Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Bundesamt für Justiz BJ
3003 Bern

Per Mail: e-id@bj.admin.ch

Bern, 5. Oktober 2021

Öffentliche Konsultation zum «Zielbild E-ID»

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Zielbild E-ID Stellung nehmen zu können. Der Schweizerische Städteverband vertritt die Städte, städtischen Gemeinden und Agglomerationen in der Schweiz und damit gut drei Viertel der Schweizer Bevölkerung.

Welches sind die drei wichtigsten **Anforderungen** an eine staatliche E-ID als digitaler Ausweis?
- Sie soll verifizierbare Identifikations-Attribute aufweisen (Name, Vorname, Geburtsdatum, AHV-Nummer), wobei dem Datenschutz grosse Bedeutung zukommt (privacy by design, Datensparsamkeit).
- Sie soll Rechtssicherheit bieten, um bspw. rechtsgültig digitale Verträge abzuschliessen (aus Sicht der Benutzer), aber auch, um öffentliche Dienstleistungen erbringen zu können (aus Sicht der öffentlichen Verwaltungen). Dabei soll sie breit einsetzbar sein (über alle föderalen Ebenen), ihre Benutzung aber freiwillig bleiben.
- Sie soll für die Benutzer tiefe Einstiegshürden aufweisen, also einfach zu bedienen, kostenfrei sowie einfach und schnell einzurichten bzw. zu erneuern sein.

Welche **Anwendungsfälle** der E-ID stehen im Vordergrund?
Online-Dienste der öffentlichen Verwaltungen (Bund, Kantone, Städte und Gemeinden, Post, etc), wie z.B. Betreibungsregisterauszüge, Erstanmeldungen Schule und Betreuung, Zugang zum Pensionskassenportal.

Welchen **Nutzen** bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?
- ein nationales Register, das die kantonalen Register überflüssig macht (z.B. für Führerscheine)
- Erleichterung der administrativen Abläufe beim Umzug zwischen Kantonen
- verbesserte Benutzerzufriedenheit
- Vermeidung von Fahrten zum Schalter für Kontrollen oder Legitimationen

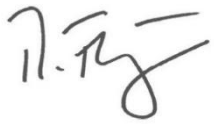
Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Schweizerischer Städteverband
Direktor



Martin Flügel

Herr
Michael Schöll
Direktor
Bundesamt für Justiz BJ
Bundesrain 20
3003 Bern

Ausschliesslich per E-Mail an:
E-ID@bj.admin.ch

6. Oktober 2021

Stellungnahme zur öffentlichen Konsultation zum «Zielbild E-ID»

Sehr geehrter Herr Schöll
Sehr geehrte Damen und Herren

Im September 2021 haben Sie uns eingeladen, im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID» Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Zusammenfassung

Für die digitale Wirtschaft stellt die E-ID eine wesentliche Infrastrukturkomponente dar. Sie steht am Anfang zahlreicher neuer Geschäftsmodelle und der Schaffung eines dynamischen digitalen Ökosystems welche erforderlich sind, die Digitalisierung in der Schweiz voranzubringen. economiesuisse begrüsst die breit geführte öffentliche Diskussion über die Anforderungen und den Nutzen an die E-ID. Gleichsam ist die möglichst zeitnahe Einführung für die Attraktivität des Wirtschaftsstandortes von enormer Bedeutung.

economiesuisse unterstützt das Ambitions-Niveau 3 und damit die Schaffung eines Ökosystems digitaler Nachweise. Damit soll es ermöglicht werden, dass die Schweiz im internationalen Vergleich wettbewerbsfähig bleibt, gleichzeitig Innovationen fördert und schliesslich auch das Digitalisierungspotenzial im vollen Umfang ausschöpft.
Eine erfolgreiche Durchsetzung und Anwendung der E-ID kann nur dann zustanden kommen, wenn diese eine breite Akzeptanz in Gesellschaft und Wirtschaft geniesst. Zur Durchsetzung und Anwendung der E-ID braucht es entsprechend einen vertrauenswürdigen und sicheren Rahmen. Im Zentrum muss dabei das Vertrauen der Gesellschaft und der Wirtschaft in die Benutzung der E-ID stehen. Grundanforderungen an die E-ID sind dabei Benutzerfreundlichkeit, angemessener Datenschutz, eine dezentrale Architektur sowie die staatliche Kontrolle. Zusätzlich sind bei der Ausstellung der E-ID auch die Entwicklungen in der EU im Auge zu behalten und es ist sich an diesen zu orientieren.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

1 Stellungnahme zu den gestellten Fragen

Nachstehend nehmen wir detailliert Stellung zu den von Ihnen gestellten Fragen im Schreiben zur öffentlichen Konsultation zum «Zielbild E-ID» vom 9. September 2021.

