglichkeiten. Es wäre aber für den weiteren Verlauf nun wünschenswert, hier einen minimalen, allgemeingültigen Anwendungsfall zu beschreiben, den die E-Id künftig mindestens abdecken wird und damit den Zweck etwas zu konkretisieren.

Artikel 3

Um die E-ID möglichst inklusiv zu gestalten, möchten wir hier die Möglichkeit anregen, auch Menschen ohne gültige Aufenthaltsbewilligung den Zugang zur E-Id anzubieten, etwa auf Basis eines ausländischen Passes. Eine entsprechende Kann-Formulierung scheint uns hier sinnvoll und angebracht.

Artikel 4

CH++ schlägt vor, dass die E-ID auch vor Ort, etwa in einem Passbüro, beantragt und bezogen werden kann. Wir erhoffen uns ebenfalls inkludierende Wirkung und eine höhere Verbreitung über alle Bevölkerungsschichten hinweg.

Artikel 16

Im Sinne der in der Einleitung erwähnten Datensparsamkeit ist hier eine Überidentifikation zu vermeiden. Hierzu unterstützen wir den Vorschlag der Referendumsallianz.

Besonders wichtig ist uns hier der Aspekt Open Source. Das Entwicklungsmodell hat sich etwa bei den Covid-Apps als herausragend zweckmässig und qualitätsfördernd erwiesen. Das Gesamtsystem, von der Vertrauensinfrastruktur über das System für Sicherungskopien bis hin zu den Apps unter einer allgemein anerkannten Open Source Lizenz veröffentlicht und gepflegt werden. Dies betrifft entsprechend auch die Artikel 19, 20, und 21. Wir regen darum an, diesen Grundsatz in einem separaten Artikel klar und verbindlich festzulegen.

Artikel 26

Wir schlagen vor, hier keine Gebühren zu erheben. Die zu erwartenden Einnahmen stehen nach unserer Einschätzung in keinem guten Verhältnis zur so erreichten Verminderung der Verbreitung.

cldn:

conférence latine des
directeurs du numérique

fr · ge · ju · ne · ti · vd · vs

Par courriel
Département fédéral de justice et police
Mme Karin Keller-Sutter
Conseillère fédérale
Palais fédéral ouest
Bundesgasse 3
3003 Berne

Réf. : SDB/ABA

Genève, le 11 octobre 2022

Consultation sur l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID)

Madame la Conseillère fédérale,

Vous avez lancé le 29 juin dernier une consultation sur l'avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID). Par ce courrier, la Conférence latine des directeurs cantonaux du numérique (CLDN), créée en 2019 et seule conférence politique intercantonale traitant spécifiquement des enjeux relatifs au numérique, vous fait part de sa position.

La CLDN salue le travail qui a été effectué par le Conseil fédéral suite au refus de la loi fédérale sur les services d'identification électronique (LSIE) par le peuple le 7 mars 2021. Nous relevons que le fond et la forme s'inscrivent dans la vision que porte notre Conférence : une approche centrée sur les besoins de la population et qui s'inscrit dans la vie des gens, une législation qui est technologiquement neutre, un rôle actif de l'Etat là où il est nécessaire à la confiance, enfin une attention aux enjeux du progrès technique et de la collaboration internationale. Le mode d'élaboration de ce projet de loi fédérale dans une approche ouverte, associant les services cantonaux, le secteur privé et la société civile, nous réjouit. Nous saluons également la vitesse à laquelle un nouveau projet législatif ambitieux a été élaboré.

Ceci étant posé, la CLDN soutient globalement la prise de position commune présentée par la Conférence des gouvernements cantonaux (CdC). Elle souhaite cependant préciser et formuler trois réserves, relatives aux trois articles suivants :

- 1) Art. 3 : nous relevons que le périmètre des personnes pouvant obtenir une e-ID n'est pas identique au périmètre des personnes susceptibles d'interagir avec les administrations cantonales. Si cela n'est pas le cas, les cantons pourraient être contraints de maintenir des moyens d'identification électronique cantonaux afin de ne pas priver une partie de leur population. Il s'agit par exemple de personnes vivant

en Suisse sans disposer d'un permis de séjour, de membres de famille de fonctionnaires d'organisations internationales ou encore de propriétaires de résidences secondaires ou de touristes à qui des prestations numériques spécifiques sont également destinées.

- 2) Art. 8 : les points de contact cantonaux ne sont pas nécessairement établis actuellement. Il serait judicieux de considérer une solution de support sur le plan national. En complément, de même que la Confédération souhaite financer certains investissements par l'Administration numérique suisse (ANS), il semblerait pertinent d'explorer un financement par l'ANS visant à la mise en place initiale de points de contact cantonaux.
- 3) Art. 26 : le projet prévoit des émoluments pour les cantons et les communes afin de les inscrire dans le registre de base et dans le système de confirmation des identifiants au titre d'émetteurs et de vérificateurs. Ce, alors que les autorités sont obligées d'accepter l'e-ID (art. 9). Or, l'art. 3, al. 2, OGEmol énonce que l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes pour autant qu'ils lui accordent la réciprocité. Il convient de veiller à ce que cette disposition s'applique également au cas présent et à ce que les compensations entre les collectivités publiques soient réduites au minimum ou, de préférence, que les collectivités publiques soient exonérées de ces émoluments. De plus, les autres acteurs prestataires de services publics numériques devraient se voir exonérés d'émolument, afin d'assurer une adhésion élevée à ce système, par exemple dans le domaine de la santé.

Par ailleurs, nous prenons bonne note de l'intention de clarifier le rôle de l'identité électronique nationale par rapport à des moyens d'identification sectoriels, par exemple dans le domaine de la santé, et soutenons cette orientation, tout en relevant le point d'attention sur les publics qui pourraient être exclus d'un accès, par exemple, au dossier électronique du patient.

Les gouvernements des cantons membres de la CLDN adresseront par ailleurs chacun un courrier de prise de position.

En vous remerciant d'avance de l'attention accordée aux arguments de la CLDN, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.



Serge Dal Busco
Président de la CLDN

Copies

- Membres de la CLDN



eAHV/IV – eAVS/AI
p.a. mundi consulting ag
Marktgasse 55
Postfach
3001 Bern
Mail info@eahv-iv.ch
Web www.eahv-iv.ch
Tf. +41 31 326 76 76

Geht an
Eidgenössisches Justiz- und Poli-
zeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter

Via Mail an
rechtsinformatik@bj.admin.ch

Bern, 18. Oktober 2022

**Antwort zur Vernehmlassung:
Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektro-
nische Nachweise (BGEID)**

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, uns zum erwähnten Gesetzesentwurf zu äussern. eAHV/IV ist verantwortlich für den Datenaustausch und Digitalisierung in der 1. Säule der Sozialversicherungen und Familienzulagen. Unsere Vereinsmitglieder sind die Konferenz der kantonalen Ausgleichskassen (KKAK), die Vereinigung der Verbandsausgleichskassen (VVAK), die IV-Stellen-Konferenz (IVSK) sowie die Zentrale Ausgleichsstelle (ZAS).

Die vertretenen rund 110 Durchführungsstellen sehen sich aufgrund ihrer gesetzlichen Aufgaben in den Sozialversicherungen zur Nutzung der elektronischen Identität (eID) zur elektronischen Identifikation verpflichtet (Art. 9 BGEID). Über die gesetzliche Verpflichtung hinaus sind die Akteure der 1. Säule eine wichtige künftige Akteursgruppe im Ökosystem der eID: Zum einen ist die ZAS als Datenlieferantin für die Angaben zur AHV-Nummer wichtig. Mit der Einbindung dieser bewährten und qualitativ hochwertigen Angaben kann die Qualität garantiert und die Verwendung durch die vielen Akteure, die bereits heute die AHV-Nummer als Identifikationsmerkmal verwenden, nahtlos sichergestellt werden. Zum anderen stellen die Millionen von versicherten Personen eine grosse Gruppe von potenziellen Nutzerinnen und Nutzern dar. Mit einer guten Einbindung in die Dienstleistungen der Durchführungsstellen kann die 1. Säule einen wichtigen Beitrag zur Akzeptanz der eID bei den Benutzerinnen und Benutzern leisten.

1. Im Grundsatz

Wir unterstützen die Stossrichtung des Gesetzes und befürworten eine schnelle Umsetzung der Lösung auf dessen Basis. Ein digitaler Nachweis der Identität ist für die medienbruchfreie Umsetzung von digitalen Leistungen in vielen Bereichen des eGovernments zentral und hat auch für die Kommunikation zwischen den Durchführungsstellen der 1. Säule und der Familienzulagen und den versicherten Personen eine grosse Bedeutung.

Für einen maximalen Nutzen ist für eAHV/IV wichtig, dass ein vielfältiges Ökosystem rund um die eID entsteht. Die eID muss eine hohe Akzeptanz und eine grosse Verbreitung unter der Bevölkerung haben, damit Sie von den Durchführungsstellen ebenfalls zu Identifikation von Versicherten genutzt werden kann.

Einen einfachen Zugang zur elektronischen Identität ist in der 1. Säule auch für die Kundengruppen im Ausland, insbesondere die Auslandsschweizerinnen und -schweizer, wichtig. Für Personen, die ausserhalb der EU wohnen und nicht von potenziell interoperablen Systemen profitieren können, hat diese Anforderung die grösste Bedeutung.

2. Form und Inhalt (Art. 2)

eAHV/IV begrüsst, dass die AHV-Nummer Teil der Angaben der eID ist und sieht darin die Möglichkeit, das wichtigste Identifikationsmerkmal in den Sozialversicherungen direkt von der eID zu beziehen.

3. Ausstellungsprozess (Art. 4)

Die Ausstellung der eID für muss aus unserer Sicht auch für Auslandsschweizerinnen und -schweizer einfach möglich sein. Dieser Grundsatz sollte im Art. 4 enthalten sein, die Verordnung soll dann die passende Umsetzung sicherstellen. Gleichzeitig muss die Qualität der Identität den hohen datenschutzrechtlichen Anforderungen der Sozialversicherungen entsprechen.

4. Gültigkeitsdauer (Art. 6)

Bei der Festlegung der Gültigkeitsdauer durch den Bundesrat sind nicht nur Sicherheitsaspekte, sondern auch die Vorteile für Personen im Ausland bei einer maximal langen Gültigkeitsdauer berücksichtigt werden.

5. Hohe Usability und gute Unterstützung (Art. 8, Art. 14, Art. 16)

Das Konzept der Self-Sovereign Identity schafft im Hinblick auf die Usability zusätzliche Herausforderungen. Die Unterstützung der Nutzenden ist entscheidend. Die vorgesehene Unterstützung durch von den Kantonen bezeichneten Stellen muss sich in der Umsetzung als funktionierende Anlaufstelle erweisen. Die technische Umsetzung des Wallets und das Vorweisen muss verschiedene Bedürfnisse berücksichtigen, so soll eine Nutzung auf mehreren Geräten möglich sein.

6. Ökosystem (5. Abschnitt sowie Art. 26)

Den Einbezug aller interessierten Akteure und das Fördern und Entwickeln eines Ökosystems ist aus unserer Sicht ein entscheidender Erfolgsfaktor. Diese Zielsetzung ins Gesetz zu integrieren wäre deshalb angezeigt. Die Gebühren müssen in einem Rahmen angesetzt sein, der keine Hürde für die Integration von weiteren Akteuren darstellt.

7. Weiterentwicklung (Art. 25)

Die Ausgestaltung des Gesetzes mit einem besonderen Augenmerk auf die Technologieutralität wird sehr begrüsst. Die mit dem Artikel zur technischen Entwicklung ermöglichte schnelle Anpassung der Lösung erscheint uns zweckmässig.

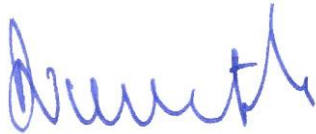
Abschliessend möchten wir nochmals unsere Unterstützung für dieses Gesetzesprojekt betonen: Die elektronische Identitätsinfrastruktur erlaubt es den Akteuren der ersten Säule die Interaktionen mit den versicherten Personen weiter zu digitalisieren. Die spezifischen gesetzlichen Grundlagen der Sozialversicherungen müssen in einem zweiten Schritt die erfolgreiche Einbindung unterstützen. Neben der Nutzung des digitalen

Identitätsnachweises muss auch die Unterschriftspflicht, wo immer möglich, aufgehoben werden. Nur so ist eine vollständige digitale Abwicklung umsetzbar. eAHV/IV zählt auf diese wichtigen Grundlagen, um die die Ziele unseres Vereines in der Durchführung der Sozialversicherungen umsetzen zu können.

Freundliche Grüsse



Christian Zeuggin
Präsident eAHV/IV



Andreas Dummermuth
Präsident Konferenz der Kantonalen Ausgleichskassen



Yvan Béguelin
Präsident der Schweizerischen Vereinigung der Verbandsausgleichskassen



Florian Steinbacher
Präsident der IV-Stellen-Konferenz



Adrien Dupraz
Direktor der Zentralen Ausgleichsstelle (ZAS)

Eidgenössisches Justiz- und Polizeidepartement
3003 Bern

Via Mail an rechtsinformatik@bj.admin.ch

Bern, 19. Oktober 2022

Antwort auf die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, uns zum erwähnten Gesetzesentwurf zu äussern und nehmen diese gerne wahr. Der Verein eGov-Schweiz bezweckt die Förderung der Innovation im eGovernment. In dieser Perspektive ist die Schaffung von Rechtsgrundlagen für eine digitale Identitätsinfrastruktur von besonderem Interesse für unseren Verein.

Der Verein eGov-Schweiz begrüsst den vorliegenden Gesetzesentwurf und unterstützt die rasche Umsetzung und den Aufbau der definierten Infrastruktur. Die Kernanliegen aus dem politischen Auftrag, die Grundsätze «privacy by design», «Datensparsamkeit» und «dezentrale Datenspeicherung», sind umfassend berücksichtigt worden.

Eine digitale Identitätsinfrastruktur ist aus Sicht des Vereins ein zentraler Bestandteil des eGovernments und erlaubt eine weitere Digitalisierung der Prozesse. Entscheidend ist, dass um die eID ein lebendiges Ökosystem von Akteuren und Nutzungen entsteht. Nur damit kann die Verbreitung und Nutzung der eID in der Bevölkerung nachhaltig verankert werden und ein umfassender gesellschaftlicher und wirtschaftlicher Nutzen geschaffen werden. In dieser Perspektive ist eine Verankerung des Ökosystem-Gedankens als Teil der Zweckbestimmung anzustreben.

Die Unterstützung der Benutzenden ist für einen erfolgreichen Betrieb der eID zentral. Ob die Zuweisung dieser Rolle an die Kantone in Art. 8 BGEID für eine flächendeckende Unterstützung sorgen kann, wir von unserem Verein in Frage gestellt. Ein identisches Supportangebot, das flächendeckend und niederschwellig für alle Benutzerinnen und Benutzer bereitsteht, muss das Ziel sein.

Weiter muss dem Risiko einer nicht gerechtfertigten Abfrage und Speicherung von Identitätsdaten vorgebeugt und damit Überidentifikation durch Anbieter verhindert werden. Eine Bestimmung, die die Datenbearbeitung auf ein unbedingt notwendiges Minimum einschränkt, sowie eine Informations- und Zustimmungspflicht vorschreibt, sind einzufügen.

Der definierte Rahmen für die Umsetzung der Lösung erscheint zweckmässig, zumal keine technologischen Umsetzungsentscheide enthalten sind. Gleichwohl ist eine hohe Usability für die Benutzerinnen und Benutzer sicherzustellen, indem eine Verwendung auf verschiedenen Geräten ermöglicht wird und auch die Weiternutzung bei einem

Gerätewechsel unterstützt. Die technische Umsetzung muss ermöglichen, dass allen Benutzerinnen und Benutzern die eID nutzen können, insbesondere muss sie auch nach den Kriterien der Barrierefreiheit entwickelt werden.

Die Realisierung der Lösung als Ökosystem im Zusammenspiel mit den verschiedenen öffentlichen und privaten Anbietern ist eine zentrale Anforderung. Unsere Zielvorstellung eines Ökosystems (entsprechende dem Ambitionslevel 3 in früheren Diskussionsunterlagen) beinhaltet, dass verschiedene Akteure – private und staatliche – mit ihren Lösungen zum vielfältigen Ökosystem beitragen und keine Beschränkungen bestehen, so sollten zum Beispiel auch weitere Wallets von privaten Anbietern genutzt werden können.

Die Einbindung von weiteren privaten Akteuren hängt auch vom Gebührenmodell ab. eGov-Schweiz unterstützt das Prinzip, dass eine minimale Gebühr für den Eintrag ins Basisregister, aber keine Gebühr für die Ausstellung oder die Verifikation eines Nachweises erhoben werden. Die Widerrufe der elektronischen Nachweise würden durch tägliche Aktualisierungen zum System kommuniziert. Für ausstellende Akteure wären auf den verbundenen 'Revocation Update' Gebühren erhoben.

Zusammenfassend sind wir davon überzeugt, dass die vorgeschlagene gesetzliche Grundlage sinnvolle Regeln zur Entwicklung einer eID als wichtiger Teil einer digitalen Infrastruktur definiert. Mit punktuellen Anpassungen und einer schnellen und klaren Detaillierung in den nachgelagerten Bestimmungen könnte das Ziel eines umfassenden, vielfältigen Ökosystems besser erreicht werden.

Freundliche Grüsse

eGov-Schweiz



Renato Gunc
Präsident



Christoph Beer
Geschäftsführer



CH-3003 Bern

BSV; Nom

POST CH AG

Bundesamt für Justiz
Eidgenössisches Justiz- und Polizeidepartement

Per E-Mail an: rechtsinformatik@bj.admin.ch

Bern, 06.10.2022

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID): Stellungnahme der EKKJ

Sehr geehrte Damen und Herren

Die EKKJ möchte in ihrer Stellungnahme den erfolgten Prozess zur Erarbeitung des Gesetzesentwurfes würdigen und einen aus ihrer Sicht wichtigen Hinweis auf kommende begleitende Kommunikationsmassnahmen abgeben.

Würdigung des partizipativen Vorgehens

Die EKKJ möchte den Entstehungsprozess der Gesetzesvorlage würdigen. Sie ist überzeugt, dass das konsequent partizipative Vorgehen und die transparente Information über die gesamte Dauer des Entstehungsprozesses zu einer in allen Belangen fundierten Gesetzesvorlage geführt hat. Wir hoffen, dass eine solche Praxis in Zukunft öfter bei der Erarbeitung von Gesetzesvorlagen zur Anwendung kommt.

Hinweise: spezielle Bedürfnisse von Jugendlichen

Wir sind überzeugt, dass der zu schaffende elektronische Identitätsnachweis für viele Bürgerinnen und Bürger einen gewinnbringenden Zugang zu wichtigen Dienstleistungen ermöglichen wird. Aus unserer Erfahrung ist für den Zugang von Kindern und Jugendlichen eine entsprechend angepasste Kommunikation entscheidend.

Die Kommission möchte darauf hinweisen, dass der Zugang zum elektronischen Identitätsnachweis viele Vorteile speziell für Jugendliche und einen verbesserten Jugendschutz darstellen. Dies vor allem, weil das neue Bundesgesetz über den Jugendschutz in den Bereichen Film und Videospiele (JSFVG) auch Alterskontrollen beinhaltet.

Weiter zeigen unsere Erfahrungen, dass sich viele Jugendliche selbst um einen solchen Zugang bemühen müssten. Dazu ist es in vielen Familien üblich, dass Jugendliche, für ihre fremdsprachigen Eltern, Behördengänge erledigen.

Eidgenössische Kommission für Kinder- und Jugendfragen EKKJ
c/o Bundesamt für Sozialversicherungen BSV
Effingerstrasse 20, 3003 Bern
Tel. +41 58 462 92 26
ekkj-cfej@bsv.admin.ch
www.ekkj.admin.ch



Es ist daher darauf zu achten, dass Informationen auch in einfacher Sprache und leicht verständliche Anleitungen zur Beantragung und Nutzung der E-ID zur Verfügung gestellt werden.

Eine jugendgerechte Kommunikation beinhaltet:

- Sie ist leicht zugänglich und niederschwellig nutzbar.
- Sie ist in einfacher, verständlicher Sprache formuliert.
- Sie wird mehrsprachig angeboten.
- Sie ist auf zeitgemässen, zielgruppengerechten Kanälen verfügbar.

Es bieten sich Inhalte auf einer Webseite an. Dies macht es für die grossen Portale, die Informationen für Jugendliche anbieten, einfach, auf diese zu verweisen. Folgende Seiten sind u.a. bei Jugendlichen in der Deutschschweiz bekannt: Feek-ok.ch; tschau.ch; be-freelance.net. In der Romandie ist ciao.ch das geeignete Portal und für die ganze Schweiz kann auf 147.ch verwiesen werden.

- Die Informationen sind barrierefrei zugänglich.
- Sie sollte von einem klar erkennbaren, vertrauenswürdigen Absender stammen.
- Sie enthält, ergänzende Informationen, die helfen das Thema einzuordnen (z.B. Warum ist die E-ID wichtig? Wovor schützt sie? Wovor nicht? Werden Daten gespeichert? usw.)

Die EKKJ dankt für die Aufmerksamkeit, die Sie ihrer Stellungnahme entgegenbringen, und wünscht Ihnen gutes Gelingen für den weiteren Gesetzgebungs- und Umsetzungsprozess.

Eidgenössische Kommission für Kinder- und Jugendfragen EKKJ



Fédération des
Entreprises
Romandes

FER Genève - FPE Bulle - UPCF Fribourg
FER Arcju - FER Neuchâtel - FER Valais

rechtsinformatik@bj.admin.ch

Département fédéral de justice et
police (DFJP)
3003 Berne

Madame Karin Keller-Sutter,
Conseillère fédérale

Genève, le 20 octobre 2022

DZ/3449 - FER No 42-2022

Loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques

Madame la Conseillère fédérale,

Notre fédération vous remercie de l'avoir consultée dans le cadre de la modification citée en titre, dont elle a pris connaissance avec intérêt. Elle vous livre ci-après sa prise de position.

La FER salue l'approche et le travail effectué. Le contenu de cet avant-projet est en adéquation avec la gestion des identités électroniques dans son état actuel.

Notre fédération est alignée sur les propositions techniques et organisationnelles, comme présentées par ce projet :

- Un système qui fonctionnera dans une infrastructure gérée par l'État et garantie par la Confédération,
- L'applicabilité de la nLPD garantissant ainsi le respect de la vie privée dès la conception,
- Faire en sorte que cette nouvelle e-ID soit compatible avec celle de l'UE,
- La possibilité d'intégrer d'autres types de documents (notion de portefeuilles),
- Le tout transportable sur un appareil électronique protégé par une authentification à double facteur, et servant de preuve au quotidien.

Tout cela correspond au niveau de maturité attendue, et n'attire pas de remarques de notre part, mais nous nous permettons de nous interroger quant à la limite d'attribution de l'e-ID et de sa durée de validité.

Comme le laisse entrevoir cet avant-projet, l'identité électronique semble être une affaire d'État à part entière.

Si tel est le cas, il faudrait intégrer l'e-ID dans le flux, lors de la délivrance des pièces d'identité physiques. Dès lors, l'attribution d'une identité électronique n'est que l'extension des documents physiques déjà remis à tous les citoyens, dès la naissance, ou lors de l'attribution d'un droit officiel valable, pour les étrangers.

Non seulement l'e-ID pourrait être créée à ce moment (naissance, attribution), mais sa durée de validité indexée sur la durée des documents physiques : la création, le renouvellement, ou la révocation des documents physiques adapterait l'e-ID en conséquence, automatiquement.

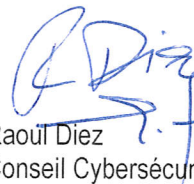
En somme, cela reste toujours une identité électronique étatique gratuite et volontaire, pour tout titulaire d'un document d'identité émis par les autorités, comme proposé par l'avant-projet : au citoyen de se servir des documents se trouvant sur son portefeuille virtuel, ou préférer les documents physiques. Mais les deux existeraient, par défaut, pour chacun de nous.

En conclusion, notre fédération soutient cet avant-projet permettant une fois de plus à la Suisse de répondre aux défis actuels et futurs.

En vous remerciant de l'attention que vous porterez à la présente, nous vous prions de croire, Madame la Conseillère fédérale, à l'expression de notre haute considération.



Blaise Matthey
Secrétaire général



Raoul Diez
Conseil Cybersécurité PME
FER Genève

La Fédération des Entreprises Romandes en bref

Fondée le 30 juillet 1947 à Morat, son siège est à Genève. Elle réunit six associations patronales interprofessionnelles cantonales (GE, FR, NE, JU, VS), représentant la quasi-totalité des cantons romands. La FER comprend plus de 45'000 membres.

Eidgenössisches Justiz- und Polizeidepartement

Per E-Mail: rechtsinformatik@bj.admin.ch

Bern, 17. Oktober 2022

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise

Stellungnahme der FMH – Verbindung der Schweizer Ärztinnen und Ärzte

Sehr geehrte Frau Bundesrätin Keller-Sutter,
sehr geehrte Damen und Herren

Die FMH bedankt sich für den Einbezug in den partizipativen Prozess zur Erarbeitung des elektronischen Identitätsnachweises sowie für die Möglichkeit der Stellungnahme. Sie nimmt Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere Nachweise (BGEID) wie folgt Stellung.

Für das Gesundheitswesen ist ein elektronischer Identitätsnachweis (E-ID) ein entscheidender Baustein, der eine vertrauenswürdige Kommunikation und Nutzung von digitalen Dienstleistungen ermöglicht. Die Vorlage zum BGEID ist daher für die Schweiz ein wichtiger Meilenstein, der nun rasch und unter Einbezug derjenigen, die eine solche E-ID im praktischen Alltag verwenden, umgesetzt werden muss. Die Daten der Nutzerinnen und Nutzer der E-ID müssen mit dem höchsten Grad an Sicherheit behandelt werden. Die Entwicklungen in diesem Bereich müssen daher unter der Leitung des Bundesamts für Justiz bleiben und dürfen nicht anderen Ämtern übertragen werden. Dabei ist es von Bedeutung, dass die E-ID einfach genutzt werden kann und administrative Abläufe für Ärztinnen und Ärzte erleichtert. Dies muss in jeder Phase der Konzeptionalisierung der technischen Umsetzung berücksichtigt werden.

Hierzu gehört auch die Verwendung des elektronischen Patientendossiers (EPD), dessen Hauptlast von Ärztinnen und Ärzten getragen werden. Mit dieser Vorlage soll der im Artikel 4 EPDG verwendete Begriff «elektronische Identität» durch den Begriff «Identifikationsmittel» ersetzt werden. Die FMH begrüsst diesen Schritt, da der für die Ausstellung von Identifikationsmitteln notwendige Identitätsnachweis künftig durch einen vom Bund herausgegebenen vertrauenswürdigen Nachweis ersetzt wird.

Gemäss dem erläuternden Bericht soll langfristig das Identifikationsmittel für das EPD vom Bund herausgegeben werden. Ein Zusammenhang mit dem politischen Willen des Volkes mit der Ablehnung des E-ID-Gesetzes in der Volksabstimmung vom 7. März 2021 lässt sich hieraus jedoch nicht ablei-

ten. Gemäss Artikel 2 Absatz 2 Buchstabe b des EPDG ist eine (Stamm-)Gemeinschaft eine organisatorische Einheit von Gesundheitsfachpersonen und deren Einrichtungen. Das EPDG geht davon aus, dass sich die Gemeinschaften und Stammgemeinschaften privatrechtlich organisieren.

Zum jetzigen Zeitpunkt gibt es in der Schweiz fünf zertifizierte Herausgeber von Identifikationsmitteln für das EPD. Das EPDG sieht vor, dass sich die Herausgeber zertifizieren lassen müssen und dass die Zertifizierung nach Art. 12 Buchstabe b regelmässig überprüft wird. Aufgrund der hohen Zertifizierungs- und Weiterentwicklungskosten besteht die Gefahr, dass die Anbieter nicht bereit sind, diese Investitionen zu tätigen. Die FMH fordert, dass im Zusammenhang mit der Gesamtrevision des EPDG zwingend Massnahmen ergriffen werden müssen, damit das Angebot von privaten Herausgebern von Identifikationsmitteln weiterhin bestehen kann. Weiterhin muss zwingend eine Übergangsfrist für die gemäss EPDG herausgegebenen Identifikationsmitteln festgelegt werden.

Die FMH nimmt zu weiteren Bestimmungen der Vorlage wie folgt Stellung:

Art. 1

Art. 1. Abs. 2.: Das revidierte Datenschutzgesetz verankert die Prinzipien «Privacy by Design» (Datenschutz durch Technik) sowie «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen). Auch die Voreinstellungen, beispielsweise bei Apps, welche digitale Nachweise speichert, sind so auszugestalten, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist. Die FMH beantragt, «Privacy by Default» in Art. 1 Abs. 2 Bst. b aufzunehmen.

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Art. 14 statuiert, dass Inhaberinnen und Inhaber ihre elektronischen Nachweise als Datenpaket erhalten und mittels selbst gewählter technischer Mittel aufbewahren. Der Vorentwurf enthält jedoch keine Anforderungen betreffend die technischen Mittel. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Die FMH fordert eine Ergänzung betreffend Art. 14, dass der Bundesrat die Anforderungen an die technischen Mittel zur Aufbewahrung festlegt.

Art. 16 Vorweisen von elektronischen Nachweisen

Nach Art. 16 Abs. 1 bestimmen die Inhaberinnen und Inhaber der E-ID, welche Bestandteile des Nachweises von der Verifikatorin geprüft werden. In den Erläuterungen wird jedoch ausgeführt, dass diese Bestandteile durch die Verifikatorin bestimmt werden. Die Verifikatorin darf im Sinne der Datensparsamkeit nicht mehr solcher Bestandteile verlangen als absolut notwendig. Darüberhinausgehende Informationen dürfen nur von der Inhaberin bestimmt werden. Die Erläuterungen sind im Einklang mit Art. 16 Abs. 1 anzupassen.

Art. 16 Abs. 3 statuiert, dass die Betreiberin der Systeme nach dem 5. Abschnitt möglichst keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen kann. Die Formulierung, dass möglichst keine Rückschlüsse über die Verwendung gezogen werden können, unterläuft das im neuen Datenschutzgesetz verankerte Prinzip «privacy by default». Die FMH fordert, dass die Betreiber keine Rückschlüsse ziehen dürfen, sofern dies technisch umsetzbar ist.


Art. 17 Basisregister

Art. 17 Abs. 3 legt fest, dass die Ausstellerinnen und Verifikatorinnen ihre Daten in das Basisregister eintragen. Eine Eintragung ohne vorgängige Prüfung durch die entsprechende Stelle des Bundes ist

nach Meinung der FMH fahrlässig, da sie dem Identitätsdiebstahl Tür und Tor öffnet. Zudem schadet dies dem Vertrauen in das Basisregister, wenn Einträge von Ausstellerinnen und Verifikatorinnen im Nachhinein widerrufen werden müssen. Der Prozess der Überprüfung ist daher auf Stufe der Verordnung zu präzisieren.

Wir bedanken uns für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse



Dr. med. Yvonne Gilli
Präsidentin



Stefan Kaufmann
Generalsekretär



Föderation der Schweizer Psychologinnen und Psychologen
Fédération Suisse des Psychologues
Federazione Svizzera delle Psicologhe e degli Psicologi

Ansprechpartner: Muriel Brinkrolf
Direktnummer: +41 31 388 88 41
muriel.brinkrolf@fsp.psychologie.ch

Bern, 18. Oktober 2022

Per Mailversand an:
rechtsinformatik@bj.admin.ch
Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und
Polizeidepartementes
EJPD Bundeshaus West
3003 Bern

Vernehmlassung Bundesgesetz über den elektronischen Identitätsausweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin Keller-Sutter

Als Dachverband der Psychologinnen und Psychologen nimmt die FSP gerne Stellung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Grundsätzlich schliessen wir uns den Stellungnahmen und somit den Änderungsvorschlägen der Interessengemeinschaft eHealth vom 29. September 2022 sowie von Health Info Net (HIN) vom 10. Oktober 2022 (siehe Beilagen) an und bedanken uns für die rasche und umsichtige Entwicklung des Gesetzesentwurfes für die E-ID, welche für das gesamte Gesundheitswesen von höchster Bedeutung ist. Das Gesetz ist unserer Meinung nach gut formuliert und umfasst alle relevanten Regelungen.

Ergänzend zur Stellungnahme der IG eHealth würden wir für den Ausstellungs- und Widerrufsprozess (Art. 4 und 5) noch folgende Präzisierung empfehlen:

Artikel 4 Ausstellung

Entwurf Bundesrat	⁵ Der Bundesrat regelt den Ausstellungsprozess.
Vorschlag fsp	⁵ Der Bundesrat regelt den Ausstellungs- und Mutationsprozess. Entsprechend müsste der Titel des Artikels auf «Ausstellungs- und Mutationsprozess» geändert werden.

Artikel 5 Widerruf

Entwurf Bundesrat	Das fedpol widerruft die E-ID unverzüglich, wenn: [...] d. es informiert wird, dass: [...] 2. sich die Personenidentifizierungsdaten nach Artikel 2 Absatz 2 geändert haben, oder [...]
Vorschlag fsp	d.2. sich die Personenidentifizierungsdaten nach Artikel 2 Absatz 2 geändert haben. Der Bundesrat sieht Ausnahmen vor, bei welchen die

	Änderung von Personenidentifizierungsdaten lediglich zu einem Mutationsprozess gemäss Artikel 4 Absatz 5 führen. Oder
Begründung	<p>Art. 5, Abschnitt d, Punkt 2 besagt, dass eine Änderung der Personenidentifizierungsdaten nach Art. 2 Abs. 2 zu einem unverzüglichen «Widerruf» der E-ID führt. Diese Personenidentifizierungsdaten können allerdings u.U. relativ «oft» ändern, z.B. bei Heirat, Scheidung, oder auch bei der Neuausstellung eines Passes mit neuem Gesichtsbild.</p> <p>Aus unserer Sicht wäre es sinnvoll, dass eine Änderung der Personenidentifizierungsdaten nicht zwingend einen Widerruf der E-ID fordert, sondern dass bestimmte Änderungen - gemäss des zu definierenden Mutationsprozesses - zu einem Änderungsprozess führen, bei welchem nicht in jedem Fall ein Widerruf bzw. ein neuer Ausstellungsantrag bei fedpol notwendig ist.</p>

Für die Prüfung und Berücksichtigung unserer Eingabe danken wir Ihnen.

Freundliche Grüsse

Yvik Adler
Co-Präsidentin

Stephan Wenger
Co-Präsident

Beilagen:

- Stellungnahme der Interessengemeinschaft ehealth vom 29. September 2022
- Stellungnahme der Health Info Net AG (HIN) vom 29. September 2022

IG eHealth, Amthausgasse 18 3011 Bern

Per Mail an: rechtsinformatik@bj.admin.ch

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements
EJPD Bundeshaus West
3003 Bern

Bern, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Die IG eHealth bedankt sich beim eidgenössischen Justiz- und Polizeidepartement EJPD und beim Bundesamt für Justiz BJ für den partizipativen Prozess bei der Erarbeitung des Entwurfs des E-ID-Gesetzes, den wir als mustergültig und nachahmenswert erachten. Wir bedanken uns auch für die rasche Ausarbeitung der Vernehmlassungsvorlage, die wir insgesamt als sehr gelungen und praxistauglich einschätzen.

Für das Gesundheitswesen ist ein elektronischer Identitätsnachweis (E-ID) eine zentrale Voraussetzung für die Nutzung von digitalen Dienstleistungen und eine vertrauenswürdige Kommunikation zwischen Gesundheitsfachpersonen und PatientInnen. Insofern wünschen wir eine zeitnahe Verabschiedung und Überweisung der Botschaft und des Gesetzesentwurfs ans Parlament.

Gemäss dem Gesetzesentwurf ist die Ausstellung und die Verwendung der neuen E-ID freiwillig. Wir begrüssen es, dass die Bevölkerung und die Gesundheitsfachpersonen die Wahl haben, wie sie auf das EPD zugreifen wollen. Die E-ID gemäss vorliegendem Gesetzesentwurf ist ein digitales Pendant zum physischen Pass oder zur Identitätskarte. Es ist kein «Login» im Sinne einer Authentifikation. Zu prüfen ist, ob dieser Punkt im Gesetz aufzunehmen ist.

Wir möchten einen Punkt zu Art. 16 Abs 1 Vorweisen von elektronischen Nachweisen anfügen. Der Artikel ist gut formuliert, wir erachten aber die Erläuterungen als unpräzise. Gemäss des Gesetzesartikels bestimmt die InhaberIn der E-ID, welche Bestandteile vom Verifikator geprüft werden. In den Erläuterungen steht unserer Meinung nach fälschlicherweise, dass dies der Verifikator bestimmt. Die Verifikatorin darf im Sinne der Datensparsamkeit nicht mehr Inhalte verlangen als absolut notwendig sind.

Nachfolgend gehen wir auf ausgewählte Elemente im Gesetzesentwurf ein, die aus unserer Sicht zu präzisieren sind:

Artikel 1

Entwurf Bundesrat	<p>2 Es hat zum Zweck:</p> <p>a. die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten;</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, 2. Datensicherheit, 3. Datensparsamkeit, und 4. dezentrale Datenspeicherung; <p>c. zu gewährleisten, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen;</p> <p>d. die Standardisierung der E-ID sowie die Sicherheit der Infrastruktur und der Ausstellung und Überprüfung der elektronischen Nachweise zu gewährleisten, ohne die technische Entwicklung unnötig einzuschränken.</p>
Änderungsvorschlag	<p>...</p> <p>b. den Schutz der Persönlichkeit und der Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden, insbesondere durch die Umsetzung der folgenden Grundsätze:</p> <ol style="list-style-type: none"> 1. Datenschutz durch Technik, <u>2. Datenschutz durch datenschutzfreundliche Voreinstellungen</u> <u>3.</u> Datensicherheit, <u>4.</u> Datensparsamkeit, und <u>5.</u> dezentrale Datenspeicherung; <p>...</p>
Begründung	<p>Das revidierte Datenschutzgesetz verankert die Prinzipien «Privacy by Design» (Datenschutz durch Technik) sowie «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen). Im E-ID-Gesetz wird nur das Prinzip «Datenschutz durch Technik» explizit erwähnt. Aus unserer Sicht ist ebenfalls der «Datenschutz durch datenschutzfreundliche Voreinstellungen» aufzunehmen. Somit kann sichergestellt werden, dass beispielsweise die Voreinstellungen von Apps, die digitale Nachweise speichern, auf das nötige Mindestmass beschränkt werden.</p>

Art. 8 Anlaufstellen der Kantone

Entwurf Bundesrat	Die Kantone bezeichnen die Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Änderungsvorschlag	Die Kantone bezeichnen die <u>öffentlichen oder privaten</u> Stellen, die in Zusammenhang mit der Ausstellung und dem Einsatz der E-ID Unterstützung anbieten.
Begründung	Der Gesetzesartikel ist so zu präzisieren, dass die Kantone öffentliche und private Stellen für die Unterstützung bezeichnen können.

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung zu definieren hat. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art. 16 Abs 3 Vorweisen von elektronischen Nachweisen

Entwurf Bundesrat	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann möglichst keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen.
Änderungsvorschlag	3 Die Betreiberin der Systeme nach dem 5. Abschnitt hat keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise und kann <u>möglichst darf</u> keine Rückschlüsse über deren Verwendung und die Beteiligten ziehen <u>können</u> .
Begründung	Die E-ID muss technisch so ausgestaltet sein, dass keine Rückschlüsse möglich sind. Ansonsten würde das das Prinzip «privacy by default» verletzt.

Art. 17 Basisregister

Entwurf Bundesrat	3 Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten in das Basisregister ein.
Änderungsvorschlag	3 Der Bundesrat regelt, welche Daten die Ausstellerinnen und Verifikatorinnen in das Basisregister einstellen dürfen.
Begründung	Gemäss dem Artikel müssen Ausstellerinnen und Verifikatorinnen ihre Daten in das Basisregister eintragen. Eine Eintragung ohne vorgängige Prüfung durch die entsprechende Stelle des Bundes öffnet dem Identitätsdiebstahl Tür und Tor. Es dürfte dem Vertrauen in das Basisregister schaden, wenn Einträge von Ausstellerinnen und Verifikatorinnen widerrufen werden müssen. Es ist eine Delegationsnorm zu schaffen, damit der Prozess der Überprüfung auf Verordnungsstufe präzisiert werden kann.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat <u>sieht vor</u> kann vorsehen , dass der Bund die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

Art. 24bis (neu) Überprüfung der Vertrauensinfrastruktur

Entwurf Bundesrat	-
Ergänzungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bedanken uns für die Prüfung und ggf. Berücksichtigung unserer Eingabe im Rahmen der Erarbeitung der Botschaft des Bundesrats und des Gesetzesentwurfs, der zu Händen des Parlaments verabschiedet wird.

Freundliche Grüsse
Im Namen des Vorstands

Anna Winter
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements EJPD Bundeshaus West
CH-3003 Bern

Einreichung per Mail an: rechtsinformatik@bj.admin.ch

Wallisellen, 29. September 2022

Vernehmlassung Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zum neuen Vorschlag für ein E-ID-Gesetz äussern zu können, welche wir hiermit gerne wahrnehmen. Einleitend möchten wir dem EJPD für den partizipativen Prozess der Erarbeitung des BG E-ID danken, den wir als mustergültig und nachahmenswert erachten.

Grundsätzlich sind wir der Überzeugung, dass der Vorschlag für das E-ID-Gesetz eine sehr gute Basis darstellt und den Rahmen für eine Vertrauensinfrastruktur setzt, in dem eine staatlich herausgegebene E-ID das Kernelement darstellt. Wir begrüssen den Paradigma-Wechsel im Umgang mit personenbezogenen Daten und die Schaffung eines Rechtsrahmens für eine Vertrauensinfrastruktur.

Eine verlässliche Vertrauensinfrastruktur hat für das Gesundheitswesen und dessen Digitalisierung eine zentrale Bedeutung. Wir erachten es als äusserst wichtig, dass die Vertrauensinfrastruktur offen, sicher und verlässlich gestaltet ist und diese von allen Marktteilnehmern gleichermassen genutzt werden kann. Zudem sollte sie auch regelmässig von einer unabhängigen Instanz überprüft werden. Die E-ID soll sich darin als zentraler Nachweis der Identität von Personen verstehen und für die verschiedensten sektorspezifischen Anwendungen eingesetzt werden können. Grosse Wichtigkeit wird auch der zeitnahen Anpassung der Gesetze zugeschrieben, welche die Verwendung von elektronischen Identitäten definieren. Insbesondere sollte das Bundesgesetz über das elektronische Patientendossier EPDG entsprechend angepasst werden. Gemäss EPDG zertifizierte Identity Provider IDP sind per Inkraftsetzung des BG E-ID von Zertifizierungspflichten des EPDGs zu entbinden.

Spezifisch sehen wir folgende Punkte, die im Gesetzesentwurf präzisiert werden müssen:

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Entwurf Bundesrat	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Änderungsvorschlag	Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket und bewahrt ihn mithilfe selbst gewählter, <u>den Vorgaben des Bundes entsprechenden</u> technischer Mittel unter ihrer oder seiner alleinigen Kontrolle auf.
Begründung	Die technischen Mittel sollen frei gewählt werden können, sofern diese Voraussetzungen erfüllen, die der Bundesrat auf Stufe Verordnung definieren muss. So muss beispielsweise sichergestellt sein, dass das Datenpaket nicht von unbefugten Dritten eingesehen oder kopiert werden kann.

Art 15 Übertragbarkeit von elektronischen Nachweisen

Entwurf Bundesrat	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. ...
Änderungsvorschlag	Art. 15 Übertragbarkeit von elektronischen Nachweisen 1 Elektronische Nachweise können nicht einer anderen Inhaberin oder einem anderen Inhaber übertragen werden. <u>1^{bis (neu)} Der Bundesrat sieht Ausnahmen für die Vormundschaft gemäss Art. 327a ff. ZGB für Minderjährige und die umfassende Beistandschaft gemäss Art. 388 ff. ZGB von Erwachsenen vor.</u> ...
Begründung	Es braucht eine Ausnahmeregelung für die Vormundschaft für Minderjährige und die umfassende Beistandschaft bei Erwachsenen mit einer entsprechenden Referenzierung der relevanten ZGB-Artikel.

Art. 18 System zur Bestätigung von Identifikatoren

Entwurf Bundesrat	... 2 Der Bundesrat kann vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Änderungsvorschlag	... 2 Der Bundesrat sieht vor kann vorsehen , dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt. ...
Begründung	Das Gesetz muss eine die Anbindung von markt- und sektorspezifischen Nachweisen und deren Ausstellung und Überprüfung gewährleisten und aktiv fördern bzw. unterstützen.

	Ein konkretes Beispiel: die Erteilung von Facharzttiteln durch das Schweizerische Institut für ärztliche Weiter- und Fortbildung SIWF.
--	--

Art. 24^{bis} (neu) Überprüfung der Vertrauensinfrastruktur

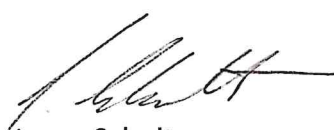
Entwurf Bundesrat	-
Änderungsvorschlag	Der Bundesrat stellt sicher, dass die Vertrauensinfrastruktur des Bundes regelmässig von einer unabhängigen Stelle überprüft und dem aktuellen Stand der Technik angepasst wird.
Begründung	Gemäss Art 24 betreibt eine Leistungserbringerin innerhalb der Bundesverwaltung die Vertrauensinfrastruktur. Diese soll von einer unabhängigen Stelle regelmässig überprüft und dem Stand der Technik angepasst werden. Dies leistet einen Beitrag zur Sicherheit und erhöht das Vertrauen der Anwenderinnen in die Infrastruktur.

Wir bitten den Bundesrat, Experten der Zivilgesellschaft, der Wissenschaft und der Wirtschaft für die Ausarbeitung der entsprechenden Verordnung und Ausführungsbestimmung beizuziehen.

Wir sind davon überzeugt, dass mit einer speditiven Implementierung der Vertrauensinfrastruktur in der Schweiz der Digitalisierung in den verschiedenen Bereichen eine signifikante Weiterentwicklung ermöglicht wird.

Freundliche Grüsse

HEALTH INFO NET AG



Lucas Schult
Geschäftsführer (CEO)



Peer Hostettler
Leiter Vertrieb

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 20. Oktober 2022

Vernehmlassungsantwort: Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz)

Sehr geehrte Damen und Herren

GastroSuisse, der grösste Branchenverband der Schweiz mit rund 20'000 Mitgliedern (Hotels, Restaurants, Cafés, Bars etc.) in allen Landesgegenden, organisiert in 26 Kantonalsektionen und fünf Fachgruppen, nimmt im obengenannten Vernehmlassungsverfahren gerne wie folgt Stellung:

I. Allgemeine Würdigung

GastroSuisse anerkennt die Notwendigkeit der Einführung eines digitalen Ausweises im Grundsatz. Die Digitalisierung schreitet voran und soll nicht bei den Bundesbehörden und deren Dienstleistungen stoppen. Der nachfolgende Anpassungsvorschlag des Vorentwurfes bezieht sich auf den gastgewerblichen Kontext, beispielsweise auf die Alterskontrolle mittels amtlichen Ausweises bei der Alkoholabgabe oder in Bezug auf den Zutritt zu Nachtclubs.

II. Anwendung im analogen Raum

Die Vorlage bezieht sich inhaltlich primär auf den Anwendungsfall im digitalen Raum. Einzig Artikel 10 behandelt eine Situation, in der die E-ID innerhalb eines Prozesses zur Anwendung kommt, bei welchem die sich ausweisende Person persönlich erscheint. Gemäss Artikel 10 des Vorentwurfs muss die sich ausweisende Person die Wahl zwischen einem analogen Ausweisdokument und der E-ID haben.

GastroSuisse spricht sich dafür aus, dass der Bund eine einfach umsetzbare und kostengünstige Überprüfung der elektronischen Nachweise im analogen Raum gewährleistet. Eventualiter schlägt der Branchenverband vor, Artikel 10 insofern einzugrenzen, als dass Private, die die Prüfung eines Ausweises vornehmen, weiterhin auf ein physisches Ausweisdokument bestehen können. GastroSuisse schlägt folgende Ergänzung vor:

Art. 10 Vorweisen einer E-ID

¹ [...]

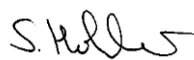
² **NEU** *Private, die zur Erfüllung ihrer Dienstleistung einen amtlichen Ausweis prüfen, sind nicht verpflichtet, die E-ID zu akzeptieren.*

Wir danken Ihnen für die Berücksichtigung der Haltung von GastroSuisse.