2 Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Aus Sicht der economiesuisse definieren drei unterschiedliche Kategorien die wichtigsten Anforderungen. Dies sind a) die technischen und b) die organisatorischen Anforderungen an die Rahmenbedingungen der E-ID sowie c) die Anforderungen an das Ökosystem:

a) Technische Anforderungen an die Rahmenbedingungen der E-ID

Benutzerfreundlichkeit und Transparenz: Die E-ID wird sich nur dann breit durchsetzen, wenn sie in der Gesellschaft und Wirtschaft auf grösstmögliche Akzeptanz stösst. Diese wird jedoch nur dann erreicht, wenn genügend Vertrauen von Seiten der Gesellschaft und Wirtschaft vorhanden ist. Für das Vertrauen der Bevölkerung ist dementsprechend wichtig, dass der Bund die notwendige Transparenz hinsichtlich der E-ID gewährt. Zudem soll der Zugriff auf die E-ID benutzerfreundlich und sicher gewährleistet sein.

Datenschutz und Datenhoheit: economiesuisse befürwortet das Prinzip «Privacy by Design». In den Augen der Endnutzer muss sowohl der Datenschutz sowie die Datenhoheit als sicher und bereits auf Grund der Systemarchitektur gegeben betrachtet werden. Die Thematik des Datenschutzes sowie der Schutz der Privatsphäre sind in das Zentrum der Öffentlichkeit gerückt und werden auch in Zukunft an Bedeutung zunehmen.

Datensparsamkeit: Als sinnvoll wird von Seiten economiesuisse eine attributisierte E-ID erachtet. Diese soll nur die notwendigen Datenpunkte der E-ID Inhaber an den Verifier herausgeben. Damit sollen das Vertrauen der Endnutzer sowie die Privatsphäre langfristig erhöht werden. Auch aufgrund der Anforderungen des neuen DSG und der Entwicklungen auf EU-Ebene ermöglicht die Datensparsamkeit die Wahrung des Anschlusses an ein EU-System.

Dezentrale Architektur: economiesuisse spricht sich für einen dezentralen Ansatz hinsichtlich der Speicherung und Verifizierung aus. Eine dezentrale Speicherung und Verifizierung der Daten bilden eine essenzielle Anforderung an die E-ID. Es braucht aber noch die Klärung von Grundsatzfragen der Self-Sovereign Identitiy (SSI).

b) Organisatorische Anforderung an die Rahmenbedingungen der E-ID

Staatliche Kontrolle: economiesuisse wünscht sich bei der Entwicklung, der Ausstellung und dem Betrieb der E-ID eine Federführung von Seiten des Bundes innerhalb des Ambitions-Niveaus 3. In einem solchen Ökosystem stellt die E-ID nur noch einen von vielen digitalen Nachweisen dar. Dabei ist sie jedoch Kernelement, da über sie die Verknüpfung zu anderen digitalen Nachweisen erlaubt wird. Folglich wird es als notwendig erachtet, dass Entwicklung, Ausstellung und der Betrieb dieses Kernelements durch staatliche Behörden erfolgen. Als positives Beispiel kann hierzu die Umsetzung des Grossprojekts des Covid-Zertifikats durch das Bundesamt für Informatik und Telekommunikation genannt werden.

Inklusive Pilotierung: Es sollten frühzeitig unterschiedliche Arbeitsgruppen aus Wirtschaft, Wissenschaft und Gesellschaft in den Prozess zur Erstellung der E-ID miteinbezogen werden, wobei diese inklusive Begleitung nicht zu Verzögerungen bei der Umsetzung führen darf.

c) Anforderungen an das Ökosystem

Erweiterbarkeit: Es ist von grundsätzlicher Bedeutung, dass ein offenes und inklusives Ökosystem angestrebt wird. So wird eine Skalierung in Bezug auf die Anzahl und Vielfalt der Nachweise und Verifizierer möglich. Wie bereits dargelegt ist die Summe der möglichen Anwendungsfälle eines der wichtigen Bewerbungskriterien bei der Evaluation der E-ID Lösungsansätze. Darin ist auch die Ausweitung der Identifizierung und Verifizierung auf andere Subjekte, beispielsweise Organisationen miteinzubeziehen.

Internationale Anschlussmöglichkeit: Bei der Einführung und Durchsetzung der E-ID soll sich die Schweiz an der Entwicklung in der Europäischen Union orientieren. Die Schweizer E-ID sollte im Grundsatz der EUid und somit der europäischen Version der elektronischen ID entsprechen. Hervorzuheben ist dabei insbesondere, dass eine digitale Vertrauensinfrastruktur nicht an den Landesgrenzen aufhören soll, sondern ein Austausch über die Landesgrenzen zum Alltag gehört. Dies hat sich beispielsweise bei der Nutzung des Covid-Zertifikates gezeigt.

3 Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Damit der Mehrwert der Digitalisierung maximal ausgeschöpft wird, braucht es Ökosysteme, in denen digitale Nachweise über Organisations- und Ländergrenzen hinweg sicher und unfälschbar ausgetauscht und überprüft werden können. Nachfolgend werden einige Beispiele genannt, wobei die Beziehungen der Issuer, Verifier und Holder im Vordergrund stehen.

G2C-Anwendungsfälle: G2C-Anwendungsfälle ermöglichen das Vertrauen der Enduser in die staatliche E-ID und können somit weiteren Anwendungsfällen im B2C- und G2B2C- Bereich den Weg öffnen.

B2C-Anwendungsfälle: Bei Anwendungsfällen, in denen die Überprüfung bestimmter Identitätsattribute erforderlich ist (z. B. Alkoholkauf), soll die E-ID sicherstellen, dass nur die minimal notwendigen Daten, beispielsweise die Volljährigkeit, übermittelt werden.

G2B2C-Anwendungsfälle: Als Beispiel kann hierzu die Meldeschein-Pflicht beim Hotel Check-In genannt werden, wobei der Gast dem Hotel gewisse Identitätsattribute nachweisen können muss. Das Hotel ist verpflichtet, diese Liste an Attributen via Meldeschein der kantonalen Behörde weiterzuleiten. Eine E-ID Lösung unter Nutzung der geeigneten Übermittlungsschnittstellen würde dabei für Hotel und Behörden zu erheblichen Effizienzgewinnen führen.

4 Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können?

Ein Ökosystem des Ambitions-Niveaus 3 bringt die nachstehenden Vorteile mit sich:

Eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und zu überprüfen, bietet gleichzeitig eine erhöhte **Sicherheit** für die Endnutzer. Digitale Nachweise können, wie beispielsweise zwischen Personen und Organisationen unfälschbar ausgetauscht sowie überprüft werden. Die erhöhte Vertrauenswürdigkeit der Infrastruktur hat die Steigerung der Angebote zur Folge. Wir unterstützen daher eine dezentrale Ausstellung und eine Überprüfung digitaler Nachweise. Dies ist die beste Möglichkeit, um die **Vertrauenswürdigkeit** einer solchen Infrastruktur zu steigern. Gleichzeitig wird dadurch das Bedürfnis nach mehr Datenschutz, Datenhoheit und Datensparsamkeit aufgegriffen. Die Folge davon ist, dass die Endnutzer Vertrauen in die Anwendungen sowie den digitalen Raum entwickeln können. Zudem erlaubt es ein Ökosystem des Ambitions-Niveaus 3 digitale Nachweise organisationsüberschreitend und grenzüberschreitend zu

verwenden. Dies führt zu einer erhöhten **erweiterbaren** Infrastruktur und gewahrt damit zusätzlich die internationalen Anschlussmöglichkeiten.

Ein Ökosystem, welches vertrauenswürdig, sicher und erweiterbar ist, kann die treibende Kraft für Innovationen in Wirtschaft und Gesellschaft darstellen. Potenzielle volks- und betriebswirtschaftliche Mehrwerte könnten so besser ausschöpft werden. Mittels des Ambitions-Niveaus 3 sowie dem Self-Sovereign Identity Ansatzes kann die Digitalisierung in der Schweiz vorangetrieben werden. Zugleich werden Innovationen ermöglicht und die Wettbewerbsfähigkeit des Wirtschaftsstandortes Schweiz auf internationaler Ebene wird gewahrt.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Erich Herzog
Mitglied der Geschäftsleitung

Antonija Martinovic
Wissenschaftliche Mitarbeiterin Wettbewerb & Regulatorisches

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Office fédérale de la justice
Département fédéral de justice et police DFJP
3003 Berne

E-ID@bj.admin.ch

Berne, le 30 Septembre 2021 usam-MH/ad

Réponse à la consultation publique
« Document de travail concernant le projet d'identité électronique (e-ID) »

Mesdames et Messieurs,

Plus grande organisation faîtière de l'économie suisse, l'Union suisse des arts et métiers usam représente plus de 230 associations et quelque 500 000 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 2 septembre 2020, l'Office fédéral de la justice nous a convié à prendre position dans le cadre de la consultation publique sur le « Document de travail concernant le projet d'identité (e-ID) ».