Freundliche Grüsse



Casimir Platzer
Präsident



Severin Hohler
Leiter Wirtschaftspolitik



Position du Groupement Romand de l'Informatique sur la Loi sur l'identification électronique (LeID) en octobre 2022

- Le GRI avait été favorable avec quelques réserves à l'eID proposée par le passé par le Conseil fédéral, balayée ensuite par le peuple.
- Le GRI est fondamentalement enthousiaste de pouvoir avancer ; l'urgence et la **neutralité technologique** ayant été ses arguments principaux par le passé, les citoyens en Suisse méritent les gains d'efficacité, d'efficience et de rapidité dans les transactions avec l'administration **dans un futur proche**. Il s'agit de l'attractivité de la place économique. Le GRI espère que la nouvelle loi pourrait-elle être mise en œuvre rapidement.
- La Confédération garantissant l'entier du processus paraît **rassurant**, en particulier pour la majorité ayant refusé la loi.
- L'identité électronique est un moyen de prouver électroniquement son identité. Les risques que le numéro AVS soit volé via l'eID que en le gardant dans son portefeuille via une carte plastique d'assuré de caisse maladie est relativement faible.
- Cette eID reste **facultative** et elle devrait le rester tant que la quasi-unanimité des citoyens/utilisateurs ne demandent pas la suppression de l'ID papier. Par conséquent, la question de l'accès à cette identité électronique par des personnes sans aucun moyen électronique pour les rares personnes qui vivent encore sans smartphone ou ordinateur ne se pose pas vraiment.
- Le GRI apprécie le principe « privacy by design » exprimée en page 7 art 1. Al. 2 let. b. « Selon les motionnaires, l'identité électronique de la Confédération doit respecter les principes suivants : prendre en compte la protection de la vie privée dès la conception du produit (privacy by design), ne collecter que les données nécessaires et enregistrer celles-ci de manière **décentralisée** (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification) » : c'est ce qui a été pratiqué avec l'application CovidCert.
- En page 20 chapitre 5. Conséquences : Les coûts des cantons et des communes devraient être ajoutés à ceux de la Confédération.



- Le GRI soutient l'idée que les développements au sein de l'Union européenne doivent être suivis et compris avec rapidité et dynamisme. Les changements au niveau de l'UE ne doivent pas impliquer un blocage à la « Swiss finish ». Le Conseil fédéral estime nécessaire de tenir compte de ces développements dans la réflexion menée au plan national. Comme il est écrit dans le rapport, « La Suisse n'a pas d'obligation juridique d'adopter le règlement de l'UE et les modifications qui s'y rapportent. Toutefois, compte tenu de l'étroitesse des rapports commerciaux et sociaux qu'elle entretient avec la plupart des pays membres de l'Union européenne, la Suisse a tout intérêt à rendre son système d'identité électronique interoperable avec celui de l'Union européenne ».

Contact : Olivier Naray, Responsable Affaires publiques
Groupement romand de l'Informatique (GRI)

Email : olivier@naray.ch

Tel. : +41 76 584 83 89

Stellungnahme

Basel, 26. Oktober 2022 ch

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Nach dem klaren Nein an der Urne im März 2021 kommt ein neuer Gesetzes Vorentwurf zur E-ID. Die Handelskammer beider Basel kann die vom Bundesrat vorgeschlagene Vorlage unterstützen. Das Wichtigste ist, dass wir den elektronischen Identitätsnachweis rasch und unbürokratisch einführen können. Der Datenschutz soll durch das System selbst (Privacy by Design), aber auch durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit) sowie eine dezentrale Datenspeicherung gewährleistet werden.

Zur Vernehmlassungsvorlage

Die Stimmbevölkerung hat am 7. März 2021 dem E-ID-Gesetz und der Privatisierung des digitalen Passes mit 64.4% eine deutliche Abfuhr erteilt. Die Herausgabe von Identitätsausweisen muss in staatlicher Verantwortung bleiben und gehört unter demokratische Kontrolle.

Der Gesetzesvorentwurf schafft die Grundlagen für die Einführung der staatlichen elektronischen Identität (E-ID) in der Schweiz. Der Bund überprüft die Identität einer Person und stellt ihr eine E-ID aus. Die E-ID und andere elektronische Nachweise werden über eine vom Bund zur Verfügung gestellte staatliche Vertrauensinfrastruktur herausgegeben. Der Gesetzesvorentwurf regelt die Anforderungen an diese Infrastruktur, die sowohl öffentlichen als auch privaten Akteurinnen zur Verfügung stehen wird. Gestützt auf die Ergebnisse der informellen öffentlichen Konsultation hat der Bundesrat am 17. Dezember 2021 über die neue Stossrichtung der E-ID entschieden. Demnach soll die E-ID-Vorlage einen Ansatz verfolgen, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung sowie auf einer staatlichen Vertrauensinfrastruktur beruht, mit der ein Ökosystem für elektronische Nachweise eingeführt werden kann, die von Akteuren des öffentlichen und des privaten Sektors ausgestellt werden.

Die Vernehmlassung 2022/19 wurde nun in genau diesen Punkten angepasst und adressiert die relevanten Gegen-Argumente der letzten Vorlage. Der Bund ist neu nicht nur für die

Handelskammer beider Basel
St. Jakobs-Strasse 25
Postfach
CH-4010 Basel

T +41 61 270 60 60
F +41 61 270 60 05

www.hkbb.ch

Identifikation verantwortlich, sondern auch für die gesamte Infrastruktur. Weitere Kritikpunkte werden neu durch Konzepte wie Privacy by Design, das Prinzip der Datensparsamkeit sowie eine möglichst dezentrale Datenspeicherung adressiert.

Konzeption

Die Handelskammer begrüsst es, die Gesetzgebungsarbeiten im Bereich der E-ID wiederaufzunehmen und neu auszurichten. Der Staat tritt dabei als Herausgeber der E-ID auf und sorgt für den Betrieb der nötigen Vertrauensinfrastruktur. Den Nutzerinnen und Nutzern soll grösstmögliche Kontrolle über ihre Daten ermöglicht werden.

Für Firmen mit digitalen Angeboten und deren Kunden erleichtert eine E-ID das Online-Onboarding erheblich, zudem erhöht es die Sicherheit gegenüber aktuellen Verfahren (Videoidentifikation) massgeblich. Es können Prozesse vereinfacht und beschleunigt werden, welche heute für die Einwohnerinnen und Einwohner wie auch für die Verwaltung und die Unternehmen unnötige Aufwände verursachen. Ausserdem stärkt eine E-ID den Standort Schweiz im europäischen und internationalen Vergleich. Zu den Ländern, die derzeit staatliche E-ID's ausgeben, gehören unter anderem Belgien, Finnland, Deutschland, Italien, Luxemburg, die Niederlande und viele mehr.

Es ist richtig und wichtig, dass, anders als bei der abgelehnten Vorlage der Bund für die Herausgabe der E-ID verantwortlich ist und die Infrastruktur betreibt, welche als Grundlage für die E-ID dient.

Anliegen

Am 7. März 2021 hat die Stimmbevölkerung das Bundesgesetz über elektronische Identifizierungsdienste (BGEID) abgelehnt. Die Notwendigkeit der Schaffung einer E-ID ist aber grundsätzlich unbestritten. Bereits am 10. März 2021 wurden in der Frühjahrsession von Vertreterinnen und Vertretern aller Fraktionen sechs gleichlautende Motionen für eine "Vertrauenswürdige, staatliche E-ID" eingereicht. Nutzerinnen und Nutzer der künftigen staatlichen E-ID sollen grösstmögliche Kontrolle über ihre Daten haben (Self-Sovereign Identity). Der Datenschutz soll - wie in den Motionen gefordert - durch das System selber (Privacy by Design), aber auch durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit) sowie eine dezentrale Datenspeicherung gewährleistet werden.

Die Handelskammer beider Basel kann die vom Bundesrat vorgeschlagene Vorlage im Sinne der vorstehenden Ausführungen unterstützen.

Département fédéral de justice et police DFJP

Par e-mail à:
rechtsinformatik@bj.admin.ch

Berne, le 26 août 2022

Avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (loi sur l'e-ID, LeID)

Réponse de l'association Médecins de famille et de l'enfance Suisse (mfe)

Chère Madame la Conseillère fédérale,
Mesdames et Messieurs,

Nous vous remercions de nous offrir l'opportunité de participer à la consultation relative à l'objet susmentionné. mfe Médecins de famille et de l'enfance Suisse représente les intérêts professionnels des médecins de famille et de l'enfance au niveau national.

Appréciation générale

Les médecins de famille et de l'enfance sont concernés par ce sujet, car ils ont entre leurs mains des données et informations très sensibles, qui nécessitent une identité sûre pour être en mesure de les communiquer. Toute communication, aussi bien avec les patient-e-s qu'entre professionnel-le-s de la santé, doit avoir une identification électronique unique et claire. Le dossier électronique du patient (DEP), outil utilisé par les médecins de famille et de l'enfance, est aussi touché par cet avant-projet de loi. En effet, les moyens d'identification électronique pour l'accès au dossier électronique du patient (DEP) seront à l'avenir émis par la Confédération, ils ne seront donc plus émis par des acteurs privés, ce que mfe soutient. Dans cette consultation mfe se positionne sur des points de portée générale et soutient la position de la FMH pour ce qui touche aux aspects techniques.

mfe salue la direction de l'avant-projet de loi mis en consultation. Il s'agit d'une contribution à la numérisation de la société, virage que la Suisse doit absolument prendre, car en comparaison internationale la Suisse est en retard, et ce plus spécifiquement dans le domaine de la santé.

mfe tient à souligner que les pays avancés dans la transformation numérique, telles que le Danemark et l'Estonie, donnent à leurs citoyen-ne-s une identité unique sous la souveraineté de l'Etat. mfe trouve pertinent que l'e-ID soit sous la souveraineté de l'Etat au vu de la sensibilité des données et conformément à la volonté populaire. Mais cela va de pair avec un grand devoir de responsabilité de la Confédération : ces données doivent être traitées avec le plus haut degré de sécurité.

Pour que l'e-ID soit adopté par la population de manière générale et plus particulièrement par les patient-e-s et professionnel-le-s de la santé, il est essentiel que les différents paramètres en lien avec l'e-ID soient facile d'accès et « user friendly ». Il s'agit de deux facteurs clés, dont il faut tenir compte à chaque étape de la conceptualisation de cette technologie.

Dossier électronique du patient (DEP)

Le présent avant-projet de loi touche les articles 7 et 11 de la loi fédérale du 19 juin 2015 sur le dossier électronique du patient

L'art. 11 admet les moyens d'identification privés actuels durant un certain temps pour accéder au DEP, avant que cette tâche soit à terme reprise par la Confédération. Pour mfe la « période transitoire » doit être accordée en dernier recours et si elle est jugée nécessaire, elle doit être aussi courte que possible.

Par ailleurs, tous les développements dans ce secteur doivent rester sous la houlette du département de la Justice et ne doivent pas être transférés à d'autres départements au vu des données sensibles dont il est question, y compris tous les identifiants et toutes les données qui touchent au domaine la santé.

Définition de conditions-cadres au niveau politique

Pour terminer, mfe souhaite une stratégie numérique nationale dans le domaine de la santé allant au-delà du DEP. La définition de conditions-cadres politiques claires et pratiques sont des éléments-clés pour pouvoir rattraper le retard de la Suisse. Dans l'intérêt des patient-e-s et des

soins de santé, il est important d'accorder une grande priorité à la numérisation de la santé, mfe espère que l'adoption de cette loi soit un moteur. La numérisation de la santé permettra des gains d'efficience, l'amélioration des prestations, une meilleure collaboration interprofessionnelle et ainsi un renforcement de la qualité et de la sécurité des soins.

Nous vous remercions de votre attention et vous prions de recevoir, Chère Madame la Conseillère fédérale, Mesdames, Messieurs, nos salutations distinguées.

A handwritten signature in blue ink, appearing to read 'Luchsinger'.

Philippe Luchsinger
Président de l'association Médecins
de famille et de l'enfance Suisse



LAW FIRM
ÉTUDE D'AVOCATS

DFJP

Département fédéral de justice et police
Office fédéral de la justice
Bundesrain 20
3003 Berne

Uniquement par courriel
rechtsinformatik@bj.admin.ch

Lausanne, le 20 octobre 2022

DRA

**Avant-projet de loi sur l'identité électronique et les autres moyens de preuve
électroniques (loi sur l'e-ID, LeID)**

Prise de position dans le cadre de la procédure de consultation

Madame, Monsieur,

Dans le délai imparti pour ce faire, et agissant pour le compte de l'Etude d'avocats HDC à Lausanne, je vous prie de trouver ci-après la prise de position de notre Etude par rapport au projet de loi visé en titre.

Dans l'ensemble, nous accueillons très favorablement ce projet ainsi remanié, tant l'identité électronique constitue un volet central de la modernisation de nos institutions et du fonctionnement de la société en général. Il est essentiel à ce titre que la population puisse bénéficier d'un système d'identification sûr, officiel et digne de confiance, sur lequel baser sa vie électronique. Une telle identité électronique fiable et efficace permettra indéniablement d'accélérer la transition numérique ainsi que l'efficacité des liens pouvant être créés entre individus et avec l'administration publique.

A ce titre, la rapidité avec laquelle le Conseil fédéral a repris le dossier suite au refus en votation populaire du précédent projet de loi en mars 2021 est à saluer. Ceci surtout dans la mesure où une grande partie des critiques qui avaient été émises vis-à-vis de ce premier projet ont été prises en compte dans l'avant-projet.

Ces remarques introductives données, les commentaires et éléments suivants doivent néanmoins être communiqués afin que certaines failles du système actuellement prévu puissent être corrigées.

I. Remarques générales

a) Rôle de l'autorité publique dans l'émission de l'e-ID et la gestion de l'infrastructure de confiance

Le rôle confié exclusivement à l'autorité publique – soit essentiellement la Confédération et, dans la mesure de l'art. 8 LelD, les cantons – dans l'émission et la gestion de l'e-ID est à saluer positivement. Cela assure un parallélisme bienvenu par rapport aux documents d'identité et de légitimation servant à l'établissement de l'e-ID (conformément à l'art. 3 let. a et b LelD), apte à renforcer la confiance de la population dans le système.

b) Volet relatif aux moyens de preuve électroniques (art. 12 ss)

La portée supplémentaire accordée à l'e-ID sous l'angle des moyens de preuve électroniques pouvant être émis à l'aide de l'infrastructure de confiance est également à considérer positivement. Il s'agit en effet là d'un moyen central permettant d'assurer l'utilité de l'e-ID ainsi que son inscription dans la vie pratique et journalière de la population.

c) Interopérabilité avec les systèmes européens (art. 27 LelD)

De façon particulièrement marquée, l'interopérabilité des systèmes et technologies liés à l'e-ID avec ceux appliqués et utilisés dans l'UE est centrale et doit permettre une efficacité concrète du système. A terme, une réelle identité reconnue à l'échelle européenne est un objectif impératif, là également à l'image de ce qui s'applique aux documents d'identité constituant le fondement « physique » de l'e-ID.

II. Remarques article par article

Outre les commentaires et remarques généraux qui précèdent, les points spécifiques suivants peuvent encore être relevés pour chacun des articles mentionnés.

a) Ad article 1

Les commentaires suivants peuvent être faits :

- Ad al. 2 let. a : l'extension de l'utilisation de l'e-ID non seulement entre personnes physiques et autorités, mais aussi entre personnes privées, est une condition essentielle au bon fonctionnement du système et à sa popularité.
⇒ Cette caractéristique doit donc impérativement être conservée.
- Ad al. 2 let. b :
 - o la protection des données dès la conception (*privacy by design*) n'est pas un principe, mais bien une obligation selon le système exprimé par

la nouvelle version de la LPD qui entrera en vigueur au 1^{er} septembre 2023. En particulier, une violation des impératifs liés à cette obligation ne peut être rendue légale par l'existence d'un motif justificatif au sens de l'art. 31 LPD, ceci au contraire de ce qui vaut pour les « principes » au sens strict.

- ⇒ Il convient donc de reformuler cette disposition en parlant de « l'obligation de la protection des données dès la conception ».
- la référence au principe de la minimisation des données doit s'inscrire dans le cadre plus large du principe de proportionnalité dont il fait partie, tant ce principe doit également s'étendre à l'e-ID. En particulier, la durée de conservation des données doit être limitée en vertu du principe de proportionnalité, et non uniquement du principe de la minimisation des données.
 - ⇒ Il convient donc de reformuler cette disposition en mentionnant explicitement le « principe de proportionnalité », en plus de la référence au principe de la minimisation des données.

b) Ad article 2

Les commentaires suivants peuvent être faits :

- Ad al. 2 let. a : la référence au « nom officiel » peut engendrer des problèmes d'interprétation, notamment dans la mesure où la personne aurait un nom d'usage qui serait néanmoins mentionné sur son document d'identité établi conformément à la LDI.
 - ⇒ Il convient donc d'évoquer plutôt le « nom tel que figurant sur le document d'identité ou la pièce de légitimation selon l'art. 3 LeID ».
- Ad al. 2 let. e : la référence au lieu de naissance peut représenter un doublon pour les personnes qui disposent d'un lieu d'origine, ce dernier étant le seul mentionné dans les documents d'identité conformes à la LDI.
 - ⇒ Il convient donc de modifier ce critère en indiquant « le lieu d'origine ou, à défaut, le lieu de naissance », notamment afin de respecter le parallélisme nécessaire avec les documents d'identité servant de base à l'e-ID ainsi que respecter le principe de minimisation des données.
- Ad al. 3 let. a : la référence au numéro AVS dans l'e-ID peut être particulièrement problématique en cas de faille de sécurité, dans la mesure où ce numéro n'est jamais modifié. En tant que les autres données figurant dans l'e-ID suffisent pour assurer l'identification de la personne, cette information ne devrait pas y figurer.
 - ⇒ Il convient donc de supprimer la référence au numéro AVS.

- Ad al. 3 let. f : les indications relatives à la procédure d'émission doivent exclusivement se limiter à des données de journalisation techniques, à l'exclusion notamment de détails relatifs à la procédure elle-même, là également afin d'assurer le respect du principe de la minimisation des données.
 - ⇒ Il convient donc de préciser les indications qui sont visées dans cette disposition, en en limitant le cercle à ce qui est absolument nécessaire.

c) *Ad article 3*

Les commentaires suivants peuvent être faits :

- Ad let. b : la référence à la « pièce de légitimation valable » n'est pas conforme à la terminologie utilisée dans la LEI pour qualifier les documents d'identification des personnes étrangères, mais correspond au passeport ou à la pièce d'identité de la personne concernée au sens de l'art. 13 LEI.
 - ⇒ Afin d'assurer le parallélisme nécessaire avec les documents d'identification établis par l'Etat ainsi que tenir compte du fait que certains étrangers peuvent ne pas disposer en tout temps d'un passeport ou d'une pièce d'identité, il convient de remplacer cette référence par une mention au « titre de séjour valable ».
- Ad commentaire : le commentaire relatif à cette disposition prévoit la possibilité de « limiter l'accès à certains services aux titulaires d'un permis étranger dont l'identité n'a pas pu être vérifiée de façon fiable. ». En tant que cette éventualité n'existe pas dans le projet de loi, cette référence doit être supprimée du commentaire.

d) *Ad article 4*

Les commentaires suivants peuvent être faits :

- Ad al. 4 :
 - la possibilité de prélever des données biométriques « à des fins de vérification » est rédigée de façon trop large et ne précise pas les hypothèses dans lesquelles ceci serait nécessaire. En tant que les informations et données contenues dans l'e-ID selon l'art. 2 LeID sont d'ores et déjà très détaillées, cette possibilité de vérification par le biais de données biométriques doit être limitée au maximum et correctement cadrées dans la loi quant aux critères et conditions applicables.
 - ⇒ Il convient de préciser les cas dans lesquels le recours aux données biométriques est possible.

- la durée pour laquelle les données biométriques peuvent être conservées dans le cadre de l'al. 4 n'est pas précisé, et le sort de ces données n'est pas non plus indiqué – la règle de l'art. 11 al. 5 LeID ne paraissant pas nécessairement s'appliquer aux données biométriques ainsi utilisées.
 - ⇒ Il convient donc de préciser explicitement, à l'art. 3 al. 4 LeID, que les données biométriques utilisées à des fins de vérification ne sont pas conservées au-delà de ce qui est nécessaire pour procéder à cette vérification.

e) *Ad article 5*

Les commentaires suivants peuvent être faits :

- *Ad al. 1 :*
 - de façon générale, les modalités appliquées à la révocation de l'e-ID par fedpol ne sont pas claires et doivent être précisées au niveau de la loi elle-même, en particulier s'agissant (i) de la forme d'une telle révocation (décision au sens de l'art. 5 PA), (ii) du processus suivi et (iii) des droits de la personne concernée.
 - ⇒ Les concours de la possibilité de révocation doivent être précisés.
 - la possibilité pour fedpol de révoquer l'e-ID en cas de « soupçon fondé d'utilisation abusive » (let. c) n'est pas claire et ouvre la voie à des problèmes d'interprétation ainsi que d'application. Ainsi et notamment, il n'est pas clair de savoir (i) selon quelle procédure cette révocation intervient, (ii) quelle forme peut prendre « l'utilisation abusive » ou (iii) les droits de la personne concernée dans une telle hypothèse. De façon générale, l'e-ID ne devrait pas être révoquée en cas d'utilisation abusive, mais cette dernière devrait plutôt donner lieu à sanction – à l'image de ce qui s'applique aux documents d'identité de la LDI.
 - ⇒ La possibilité de révocation prévue à l'al. 1 let. e devrait par principe être supprimée et le régime utilisé devrait être identique à celui valant pour les abus relatifs à des documents d'identité. Si cette possibilité devait néanmoins être conservée, il conviendra en tout cas de préciser les critères pouvant mener à la révocation de l'e-ID ainsi que les conditions et modalités devant être respectées dans ce cadre, à l'image de ce qui a été mentionné *supra* pour l'al. 1 en général.

- les échanges de données qui peuvent mener à une révocation conformément à l'art. 5 LeID ne sont pas clarifiés dans la LeID.
 - ⇒ Il est nécessaire de préciser, au niveau de la loi, quelles autorités peuvent communiquer des informations à fedpol sous l'angle des hypothèses couvertes par l'art. 5 LeID.
 - ⇒ De même, les communications provenant de fedpol aux autres autorités pouvant être concernées ou affectées par la révocation de l'e-ID doivent aussi être précisées au niveau de la loi.

f) Ad article 7

Les commentaires suivants peuvent être faits :

- Alors que l'existence d'un devoir de diligence est bienvenue sur le principe, la LeID ne précise aucune sanction à l'égard de la personne qui ne respecterait pas son devoir de diligence ou qui enfreindrait autrement les principes qui sont exprimés dans cette disposition. Les conséquences notamment de l'absence de mesures visées à l'art. 7 al. 1 LeID ne sont pas claires.
 - ⇒ D'éventuelles conséquences liées à une violation des devoirs de diligence pourraient être précisées.

g) Ad article 11

Les commentaires suivants peuvent être faits :

- Al. 2 : il n'est pas clair si le système d'information contient également les données d'identification prévues à l'art. 2 al. 2 LeID.
 - ⇒ Si tel est le cas, il convient de compléter l'art. 11 al. 2 en indiquant que le système d'information contient également les données visées à l'art. 2 al. 2 LeID.
- Al. 3 : tous les échanges de données avec les systèmes d'information doivent intervenir sur un système centralisé et non par duplication ou transmission des informations. Il s'agit d'un impératif sous l'angle du principe de minimisation des données ainsi que de sécurité des données.
 - ⇒ Il est nécessaire de préciser que tout accès aux données est fait directement dans le système, sans duplication ou communication.
- Al. 5 :
 - la durée de conservation pouvant aller jusqu'à 5 ans après la date de validité ou la révocation de l'e-ID est trop longue et ne se justifie par principe pas au regard des objectifs et buts poursuivis par le système

d'information de l'art. 11 LelD. Une durée d'une année au maximum apparaît suffisante.

- ⇒ La durée de conservation maximale doit être fixée à une année après la date de validité ou la révocation de l'e-ID.
- aucune durée de conservation claire n'est précisée s'agissant des éventuelles données biométriques utilisées à des fins de vérification (art. 4) ni pour les autres données qui ne sont pas directement intégrées dans le système d'information. Comme indiqué *supra*, ces données ne devraient pas être dupliquées ou intégrées dans le système d'information – une précision qui devrait toutefois figurer expressément dans la loi. Si une telle duplication est néanmoins nécessaire, une durée de conservation réduite devrait alors être prévue.
 - ⇒ Le régime applicable à la durée de conservation de tous les documents utilisés en lien avec l'e-ID, tout comme les modalités d'accès et l'exclusion de principe de la duplication, devraient être précisés dans la loi.

h) Ad article 12

Les commentaires suivants peuvent être faits :

- Il doit être précisé si les moyens de preuve électroniques sont également disponibles pour les personnes ne disposant pas d'une e-ID ou, au contraire, si cette dernière constitue une condition nécessaire à pouvoir disposer d'un tel moyen de preuve
- La question de savoir si une personne ou entité morale peut n'utiliser qu'exclusivement des moyens de preuve électroniques, à l'exclusion d'autres moyens de preuve, n'est pas clairement définie dans la loi. Cette dernière ne prévoit en effet pas une disposition similaire à l'art. 10 LelD par rapport à ces moyens de preuve électroniques – quelque chose qui est pourtant nécessaire.
 - ⇒ La possibilité, voire le droit, de disposer d'une alternative aux moyens de preuve électroniques devrait être précisée.

i) Ad article 13

Il peut être renvoyé *ceteris paribus* aux remarques relatives à l'art. 5 LelD s'agissant des procédures de révocation.

j) *Ad article 23*

Le caractère *open source* du code source de l'infrastructure de confiance est essentiel et doit être très favorablement accueilli.

k) *Ad article 24*

A la lecture de l'art. 24 LeID, l'on comprend que l'exploitation de l'infrastructure de confiance ne peut être déléguée à un sous-traitant. Un point qu'il convient cependant de préciser, afin d'éviter tout problème de compréhension et interprétation différente.