L'usam plaide pour une e-ID mise en place le plus rapidement avec les moyens technologies à la pointe du savoir-faire en matière d'authentification. Ceci suppose que l'Administration fédérale collabore avec le secteur privé pour qu'une solution efficace et sûre voit enfin le jour. L'idée d'un portefeuille d'identité étatique est à rejeter, puisque la sphère privée est à protéger.

I. Point de situation

L'usam se présente pour une e-ID portée par les compétences et à savoir du secteur privé. L'e-ID a malheureusement échoué dans les urnes en 2021. Raison pour laquelle l'Administration fédérale doit représenter sa copie en stipulant clairement que l'État a le contrôle et la surveillance sur les données d'identification des citoyens suisses. En tant que maître d'ouvrage, l'État doit pouvoir assurer que les technologies mise en œuvre peuvent garantir un degré de sécurité des informations personnelles très élevés autant contre un mauvais usage d'entreprises privées que des autorités publiques.

L'économie privée attend impatiemment que ce dossier de la numérisation avance rapidement. L'enjeu consiste à pouvoir 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. Sans cet instrument de l'e-ID, l'économie suisse risque de

prendre beaucoup de retard sur le dossier de la numérisation, ce qui se traduit concrètement par un manque d'attractivité et une baisse de la compétitivité internationale de nos entreprises et PME.

II. Appréciation de l'usam

Pour l'usam, les trois principales exigences auxquelles doit satisfaire une e-ID sont le respect de la sphère privée, l'utilisation des meilleures technologies, et surtout la facilité d'utilisation. D'abord, en ce qui concerne la sécurité des données, la sphère privée des individus doit pouvoir être respectée. Concrètement, cela signifie que l'usage de leur e-ID est l'affaire des citoyens et non de l'Administration fédérale. Ensuite pour les meilleures technologies, il faut pouvoir proposer ce qu'il y a de mieux en matière d'authentification numérique. Ces savoir-faire se trouvent tout particulièrement dans l'économie privée. Il est aussi important de prendre en compte dès le début le caractère évolutif des technologies du numérique pour rester à la pointe dans le long terme. Enfin, la facilité d'utilisation requiert que l'e-ID puisse être très facilement appliquée sur tout type de reconnaissance d'identité et cela même par des tranches de la population n'ayant pas d'affinité d'utilisation de ces nouvelles technologies. Avec ces trois exigences, l'e-ID doit pouvoir s'imposer rapidement au sein de la société.

À l'avis de l'usam, les principaux domaines d'utilisations de l'e-ID concerne la signature et la reconnaissance d'identité. Sans cela, la chaîne numérique est cassée et les processus sensiblement ralentis. La numérisation est un facteur d'implantation important pour la Suisse ainsi que de compétitivité internationale. Toutefois, la numérisation n'est un succès que si un processus commencé numériquement peut également être achevé numériquement. Ainsi, le premier avantage pour les utilisateurs de l'e-ID réside dans l'accès pour tous de la signature électronique qualifiée. Par ce biais, la signature électronique pourrait être facilement répandue et utilisée au sein de la population suisse. L'e-ID permettrait une certaine sécurité dans le développement des affaires de nombreuses PME. Par exemple, aujourd'hui, la grande majorité des commandes sont passées via l'internet. Le commerce en ligne est en plein essor – et pas seulement à cause de la pandémie. De plus en plus de PME se lancent également dans ce domaine prometteur. Toutefois, si un client ne paie pas sa facture, ces commerçants ont du mal à faire valoir leurs droits clairement établis. Parce qu'ils ne disposent pas d'une reconnaissance de dette confirmée par signature en raison du processus de commande numérique, ils ne disposent pas de la procédure sommaire efficace d'ouverture judiciaire provisoire pour le recouvrement des créances. Dans ce cas, l'utilisation de l'e-ID résoudrait ce problème épineux pour les PME. Mais, l'e-ID devrait aussi pouvoir être utilisée dans la signature de contrat de travail puisque l'authentification numérique est ainsi protégée et contrôlée. Dans ce sens, l'usam demande, indépendamment de l'e-ID, la signature électronique simplifiée. Elle peut être introduite plus rapidement et sans législation spéciale et profiterait beaucoup plus aux PME que l'e-ID.