⇒ Il convient de préciser que l'exploitation visée à l'art. 24 LeID ne peut être déléguée à l'externe de l'administration fédérale.

* * *

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes sentiments dévoués.

Au nom de l'Etude d'Avocats HDC

David Raedler
Avocat (Dr en droit)
raedler@hdclegal.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Karin Keller-Sutter
Bundeshaus West
3003 Bern

per E-Mail:
rechtsinformatik@bj.admin.ch

Zürich, 20. Oktober 2022

Stellungnahme des HEV Schweiz

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

I. Einleitende Bemerkung

Mit Ihrem Schreiben vom 29. Juni 2022 haben Sie das Vernehmlassungsverfahren zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) eröffnet. Der HEV Schweiz ist mit seinen rund 340'000 Mitgliedern der grösste Vertreter der Haus-, Grund- und Stockwerkeigentümer in der Schweiz. Da die Interessen unserer Mitglieder von der Änderung des E-ID-Gesetzes (BGEID) betroffen sind, halten wir Folgendes fest.

II. Zur Vorlage

Der Gesetzesvorentwurf soll die Grundlagen für die Einführung der staatlichen elektronischen Identität (E-ID) in der Schweiz schaffen. Der Bund überprüft die Identität einer Person und stellt ihr eine E-ID aus. Die E-ID und andere elektronische Nachweise werden über eine vom Bund zur Verfügung gestellte staatliche Vertrauensinfrastruktur herausgegeben. Der Gesetzesvorentwurf regelt die Anforderungen an diese Infrastruktur, die sowohl öffentlichen als auch privaten Akteuren zur Verfügung stehen wird.

Der HEV Schweiz stellt sich nicht gegen eine staatliche E-ID. Aber der HEV Schweiz hat sich seit jeher gegen eine systematische Verwendung der AHV-Nummer als Personenidentifikator aufgrund des hohen Missbrauchspotentials ausgesprochen und gegen deren Verknüpfung mit anderen Registern.

Der HEV Schweiz äussert sich im Folgenden nur zur Bestimmung betreffend AHV-Nummernverwendung und erlaubt sich überdies einen Hinweis zum 14. Altersjahr als Grenze für die Errichtung bzw. den Widerruf der E-ID.

1. Art. 3 lit. a nBGEID Form und Inhalt: AHV-Nummer

Gemäss nBGEID enthält eine E-ID die folgenden Personenidentifikationsdaten: den amtlichen Namen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, die Nationalität und das Gesichtsbild aus dem Informationssystem Ausweisschriften (ISA) oder dem zentralen Migrationsinformationssystem (ZEMIS). Diese Daten sind in den amtlichen Registern des Staates verfügbar, auf die fedpol nach Art. 11 Abs. 3 nBGEID Zugriff hat. Verlangt ein Verifikatorin einen Nachweis, so kann der Inhaber ihr alle diese Daten oder gewisse davon übermitteln (Art. 2 nBGEID). Neben den Personenidentifikationsdaten enthält eine E-ID zusätzliche Informationen. Es handelt sich um folgende Daten: die AHV-Nummer; die E-ID-Nummer; ihr Ausstellungsdatum; ihr Ablaufdatum; Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises; und Angaben zum Ausstellungsprozess (diese werden auf Verordnungsstufe ausführlicher geregelt, Art. 3 nBGEID).

Der erläuternde Bericht zum Vorentwurf führt dazu Folgendes aus: «Aus Gründen der Transparenz werden in Artikel 2 die Daten aufgeführt, die die E-ID enthält. Dabei handelt es sich um Personenidentifizierungsdaten (Abs. 2) und weitere Daten (Abs. 3). Die Personenidentifizierungsdaten der Inhaberin oder des Inhabers umfassen: den amtlichen Namen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, die Nationalität und das Gesichtsbild aus ISA und ZEMIS. Diese Daten sind in den amtlichen Registern des Staates verfügbar, auf die fedpol nach Artikel 11 Absatz 3 Zugriff hat. Nebst den Personenidentifizierungsdaten enthält eine E-ID die AHV-Nummer sowie weitere Daten, welche bei der Ausstellung der E-ID generiert werden: Dabei handelt es sich um die E-ID-Nummer, das Ausstellungsdatum, das Ablaufdatum und die Angaben zum Ausstellungsprozess. Ferner enthält die E-ID Daten zum Ausweis, der zur Ausstellung der E-ID verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises. Details werden in einer Verordnung noch präzisiert werden.»

Das Problem der systematischen Verwendung der AHV-Nummer als Personenidentifikator stellte sich erstmals im Rahmen der ZGB-Revision im Bereich Personenstand und Grundbuch. Der HEV Schweiz lehnt diese Verwendung aus Gründen des Datenschutzes und der Missbrauchsgefahr nach wie vor ab. Auch Adrian Lobsiger, eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter und die kantonalen Datenschutzbeauftragten lehnen diese Verwendung der AHV-Nummer ab. Eine Verknüpfung der verschiedenen Register birgt enormes Missbrauchspotential und erleichtert den „Identitätsklau“ immens. Eine ETH Studie von Prof. Dr. David Basin teilt diese Meinung. Sie hält fest, dass bereits jetzt in über 14'000 administrativen und organisatorischen Registern persönliche und sensible Daten gespeichert und mit der AHV-Nummer indexiert sind. Sowohl die AHV-Nummer als auch Vorname, Nachname und Geburtsdatum werden in diesen Registern verwendet, um Personen mit Daten zu verknüpfen. Falls die Daten entwendet werden, sind die dazugehörigen Personen deshalb identifizierbar.

Die Verknüpfung der verschiedenen Register ermöglicht es Angreifern, umfangreiche Informationsprofile der betroffenen Personen zu erstellen, so die Studie. Diesem Missbrauchsrisiko gilt es Einhalt zu gebieten und der „Identitätsklau“ muss verhindert werden. Mit dem automatischen Informationsaustausch in Steuersachen wird die AHV-Nummer, welche als Steueridentifikator dient, sogar ins Ausland übermittelt. Dies erhöht das Risiko des Missbrauchs. Trotz aller Risiken beschloss das Parlament die AHV-Nummer als Personenidentifikator zu verwenden, weshalb diese inskünftig direkt im Grundbuch vermerkt wird (nArt. 949b ZGB). Immer mehr Gesetze sehen die Verwendung der AHV-Nummer als Personenidentifikator vor.

Nach der Vernehmlassung zum aBGEID hat der Bundesrat aufgrund der geäußerten Kritik von der Verwendung der AHV-Nummer zwecks Generierung der E-ID abgesehen, was der HEV Schweiz begrüsst hat. Das aBGEID wurde an der Urne am 7. März 2021 deutlich mit 65% Nein-Stimmen abgelehnt.

Auch im vorliegenden Entwurf sieht der Bundesrat von der Verwendung der AHV-Nummer zwecks Generierung der E-ID ab. Der HEV Schweiz begrüsst dies ausdrücklich.

Umso unverständlicher ist aber, dass der Bundesrat nun im vorliegenden Entwurf zum nBGEID vorschlägt, dass nebst weiteren Angaben (beispielsweise E-ID-Nummer) auch die AHV-Nummer in der E-ID enthalten sein soll. Die E-ID Nummer und die AHV-Nummer werden somit nebeneinander in der E-ID aufgeführt, damit findet eine weitere Verknüpfung statt. Angesichts der inzwischen beschlossenen Änderung des AHVG, welche die umfassende Verwendung der AHV-Nummer als Personenidentifikator durch dazu berechnigte Behörden, und damit einer immensen Anzahl an Personen, erlaubt, wird der Datenschutz vorliegend erst recht torpediert. Die Gefahr des «Identitätsklau» steigt umso mehr und ebenso die Missbrauchsgefahr. **Der HEV Schweiz lehnt deshalb Art. 3 lit. a nBGEID ab.**

Antrag HEV Schweiz zu Art. 3 lit. a nBGEID: streichen.

2. Art. 4 Abs. 2 nBGEID Ausstellung: Alter und Art. 5 lit. b nBGEID Widerruf

Der HEV Schweiz erlaubt sich folgenden Hinweis:

Unklar ist, weshalb der Bundesrat das 14. Altersjahr für die Errichtung bzw. den Widerruf einer E-ID für bedeutsam erklären will. Zwar verweist der Erläuterungsbericht auf eine (für die Schweiz nicht verbindliche) EU-Verordnung, welche eine Altersgrenze von 16 Jahren vorsieht, welche von den Mitgliedstaaten bis auf 13 Jahre gesenkt werden kann (der Inhalt des entsprechenden Artikels wurde sodann bei der Reform des Datenschutzgesetzes nicht übernommen). Dies begründet aber nicht im geringsten, weshalb Schweizer Jugendliche ausgerechnet mit 14 Jahren mit der entscheidenden Urteilskraft ausgestattet sein sollten. Es gäbe dann in der Schweiz die folgenden, diversesten «Mündigkeiten» - das heisst Urteilsfähigkeit und (uneingeschränkte) Handlungsfähigkeit:

- 10 Jahre (Jugend-)Strafmündigkeit
- 13 Jahre medizinische Mündigkeit
- *14 Jahre informationelle Mündigkeit*
- 16 Jahre sexuelle Mündigkeit
- 18 Jahre in allen übrigen Bereichen.

Der HEV Schweiz regt an, das 14. Altersjahr für die Errichtung bzw. den Widerruf der E-ID nochmals zu überdenken, damit in diesem Bereich nicht ein «Wildwuchs» entsteht – und dies ohne Not.

III. Fazit

Der HEV Schweiz begrüsst zwar, dass von der Verwendung der AHV-Nummer zwecks Generierung der E-ID abgesehen wurde. Er lehnt aber die parallele Führung von AHV-Nummer und E-ID Nummer in der E-ID aufgrund der Gefährdung des Datenschutzes, des grossen Missbrauchspotential und der Gefahr des «Identitätsklaus» aufgrund der Verknüpfung ab. Zudem regt er an, die Altersgrenze (14. Altersjahr) für die Errichtung und den Widerruf der E-ID zu überdenken.

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Hauseigentümerverband Schweiz

aNR Hans Egloff
Präsident HEV Schweiz

MLaw Annekäthi Krebs
Rechtskonsulentin

Vernehmlassungsantwort: Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Die Grundsätze des Vorentwurfs des neuen E-ID Gesetzes, wie Privacy by Design, Datensicherheit und Datensparsamkeit, sind sehr zu begrüßen. Die Beachtung dieser Grundsätze erlaubt eine Minimierung der Datenflüsse und gewährt den Inhaber*innen zusätzliche Kontrolle über ihre Daten.

Wir werden auf folgende Punkte eingehen, die wir bezüglich der Informationssicherheit und der technologieneutralen Formulierung des E-ID Gesetzes als wichtig erachten:

- Das Gesetz sollte die Funktionalität und Sicherheit der E-ID, anderer elektronischer Nachweise und deren Infrastruktur beschreiben und nicht die Architektur für die Implementierung dieser Infrastruktur.
- Sicherheitsbeweise, formale Spezifikationen und formale Sicherheitsanforderungen sind notwendig, um einen hohen Sicherheitsstandard zu gewährleisten.
- Wir beleuchten Aspekte, die bei der Ausstellung der E-ID abzuwägen sind und schlagen die Einführung einer Opt-Out-Funktion vor.
- Wir weisen auf weitere Punkte hin, die im Zusammenhang mit dem Schutz der Privatsphäre zu beachten sind.

Definieren der Funktionalität und Sicherheit anstatt der Implementierungsarchitektur

Im Vorentwurf wird definiert, dass die Vertrauensinfrastruktur aus fünf Komponenten¹ besteht. Dabei wird der Funktions- und Sicherheitsspezifikationen des Systems zu wenig Aufmerksamkeit geschenkt und stattdessen eine Architektur vorgeschrieben, die die technischen Realisierungsmöglichkeiten unnötig einschränkt. Eine grösstenteils funktionale und sicherheitsbezogene Spezifikation hingegen würde sowohl zu besseren Sicherheitsgarantien als auch zu mehr Flexibilität führen.

Funktions- und Sicherheitsspezifikationen sind notwendig, um eine Implementierung zu evaluieren. Wird ein System nur mit einer Spezifikation ihrer Architektur verglichen, kann zwar evaluiert werden, ob das System die vorgegebene Struktur hat, nicht aber ob es korrekt funktioniert. Ohne Funktions- und Sicherheitsspezifikationen ist es nicht klar, welche Verhaltensweisen von einer Implementierung erwartet werden und welche nicht erlaubt sind. Wird eine potenzielle Sicherheitslücke oder ein möglicher Bug gefunden, ist nicht klar, ob das gefundene Verhalten unerwünscht ist oder nicht. Bei der Entwicklung eines Systems sollten also die Architektur und die Technologien aufgrund von zuvor verfassten Funktions- und Sicherheitsspezifikationen gewählt werden. Da das E-ID-Gesetz die Grundlage für die Entwicklung eines solchen Systems sein soll, sollte es als Grundlage für die Funktions- und Sicherheitsspezifikationen dienen und nicht eine Architektur beschreiben.

1 Nämlich: das Basisregister (Art. 17), das System zur Bestätigung von Identifikatoren (Art. 18), eine Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen (Art. 19), eine Anwendung zur Prüfung von elektronischen Nachweisen (Art. 20) und ein System für Sicherungskopien (Art. 21).

Im Vorentwurf wird zum Beispiel das Basisregister als architektonische Komponente beschrieben. Es beinhaltet Daten über die Ausstellerinnen, Verifikatorinnen und zu widerrufenen Nachweisen. Diese Daten müssen jedoch nicht notwendigerweise in derselben Komponente enthalten sein. Es könnte sich auch um mehrere Komponenten handeln, je nachdem, welche Technologien und Architektur gewählt werden.

Somit ist der Vorentwurf zu konkret und zu strikt. Die Wahl der Technologie und der Architektur des Systems würde bereits von vorgeschriebenen Architekturkomponenten abhängen. Dies könnte gute Lösungen verhindern oder verkomplizieren und widerspricht der vom Vorentwurf angestrebten Technologieneutralität.

Insbesondere sollte das Gesetz die Anforderungen an die Vertrauensinfrastruktur regeln und nicht deren Architektur. Diese Anforderungen sollen die Funktionen und die Sicherheitseigenschaften des Systems beschreiben, etwa: Wem werden welche Daten zur Verfügung gestellt, welche Daten sollen zum Schutz der Privatsphäre geheim bleiben oder fälschungssicher sein.

Beispielsweise könnten die Daten über den Widerruf von elektronischen Nachweisen im Basisregister folgendermassen als Funktionalität mit assoziierten Sicherheitseigenschaften beschrieben werden:

Für das Verifizieren von Nachweisen stellt die Vertrauensinfrastruktur eine Funktion zur Verfügung, die bestätigt, dass ein bestimmter Nachweis nicht widerrufen wurde.

- Dieser Prozess soll die Privatsphäre der Inhaber*in des Nachweises möglichst gut schützen.
- Bei diesem Prozess dürfen die Verifikatorin, die den Nachweis verifiziert, die Inhaber*in dieses Nachweises, die Ausstellerin des Nachweises und die Vertrauensinfrastruktur involviert sein.
- Die Ausstellerin darf die Identität der Verifikatorin und die vorgewiesenen Daten nicht erfahren.
- Die Verifikatorin darf nur erfahren, ob der Nachweis widerrufen wurde, sowie auf die Daten Zugriff erhalten, die die Inhaber*in vorweisen will.
- Auch darf die Betreiberin der Vertrauensinfrastruktur nichts über den Inhalt des Nachweises oder deren Inhaber*in lernen.
- Falls nötig, darf die Vertrauensinfrastruktur Daten zu widerrufenen Nachweisen speichern, wie zum Beispiel Identifikatoren von widerrufenen Nachweisen.

Diese Beschreibung ist zwar länger als die Beschreibung der widerrufenen Nachweise im Vorentwurf, gleichzeitig aber viel flexibler formuliert. Beispielsweise wäre ein interaktiver Null-Wissen-Beweis (Zero-Knowledge-Proof) ähnlich wie bei E-Voting-Protokollen möglich, bei dem die Inhaber*in Nachrichten von der Verifikatorin an die Ausstellerin weiterleitet. Ein solcher Zero-Knowledge-Proof würde dann das Verknüpfen zweier Vorweisungen desselben Nachweises verhindern, was zum Datenschutz beiträgt. Eine solche interaktive Lösung ist im Vorentwurf nicht vorgesehen, da die Ausstellerin keine Kenntnis vom Vorweisen haben darf. Gleichzeitig erlaubt die obige Beschreibung eine Lösung mit einem Basisregister, wie im Vorentwurf definiert.

Das Beschreiben funktionaler Anforderungen und Sicherheitseigenschaften anstelle der Architektur ermöglicht also mehr Flexibilität bei der Wahl der Technologien und dem Design des Systems. So kann die Vertrauensinfrastruktur ohne Gesetzesänderungen an zukünftige technologische Entwicklungen angepasst werden. Ausserdem ist mit solchen Anforderungen viel klarer geregelt, wie sich ein System verhalten soll.

Anmerkung: Dies betrifft nur die Komponenten der Vertrauensinfrastruktur, nicht aber die Unterscheidung zwischen der Vertrauensinfrastruktur und dem Informationssystem des Fedpol. Da diese beiden Systeme von unterschiedlichen Stellen betrieben werden, ist eine Trennung sinnvoll. Somit bleiben die Daten für die Ausstellung der E-ID beim Fedpol und die Daten, die zur Betreuung der Vertrauensinfrastruktur benötigt werden, bei der Betreiber*in der Vertrauensinfrastruktur.

Notwendigkeit von Sicherheitsbeweisen

Die Sicherheit der E-ID ist zentral. So ging aus der öffentlichen Konsultation hervor: «Um Vertrauen in die E-ID zu entwickeln, fordert die Mehrheit (35) eine hohe Sicherheit der E-ID und des damit genutzten Systems.» Um die Sicherheit eines Systems zu gewährleisten, müssen Sicherheitseigenschaften definiert und bewiesen werden. Im Vorentwurf werden solche Sicherheitsbeweise jedoch nicht erwähnt.

Sicherheitsbeweise oder Konformitätsbeweise werden gemäss VELeS für das E-Voting verlangt. Sicherheitsbeweise sind auch für die E-ID und deren Infrastruktur sinnvoll. E-Voting und E-ID verlangen beide, dass ein grosses Vertrauen in die jeweiligen Systeme besteht. Selbstverständlich unterscheiden sich E-Voting und E-ID in ihren Sicherheitsanforderungen. Jedoch spricht nichts dafür, dass bei der E-ID die Einhaltung niedrigerer Sicherheitsstandards ein ausreichendes Vertrauensniveau gewährleisten würde. Sowohl beim E-Voting als auch der E-ID sollen koordinierte, grossflächige Angriffe verhindert werden. Zusätzlich können bei der E-ID einzelne Identitätsdiebstähle für die Geschädigten verheerend sein; dies betrifft sowohl die Personen, deren Identität gestohlen oder gefälscht wurde, als auch die getäuschten Verifikatorinnen. Somit müssen eine E-ID und deren Infrastruktur mindestens ähnliche Sicherheitsstandards wie ein E-Voting-System erfüllen.

Es stellt sich ausserdem die Frage, ob das Konzept der Sicherheitsbeweise auf eine E-ID und andere elektronische Nachweise überhaupt anwendbar ist. Im Gegensatz zu einem E-Voting-Protokoll handelt es sich bei der E-ID, den anderen elektronischen Nachweisen, der Vertrauensinfrastruktur und dem System des Fedpol nicht um ein *einzelnes* Protokoll. Daher wird es vermutlich nicht sinnvoll oder möglich sein, alle Komponenten in einem Beweis zu verifizieren. Es wäre jedoch möglich, für einzelne Komponenten, Protokolle und Zertifikate symbolische und/oder kryptographische Beweise durchzuführen. Die genauen Anforderungen an solche Beweise müssten wohl ähnlich wie für das E-Voting auf Verordnungsstufe geregelt werden.

Um Sicherheitsbeweise durchzuführen, müssen zuerst die Sicherheitsanforderungen formal definiert werden. Diese Anforderungen können Eigenschaften wie Unfälschbarkeit von Nachweisen, Untraceability oder die Geheimhaltung von privatem Schlüsselmateriale beinhalten. Weiterhin wird eine formale Spezifikation des Systems benötigt, zum einen, um die Sicherheitseigenschaften der Spezifikation zu beweisen, zum anderen, um zu überprüfen, dass sich die Implementierung an die Spezifikation hält. Zu diesem Zweck können Code-Reviews durchgeführt und Programmverifikationstechniken angewendet werden. Eine formale Spezifikation und formale Sicherheitsanforderungen sind also nicht nur mit Blick auf Sicherheitsbeweise, sondern für jede Art von Sicherheitsüberprüfung essenziell. Wenn ein potenzieller Bug oder eine mögliche Sicherheitslücke gefunden wird, ist ohne formale Spezifikation und ohne formale Sicherheitsanforderungen nicht klar, ob das gefundene Verhalten unerwünscht ist oder nicht.

Flexibilität und Sicherheit des Ausstellungsprozesses

Der Ausstellungsprozess der E-ID, insbesondere die Verifikation der Identität der antragstellenden Person, ist extrem sicherheitskritisch. Bisher wurde vorgeschlagen, den Ausstellungsprozess digital und mithilfe einer App umzusetzen. In den Partizipations-Meetings und auf GitHub gab dieses Thema Anlass zu intensiven Diskussionen. Es wurden Bedenken geäussert, dass eine rein digitale Lösung im Vergleich zu einer Lösung, bei der das physische Erscheinen vorausgesetzt wird, nicht gleich starke Sicherheitseigenschaften garantieren kann. Gegen das persönliche Erscheinen sprechen die benötigten Ressourcen und die verringerte Benutzerfreundlichkeit. Diese Aspekte müssen gegeneinander abgewogen werden. Dabei ist es wichtig, wie oben erwähnt, die Sicherheitseigenschaften der gewählten Lösung formal zu definieren. Alternativ könnte, wie beispielsweise von der europäischen eIDAS-Richtlinie² vorgesehen, zwischen verschiedenen Identitätssicherungsniveaus (*assurance levels*) mit unterschiedlichen Anforderungen an den Ausstellungsprozess unterschieden werden.

Art. 14 verlangt, dass die Inhaber*in das Mittel zur Aufbewahrung selbst wählen kann. Dies ermöglicht eine grössere Kontrolle der Inhaber*in über ihre Daten. Die bisherigen vorgeschlagenen Ausstellungsprozesse sind aber ausschliesslich an eine Smartphone-App gekoppelt. Wenn, wie vorgeschlagen, die E-ID an das Smartphone gekoppelt würde, könnten keine anderen technischen Mittel, wie z.B. Desktop-Applikationen, Hardware-Wallets oder USB-Sticks, gewählt werden. Wird also festgelegt, dass die E-ID an ein Smartphone gekoppelt wird, würde dies dem aktuellen Vorentwurf widersprechen. Hierbei gilt es erneut zwischen der Kontrolle der Inhaber*innen über ihre Daten, den Sicherheitsgarantien der einzelnen Lösungen und der Benutzerfreundlichkeit abzuwägen.

Personen, die keine E-ID beantragen, könnten befürchten, dass jemand sich in ihrem Namen eine E-ID ausstellt. Diese Sorge könnte deutlich gemindert werden, wenn eine Opt-Out-Funktion eingeführt würde: Personen, die keine E-ID möchten, könnten sich auf eine Liste setzen lassen, die die Ausstellung von E-IDs im Namen dieser Person verhindert. Somit könnten diese Personen auch beweisen, dass eine E-ID in ihrem Namen gefälscht wurde.

Privatsphäre

Der Schutz der Privatsphäre ist ein wichtiges Recht (Art. 13 BV), das mit dem Grundsatz Privacy by Design im Vorentwurf des E-ID Gesetzes verankert ist. Dabei sollte zwischen Situationen unterschieden werden, in denen die Identität der Inhaber*in entscheidend ist, zum Beispiel beim Eröffnen eines Bankkontos, und Situationen, in denen nur einzelne Attribute relevant sind, zum Beispiel bei einer Alterskontrolle. Im ersten Fall wird die Identität übermittelt. Im zweiten Fall kann die Anonymität der Inhaber*in entscheidend sein.

Zu beachten ist, dass auch aus anonymisierten Daten Informationen gewonnen werden können. Zum Beispiel: Würde der Identifier der E-ID immer mitgesendet, um zu überprüfen, dass sie nicht widerrufen wurde, könnten zwei unabhängige Verifikationsinteraktionen mit derselben E-ID verknüpft werden. Eine Methode zur Überprüfung der Gültigkeit einer E-ID sollte also keine solchen Identifikatoren preisgeben.

2 Siehe eIDAS, insb. Art. 8 „Sicherheitsniveaus elektronischer Identifizierungssysteme“.

Die Daten in einem elektronischen Nachweis werden von der Ausstellerin authentifiziert. Im Fall der E-ID bestätigt also das Fedpol die Validität der Daten. Damit sind diese Daten viel wertvoller, als beispielsweise Daten aus einem Freitextfeld. Zwecks der Datenminimierung sollte deshalb verhindert werden, dass bei jeder digitalen Interaktion ein elektronischer Nachweis verlangt wird. Dies sollte durch das Datenschutzgesetz gegeben sein. Sowohl die Inhaber*innen der Daten, also auch die Verifikatorinnen und Ausstellerinnen sollten darauf sensibilisiert werden.

Art. 16 enthält einen wichtigen Punkt zum Schutz der Privatsphäre: Inhaber*innen sollen entscheiden, welche Bestandteile des Nachweises übermittelt werden. In bisherigen proof-of-concept Wallets gibt die Verifikatorin vor, was übermittelt werden soll. Dies ist benutzerfreundlicher, da die Inhaber*in die zu übermittelnden Daten nicht einzeln auswählen muss. Es ist jedoch problematisch, wenn der Inhaber*in keine Möglichkeit gegeben wird, diese Auswahl explizit zu bestätigen oder zu ändern. Zur Wahrung der Privatsphäre muss ein einheitlicher Prozess festgelegt werden, in dem die Inhaber*in die Auswahl der zu übermittelnden Daten im Voraus bestätigen bzw. ändern kann.

Erklärung: Diese Antwort stellt ausschliesslich die Auffassung der Unterzeichnenden dar und ist nicht als Stellungnahme der ETH Zürich zu verstehen.

Xenia Hofmeier

Xenia Hofmeier ist Doktorandin am Institut für Informationssicherheit der ETH Zürich. Ihre Forschungsinteressen beinhalten das Analysieren von Sicherheitsprotokollen mit formalen Methoden und automatisierten Tools.

François Hublet

François Hublet ist Doktorand am Institut für Informationssicherheit der ETH Zürich. Seine Forschungsinteressen umfassen Privacy by Design, Datenschutzregelungen und formale Methoden.

Dr. Christoph Sprenger

Christoph Sprenger ist leitender wissenschaftlicher Mitarbeiter und Dozent am ETH Institut für Informationssicherheit. Er forscht im Bereich von formalen Methoden zur Spezifikation und Verifikation der Korrektheit und Sicherheit von verteilten Systemen im Allgemeinen und von Sicherheitsprotokollen im Speziellen.



Eidgenössisches Justiz- und Polizeidepartement EJPD

Frau Bundesrätin Karin Keller-Sutter

Ausschliesslich per E-Mail an:

rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID), Vorentwurf: Vernehmlassungsantwort der Schweizer Informatik Gesellschaft (SI)

Sehr geehrte Frau Bundesrätin Keller-Sutter,
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zu oben genanntem Geschäft Stellung zu beziehen. Da es sich um ein Informatikthema von hoher gesellschaftspolitischer Relevanz handelt, nehmen wir die Möglichkeit einer Stellungnahme gerne wahr.

Die Schweizer Informatik Gesellschaft SI ist der Verband der Informatikfachleute mit akademischer Ausbildung in der Schweiz. Die SI setzt sich für die Förderung der Informatik in Wirtschaft, Bildung, Forschung und Gesellschaft in der Schweiz ein, mit dem Ziel, dass die Schweiz auch in Zukunft zu den international führenden Technologiestandorten zählt. Hierzu gehört, dass die Schweiz auch bei der Digitalisierung und der Nutzung digitaler Werkzeuge zu den führenden Ländern gehört.

1. Zusammenfassung

Die SI begrüsst die Stossrichtung des Vorentwurfes. Ebenso begrüssen wir, dass der Entwurf weitgehend technologieneutral gehalten ist, was eine kontinuierliche technologische Weiterentwicklung der Umsetzung der E-ID-Prozesse, wie im Gesetz beschrieben, ermöglicht.

Wir begrüssen, dass dem Prinzip «dezentrale Datenspeicherung» gefolgt werden soll. Allerdings ist beim Ausstellen und der Verifikation sowie beim elektronischen Identifizieren immer die zentrale «Vertrauensinfrastruktur des Bundes» beteiligt, was der Idee der Dezentralisierung zuwiderläuft. Das Gesetz sollte daher neben der zentralisierten Verifikation eine dezentrale Offline-Verifikation zulassen, unter der Bedingung, dass diese technisch sicher realisiert werden kann.

Wir begrüssen die Möglichkeit, dass auch private Anbieter elektronische Nachweise unter Verwendung der vom Bund bereit gestellten Vertrauensinfrastruktur bereitstellen können. Insbesondere



KMUs, welche sich keine eigene Vertrauensinfrastruktur leisten können, werden von dieser Möglichkeit profitieren.

Wir bedauern, dass mit der E-ID nicht gleichzeitig die gesetzlichen Grundlagen für eine elektronische Signatur (z.B. von Dokumenten und E-Mails) unter Verwendung der E-ID geschaffen werden.

2. Die einzelnen Gesetzesbestimmungen gemäss Vorentwurf

- **Art. 1**

Im Zweck ist nur die «sichere Identifizierung mittels E-ID» genannt. Es müssen auch die Vorgänge der anderen Nachweise genannt werden, sonst macht Art1.1.b, welche eine Infrastruktur dafür vorsieht, keinen Sinn.

- **Art. 2**

Der Einbezug von Rufnamen unter den Inhalt der E-ID könnte die Akzeptanz des Gesetzes und die User Experience fördern (entspricht eCH 0011 und eCH 0201).

In Art2.2.d müsste aus unserer Sicht zudem klargestellt werden, welches Geschlecht gemeint ist, das biologische oder das wahrgenommene Geschlecht.

- **Art. 3**

Keine Anmerkungen.

- **Art. 4**

Es sollte die Möglichkeit geschaffen werden, dass neben dem Fedpol auch weitere Stellen (z.B. Passbüro, Gemeinden) zur Ausstellung der E-ID legitimiert werden. So könnte eine E-ID beispielsweise gleichzeitig mit einer physischen ID-Karte oder einem Pass beantragt werden, was die Attraktivität der E-ID steigert.

- **Art. 5**

Keine Anmerkungen.

- **Art. 6**

Keine Anmerkungen.

- **Art. 7**

Keine Anmerkungen.

- **Art. 8**

Keine Anmerkungen.

- **Art. 9**

Die E-ID sollte zwingend auch bei physischen «Kontrollen» akzeptiert werden *müssen*. Z.B. «Ich weise meine auf dem Mobile vorliegende E-ID vor, um mich beim Handelsregisteramt zu identifizieren».



Es sollte verlangt werden, dass der Vorgang der «elektronischen Identifizierung» auch offline, d.h. wenn die zentralen Komponenten der «Vertrauensinfrastruktur des Bundes» nicht verfügbar sind, funktioniert. Dazu ist der Einsatz dezentraler Komponenten der «Vertrauensinfrastruktur des Bundes» im Gesetz vorzuschreiben.

- **Art. 10**

Keine Anmerkungen.

- **Art. 11**

Im Gesetz oder auf Verordnungsstufe sollte geregelt werden, dass ab dem Zeitpunkt des Eingangs eines Widerrufs allfällige, mit der widerrufenen E-ID getätigte Transaktionen ungültig sind und als nicht erfolgt gelten. Der Inhaberin oder dem Inhaber einer E-ID dürfen keine Nachteile entstehen, wenn die Vertrauensinfrastruktur des Bundes eine E-ID nicht unmittelbar nach Eingang eines Widerrufs sperrt.

- **Art. 12**

Hier fehlt eine Aussage, wer berechtigt ist, elektronische Nachweise auszustellen und die Infrastruktur nach dem 5. Abschnitt zu nutzen. Sind dies nur staatliche Stellen oder auch private natürliche oder juristische Personen?

- **Art. 13**

Hier gilt gleiches wie beim Widerruf einer E-ID; siehe unser Kommentar zu Art. 11.

- **Art. 14**

Genügt der Satz in Art. 2 Absatz 1 um sicherzustellen, dass Art. 14 auch für die E-ID gilt und nicht nur für „Andere elektronische Nachweise“?

Es sollte im Gesetz oder auf Verordnungsstufe geregelt werden, ob die Inhaberin oder der Inhaber Kopien der E-ID bzw. von anderen elektronischen Nachweisen auf mehr als einem Gerät aufbewahren darf.

- **Art. 15**

In Art. 15 ist erstmals von elektronischen Nachweisen die Rede, welche nicht auf eine natürliche Person ausgestellt werden.

Das Gesetz sollte ausdrücklich (entweder im Ingress oder im ersten Artikel des dritten Abschnitts) festhalten, dass andere elektronische Nachweise (d.h. mit Ausnahme der E-ID) sowohl auf natürliche wie auf juristische Personen ausgestellt werden können.

- **Art. 16**

Entsprechend dem Prinzip der Datensparsamkeit sollte in Art. 16 explizit festgehalten werden, dass im Zuge eines Geschäftsvorgangs (oder zur Autorisierung eines Geschäftsvorgangs) die Verifikatorin nur Informationen des elektronischen Nachweises verlangen darf, welche zum Zweck des Geschäftsvorgangs benötigt werden.



- **Art. 17 und 18**

Das Basisregister scheint uns eine Art E-ID (Identifikator genannt) für juristische Personen zu sein, um insbesondere Amtsstellen (Bund, Kantone, Gemeinden) sicher zu identifizieren. Hier stellt sich die Frage, ob und wie weit alle Amtsstellen, welche elektronische Dienstleistungen anbieten, verpflichtet werden sollen, sich im Basisregister einzutragen.

Es ist zu prüfen, ob Art. 17 und 18 nicht technologieneutraler formuliert werden können, beispielsweise ohne die explizite Nennung kryptographischer Schlüssel.

Grammatik Art 18 Abs 3: «Alle Behörden und Private können ...»

- **Art. 19**

Der Bund bietet hiermit eine «Elektronische Briefftasche» für Inhaber einer E-ID auf der «Vertrauensinfrastruktur des Bundes» kostenfrei an. Dies wird der Verbreitung der E-ID Auftrieb verleihen. Doch die nachfolgenden Dienste gehören nach unserem Verständnis auch kostenfrei und für die Bürger einfach machbar dazu:

- Ein Prozess, wie eine auf allen Geräten verlorengegangene E-ID wieder hergestellt werden kann. Vermutlich muss der Bürger dazu physisch mit den Ausweisen noch einmal erscheinen.
- Ein Prozess zum Gerätewechsel.
- Die nahtlose Ablösung einer abgelaufenen E-ID durch eine neue E-ID und Weiterbestand der «Elektronischen Briefftasche».

- **Art. 20**

Die Formulierung als Kann-Bestimmung ist zu schwach. Die Überprüfung der Gültigkeit eines Nachweises ist unseres Erachtens ein zentraler Bestandteil der Vertrauensinfrastruktur. Art. 20 sollte daher analog zu Art. 19 gefasst werden: «Der Bund stellt eine Anwendung zur Verfügung, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können.»

- **Art. 21**

Wenn unter Art. 19 die von uns vorgeschlagenen Dienste ebenfalls angeboten werden, dann könnte dieser Artikel möglicherweise ganz entfallen.

Der Verbreitung der E-ID wären kostenlose Dienste betreffend Backup/Restore zuträglich.

- **Art. 22**

Keine Anmerkungen.

- **Art. 23**

Ein sozio-technisches System wie «E-ID und elektronische Nachweise» ist nicht allein durch Offenlegung des Quellcodes prüfbar. Man muss z.B. auch wissen, welche Anforderungen durch den Quellcode erfüllt werden (sollen), um eine Aussage darüber machen zu können, ob der Quellcode ok ist oder nicht.

Wir empfehlen zu fordern, dass eine Systemdokumentation nach den *best-practices* des Berufsstands, inkl. des Quellcodes, zu erstellen, prüfen und offenzulegen ist.

- **Art. 24**

Gehört das Fedpol-System zum E-ID-Ausstellen auch dazu? Falls ja, hier explizit erwähnen.



- **Art. 25**

Der Bezug von Absatz 1 und 2 ist klarer zu machen: Z.B. «Der Bundesrat kann **mit Verordnungen** vorsehen, dass...» und dann «... treten **diese Verordnungen** ~~die Bestimmungen~~-ausser Kraft:»

- **Art. 26**

Wir begrüssen, dass für die Nutzung der E-ID gemäss Absatz 4 keine Gebühren erhoben werden. Die Gebühren für den Eintrag ins Basisregister sollten so festgelegt werden, dass sich auch Privatpersonen und KMUs einen Eintrag leisten können.

- **Art. 27**

Das Gesetz sollte hier ausdrücklich fordern, dass der Bund geeignete Massnahmen trifft mit dem Ziel, dass die schweizerische E-ID mit ausländischen E-IDs, insbesondere denen der Europäischen Union, kompatibel ist.

- **Art. 28 und andere Erlasse**

Keine Anmerkungen.

3. Schlussbemerkung

Die SI als Berufsverband der akademisch gebildeten IT-Berufsleute und aller an den Universitäten dozierenden IT-Professoren bietet dem Bund gerne die aktive Mitwirkung bei einer Überarbeitung des G-E-ID Vorentwurfs an.

Wir danken Ihnen für die Aufmerksamkeit, die Sie unserer Antwort schenken werden.

Beste Grüsse

Für die Schweizer Informatik Gesellschaft

A handwritten signature in black ink, appearing to read 'Baud', with a long horizontal stroke extending to the right.

Francis Baud, Präsident



Département fédéral de justice et police DFJP
Madame la Conseillère fédérale Karin Keller-Sutter
Exclusivement par e-mail à :
rechtsinformatik@bj.admin.ch

Berne, le 20 octobre 2022

Loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques (loi sur l'e-ID, LeDI), avant-projet : réponse à la consultation de la Société suisse d'informatique (SI)

Madame la Conseillère fédérale Keller-Sutter,
Mesdames et Messieurs,

Nous vous remercions de nous donner la possibilité de prendre position sur l'objet susmentionné. S'agissant d'un thème informatique d'une grande importance sociopolitique, nous saisissons volontiers la possibilité de prendre position.

La Société Suisse d'Informatique SI est l'association des professionnels de l'informatique ayant une formation académique en Suisse. La SI s'engage pour la promotion de l'informatique dans l'économie, la formation, la recherche et la société en Suisse, dans le but de faire en sorte que la Suisse reste l'un des sites technologiques leaders au niveau international. Cela implique que la Suisse fasse également partie des pays leaders en matière de numérisation et d'utilisation d'outils numériques.

1. Résumé

La SI salue l'orientation de l'avant-projet. Nous saluons également le fait que le projet soit largement neutre sur le plan technologique, ce qui permet un développement technologique continu de la mise en œuvre des processus e-ID, comme décrit dans la loi.

Nous saluons le fait que le principe de "stockage décentralisé des données" soit suivi. Toutefois, l'"infrastructure de confiance de la Confédération" centrale est toujours impliquée dans l'établissement et la vérification ainsi que dans l'identification électronique, ce qui va à l'encontre de l'idée de décentralisation.

La loi devrait donc autoriser, outre la vérification centralisée, une vérification décentralisée hors ligne, à condition que celle-ci puisse être réalisée de manière sûre sur le plan technique.



Nous saluons la possibilité pour les fournisseurs privés de fournir des preuves électroniques en utilisant l'infrastructure de confiance mise à disposition par la Confédération. Les PME, en particulier, qui ne peuvent pas se permettre d'avoir leur propre infrastructure de confiance, profiteront de cette possibilité.

Nous regrettons que les bases légales pour une signature électronique (par exemple, pour des documents et courriels) utilisant l'e-ID ne soient pas créées en même temps que l'e-ID.

2. Les différentes dispositions légales selon l'avant-projet

- **Art. 1**

Dans le but, seule "l'identification sécurisée au moyen de l'e-ID" est mentionnée. Il faut également mentionner les processus des autres preuves, sinon l'art 1.1.b, qui prévoit une infrastructure à cet effet, n'a pas de sens.

- **Art. 2**

L'inclusion de l'indicatif dans le contenu de l'e-ID pourrait favoriser l'acceptation de la loi et l'expérience utilisateur (correspond à eCH 0011 et eCH 0201).

De notre point de vue, l'art 2.2.d devrait en outre préciser de quel sexe il s'agit, le sexe biologique ou le sexe perçu.

- **Art. 3**

Aucune remarque.

- **Art. 4**

Il faudrait créer la possibilité que d'autres services que Fedpol (p. ex. bureau des passeports, communes) soient légitimés à établir l'e-ID. Ainsi, une identité électronique pourrait par exemple être demandée en même temps qu'une carte d'identité physique ou un passeport, ce qui augmenterait l'attrait de l'ID électronique

- **Art. 5**

Aucune remarque.

- **Art. 6**

Aucune remarque.

- **Art. 7**

Aucune remarque.

- **Art. 8**

Aucune remarque.



- **Art. 9**

L'e-ID devrait obligatoirement être acceptée même en cas de "contrôle" physique. Par exemple : "Je présente mon e-ID disponible sur mon mobile pour m'identifier auprès de l'office du registre du commerce".

Il faudrait exiger que le processus d'"identification électronique" fonctionne également hors ligne, c'est-à-dire lorsque les composants centraux de l'"infrastructure de confiance de la Confédération" ne sont pas disponibles. Pour ce faire, l'utilisation de composants décentralisés de l'"infrastructure de confiance de la Confédération" doit être prescrite dans la loi.

- **Art. 10**

Aucune remarque.

- **Art. 11**

Il convient de régler dans la loi ou au niveau de l'ordonnance qu'à partir du moment où une révocation est reçue, les éventuelles transactions effectuées avec l'e-ID révoquée ne sont pas valables et sont considérées comme n'ayant pas eu lieu. Le titulaire d'une e-ID ne doit pas subir de préjudice si l'infrastructure de confiance de la Confédération ne bloque pas une e-ID immédiatement après réception d'une révocation.

- **Art. 12**

Il manque ici une déclaration indiquant qui est autorisé à établir des preuves électroniques et à utiliser l'infrastructure visée à la section 5. S'agit-il uniquement d'organismes publics ou également de personnes physiques ou morales privées ?

- **Art. 13**

La même chose que pour la révocation d'une ID électronique s'applique ici ; voir notre commentaire sur l'art. 11.

- **Art. 14**

La phrase de l'art. 2, al. 1, est-elle suffisante pour garantir que l'art. 14 s'applique également à l'e-ID et pas seulement aux "autres preuves électroniques" ?

Il faudrait régler dans la loi ou au niveau de l'ordonnance si le titulaire peut conserver des copies de la carte d'identité électronique ou d'autres preuves électroniques sur plus d'un appareil.

- **Art. 15**

L'art. 15 parle pour la première fois de preuves électroniques qui ne sont pas établies au nom d'une personne physique.

La loi devrait indiquer expressément (soit dans le préambule, soit dans le premier article de la section 3) que les autres preuves électroniques (c'est-à-dire à l'exception de la carte d'identité électronique) peuvent être délivrées aussi bien à des personnes physiques qu'à des personnes morales.

- **Art. 16**

Conformément au principe de minimisation des données, l'art. 16 devrait explicitement stipuler que, dans le cadre d'une transaction (ou pour autoriser une transaction), le vérificateur ne peut demander que les informations de la preuve électronique qui sont nécessaires au but de la transaction.



- **Art. 17 et 18**

Le registre de base nous semble être une sorte d'e-ID (appelé identificateur) pour les personnes morales, notamment pour identifier de manière sûre les services officiels (Confédération, cantons, communes). La question qui se pose ici est de savoir si et dans quelle mesure tous les services officiels qui offrent des prestations électroniques doivent être obligés de s'inscrire dans le registre de base.

Il convient d'examiner si les art. 17 et 18 ne peuvent pas être formulés de manière plus neutre sur le plan technologique, par exemple sans mentionner explicitement les clés cryptographiques.

Grammaire Art 18 al 3 : " Alle Behörden und Private können ..."

- **Art. 19**

Par la présente, la Confédération offre gratuitement un "portefeuille électronique" aux titulaires d'une e-ID sur l'"infrastructure de confiance de la Confédération". Cela donnera une impulsion à la diffusion de l'e-ID. Mais les services suivants en font également partie, selon nous, gratuitement et facilement réalisables par les citoyens :

- Un processus permettant de récupérer un e-ID perdu sur tous les appareils. Il est probable que le citoyen doive se présenter à nouveau physiquement avec ses documents d'identité.
- Un processus de changement d'appareil.
- Le remplacement sans faille d'un e-ID arrivé à échéance par un nouvel e-ID et le maintien du "portefeuille électronique".

- **Art. 20**

La formulation en tant que disposition facultative est trop faible. Nous estimons que la vérification de la validité d'une preuve est un élément central de l'infrastructure de confiance. L'art. 20 devrait donc être rédigé de manière analogue à l'art. 19 : "La Confédération met à disposition une application permettant de vérifier la validité des preuves électroniques".

- **Art. 21**

Si les services que nous proposons sous l'art. 19 sont mis en place, cet article pourrait éventuellement être totalement supprimé.

Des services gratuits de sauvegarde/restauration contribueraient à la diffusion de l'e-ID.

- **Art. 22**

Aucune remarque.

- **Art. 23**

Un système socio-technique tel que "l'e-ID et les preuves électroniques" ne peut pas être contrôlé uniquement par la divulgation du code source. Il faut également savoir quelles exigences sont (doivent être) remplies par le code source pour pouvoir dire si le code source est correct ou non.

Nous recommandons d'exiger qu'une documentation système conforme aux meilleures pratiques de la profession, y compris le code source, soit établie, vérifiée et divulguée.



- **Art. 24**

Le système de Fedpol fait-il également partie de l'établissement de l'identité électronique ? Si oui, il faudrait le mentionner explicitement ici.

- **Art. 25**

Le lien entre les al. 1 et 2 doit être plus clair : Par exemple : " Der Bundesrat kann mit Verordnungen vorsehen, dass..." et également "... treten diese Verordnungen ~~die Bestimmungen~~ ausser Kraft:".

- **Art. 26**

Nous saluons le fait qu'aucun émolument ne soit perçu pour l'utilisation de l'e-ID conformément à l'alinéa 4. Les frais d'inscription au registre de base devraient être fixés de manière à ce que les particuliers et les PME puissent également se permettre une inscription.

- **Art. 27**

La loi devrait ici exiger expressément que la Confédération prenne les mesures appropriées dans le but de rendre l'e-ID suisse compatible avec les e-ID étrangères, notamment celles de l'Union européenne.

- **Art. 28 et suivants**

Aucune remarque.

3. Conclusion

La SI, en tant qu'association représentant l'ensemble des professionnels de l'informatique ayant une formation académique et de tous les professeurs d'informatique enseignant dans les universités, propose volontiers à la Confédération de participer activement à une révision de l'avant-projet e-ID.

En vous remerciant de toute l'attention que vous porterez à notre réponse, je vous prie d'agréer, Madame la Conseillère Fédérale, Mesdames et Messieurs, nos plus respectueuses salutations.

Pour la Société Suisse d'Informatique

A handwritten signature in black ink, appearing to read 'Baud', with a stylized flourish at the end.