Pour l'usam, il faudrait exploiter toute la portée de l'écosystème de l'authentification numérique, à savoir que l'e-ID devient une preuve numérique de base pour d'autres nombreuses autres preuves numérique (par exemple 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.) Une opération à l'identique (avec la réception, l'enregistrement, et la présentation) représente un avantage important et permettrait une démocratisation des preuves numériques. L'idée d'un dispositif de stockage décentralisé, sécurisé et réglementé, autrement dit un portefeuille d'identité basé sur l'e-ID permettant d'obtenir des informations avec un haut degré de fiabilité est très intéressante pour les PME. En revanche, L'usam s'oppose à ce que l'État instaure un portefeuille d'identité étatique, ce qui pourrait constituer une menace contre la sphère privée individuelle et propulser les velléités d'établir un contrôle encore plus strict de la population.

III. Conclusion

L'usam exige que la transformation numérique au sein des autorités publiques conduise à des allégements dans les procédures administratives et les processus d'authentification de l'identité. À ce titre, ce projet e-ID est une pierre angulaire qu'il faudrait dans les meilleurs délais pouvoir étendre au maximum dans les procédures nécessitant l'authentification.

Le projet présente cependant deux écueils : l'absence d'un délai court pour passer à l'e-ID et un manque de représentation du secteur privée proche du terrain et des savoir-faire des entreprises privées en matière d'authentification.

Nous vous remercions de l'attention portée à notre prise de position et vous présentons, Mesdames et Messieurs, nos respectueuses salutations.

Union suisse des arts et métiers usam

Hans-Ulrich Bigler
Directeur

Mikael Huber
Responsable du dossier

digitalswitzerland

Bundesamt für Justiz BJ
Direktion
Herr Dr. Michael Schöll
Bundesrain 20, 3003 Bern

Einreichung per Mail an: E-ID@bj.admin.ch

Bern, 13. Oktober 2021

Öffentliche Konsultation zum «Zielbild E-ID»

Stellungnahme von digitalswitzerland

Sehr geehrter Herr Dr. Schöll
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, uns zum «Zielbild E-ID» äussern zu können. Diese Gelegenheit nimmt der Verein digitalswitzerland gerne wahr.

1 Betroffenheit 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 230 Organisationen, bestehend aus Vereinsmitgliedern und politisch neutralen Stiftungspartnern, transversal zusammen. digitalswitzerland ist Ansprechpartner in allen Digitalisierungsfragen und engagiert sich für die Lösung vielfältiger Herausforderungen.

2 Grundsätzliche Bemerkung und Position

Aus Sicht von digitalswitzerland ist die E-ID eine wichtige Komponente einer digitalen Vetrauensinfrastruktur, um die Schweiz bei der Digitalisierung voranzubringen. digitalswitzerland begrüsst deshalb die aktuell breit geführte öffentliche Diskussion über den Nutzen und die Anforderungen der E-ID.

Der grösste Nutzen im Sinne eines volks- und betriebswirtschaftlichen Mehrwerts resultiert, wenn eine **vertrauenswürdige**, **sichere** und **erweiterbare digitale Infrastruktur** geschaffen wird. Deshalb plädiert digitalswitzerland für das Ambitions-Niveau 3 (Ökosystem digitaler Nachweise), welches das grösste Ausschöpfungspotential für die digitale Transformation und die Wettbewerbsfähigkeit der Schweiz bietet. Es ist am besten geeignet, um die Schweiz international wettbewerbsfähig zu halten und (digitale) Innovationen zu fördern.

Aus Sicht von digitalswitzerland lassen sich zusammenfassend folgende drei Anforderungen an die E-ID adressieren, um einen grösstmöglichen Nutzen (siehe 3.3) zu erzielen und wichtige Anwendungsfälle (siehe 3.2) zu ermöglichen:

- **Technische Anforderungen** mit Fokus auf Datenschutz/Hoheit, Dezentrale Architektur, und Datensparsamkeit
- **Organisatorische Anforderungen** mit Fokus auf inklusive Pilotierung und staatliche Kontrolle
- **Ökosystem Anforderungen** mit Fokus auf Erweiterbarkeit und internationaler Anschlussmöglichkeit

Die Wahl einer bestimmten Technologie sollte abhängig gemacht werden von den Anforderungen sowie deren Prüfung auf Umsetzbarkeit durch ein breit abgestütztes Expertengremium.