Francis Baud, Président

Eidg. Justiz- und Polizeidepartement
EJPD

Versand per E-Mail an:
rechtsinformatik@bj.admin.ch

Ittigen, 20. Oktober 2022

**Vernehmlassung zum
Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und
andere elektronische Nachweise (E-ID-Gesetz, BGEID)**

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit zur Stellungnahme im Rahmen der Vernehmlassung zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise. Der Vorstand von inter-pension nimmt dazu gerne wie folgt Stellung:

Wir unterstützen grundsätzlich die Einführung einer E-ID. Die Vorsorgeeinrichtungen (Pensionskassen) werden im Gesetz und im Bericht zwar nirgends erwähnt. Trotzdem erachten wir ein solches Projekt als Chance auch für die Schweizer Vorsorgeeinrichtungen (sowohl für privatrechtliche als auch für öffentlich-rechtliche). Denn inter-pension ist überzeugt davon, dass die Digitalisierung auch bei den Vorsorgeeinrichtungen weiter voranschreitet. Während einige Einrichtungen einige digitale Prozesse bereits aufgegleist haben, so besteht u.E. noch ein grosses Ausbaupotenzial im – heute noch weitgehend fehlenden – elektronischen Datenaustausch unter den Vorsorgeeinrichtungen (die Stellenwechsel der Versicherten erfordern in der Regel einen Wechsel der Vorsorgeeinrichtung). Inter-pension setzt sich im Interesse seiner Mitglieder, der Sammel- und Gemeinschaftseinrichtungen, für einen solchen Ausbau der Digitalisierung und für eine Erhöhung der Verwaltungseffizienz ein. Hierfür könnte die E-ID äusserst nützlich sein. Unter Umständen könnten spezifische für Vorsorgeeinrichtungen geltende Regelungen auf Verordnungsstufe erlassen werden.

In diesem Sinne unterstützen wir die Einführung einer E-ID und ersuchen Sie, die spezifischen Belange der Vorsorgeeinrichtungen bei der weiteren Legiferierung in angemessener Weise zu berücksichtigen.

Wir danken Ihnen für die Kenntnisnahme und stehen für die Beantwortung allfälliger Fragen gerne zu Ihrer Verfügung.

Freundliche Grüsse

inter-pension

Laurent Schläfli
Präsident

Therese Vogt
Geschäftsstelle



Par courriel

rechtsinformatik@bj.admin.ch

Office fédéral de la justice
Bundesrain 20
3003 Berne

Berne, 20.10.2022

Avant-projet de loi fédérale sur l'identité électronique et les autres moyens de preuve électroniques

Madame, Monsieur,

Notre commission extraparlamentaire s'est penchée, lors de sa séance du 31 août 2022, sur l'avant-projet de loi sur l'identité électronique et les autres moyens de preuve électroniques (LeID). Nous remercions M. Rolf Rauschenbach et M. Urs Holenstein de votre office d'avoir participé à notre réunion et de nous avoir présenté les différents éléments du projet mis en consultation.

Les membres du Forum PME sont favorables à l'introduction d'une identité électronique étatique (e-ID) respectant le principe de neutralité technologique. Le système suisse d'identification devra à notre avis être conçu de manière à ce qu'il soit autant que possible compatible avec les autres systèmes développés à l'étranger. Pour ce faire, nous demandons qu'il respecte les normes internationales afin que l'e-ID suisse puisse être reconnue et également utilisée à l'étranger, une fois les conditions remplies.

La gratuité de l'e-ID est à notre avis une condition sine qua non à sa mise en place. L'article 26 de l'avant-projet prévoit que certains émoluments pourront cependant être perçus auprès des émetteurs et des vérificateurs du secteur privé. Nous estimons que, conformément à l'art. 46a, al. 4 de la loi sur l'organisation du gouvernement et de l'administration, le Conseil fédéral devrait prévoir dans ce domaine des dérogations, étant donné que l'e-ID présente un intérêt public prépondérant. En renonçant à la perception d'émoluments ou en les réduisant fortement, l'utilisation et la diffusion de l'e-ID seraient ainsi encore davantage encouragées.

Nous nous félicitons qu'il soit prévu que l'infrastructure qui sera mise en place puisse également être utilisée par les acteurs du secteur privé qui souhaitent établir des preuves numériques. Cet aspect du projet est à notre avis très important. Nous estimons pour cette raison que l'ouverture de l'infrastructure au secteur privé devra se faire aussi rapidement que possible. Pour que l'e-ID soit utilisée, le processus d'identification devra être simple et rapide. Nous demandons que cet aspect soit particulièrement pris en compte dans la suite des travaux.

Forum PME

Holzikofenweg 36, 3003 Berne
Tél. +41 58 464 72 32
kmu-forum-pme@seco.admin.ch
www.forum-pme.ch

Nous vous prions d'agréer, Madame, Monsieur, nos meilleures salutations.



Eric Jakob
Co-Président du Forum PME
Ambassadeur, Chef de la promotion
économique du Secrétariat d'État à l'économie

Copies à : Commissions des affaires juridiques du Parlement

**KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST
CONFÉRENCE DES AUTORITÉS CANTONALES DE SURVEILLANCE DE L'ÉTAT CIVIL
CONFERENZA DELLE AUTORITÀ CANTONALI DI VIGILANZA SULLO STATO CIVILE**

Eidg. Justiz- und Polizeidepartement
Frau Bundesrätin Karin Keller-Sutter

Per Mail an:
rechtsinformatik@bj.admin.ch

Münsingen, 29. September 2022

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)
Stellungnahme Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst (KAZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Sie laden in der eingangs erwähnten Angelegenheit zur Vernehmlassung ein. Dabei wurde davon abgesehen, die Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst (KAZ) in den Verteiler aufzunehmen. Da wir als Fachkonferenz von der Vorlage direkt betroffen sind, erlauben wir uns dennoch, nachfolgend Stellung zu nehmen.

Die vom Volk am 7. März 2021 in gleicher Angelegenheit unterbreitete und deutlich abgelehnte Vorlage trug den Titel "Bundesgesetz über elektronische Identifizierungsdienste". Diese sprachliche Verschiebung weg von "Identifizierung" neu hin zu "Identitäts (-nachweis) stiftet bis zu einem gewissen Grade Verwirrung. So soll die ausländische Wohnbevölkerung gemäss Art. 3 lit. b des Entwurfs bloss einen gültigen Ausweis nach AIG benötigen, um eine E-ID ausgestellt zu erhalten. In seiner physischen Form gilt als solcher Ausländerausweis nun aber einerseits nie als Identitätsausweis. Wie auch auf S. 9 des erläuternden Bericht ausgeführt, kann andererseits bei bestimmten Ausweiskategorien nicht davon ausgegangen werden, dass vorgängig die Identität der betreffenden Personen verlässlich festgestellt werden konnte (so N, F, S und C). Mit anderen Worten kann bei der Grundlage, die zur Ausstellung einer E-ID führt, unterschieden werden in:

- E-ID mit Identitätsnachweis
- E-ID ohne Identitätsnachweis

Der Gesetzgeber verzichtet nun darauf, den beiden in ihrer Fundiertheit und Aussagekraft

doch unterschiedlichen E-ID-Konstellationen differenzierte rechtliche Wirkungen beizumessen. So wird in Art. 9 festgehalten, dass jede Behörde oder andere Stelle, die öffentliche Aufgaben erfüllt, die E-ID akzeptieren muss, wenn sie eine elektronische Identifizierung vornimmt. Des Weiteren liest man im erläuternden Bericht zur eben genannten Bestimmung: "Dies ist angezeigt, weil die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet wird und damit vergleichbar ist mit Identitätskarte oder Pass in der physischen Welt, die auch bei jeder Identifizierung von allen Behörden akzeptiert werden."). Klar ist einmal, dass die E-ID in ihrer Wirkung nicht über diejenige des Ausländerausweises gehen darf. Dies soll so auch im Gesetz festgehalten sein. Um Missverständnissen vorzubeugen, macht es zudem Sinn, dass der Gesetzgeber terminologisch sehr deutlich zwischen einem Identifizierungsmittel und dem Identitätsnachweis unterscheidet. Mit dem Ausländerausweis kann man sich als diejenigen Person identifizieren, die in der Schweiz ein Aufenthaltsrecht unter dem im Ausweis genannten Daten (Namen, Geburtsdatum etc.) bewilligt worden ist. Ob dies Daten auch der tatsächlichen Identität entsprechen, ist hiervon klar zu trennen.

Zusammenfassend kann es nach dem Gesagten nicht genügen, in den Erläuterungen zu Art. 3 die Problematik aufzuzeigen ("fehlender Identitätsnachweis"), daran aber keine Konsequenzen zu knüpfen. Hier gilt es dringend, anzusetzen und zu differenzieren. Nicht zuletzt die Zivilstandsbehörden stellen bei der Aufnahme der Personenstandsdaten darauf ab, ob die Identität der Personen nachgewiesen ist. Ein blosser Ausländerausweis wie auch künftig eine nicht "validierte" E-ID werden hierfür auch in Zukunft nicht ausreichend sein können. Der KAZ ist jedoch bewusst, dass es im Unterschied dazu für die ausländische Wohnbevölkerung in anderen Rechtsbereichen ausreichend sein kann, sich mit den in der Schweiz in ZEMIS erfassten Daten identifizieren zu können. Auch deshalb unterstützt die KAZ unter Vorbehalt des oben Ausgeführten die Vorlage und sieht darin eine lange erwartete Entwicklung zu zeitgemässen Digitalisierungsmöglichkeiten im Verkehr zwischen Privaten und Behörden.


Wir danken Ihnen bestens für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST

Namens des Vorstandes

Der Präsident:



Jon Peider Arquint

Der Geschäftsführer:



Walter Grossenbacher

Kopie an

- Mitglieder KAZ
- KKJPD
- SVZ, Präsident Roland Peterhans

OPERATION LIBERO



Die Schweiz verwirklichen.
Réalisons la Suisse.
Realizziamo la Svizzera.
Realisain la Svizra.
Make Switzerland happen.

Adressatin:

Frau Bundesrätin
Karin Keller-Sutter
Vorsteherin EJPD

20. Oktober 2022

Stellungnahme von Operation Libero Vernehmlassung zur E-ID

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Am 29. Juni 2022 haben Sie die Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise eröffnet. Wir danken Ihnen für die Möglichkeit, zu dieser Vorlage Stellung beziehen zu können und teilen Ihnen im Folgenden die Position und Überlegungen von Operation Libero zu diesem Gesetz mit.

Für Operation Libero ist es für die Diskussion um die Digitalisierung in der Schweiz zentral, dass der Gedanke eines digitalen Ökosystems ins Zentrum gestellt wird und die Verwaltung sowie die Politik sich fokussiert und sich nicht in Einzelheiten verliert. Um die Voraussetzungen für ein digitales Ökosystem zu schaffen, ist nicht nur eine ausgereifte Digitalisierungsstrategie notwendig (wobei aktuell eine solche Strategie aus unserer Sicht teilweise fehlt), sondern auch der frühzeitige Einbezug technischer Expertise und zivilgesellschaftlicher Perspektiven, damit Rahmenbedingungen geschaffen werden können, die ein umfassendes und ansprechendes Angebot an digitalen Dienstleistungen ermöglichen.

Ausgehend von diesen Überlegungen begrüsst Operation Libero die Stossrichtung des vorliegenden Gesetzesentwurfs. Die Schaffung einer elektronischen Identität und der zugehörigen Infrastruktur, welche auch für weitere elektronische Nachweise genutzt werden kann, die Prinzipien Privacy-by-Design sowie Privacy-by-Default beherzigt und bei der Umsetzung einen zeitgemässen technischen Ansatz verfolgt, stellt eine wichtige Voraussetzung für ein Ökosystem dar, wie wir es eingangs erwähnt haben. Wir begrüssen, dass das Gesetz versucht unterschiedlichen Anspruchsgruppen gerecht zu werden und es daher vorsieht, dass Nutzern einer E-ID oder

elektronischer Nachweise von Anfang an Hilfsmittel zur Verfügung gestellt werden. Weiter begrüssen wir die Offenheit und die Mitwirkungsmöglichkeiten, die durch den veröffentlichten Quellcode entstehen. Auch die Möglichkeit für interessierte Teilnehmer, sich bereits während der Ausarbeitung des vorliegenden Gesetzesentwurfs einzubringen, begrüssen wir und hoffen, dass in Zukunft bei der Ausarbeitung von Gesetzen öfter so vorgegangen wird.

Allerdings sind der vorliegende Gesetzesentwurf und die zugehörigen Konzepte aus unserer Sicht in verschiedenen Punkten noch nicht zu Ende gedacht und fokussieren zu stark auf Einzelthemen. Auf diese Punkte möchten wir im Folgenden ausführlicher eingehen.

Hilfestellungen und technischen Hilfsmittel

Zunächst sind wir der Meinung, dass den Nutzer*innen einer E-ID oder elektronischer Nachweise von Beginn an ein breiteres Angebot an Hilfestellungen und technischen Hilfsmitteln angeboten werden sollte, auch im Hinblick auf die von ihnen erwartete Sorgfaltspflicht (siehe Artikel 7). Während im vorliegenden Gesetzentwurf bereits erste Hilfestellungen und Hilfsmittel vorgesehen sind, finden wir es für eine breite Akzeptanz einer E-ID sowie elektronischer Nachweise wichtig, die vielfältigen Bedürfnisse der Nutzer*innen von Anfang an und fortwährend zu identifizieren und auf diese einzugehen. Nutzer*innen sollten z.B. auf technische Hilfsmittel zurückgreifen können, über die physische und elektronische Ausweise zusammengeführt werden können oder die es erlauben, eine E-ID oder elektronische Nachweise ohne kommerzielle Betriebssysteme nutzen zu können. Zudem verfügt in anderen europäischen Ländern der Inhaber einer E-ID automatisch auch über eine E-Signatur. Die Nutzung des im Gesetz erwähnten Systems für Sicherungskopien (siehe Artikel 26) sollte aus unserer Sicht zumindest in einer Basisvariante kostenlos sein.

Unvollständige Prozesse

Weiter weisen auch ein paar der im Gesetzesentwurf skizzierten Prozesse Verbesserungspotential auf. So sollte eine unverzügliche Informationspflicht des fedpols gegenüber dem Inhaber einer widerrufenen E-ID bestehen (siehe Artikel 5). Dies um die Wahrscheinlichkeit zu mindern, dass sich Nutzer*innen bei einem wichtigen Vorgang unerwartet ohne ein gültiges elektronisches Identifikationsmittel wiederfinden. Zu Artikel 15 möchten wir anmerken, dass es Fälle geben kann, in denen der Inhaber eines elektronischen Nachweises diesen nicht mehr selbständig nutzen kann, etwa aufgrund einer Erkrankung. Für solche Fälle sollte ein entsprechender Delegationsprozess an eine Vertretung definiert werden können.

Umgang mit sensiblen Daten

Ein wichtiger Punkt ist auch der verantwortungsvolle Umgang mit sensiblen Daten, die als Teil einer E-ID oder eines elektronischen Nachweises an Verifikatoren übermittelt werden. Wir sind der Meinung, dass Verifikatoren in Artikel 16 explizit in die Pflicht genommen werden sollten, im Rahmen eines Prozesses oder für eine Dienstleistung nur die zwingend notwendigen Daten zu verlangen und die Datenverarbeitung nur auf das für den Prozess oder die Dienstleistung unbedingt Erforderliche zu beschränken. Wenn für einen Prozess oder eine Dienstleistung das Vorweisen einer E-ID oder eines elektronischen Nachweises nicht erforderlich ist, sollte es auch nicht verlangt werden. Abweichungen von dieser Vorgabe sollten nur in Fällen möglich sein, in denen eine informierte und explizite Zustimmung der Inhaberin einer E-ID oder eines Nachweises vorliegt. Zudem sollte für die Inhaber*innen einer E-ID oder eines elektronischen Nachweises die Möglichkeit bestehen, deren weitere Verarbeitung zu unterbinden. Schliesslich sollte sichergestellt werden, dass Behörden und Menschen mit physischer ID oder physischen Nachweisen gleich behandelt werden wie Menschen mit elektronischer ID oder denselben Nachweisen in elektronischer Form. Die in Artikel 20 skizzierte Applikation zur Überprüfung elektronischer Nachweise sollte diesen Grundsätzen und Überlegungen entsprechen.

Technische Umsetzung und Infrastruktur

Fast der wichtigste Bereich mit Verbesserungspotential ist aber die im Gesetz vorgesehene technische Umsetzung und Infrastruktur. Während wir es begrüssen, dass der Quellcode der Vertrauensinfrastruktur öffentlich zugänglich gemacht wird (siehe Artikel 23), sollte aus unserer Sicht auch der Code der in Artikel 11 erwähnten Applikation zur Ausstellung der E-ID öffentlich zugänglich gemacht werden, schliesslich handelt es sich bei diesem System um einen wichtigen Teil der Gesamtinfrastruktur. Zudem würden wir es begrüssen, wenn zusätzlich zur Offenlegung des Quellcodes ein Auftrag zur Definition von Prozessen bestünde, die für einen regelmässigen systematischen Audit des Quellcodes sorgen und zudem sicherstellen, dass sich interessierte Dritte in die Verbesserung und Weiterentwicklung des Systems einbringen können. Vor dem Hintergrund dieser von Artikel 23 geschaffenen Partizipationsmöglichkeiten sowie aufgrund der sich stetig verändernden Technik sollte Artikel 25 so überarbeitet werden, dass der Bundesrat grundsätzlich die Möglichkeit hat auch Anpassungen an bestehenden Elementen der Infrastruktur vorzunehmen oder bestehende Infrastrukturelemente sogar abzulösen, sollte dies notwendig sein. Schliesslich sollte Artikel 21 so abgeändert werden, dass das System für Sicherungskopien diese vor jeglichem Zugriff durch Dritte schützt.

Änderungen an weiteren Gesetzen

Schliesslich möchten wir im Hinblick auf die geplanten Änderungen an weiteren Gesetzen (Artikel 29, resp. Anhang) nochmals anmerken, dass wir eine Verknüpfung und gemeinsame Ausstellung einer

OPERATION LIBERO



Die Schweiz verwirklichen.
Réalisons la Suisse.
Realizziamo la Svizzera.
Realisain la Svizra.
Make Switzerland happen.

E-ID mit einer zugehörigen digitalen Signatur begrüßen, schliesslich ist diese Möglichkeit in anderen europäischen Ländern bereits Realität. Im Hinblick auf die geplanten Anpassungen am Bundesgesetz zum Patientendossier scheint uns der Begriff eines Identifikationsmittels bzw. die Unterscheidung zwischen der elektronischen Identität und einem Identifikationsmittel künstlich und verwirrend. Existierende Lösungen in anderen Staaten zeigen, dass ein Patientendossier erfolgreich mit einer elektronischen Identität zur Identifikation eingesetzt werden kann, weswegen wir diese Lösung in Betracht ziehen würden.

Wir danken Ihnen für die Berücksichtigung unserer Bemerkungen bei der weiteren Ausarbeitung des vorliegenden Bundesgesetzes.

Herzlichen Dank für Ihr Engagement für unsere liberale Verfassung und eine Schweiz mit Zukunft.

Im Namen von Operation Libero

Sanija Ameti, Co-Präsidentin

Stefan Manser-Egli, Co-Präsident

Per E-Mail an:
rechtsinformatik@bj.admin.ch
Zu Händen:
Frau Bundesrätin Keller-Sutter
Eidgenössisches Justiz- und
Polizeidepartement EJPD

Zürich, 12. Oktober 2022

Stellungnahme zum Vorentwurf des E-ID-Gesetzes

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Vielen Dank für die Möglichkeit, im Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung zu nehmen.

Als langjähriger Vertrauenspartner des Bundes bei der Herstellung für Identitätsdokumente wie Führerausweis und Pass beschäftigt sich Orell Füssli bereits seit einigen Jahren intensiv mit den Themen digitale Identitäten und digitale Nachweise. Umso mehr, als dass nach einer Mehrheitsübernahme auch Procivis als Technologiedienstleister für digitale Identitätslösungen, u.a. im Kanton Schaffhausen und der Stadt Zug, zur Unternehmensgruppe Orell Füssli gehört. Zusätzlich haben wir im Januar 2022 eine strategische Partnerschaft für digitale Nachweise mit der Swisscom kommuniziert.

Wir sehen, dass eine elektronische Identität die Voraussetzung ist, damit sich die Digitalisierung von Wirtschaft, Gesellschaft und Staat in der Schweiz erfolgreich und nachhaltig entwickeln kann.

Wir begrüssen den Plan einer bundesbetriebenen Vertrauensinfrastruktur, die neben der nationalen E-ID auch offen für andere digitale Nachweise und Akteure aus dem öffentlichen und privaten Sektor ist.

Wichtige Faktoren für eine grosse Verbreitung der staatlichen elektronischen Identität und des entstehenden Ökosystems erscheinen uns dabei die Nutzerfreundlichkeit, die Datensicherheit (und deren Kommunikation), die staatliche Förderung bestimmter Anwendungsfälle und insbesondere die Geschwindigkeit der Umsetzung bzw. der Bereitstellung der Vertrauensinfrastruktur.

1. Allgemeine Bemerkungen

Ein grosser Hinderungsgrund für vollständig digitalisierte Prozesse ist heute das Fehlen rechtsgültiger digitaler Nachweise als Ergänzung zu hochwertigen physischen Dokumenten wie Führerausweis, Pass oder Identitätskarte. Dadurch sind manuelle Prüfungen und unsichere bzw. fälschungsanfällige «Workaround»-Prozesse (z.B. Scans/ Fotos von Nachweisen) notwendig. Diese reduzieren die

Effizienz von Behörden und Unternehmen sowie die Nutzerfreundlichkeit für Endkunden und Bürger.

Um digitale, nutzerfreundliche und datensparsame Lösungen zu implementieren, scheint das Self Sovereign Identity-Konzept mit seinen selbstverwalteten Identitäten und Attributen sehr geeignet. Mit einem offenen Ökosystem und unterschiedlichen Akteuren können viele Anwendungsfälle entstehen bzw. weiterentwickelt werden und zu einer grossen Verbreitung und Nutzung der Vertrauensinfrastruktur führen.

Für eine erfolgreiche Umsetzung der E-ID zum Vorteil der ganzen Schweiz erlauben wir uns, einige Vorschläge und Anregungen mit Ihnen zu teilen.

2. Generelle Vorschläge und Anregungen

a) Sicherstellung der Planungssicherheit privater Akteure trotz technologieneutralen Rechtsrahmens

Angesichts der schnellen technologischen Weiterentwicklung und Innovationen begrüssen wir einen technologieneutralen Rechtsrahmen. Nachdem die nationale E-ID und die damit verbundene Vertrauensinfrastruktur allerdings ein grösseres Ökosystem mit weiteren Akteuren und Nachweisen ermöglichen soll, müssen diese Akteure frühzeitig genügend Informationen zur Vertrauensinfrastruktur und Sicherheit haben, um Geschäftsmodelle und Angebote ausarbeiten zu können. Andernfalls stehen diese zur Einführung der E-ID nicht bereit, was sich in einer nachhaltig geringeren Verbreitung auswirken könnte. Wir regen daher an, die Ausführungen zur Vertrauensinfrastruktur im 5. Abschnitt zu konkretisieren.

b) Sicherstellung der Agilität hinsichtlich internationaler Technologie- und Standard-Entwicklungen

Um internationalen Entwicklungen im Bereich der digitalen Identitäten und Nachweise Rechnung tragen zu können, schlagen wir zusätzlich vor, dass der Bundesrat eine Kompetenz zur Anpassung der Ausführungsverordnungen an internationale Standards erhält, soweit diese Anpassungen dem Zweck des Gesetzes entsprechen und betroffene Anspruchsgruppen vor einer Anpassung angehört werden.

c) Sicherstellung der schnellen Verbreitung der E-ID und des raschen Ökosystem-Aufbaus

Für eine erfolgreiche und schnelle Verbreitung der E-ID und anderer Nachweise halten wir signifikante Marketingmassnahmen für notwendig, um die Bevölkerung über Sinn und Zweck, Technologie und Einsatzmöglichkeiten zu informieren, um eine zögerliche Verbreitung der Lösung zu vermeiden und einer potentiellen Abwehrhaltung im Kontext des abgelehnten E-ID-Gesetzesentwurfs von 2021 entgegenzuwirken. Diese Massnahmen sollten gesetzlich verankert werden.

d) Einführung eines standardisierten Identifikationsverfahrens für Personen ohne E-ID

Artikel 3 des Vorentwurfs nennt als Voraussetzung für eine nationale E-ID einen von den Schweizer Behörden ausgestellten Ausweis. Aufgrund der starken Internationalisierung, grenzüberschreitenden Geschäftsprozessen und globalen digitalen Geschäftsmodellen empfehlen wir, ein zusätzliches, gleichwertiges digitales Identifikationssystem zur nationalen E-ID zu definieren. Dies würde zu einer stärkeren Ausdehnung des Ökosystems und einer grösseren Inklusion weiterer Personen und Akteure führen. Eine zentrale gesetzliche Standardisierung von digitalen Identifikationsverfahren würde Rechts- und Planungssicherheit schaffen.

3. Vorschläge und Anregungen zu einzelnen Artikeln des Vorentwurfs

a) Zu Art. 16 Vorweisen von elektronischen Nachweisen

Sowohl bestehende datenschutzrechtliche Grundlagen wie das revDSG Art. 6 Abs. 3 als auch das Self Sovereign Identity-Konzept sehen eine Datenminimierung vor. Trotzdem halten wir es für sinnvoll, im Gesetz explizit zu erwähnen, dass verifizierende Akteure nur diejenigen Nachweise verlangen dürfen, die aus klar genannten Gründen notwendig sind.

b) Zu Art. 18 System zur Bestätigung von Identifikatoren

Um die Sicherheit im Ökosystem zu gewährleisten, halten wir eine obligatorische Prüfung und Bestätigung für private AusstellerInnen und VerifikatorInnen durch den Bund für notwendig. Die zu erfüllenden Kriterien sollten möglichst zeitnah kommuniziert werden, damit die Akteure die Ausstellung eigener Nachweise sowie die Optionen zur Verifizierung evaluieren können.

c) Zu Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Die im erläuternden Bericht erwähnte Zulässigkeit privater Wallets sollte im Gesetzestext verankert werden. Aufgrund der sensiblen Daten, des Missbrauchspotentials sowie der Datenschutz-Bedenken in der Bevölkerung empfehlen wir eine Zertifizierungspflicht für elektronische Wallets.

f) Zu Art. 21 System für Sicherungskopien

Momentan werden Systeme für Sicherungskopien als optionales Angebot des Bundes erwähnt. Aufgrund pragmatischer Überlegungen, die stark für sogenannte Back-up-Systeme sprechen, schlagen wir vor, dass deren Angebot durch Private im Gesetzestext explizit erlaubt wird.

4. Schlussbemerkung

Orell Füssli begrüsst den Vorentwurf in seinen Grundzügen. Gleichzeitig weisen wir daraufhin, dass der Erfolg der E-ID in unseren Augen massgeblich von einem frühzeitigen Ökosystem-Aufbau rund um die Vertrauensinfrastruktur abhängt. Wir empfehlen mit Nachdruck, regulatorische und projektspezifische Arbeiten möglichst parallel durchzuführen, damit das positive Momentum in der Schweiz nicht verloren geht und bald eine Lösung bereitsteht. Die Berücksichtigung internationaler Vorhaben und Entwicklungen ist für die Interoperabilität wichtig, darf die nationale Entwicklung in unseren Augen aber nicht aufhalten.

Wir stehen jederzeit gerne für Rückfragen zur Verfügung und bedanken uns für die Berücksichtigung unserer Vorschläge.

Freundliche Grüsse

Daniel Link
CEO Orell Füssli AG

pharmaSuisse, Stationsstrasse 12, 3097 Liebefeld

Herr
Rolf Rauschenbach
Informationsbeauftragter E-ID
Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern
rechtsinformatik@bj.admin.ch

Bern-Liebefeld, 20. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID): Stellungnahme pharmaSuisse

Sehr geehrter Herr Rauschenbach

Besten Dank für die Gelegenheit zur Stellungnahme zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Fragen zu unserer Stellungnahme gerne zur Verfügung.

Freundliche Grüsse

pharmaSuisse
Schweizerischer Apothekerverband


Martine Ruggli
Präsidentin


Samuel Dietrich
Jurist



Association de
Banques Privées Suisses
Vereinigung
Schweizerischer Privatbanken
Association of Swiss Private Banks

Par e-mail

(rechtsinformatik@bj.admin.ch)

Madame Karin Keller-Sutter
Conseillère fédérale
Département fédéral de justice et police
Bundeshaus West
3003 Berne

Genève, le 20 octobre 2022

Loi fédérale sur l'identité électronique et d'autres moyens de preuve électroniques (loi sur l'e-ID)

Madame la Conseillère fédérale,

L'Association de Banques Privées Suisses (ABPS) a étudié avec attention l'avant-projet de loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID), soumis en consultation le 29 juin 2022. Nous souhaitons par la présente vous transmettre quelques remarques sur les points les plus importants pour les banques privées, tout en soutenant par ailleurs la prise de position de l'Association Suisse des Banquiers.

L'ABPS soutient globalement le projet mis en consultation. Toutefois, nous nous permettons de mettre en avant certaines remarques quant à l'importance de la protection de la sphère privée et de la sécurité des données, d'une utilisation facile pour chacun, de la compatibilité internationale et du lien avec le secteur privé. Il convient de définir un système simple et efficace et de le mettre en œuvre de manière rapide et pragmatique. En outre, il faut assurer la cohérence du projet avec d'autres lois prévoyant une identification, notamment en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

A) Commentaires généraux

La loi sur l'e-ID est une loi-cadre qui doit contenir les grands principes réglementaires en lien avec une identité électronique. Ceux-ci ont donc une portée générale et doivent rester neutre du point de vue technologique. A cet égard, les dispositions d'exécution qui seront contenues dans une ordonnance seront d'une importance déterminante.

Il est essentiel que la nouvelle identité électronique devienne rapidement le standard en la matière auprès des citoyens. Cela signifie que son usage doit être facile d'accès, aisément compréhensible, fiable et très rapidement bénéficier d'une portée très large, ce qui pourra être atteint sur la base des éléments suivants :

- La nouvelle e-ID doit rapidement gagner la confiance des utilisateurs, en ce sens qu'ils auront envie de privilégier ce moyen d'identification, même s'il reste facultatif. A côté des dispositions légales et réglementaires, les mesures de communication et d'information à la population revêtiront une importance capitale pour le succès de l'e-ID.
- L'aspect sécuritaire, en particulier dans le domaine numérique, doit rester une priorité continue de l'e-ID, c'est-à-dire pas seulement lors de sa création, mais aussi tout au long de son utilisation. Il faut qu'un contrôle régulier soit maintenu sur les standards appliqués afin de maintenir une protection élevée de la sphère privée ainsi qu'une résistance du plus haut niveau face à des attaques cyber.
- L'utilisation de la nouvelle identité électronique doit être possible de manière simple, compréhensible et transparente. Elle doit donc pouvoir s'appliquer à tous les rapports économiques et administratifs existants, à savoir avec les autorités, avec l'économie (industrie et services) et entre particuliers. Il s'agit donc de développer un écosystème qui englobe le plus grand nombre possible d'activités, de manière à ce qu'il devienne rapidement une référence en la matière. Cela présuppose une coordination étroite entre les différents acteurs, en particulier entre le secteur public et le secteur privé.

La nouvelle loi doit favoriser et autoriser des solutions provenant du secteur privé. Dans ce contexte, nous saluons et approuvons le fait que l'infrastructure étatique pourra être mise à disposition des entreprises. Les nouvelles opportunités d'affaires devraient être intégrées et reconnues aussi rapidement que possible par l'autorité compétente, ce qui aurait des avantages dans l'identification de parties tierces si celles-ci sont en Suisse. En ce qui concerne le secteur financier par exemple, on peut imaginer que des synergies importantes pourraient être réalisées dans le domaine de l'identification des clients (moyennant une adaptation correspondante de la loi sur le blanchiment d'argent). Cela suppose par conséquent une certaine flexibilité et la volonté de développer l'e-ID en fonction des besoins de l'économie et des consommateurs. A cet égard, nous proposons un réexamen régulier de la loi une fois que cette dernière sera entrée en vigueur (p.ex. à un rythme triennal).

La nouvelle identité électronique doit être compatible avec d'autres réglementations telles que celles de l'Union européenne, du Royaume-Uni, des Etats-Unis et d'autres pays importants pour la Suisse. Il s'agit de faciliter l'interopérabilité autant que faire se peut.

Le lien entre le monde numérique et le monde physique est un élément fondamental de la confiance pour les utilisateurs. Dès lors, les instances qui émettent actuellement des documents d'identités et qui sont reconnues comme telles doivent pouvoir le rester lorsqu'elles émettront des e-ID si les conditions légales, techniques et de sécurité sont remplies. Il faut donc assurer une cohérence entre les documents d'identité émis sous forme physique et électronique. Il importe également de songer à l'évolution future et de réfléchir au scénario d'un retour temporaire aux documents physiques, à supposer que l'identification électronique ne soit plus disponible pour une période indéterminée.

B) Commentaires spécifiques

- **Article 1 al. 2 let. a LeID** : l'e-ID devrait aussi servir à garantir une identification sûre entre personnes privées et entreprises, puisqu'elle a aussi vocation à être utilisée par ces dernières.
- **Article 6 LeID** : La durée de validité de l'e-ID ne devrait pas dépasser la durée de validité du document d'identité ou de légitimation qui a été utilisé lors de son émission.
- **Article 11 al. 5 LeID** : La durée de conservation des données jusqu'à 5 ans après la date de validité ou la révocation de l'e-ID paraît trop longue. Un délai de conservation d'un an après ces échéances semble plus approprié.
- **Article 14 LeID** : Il faudrait rajouter la notion de sécurité dans cet article : « ... il le conserve par les moyens techniques *sécurisés* de son choix et ... »
- **Article 15 LeID** : Il faudrait quand même pouvoir transmettre certains moyens de preuve électronique à un autre titulaire si ce dernier est le représentant légal du titulaire (p. ex. parents ou représentants légaux de personnes sous curatelle), de la même façon qu'il est possible de présenter la pièce d'identité de ses enfants.
- **Article 16 al. 3 LeID** : L'expression « dans toute la mesure du possible » amoindrit la portée de cette disposition importante et doit être supprimée. L'ignorance de l'exploitant des systèmes doit être assurée par des mesures techniques et organisationnelles appropriées.
- **Article 17 al. 2 let. b et c LeID** : le terme « clefs cryptographiques » devrait être remplacé par « informations », afin d'assurer la neutralité technologique. Il se peut en effet qu'à l'avenir, des technologies émergent qui soient meilleures que les clefs cryptographiques.
- **Article 22 LeID** : le moment à partir duquel une utilisation devient abusive n'est pas clairement précisé. En outre, le rapport explicatif laisse entendre qu'il faut compter avec des cas d'abus, ce qui est insatisfaisant. Il s'agit au contraire de lutter de manière aussi efficace que possible contre ce genre de cas.
- **Article 23 LeID** : La question se pose s'il est vraiment nécessaire d'indiquer dans la loi que « la Confédération publie le code source des éléments de l'infrastructure de confiance qu'elle met à disposition ». On préférera les termes « peut publier », aussi pour des raisons de neutralité technologique.

* * *

En vous remerciant par avance de l'attention que vous porterez à la présente, nous vous prions d'agréer, Madame la Conseillère fédérale, l'expression de notre très haute considération.

ASSOCIATION DE
BANQUES PRIVEES SUISSES



Jan Langlo
Directeur



Jan Bumann
Directeur adjoint

Für Sie zuständig:
Cécile Kessler
cecile.kessler@raiffeisen.ch

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

18.10.2022

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit der Eröffnung der Vernehmlassung laden Sie interessierte Kreise ein, zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise, Stellung zu nehmen. Diese Gelegenheit nimmt Raiffeisen Schweiz gerne wahr.

Allgemeine Bemerkungen zur Vorlage

Raiffeisen begrüsst die Einführung eines elektronischen Identitätsnachweises (E-ID). Wir bedauern jedoch, dass die bewährte Aufgabenverteilung zwischen Staat und privaten Akteuren zugunsten einer staatlichen E-ID aufgegeben wurde. Zudem fehlt aus unserer Sicht eine fundierte Risikoanalyse, in welcher der Bund aufzeigt, wie er Bürgerinnen und Bürger schützen will, wenn ihre digitalen Identitäten gelöscht, gestohlen und missbraucht werden. Insgesamt sind wir nach wie vor davon überzeugt, dass eine E-ID viele Vorteile aufweist, namentlich bei der Vereinfachung der digitalen Prozesse, der Sicherheit und der Einhaltung internationaler Standards. Raiffeisen schliesst sich den Stellungnahmen von digitalswitzerland und Swiss Fintech Innovations an und betont ergänzend dazu explizit die Notwendigkeit folgender Ergänzungen:

Präzisierung des Zwecks

Das Gesetz soll die Anbindung weiterer elektronischer Nachweise in die umfassende Vertrauensinfrastruktur aktiv anstreben und neue digitale Geschäftsmodelle ermöglichen, welche zum Vertrauen im digitalen Raum beitragen. Dies soll unter Art. 1 Abs. 2 explizit aufgeführt werden.

Bereitstellung des Mechanismus durch nicht-staatliche Akteure

Akteure, welche in der analogen Welt das Vertrauen geniessen (z.B. aufgrund der Kontrolle durch eine Aufsichtsbehörde), sollen befähigt werden, separate nicht-staatliche (private) Mechanismen bereitzustellen. Dies ebnet den Weg für den Aufbau von multisektoralen Ökosystemen und ist von zentraler Bedeutung für Nutzer und Verifikatoren, welche oft keine direkte Beziehung zu den Ausstellern haben. Die Rollen und Verantwortlichkeiten dieser Akteure sollen so schnell wie möglich geregelt werden.

Für die Gelegenheit zur Stellungnahme bedanken wir uns. Wir bitten um Berücksichtigung der Anliegen von Raiffeisen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüße

i.V.

Christian Bopp
Head Regulatory Affairs

Cécile Kessler
Beraterin Politik

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Karin Keller-Sutter
Bundeshaus West
3033 Bern

Zürich, 20. Oktober 2022

Stellungnahme von Samsung Electronics zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, im Rahmen der laufenden Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) Stellung nehmen zu können.

Weltweit stellt Samsung Electronics fest, dass das Vertrauen der Bevölkerung in mobile Geräte dank Verbesserungen der technologischen Leistungsfähigkeit zugenommen hat. Bürgerinnen und Bürger verlassen sich auf ihre Handheld-Geräte. Die Verwendung der Geräte ist weitreichend und geht über das Kommunizieren hinweg. Sie werden genutzt, um Bankgeschäfte abzuwickeln, Lebensmittel zu bestellen, den Impfstatus nachzuweisen, in Hotels einzuchecken, Sport zu treiben und um sich in einer Stadt zurechtzufinden. Samsung Electronics hat diesen globalen Trend erkannt und freut sich über die Bemühungen der öffentlichen Hand, private und öffentliche Dienstleistungen bereitzustellen.

Eine vertrauensvolle und sichere Identität für alle Akteure im digitalen Raum erachten wir als elementare Komponente für eine erfolgreiche digitale Transformation. Ein hohes Vertrauen der Bürgerinnen und Bürger in die elektronische Identität (eID) sowie ihre Benutzerfreundlichkeit erachten wir als Grundvoraussetzung, damit die eID zu einem Erfolg werden kann. Für Bürgerinnen und Bürger muss ein offensichtlicher Mehrwert durch die Anwendung dieser Lösung entstehen. Der vorliegende Gesetzesentwurf bietet aus Sicht von Samsung Electronics die Rahmenbedingungen für eine Vertrauensinfrastruktur.

Neben einer Gesetzesvorlage, welche auf Akzeptanz bei Politik und Gesellschaft stösst, erachten wir die technische Umsetzung und damit einhergehend deren Verwendung als entscheidend für die

Etablierung dieser staatlichen eID. Eine Lösung auf einer hardwarebasierten Sicherheitsarchitektur (auf dem Smartphone) stellt aus heutiger Sicht die bestmögliche Lösung dafür dar.

Aus Erfahrung in Deutschland lernen

Im Rahmen der Projekte OPTIMOS und OPTIMOS 2 in Deutschland arbeiteten das Bundesministerium des Innern, für Bau und Heimat (BMI), das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Bundesdruckerei, die Deutsche Telekom Security, Governikus und Samsung Electronics gemeinsam an der Entwicklung einer Sicherheitsarchitektur für Mobiltelefone, die Ausweisdokumente für eID-Dienste beherbergen, und zwar unter dem Paradigma der offenen Plattformbildung. Samsung Electronics stellt darin den zertifizieren, hardware-basierten Tresor für die vom Staat herausgegebene digitale Identität zur Verfügung.

Samsung Electronics arbeitete eng mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen, um sich aktiv an der Entwicklung des eID-Sicherheitsrahmens zu beteiligen. Dabei stützte man sich auf eine chipset-basierte Sicherheitszone mit Schlüsselaspekten wie dem embedded Secure Element (eSE), der Einbindung von Cryptographic Service Provider (CSP) und der embedded universal integrated circuit card (eSIM). Die Schweiz sollte die Chance nutzen und von den Erfahrungen und dem Wissen aus Deutschland und den OPTIMOS-Förderprojekten profitieren. Samsung Electronics ist gerne bereit dazu, seine diesbezügliche Expertise einzubringen, im Projektprozess zur eID sowie technischen Umsetzung zu partizipieren und sich mit den entsprechenden Fachstellen auszutauschen.

Gesetzesentwurf als ausreichende Grundlage

Der vorliegende Gesetzesentwurf ist technologie-neutral formuliert, was wir als sinnvoll erachten. Es ist jedoch noch unklar, wie die Zuständigkeit zur Auslegung des „aktuellen Stands der Technik“ aussieht. Eine entsprechende Ausführung wäre wünschenswert.

Eine Hardware-Lösung, die sensible persönliche Daten speichert und die Kontrolle über die Daten bei den Bürgern behält, bietet der Schweiz das beste Sicherheitsniveau für einen harmonisierten eID-Rahmen. Damit erfüllt sie den Anspruch auf Datenschutz durch Technik, Datensicherheit, Datensparsamkeit und dezentraler Datenspeicherung, welche mit dem Gesetzesentwurf gefordert werden. Das notwendige Vertrauen in die eID kann nur erreicht werden, indem eine hohe Vertrauensstufe garantiert wird. Dies wird unter anderem mit einem zertifizierten embedded Security Element (eSE) auf dem Smartphone sichergestellt. Die die eSE / eUICC Lösung kann - im Gegensatz zur Software eID Lösung – das Assurance Level „Hoch“ erreichen und somit auch alle Rechtsgeschäfte erledigen, welche das Assurance Level „High“ nach eIDAS benötigen (eIDAS Levels of Assurance).

Ein weiterer Aspekt, welcher die Funktionalität der eID und damit deren Akzeptanz erhöht, ist deren internationale Anwendbarkeit und Anerkennung. Dies soll gemäss Gesetzesvorlage mit international Abkommen sichergestellt werden. Auch hier gilt es, die entsprechende technische Interoperabilität zu gewährleisten, indem man in der Schweiz eine international und vor allem europäisch etablierte (und zertifizierte) technische Lösung entwickelt.

Je höher die Anwendungsmöglichkeiten dereinst sein werden, desto grösser ist die Chance, dass sich die eID bei der Bevölkerung durchsetzt. Ein rein staatlich genutzter, digitaler Ausweis erachten wir als wenig gewinnbringend. Die Lösung muss Basis für ein möglichst umfassendes Ökosystem sein

(Grundlage für Ambitionsniveau 3). Entsprechend sollte die Lösung offen für Drittanbieter sein. Dazu muss die Funktionalität auf bekannten und akzeptierten Standards basieren.

Samsung Electronics als führender Anbieter von Handheld-Geräten ist überzeugt, dass eine vertrauenswürdige und benutzerfreundliche eID nicht nur einen Mehrwert für die Bürgerinnen und Bürger, die staatlichen Institutionen sowie die Wirtschaft bietet, sondern vielmehr eine essenzielle Grundlage für die weiterführende Digitalisierung der Schweiz ist. Eine technologische Lösung, welche auf einer Sicherheitsarchitektur für Mobiltelefone basiert, bietet heute den höchsten Grad an Sicherheit. Aus Sicht von Samsung Electronics hat der vorliegenden Gesetzesentwurf die richtige Stossrichtung. Es gilt dies im weiteren Gesetzgebungsprozess, insbesondere auch bei der dazugehörigen Verordnung, sicherzustellen. Samsung Electronics ist gerne bereit, ihre technische Expertise sowie die Erfahrung bei der Umsetzung von elektronischen Identitäten in anderen Ländern (insbesondere in Deutschland) jederzeit gewinnbringend in den Projektprozess einzubringen.

Gerne stehen wir für Fragen und Anliegen sowie den Austausch zu Umsetzungsfrage zur Verfügung und danken für die Aufnahme unserer Stellungnahme in Ihre Überlegungen.



Martin Züst
Head of Corporate Communication
Samsung Electronics Switzerland GmbH



Philipp Scharpf
Corporate & Public Affairs Manager
Samsung Electronics Switzerland GmbH



Eidg. Justiz- und
Polizeidepartement
Frau Bundesrätin Karin Keller-Sutter

Per Mail an:
rechtsinformatik@bj.admin.ch

Zürich, 19. Oktober 2022

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)
Stellungnahme des Schweizerischen Verbandes für Zivilstandswesen (SVZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Sie haben am 29.06.2022 eingeladen zur Vernehmlassung zum im Titel genannten Geschäft. Unser Verband wurde nicht direkt zur Einreichung einer Stellungnahme eingeladen. Als Fachverband im Zivilstandswesen sind wir von der Vorlage direkt betroffen, weshalb wir nachstehend Stellung nehmen.

Die Schaffung einer E-ID wird seitens unseres Verbandes sehr begrüsst.

Im Zivilstandswesen ist es – z.B. im Ehevorbereitungsverfahren, bei der Trauung, bei der Anerkennung einer Vaterschaft, bei der Abgabe einer Namenserklärung – zwingend, dass sich die Personen über ihre Identität ausweisen. Heute passiert das mit Pass oder Identitätskarte. Wenn die Identität in Zukunft elektronisch nachgewiesen werden kann, ist das grundsätzlich richtig. Es wird aber dort problematisch, wo die E-ID nicht aufgrund eines Passes oder einer Identitätskarte sondern aufgrund eines Ausländerausweises ausgestellt wird. Der Ausländerausweis ist – wie z.B. der Führerausweis – ein Legitimationspapier und mit einem solchen kann die Identität nicht nachgewiesen werden. Eine I-ID kann also mit oder ohne Identitätsnachweis ausgestellt werden.

Art. 9 BGEID verpflichtet Behörden und andere Stellen, die öffentliche Aufgaben erfüllen, die E-ID zu akzeptieren, wenn sie eine elektronische Identifizierung vornehmen. Für die Zivilstandsämter wird es schwierig bis unmöglich, aufgrund der E-ID die Identität von Personen eindeutig festzustellen. Es muss daher klar ersichtlich sein, aufgrund welcher Basis die E-ID ausgestellt worden ist.

Art. 2 Abs. 2 Bst. d hält fest, dass die E-ID das Geschlecht zu den Personenidentifizierungsdaten gehört. Seit 01.01.2022 kann der Geschlechtseintrag durch eine Erklärung beim Zivilstandsamt unbürokratisch geändert werden. Vorstösse zur Einführung eines dritten Geschlechts sind eingereicht und in Diskussion. Es fragt sich daher, ob das Geschlecht in der E-ID wirklich vorhanden sein muss. Diese Frage mag verfrüht sein, denn so lang im Infostar, im Zemis, im Pass etc. das Geschlecht erwähnt ist, muss es auch in der E-ID erwähnt sein. Aber man sollte dies im Auge behalten.

Der Einsatz der E-ID im Zivilstandswesen ist im BGEID nicht geregelt; und auch nicht Gegenstand dieses Gesetzes. Wir weisen aber schon jetzt darauf hin, wie wichtig es ist, dass bei der Einführung der E-ID auch sehr genau nach Möglichkeiten gesucht wird, wie die E-ID im Zivilstandswesen zum Einsatz kommen und dadurch der Kundschaft gewisse Behördengänge erspart und bei allen Beteiligten (auch auf den Zivilstandsämtern) der Aufwand reduziert werden kann. Zu regeln wäre es dann in der Zivilstandsverordnung.

Wir bitten um Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Verband für Zivilstandswesen



Roland Peterhans
Präsident

Bundesamt für Justiz
3003 Bern

Per E-Mail
rechtsinformatik@bj.admin.ch

Bern, 20. Oktober 2022

Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Der Bundesrat hat mit dem Richtungsentscheid zur E-ID am 17.12.2021 den Aufbau eines Ökosystems für die E-ID beauftragt. Die asa und das ASTRA können mit dem Teilprojekt T1 (digitaler Führerausweis, mDL) ein Pilotprojekt im Rahmen des Vorhabens E-ID realisieren. In enger Zusammenarbeit mit der asa strebt die vks den digitalen Schiffsführer- und Schiffsausweis an.

Die Vereinigung der Schifffahrtsämter (vks) bedankt sich für die Möglichkeit, im vorliegenden Vernehmlassungsverfahren mitzuwirken.