3 Stellungnahme zu den drei zentralen Fragen der öffentlichen Konsultation

Im Folgenden wird auf die drei Hauptfragen der Konsultation näher eingegangen. Die Positionen wurden in Zusammenarbeit mit Expertinnen und Experten des Netzwerks von digitalswitzerland erarbeitet.

3.1 Welche sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

*3.1.1 **Technische Anforderungen** mit Fokus auf Dezentrale Architektur, Datenschutz/Hoheit, und Datensparsamkeit*

- **Dezentrale Architektur:** digitalswitzerland befürwortet einen dezentralen Ansatz. Das heisst eine elektronische Identität, welche nicht durch ein zentrales System verwaltet wird und nur mittels dessen genutzt werden kann. Wir sehen die dezentrale Speicherung und Verifizierung von Daten als eine essenzielle Anforderung an eine E-ID, auch wenn die Grundsatzfragen solcher Lösungsansätze noch nicht abschliessend geklärt sind. In der Transition – von den heutigen Identity-Modellen (zentralisiert & föderiert) zu jener einer dezentralen Architektur – erscheinen Verbindungspunkte für Users (evt. zu bestehenden Accounts) und entsprechende Anreize für die Stakeholder im Ökosystem sinnvoll und notwendig. Zudem muss Klarheit geschaffen werden, über welchen Zeithorizont eine solche Transition zu erfolgen hat und welche Kosten damit verbunden sind. Die Möglichkeit einer organischen Transition mit inkrementellem Aufgleisen von Services und Ausbaustufen, zielgruppen-orientierter Hilfestellung und Support erscheint opportun.
- **Datenschutz und -hoheit:** digitalswitzerland befürwortet den Wandel vom Prinzip «Privacy by Trust» hin zum «Privacy by Design». Das Diskussionspapier weist zu Recht darauf hin, dass der Schutz der Privatsphäre in den Augen der Öffentlichkeit ein noch wichtigeres Thema geworden ist. Dies entspricht dem aktuellen Zeitgeist und dürfte in Zukunft weiter zunehmen. Gleichermassen wird das Bedürfnis der Endnutzer:innen nach Hoheit über ihre Identifikations-Daten wachsen. Datenschutz- und Datenhoheit sollten daher eine Anforderung darstellen.
- **Datensparsamkeit:** digitalswitzerland erachtet eine attributbasierte E-ID als sinnvoll, welche nur die notwendigen Datenpunkte vom E-ID Holders an den Verifier der E-ID übermittelt. Dies erhöht die Privatsphäre und langfristig auch das Vertrauen, dass die Nutzer:innen in eine E-ID haben werden. Auch aufgrund der Entwicklung im europäischen Datenschutz (DSGVO), die den Schutz personenbezogener Daten stark gewichtet, ermöglicht die Anforderung der Datensparsamkeit, dass der Anschluss an Europa gewahrt wird.

*3.1.2 **Organisatorische Anforderungen** mit Fokus auf staatliche Kontrolle der E-ID und inklusive Pilotierung*

- **Staatliche Kontrolle:** digitalswitzerland spricht sich dafür aus, dass der Bund federführend bei Entwicklung, Ausstellung, und Betrieb der E-ID sein sollte (innerhalb des Ambitions-Niveau 3). Unter einem solchen Ökosystem digitaler Nachweise ist die E-ID nur noch eine von vielen digitalen Nachweisen. Die E-ID ist dabei jedoch ein Kernelement, da es Verknüpfung zu anderen digitalen Nachweisen erlaubt (z.B. ÖV-Ticket). Darum sehen wir es als notwendig, dass die Entwicklung, Ausstellung, und Betrieb dieses Kernelements (d.h. der E-ID) durch staatlich spezialisierte Behörden erfolgt, welche als einzige Quelle bereits heute über die notwendige Authoritäten verfügen. Diese E-ID darf auf privatwirtschaftlich entwickelten Produkten und Diensten beruhen. Die entstehende Vertrauens-Infrastruktur (vom Bund gewährleistet) soll den Wettbewerb innovativer Lösungen im Ökosystem digitaler Nachweise erlauben. Gemäss dem Grundprinzip dezentraler Systeme sollte die Gesamtkontrolle für die Entwicklung des ganzen Ökosystems nicht bei einer einzelnen Instanz sein. Die Frage wer die dezentrale Infrastruktur (Registry DLT, Wallets und Secure Cloud Agents) zur Verfügung stellt, ist aus unserer Sicht in einem gesamtheitlichen Trust- und Rollenmodell durch ein breit abgestütztes Expertengremium zu definieren.
- **Inklusive Pilotierung:** digitalswitzerland plädiert dafür, dass verschiedene Anspruchsgruppen (z.B. Wissenschaft, Wirtschaft und Zivilgesellschaft) frühzeitig in den Prozess mit einbezogen werden. Wir schlagen auch vor, dass eine Gruppe aus Testusern, bestehend aus einem repräsentativen Querschnitt der Schweizer Bürger:innen, den Pilotierungsprozess eng begleitet. Entsprechend soll der Prozess zur Erstellung einer E-ID möglichst iterativ und transparent gestaltet werden.