Allgemeine Bemerkungen:

- Wir begrüßen die Einführung des elektronischen Identitätsnachweises E-ID sehr. Die E-ID schafft die Grundlage um in den Strassenverkehrs- und Schifffahrtsämtern in Zukunft viele Prozesse mit unseren Kunden vereinfacht zu digitalisieren.
- Zudem wird die auch von der E-ID genutzten Basisinfrastruktur die zeitnahe Einführung digitaler Ausweise der Verkehrszulassung (Lernfahrausweis – 300'000/Jahr; Führerausweis - 6.5 Mio.; Ausweis 95 / Chauffeurzulassung; Fahrzeugausweis - 6 Mio.; Schiffsführerausweis – 300'000 und Schiffsausweis – 100'000) ermöglichen.
- In der gewählten Technologie „Self-Sovereign Identity“ (SSI) besteht noch wenig praktische Erfahrung. Dadurch ist diese entsprechend risikobehaftet in Bezug auf die praktische Umsetzung und den Betrieb. Unseren Kunden ermöglicht diese jedoch einen zeitgemässen und selbstbestimmten Schutz der Privatsphäre bei der Nutzung der digitalen Ausweise, was wir sehr begrüßen.
- Wir begrüßen es, dass der Bund sich in der Verantwortung für die Basisinfrastruktur (Vertrauensinfrastruktur) sieht und hier die Führung übernommen hat.

Bemerkungen zu den einzelnen Gesetzesartikeln:

Art. 2 Form und Inhalt

- Mittelfristig wäre es zielführend, die Personenidentifizierungsdaten von ISA, ZEMIS und weiteren Umsystemen wie denen des Informationssystems (IVZ) des ASTRA zu harmonisieren.
- Das Ablaufdatum der E-ID darf keine Auswirkungen auf gültige digitale Ausweise (Credentials) haben, da z.B. der heutige Führerausweis unbefristet gültig ist. Auch andere Ausweise werden unterschiedliche Ablaufdaten haben. Eine Erneuerung der E-ID darf diesbezüglich keinen grossen Mehraufwand auf die vorhandenen Ausweise haben. Namentlich müssen die Kunden bei einer Erneuerung der E-ID einfach und rasch die fortbestehenden digitalen Ausweise wieder aktivieren können.

Art. 8 Anlaufstelle der Kantone

Der Bund (BIT) ist für die Basisinfrastruktur und somit auch für dessen Support zuständig. Kantonale Anlaufstellen können, wenn nötig, die Bundesstellen in dieser Aufgabe unterstützen.

Die unterschiedlichen Anbieter von digitalen Ausweisen (eLernfahrausweis, eFührerausweis, ePersonalausweis, eWohnsitzbestätigung, eStrafregisterauszug, usw.) sind hingegen für den jeweiligen Support zuständig. In der Einführungsphase ist eine direkte Absprache zwischen den unterschiedlichen Organisationen dringend notwendig.

Art. 15 Übertragbarkeit von elektronischen Nachweisen

Die Strassenverkehrsämter planen auch den Fahrzeugausweis (ca. 6 Mio.) als digitalen Ausweis abzugeben. Der Fahrzeugausweis verbleibt beim Halter eines Fahrzeuges. Der Halter hat jedoch die Möglichkeit, das Fahrzeug und damit den Fahrzeugausweis einer anderen Person für eine bestimmte Zeit «auszuleihen». Es muss deshalb die Möglichkeit bestehen, einen digitalen Ausweis zeitbefristet oder unbegrenzt «teilen» zu können, beispielsweise innerhalb der Familie. Die Schifffahrtsämter bezwecken ebenfalls eine digitale Lösung für den Schiffs- und Schiffsführerausweis.

Art. 26 Gebühren

Die Gebühren für den Eintrag im Basisregister müssen frühzeitig bekannt und angemessen sein. Im Kontext der Führerausweise wäre eine Gebühr in der Grössenordnung der Gestehungskosten heutiger physischer Ausweise wünschenswert. Ansonsten müssen die Kantone die Kosten durch höhere Gebühren für diese Produkte auf die Bürger abwälzen. Dies könnte zu Widerständen gegen die Digitalisierungsvorhaben führen.

Art. 27 Internationale Abkommen

Es muss unbedingt die Möglichkeit geschaffen werden, dass die unterschiedlichen digitalen Ausweise der Strassenverkehrsämter auch im EU-Raum genutzt werden können.

Art. 28 Ausführungsbestimmungen

Es muss die Möglichkeit geschaffen werden, dass gewisse digitale Ausweise (Beispiel eFahrzeugausweis, ca. 6 Mio.) mit anderen Personen «geteilt» werden können (Weitergabe eines Fahrzeugausweises für eine bestimmte oder unbestimmte Zeit bei der privaten oder kommerziellen Ausleihe). Siehe auch Bemerkung zu Art. 15. Wir schlagen daher vor, dass eine neue lit. e aufgenommen wird:

e. zu den Möglichkeiten einer temporären Verwendung von Nachweisen durch andere E-ID-Benützer (Teilen).

Allgemeine Bemerkungen:

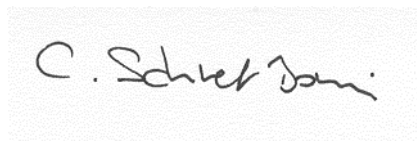
Die erwähnten Betriebskosten (jährlich CHF 15 – 20 Mio.), welche durch Gebühren bezahlt werden müssen, sind im Verhältnis zu den Projektkosten von ca. CHF 25 – 30 Mio. aus unserer Sicht viel zu hoch. Es darf nicht sein, dass der Bund die E-ID «gratis» zur Verfügung stellt und die Kantone, Gemeinden und Private bezahlen mit den Gebühren für ihre digitalen Ausweise die hohen Betriebskosten, welche dann in irgendeiner Form an die Kunden überwältzt werden müssen. Es besteht somit die Gefahr, dass digitale Ausweise von Kantonen und Dritten nicht über die Basisinfrastruktur und das zugehörige Bundeswallet des Bundes verteilt werden und sich alternative Kanäle etablieren.

Vielen Dank für die Kenntnisnahme und die weitere Prüfung.

Freundliche Grüsse



Peter Kiser
Präsident vks



Chantal Schweizer Bourqui
Geschäftsführer vks

Herr Rolf Rauschenbach
Informationsbeauftragter E-ID
Bundesamt für Justiz

rechtsinformatik@bj.admin.ch

Zürich, 18. Oktober 2022

**Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise
(E-ID-Gesetz, BGEID)**

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Gerne nimmt der Schweizerische Versicherungsverband SVV die Möglichkeit wahr, sich zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise zu äussern.

Der SVV unterstützt den Entwurf zum Bundesgesetz über den elektronischen Identitätsnachweis (BGEID) und begrüsst das Vorgehen des EJPD. Die Vorlage ist von hoher Bedeutung für den Schweizer Wirtschaftsstandort. Die Digitalisierung ist zudem von zentraler Bedeutung für die Gesellschaft – und die Schaffung einer E-ID ist somit ein logischer und wichtiger Schritt für die Schweiz. Gleichzeitig trägt die Vorlage den Bedenken gebührend Rechnung, die zur Ablehnung der ersten Vorlage zur Schaffung einer E-ID im März 2021 geführt haben. Die nun vorliegende Vorlage sollte so rasch wie möglich umgesetzt werden, damit die Schweiz im internationalen Wettbewerb über gleichwertige Instrumente verfügt (siehe eIDAS-Verordnung auf EU-Ebene).

Für die Versicherungsbranche vereinfacht eine E-ID den digitalen Vertrieb. Die Branche ist bereits stark digitalisiert, doch eine digitale Identität würde neue Möglichkeiten und Vereinfachungen für die Kundinnen und Kunden eröffnen und damit Innovationen für die Versicherer vereinfachen. Der SVV ist der Überzeugung, dass sich die elektronische Identität in der Schweiz jedoch nur dann in der Breite durchsetzen kann, wenn sie in ein inklusives Ökosystem von elektronischen Nachweisen eingebettet wird. Deshalb schlagen wir vor, diesen Aspekt schon in den Zweckartikel des Gesetzes aufzunehmen. Dazu erachten wir aus Sicherheitsgründen eine regelmässige

technologische Prüfung der Infrastruktur wie ein Vehikel für Experteninput zur technologischen Gesetzesumsetzung als sinnvoll.

Wir danken Ihnen für die Kenntnisnahme und die Berücksichtigung unserer Anliegen im Rahmen der weiteren Arbeiten. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Schweizerischer Versicherungsverband SVV



Urs Arbter

Direktor



Jan Mühlethaler

Leiter Ressort Public Affairs und Kommunikation,
Mitglied der Geschäftsleitung

Gregor Zemp

EJPD
Per E-Mail:
rechtsinformatik@bj.admin.ch

Luzern, 20. Oktober 2022

**Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID);
Vernehmlassungsverfahren vom 29. Juni 2022**

Sehr geehrte Damen und Herren

Nachstehend lasse ich Ihnen folgende Überlegungen zum an sich verdienstvollen Entwurf zukommen:

Artikel 1 (Gegenstand und Zweck)

In Artikel 1 Absatz 2 litera b E-ID-Gesetz ist von "Grundsätzen" des Datenschutzes durch Technik, der Datensicherheit, der Datensparsamkeit und der dezentralen Datenspeicherung die Rede. Doch stellen die erwähnten Grundsätze lediglich Stichworte dar und sind – entgegen den Ausführungen in Kapitel 6.7 des erläuternden Berichts – nicht spezifisch ausformuliert. Im neuen eidgenössischen Datenschutzgesetz vom 25. September 2020 (beschlossen, aber noch nicht in Kraft) werden die Anforderungen des Datenschutzes durch Technik und der Datensicherheit in Artikel 7 und 8 genannt und ausformuliert. Der Grundsatz der Datensparsamkeit dürfte wohl im Verhältnismässigkeitsgrundsatz nach Artikel 6 DSG-2020 verankert sein. Beim Grundsatz der dezentralen Datenspeicherung gibt es keine Grundlage im DSG-2020. Dagegen gibt es den Grundsatz der Datenrichtigkeit (Art. 6 Abs. 5 DSG-2020).

Artikel 1 ist wie folgt zu ändern: Die genannten **Grundsätze** sind zu überprüfen und auf das neue Datenschutzgesetz abzustimmen. Wo der Entwurf des E-ID-Gesetzes neue Grundsätze aufstellt, sind diese ähnlich wie im Datenschutzgesetz und ergänzend zu diesem Gesetz **näher auszuführen**. Dies trifft namentlich auf die Datensparsamkeit zu. Es ist zweifelhaft, ob Artikel 2 dem Grundsatz der Datensparsamkeit genügt. So «enthält» die E-ID die AHV-Nummer. Wird damit dem Missbrauch nicht Tür und Tor geöffnet, ist doch diese Nummer heute neben Namen und Geburtsdatum nur wenigen Personen bekannt? Dass die Nummer für den Ausstellungsprozess nötig ist, dem kann nicht widersprochen werden. Desweiteren sollten **Grundsätze über die zulässige Verwendung** der E-ID im Sinn der genannten Datensparsamkeit ins Gesetz aufgenommen werden (z.B. Beschränkung auf den notwendigen Einsatz in Zusammenhang mit der behördlichen Leistungserbringung), gehört doch dies zu den in Artikel 1 Absatz 1 genannten Zwecken des elektronischen Nachweises und der Nutzung der Identitätsinfrastruktur.

Auch der Grundsatz der dezentralen Datenspeicherung wäre zu präzisieren, ist doch das in Artikel 11 geregelte Informationssystem von fedpol zentralisiert, weshalb sich ein **Widerspruch** auf tut.

Art. 4 (Ausstellung)

Gemäss Artikel 4 Absatz 2 soll ab **Altersjahr 15** die E-ID von jeder Person eigenständig beantragt werden können. Bis zum vollendeten 14. Altersjahr braucht es die Einwilligung der Eltern beziehungsweise des gesetzlichen Vertreters.

Die Begründung dieser Altersgrenze in den Erläuterungen überzeugt nicht, zumal man eine Identitätskarte auch erst mit 18 eigenständig bekommt, und wie allgemein bekannt ist, das Alter 16 eine weitere Bedeutung hat.

An der Norm stört auch der im Entwurf verwendete **Begriff "Lebensjahr"**. Der Begriff "Altersjahr" ist in der Schweiz verbreiteter (vgl. z.B. im ZGB).

Art. 20 (Prüfung von elektronischen Nachweisen)

Die Kann-Bestimmung ist durch eine **Muss-Bestimmung** zu ersetzen, um das Vertrauen in die E-ID sicherzustellen.

Freundliche Grüsse



Gregor Zemp
Unterlöchlstrasse 17
6006 Luzern

Vernehmlassungsantwort zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Wir bedanken uns für die Vorlage und den erläuternden Bericht zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID).

Der Schweizerische Zentralverein für das Blindenwesen SZBLIND begrüsst die Einführung eines staatlichen elektronischen Identitätsnachweises grundsätzlich. In unserer Stellungnahme beschränken wir uns auf den Aspekt der Barrierefreiheit, der beim hier vorliegenden Gesetzesvorhaben von grosser Bedeutung ist.

Grundsätzliche Erwägungen

Der SZBLIND ist überrascht, dass der Aspekt der E-Accessibility keine Erwähnung in der Vorlage findet. Weder im Vorentwurf für das E-ID-Gesetz noch im erläuternden Bericht wird auf diesen wichtigen Aspekt eingegangen. Diesen Mangel gilt es zu beseitigen, indem im Gesetz sowie den ausführenden Bestimmungen detailliert geregelt wird, wie die digitale Barrierefreiheit (E-Accessibility) auf allen Ebenen sichergestellt wird. In der Entwicklung sind sämtliche Umsetzungsschritte im Hinblick auf den Standard eCH-0059 Version 3.0 (oder spätere Versionen) zu prüfen, der sich auf die international anerkannten Web Content Accessibility Guidelines WCAG 2.1 des World Wide Web Consortium W3C stützt und ergänzend Instrumente zur Förderung von E-Accessibility nutzt, welche von der E-Accessibility-Richtlinie der EU inspiriert sind.

Die Schweiz hat 2014 die UNO-Behindertenrechtskonvention (UNO-BRK, Übereinkommen über die Rechte von Menschen mit Behinderungen) unterzeichnet. Artikel 9 der UNO-BRK fordert den gleichberechtigten Zugang für Menschen mit Behinderungen zu allen zentralen Bereichen des täglichen Lebens, um ihnen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies gilt auch für die Information und Kommunikation, einschliesslich der entsprechenden Technologien und Systeme. Das Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen, kurz BehiG, schreibt in Art. 14 vor, dass die Behörden im Verkehr mit der Bevölkerung Rücksicht auf die besonderen Anliegen der Sprach-, Hör- oder Sehbehinderten nehmen müssen. Ohne Berücksichtigung der E-Accessibility wären Menschen mit Sehbeeinträchtigung vom staatlichen Angebot in Form eines staatlichen elektronischen Identitätsnachweises sowie einer staatlichen elektronischen Brieftasche ausgeschlossen. Die Schweiz ist also vertraglich und gesetzlich verpflichtet, die barrierefreie Nutzung elektronischer Dienste sicherzustellen.

Praktische Erwägungen

Für Menschen mit Sehbeeinträchtigung stellt die Digitalisierung eine Chance dar zu einem breiteren Zugang zu Dienstleistungen aller Art. Die digitalen Kommunikationskanäle sind das eigentliche Tor zu den Informationen für die sehbehinderten Menschen. Zwingende Voraussetzung für die Nutzbarkeit der digitalen Angebote ist aber, dass diese barrierefrei zur Verfügung stehen. Deshalb muss vor jeder Publikation eines webbasierten Produkts und auch vor jedem Update geprüft

werden, ob dieses barrierefrei zugänglich ist. Bei der Beschaffung von digitalen Produkten muss zudem zwingend das Prinzip "Design for all" zur Anwendung kommen. Die entsprechenden europäischen Normen ist bereits des nationalen Normenwerks. Im Fall des BGEID soll die Anwendung dieser Normen jedoch nicht freiwillig, sondern verpflichtend sein.

Zu diesem Zweck ist die zu entwickelnde Informatikinfrastruktur unbedingt auf sämtlichen Ebenen nachhaltig barrierefrei zu planen und die Barrierefreiheit durch entsprechende Tests sicherzustellen. Die Freigabe bzw. Lancierung der E-ID darf erst erfolgen, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist.

Wie die Antwort auf die Frage 22.7406 von Nationalrätin F. Ryser zeigt, ist sich der Bundesrat der Notwendigkeit solcher Tests (Usability-Tests) bewusst. Der standardmässige Einsatz von Usability-Tests ist bei anspruchsvollen elektronischen Diensten und Anwendungen des Bundes, die für ein breites Publikum bestimmt sind, durchzuführen. In der vorliegenden Vernehmlassungsvorlage fehlt dieser Aspekt jedoch. Der SZBLIND ist klar der Meinung, dass die Barrierefreiheit und der Einsatz von entsprechenden Tests in das BGEID aufgenommen werden müssen.

Es ist zudem sicherzustellen, dass bei jeder Anpassung und jedem Update die Barrierefreiheit erneut geprüft wird. Neue Versionen dürfen erst freigegeben werden, wenn die Barrierefreiheit durch Fachpersonen aus dem Kreis der Betroffenen bestätigt worden ist. Dies ist leider aktuell nicht gewährleistet, wie aktuelle Beispiele beim Bund zeigen. (z.B. Elektronisches Patientendossier; Elektronisches Einreiseformular; Covid-Zertifikat)

Anträge

- 1) Im Bundesgesetz über den elektronischen Identitätsnachweis (E-ID-Gesetz, BGEID) sei ein eigener Artikel «Barrierefreiheit» aufzunehmen. Darin ist der Grundsatz der barrierefreien Nutzbarkeit festzuschreiben. Dies gilt für sämtliche Infrastrukturebenen die von Antragstellenden, Inhaber: innen einer E-ID, Aussteller: innen, Verifikator: innen und weiteren Usergruppen genutzt oder betrieben werden können.
- 2) In den Ausführungsbestimmungen zum E-ID-Gesetz sei ein eigenes Kapitel zur Barrierefreiheit aufzunehmen. Dieses beschreibt detailliert, wie die Zugänglichkeit des elektronischen Identitätsausweises für Menschen mit Beeinträchtigungen sichergestellt wird.
- 3) Zur Kontrolle der Barrierefreiheit sei ein Auftrag an eine anerkannte Fachinstitution zu erteilen, die zusammen mit betroffenen Personen die Infrastruktur im Hinblick auf die Barrierefreiheit prüft.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Freundliche Grüsse



Pierre-Alain Uberti
Geschäftsführer SZBLIND



Jan Rhyner
Verantwortlicher Interessenvertretung SZBLIND

Per E-Mail

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zetamind AG
André Gollier
Founding Partner
Zurlindenstrasse 111
8003 Zürich

Vernehmlassung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrte Damen und Herren

Zetamind AG begrüsst grundsätzlich das vorgeschlagene Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) und stellt ergänzend den folgenden Antrag:

Antrag

Artikel 2 des vorgeschlagenen Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) erhält neu den folgenden Absatz:

«Absatz 4 (neu)

Sie kann schliesslich auf Verlangen der antragstellenden Person Allianz-, Ordens-, Künstler- oder Partnerschaftsnamen sowie Angaben über besondere Kennzeichen wie Behinderungen, Prothesen oder Implantate enthalten.»

Begründung

Gemäss Abschnitt 1.2 des erläuternden Berichts soll das neue Gesetz die Motionen aller Fraktionen 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129 «Vertrauenswürdige staatliche E-ID» umsetzen, d.h. «Der Bundesrat wird damit beauftragt, ein staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität (Authentifizierung) in der virtuellen Welt, vergleichbar mit Identitätskarte oder Pass in der physischen Welt, zu schaffen.»

Eine solche Vergleichbarkeit mit Identitätskarte oder Pass ist jedoch nur dann hergestellt, wenn die vorgesehenen digitalen Attribute auch den im Ausweisgesetz verankerten Kann-Attributen zu entsprechen vermögen.

Artikel 2 Absatz 4 des Ausweisgesetzes AwG lautet: "Auf Verlangen der Antrag stellenden Person kann der Ausweis Allianz-, Ordens- oder Künstlernamen sowie Angaben über besondere Kennzeichen wie Behinderungen, Prothesen oder Implantate enthalten". Es macht wenig Sinn, wenn solche auf der Identitätskarte vorhandenen Angaben in der digitalen Welt nicht ebenfalls verfügbar gemacht werden.

Ein konkretes Anwendungsbeispiel der heutigen Nutzung der Identitätskarte sind die Bestimmungen zur Identifikation einer Person in SR 221.411, der Handelsregisterverordnung (HRegV). Demgemäss werden nach Artikel 24b Absatz 2a auf der Grundlage des Ausweisdokuments u.a. die folgenden Angaben im Handelsregister erfasst: «allfällige Ruf-, Kose-, Künstler-, Allianz-, Ordens- oder Partnerschaftsnamen;».

Diese Erfassung sollte auch dann möglich sein, wenn anstelle einer herkömmlichen Identitätskarte ein elektronischer Identitätsnachweis vorgelegt wird. Dies wäre künftig beispielsweise bei einer Unternehmensgründung auf durchgängig elektronischem Weg z.B. via EasyGov.swiss der Fall.

Schliesslich sei noch erwähnt, dass die Rechtskommission des Nationalrats im Juni 2022 eine Vernehmlassung zu amtlichen Doppelnamen eröffnet hat. In der sogenannten grossen Lösung ist u.a. vorgesehen, dass die Eheleute unabhängig von der Wahl eines gemeinsamen Familiennamens jede/r für sich wählen können, einen amtlichen Doppelnamen zu führen. Insofern drängt es sich auf, die Gestaltung der Namens-Attribute beim elektronischen Identitätsnachweis flexibler zu gestalten als es zurzeit vorgesehen ist.

Für die Berücksichtigung dieses Anliegens bedanken wir uns vielmals.

Freundliche Grüsse

André Golliez
Founding Partner Zetamind AG

Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

per E-Mail:
rechtsinformatik@bj.admin.ch

Zürich, 12. Oktober 2022

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz); Stellungnahme der Zürcher Handelskammer

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Mit Schreiben vom 29. Juni 2022 wurden interessierte Kreise dazu eingeladen, sich zum Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) zu äussern. Die Zürcher Handelskammer (ZHK) vertritt als Wirtschaftsorganisation die Interessen von über 1'100 Unternehmen am Wirtschaftsstandort Zürich und setzt sich für eine wettbewerbsgesteuerte Marktwirtschaft mit möglichst günstigen Rahmenbedingungen ein. Wir erlauben uns deshalb, zur vorliegenden Vernehmlassung Stellung zu nehmen.

Position der ZHK

Die Volksabstimmung vom 7. März 2021 zum Bundesgesetz über elektronische Identifizierungsdienste (BGEID) scheiterte am grössten Kritikpunkt der privaten Herausgeber. Unbestritten sind die Vorteile einer elektronischen Identität. Die ZHK begrüsst deshalb die Stossrichtung der Vernehmlassungsvorlage über das E-ID-Gesetz. Aus Sicht der Zürcher Handelskammer ist es zentral, dass die rasche Digitalisierung von öffentlichen Prozessen und der Wirtschaft vorangetrieben wird. Dies trägt sowohl zur Wettbewerbsfähigkeit als auch zur Innovationskraft des Wirtschaftsstandorts bei.

Zur Begründung

Der Bundesrat möchte mit einer neuen Vorlage zum E-ID-Gesetz die Einführung einer elektronischen Identität vorantreiben. Aus Sicht der Wirtschaft ist es zentral, dass die Funktionalität zu jeder Zeit gewährleistet ist und sich die Fehler aus vergangenen IT-Projekten des Bundes nicht wiederholen. Es ist deshalb entscheidend, dass sich der Bund an bereits bestehenden, marktwirtschaftlichen Lösungen orientiert und keine komplett neue Eigenentwicklung anstrebt. Ebenso wichtig ist die Interoperabilität der staatlichen Infrastruktur. Sie muss so aufgebaut sein, dass staatliche und private Stellen möglichst einfach andere elektronische Nachweise, wie beispielsweise Hochschuldiplome oder ärztliche Rezepte, ausstellen können. Ausbauschritte eines entsprechenden Ökosystems müssen möglichst rasch vorangetrieben werden. Des Weiteren ist


eine gute Koordination zwischen den föderalen Ebenen und der EU (eIDAS) nötig. Die ZHK begrüsst deshalb den Rechtsvergleich mit der Europäischen Union sowie das Bestreben des Bundesrats, Abkommen zur internationalen Anerkennung der E-ID zu erreichen. Auf der föderalen Ebene ermöglicht die E-ID neue Geschäftsmodelle von privaten Anbietern im Bereich E-Commerce. Für Unternehmen eröffnet sich die Möglichkeit des Verkehrs mit den Behörden und der Verwaltung im Bereich von E-Government möglichst über nur eine Schnittstelle (One-Stop-Shop). Solche Bestrebungen begrüsst die ZHK und sind auch zukünftig in den Gesetzgebungsprozess miteinzubeziehen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse
Zürcher Handelskammer



Dr. Regine Sauter
Direktorin



Sven Marti
Wirtschaftspolitik