*3.1.3 **Ökosystem Anforderungen** mit Fokus auf Erweiterbarkeit und international Anschlussmöglichkeit.*

- **Erweiterbarkeit:** Es ist enorm wichtig, dass ein offenes und inklusives Ökosystem aufgebaut wird, welches eine Skalierung in Anzahl und Vielfalt der Nachweise, Aussteller und Verifizierer ermöglicht. Wir sind der Ansicht, dass die Summe der möglichen Anwendungsfälle einer der wichtigen Bewertungskriterien ist, um die verschiedenen E-ID Lösungsansätze zu evaluieren. Darin ist auch die Ausweitung der Identifizierung und Verifizierung auf andere Subjekte, mit denen wir in der analogen Welt interagieren, seien es Organisationen oder Dinge, mit einzubeziehen. Dies ist besonders kritisch, da viele Initiativen für nationale elektronische Identitäten mit dem Huhn-Ei-Problem kämpfen. Das heisst konkret: Ohne E-ID werden keine Anwendungsfälle geschaffen und ohne Anwendungsfälle wird keine E-ID benötigt. Die Erweiterbarkeit ist daher eine essenzielle Anforderung um eine verstärkende Adoptionsdynamik des ID-Ökosystems zu schaffen.
- **Internationaler Anschlussmöglichkeit:** Aus Sicht von digitalswitzerland ist es wichtig, dass eine E-ID-Infrastruktur nicht national, sondern mindestens europäisch gedacht wird und globale Standard befolgt. Die Möglichkeit zum Anschluss an den rechtlichen Rahmen (zumindest) von Europa muss offengelassen werden. Dies ist wichtig, da eine digitale Vertrauensinfrastruktur nicht an den Landesgrenzen Halt macht. Dies zeigt das Covid-Zertifikats derzeit deutlich.

3.2 Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Um mit den Möglichkeiten der Digitalisierung möglichst viel Mehrwerte schaffen zu können, braucht es Ökosysteme, in denen digitale Nachweise über Organisations- und Ländergrenzen hinweg sicher und unfälschbar ausgetauscht und überprüft werden können. Im Folgenden werden Beispiele genannt. Dabei sind die Beziehungen der Issuer, Verifier und Holder im Vordergrund zu stellen, sowie welche Funktionalität im Vordergrund steht (Ausweis, Login oder Signatur).

- **G2C Anwendungsfälle**: digitalswitzerland ist der Meinung, dass G2C-Anwendungsfälle (E-Government) über den föderalen Ebenen hinweg der Ausgangspunkt sein sollten (z.B. kantonale Fahrzeugzulassung). Sie schaffen das Vertrauen der Enduser in die staatliche E-ID und können so weiteren Anwendungsfällen im B2C- und G2B2C-Bereich den Weg ebnen.
- **B2C Anwendungsfälle**: Hier werden Beispiele aufgegriffen, die im Diskussionspapier des Bundes aufgeführt werden. Mit einer geeigneten E-ID könnte bei Handlungen (z.B. Alkohol- oder Medikamentenverkäufe), die eine Überprüfung bestimmter Identitätsattribute erfordern, sichergestellt werden, dass nur die minimal notwendigen Daten (z.B. binäres Attribut «Volljährigkeit») übermittelt werden. Die Liste an Anwendungsfällen kann ergänzt werden mit Interaktionen zwischen Nutzer und Organisation in welchen Qualifikationen und (Zugangs-) Berechtigungen aller Art notwendig sind (z.B. Ausbildungs- und Gesundheitsnachweise, Herkunftszeugnisse, Mitarbeiter- und Mitgliedschaftsausweise).
- **G2B2C Anwendungsfälle**: Als Beispiel wird die Meldeschein-Pflicht bei Hotel Check-Ins aufgeführt. Der Gast muss beim Check-In dem Hotel gewisse Identitätsattribute nachweisen können. Das Hotel ist verpflichtet, diese Liste an Attributen via Meldeschein der kantonalen Behörde weiterzuleiten. Die Liste an Attributen und wie diese übermittelt, bzw. gespeichert werden muss, unterscheidet sich kantonal. Eine E-ID Lösung basierend auf den oben aufgeführten technischen Anforderungen würde für Hotel und Behörden erhebliche Effizienzgewinne und eine besseres Gästeerlebnis ermöglichen.

3.3 Was ist der Nutzen einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise auszustellen und überprüfen zu können?

Eine solche digitale Infrastruktur, welche wir als ein Ökosystem des Ambitions-Niveau 3 verstehen, hat folgenden Nutzen:

- **Vertrauenswürdigkeit**: Die dezentrale Ausstellung/Überprüfung digitaler Nachweise ist ideal, um auf die Bedürfnisse von mehr Datenschutz- und Hoheit sowie Datensparsamkeit einzugehen. Dies schafft Vertrauen in Anwendungen und den digitalen Raum.
- **Sicherheit**: Digitale Nachweise zwischen Subjekten (z.B. Personen, Organisationen oder Dinge) können sicher und unfälschbar ausgetauscht sowie überprüft werden. Die erhöhte Sicherheit bietet Möglichkeiten für neue Angebote und steigert ebenfalls das Vertrauen.
- **Erweiterbarkeit**: Digitale Nachweise in einem Ökosystem des Ambitions-Niveau 3 können organisations- und grenzüberschreitend eingesetzt werden, und bewahren die internationale Anschlussmöglichkeit.

Die vertrauenswürdige, sichere und erweiterbare Infrastruktur ist die Grundlage, damit der potenzielle Nutzen sowie volks- und betriebswirtschaftliche Mehrwerte der Digitalisierung in der Schweiz bestmöglich ausgeschöpft werden können. digitalswitzerland ist überzeugt, dass das Ambitions-Niveau das Ausschöpfungspotential der digitalen Transformation und die Wettbewerbsfähigkeit der Schweiz bestimmen wird. Das Ambitions-Niveau 3 ermöglicht es, die Schweiz international wettbewerbsfähig zu halten und (digitale) Innovationen zu fördern.

3.4 Abschliessende Bemerkungen

Damit der volle Nutzen einer E-ID-Infrastruktur ausgeschöpft werden kann, müssen die Governance-Grundsatzfragen und technischen Standards geklärt werden. Erst dann können Anwendungsfälle dynamisch entwickelt und kontinuierlich an die Bedürfnisse der Nutzer:innen angepasst werden. Es ist daher von Bedeutung, dass wir unter Einbeziehung der Schweizer Wirtschaft, der Wissenschaft und ziviler Akteure zusammenarbeiten, um:

- Governance-Grundsatzfragen breit abzustimmen;
- technische Standards zu vervollständigen;
- Pilot-Anwendungen durchzusetzen für eine frühe Klärung von Fragen in der Praxis.

digitalswitzerland steht mit seinem branchenübergreifenden Netzwerk von über 240 Organisationen weiterhin für den offenen Dialog bereit.

Wir danken für die Aufmerksamkeit und stehen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse,

Nicolas Bürer
Managing Director digitalswitzerland

Andreas W. Kaelin
Deputy Managing Director digitalswitzerland

Für weitere Auskünfte:
Guillaume Gabus, digitalswitzerland | Geschäftsstelle Zürich
Tel. +41 76 589 71 99 │ guillaume@digitalswitzerland.com

/ISSS information security society switzerland

Bundesamt für Justiz
Fachbereich Rechtsinformatik
Urs Paul Holenstein
3003 Bern

Bern, den 29.10.2021

Beratende Stellungnahme: Neue Lösung (SSI – Self-Sovereign Identity) zur elektronischen Identifizierung (E-ID Gesetz BGEID)

Sehr geehrte Damen und Herren

Gerne nehmen wir Stellung zum Vorschlag der Bundesverwaltung (Bundesamt für Justiz) über die mögliche Verwendung von SSI als Verfahren für die e-ID.

Vorstellung Taskforce e-ID ISSS

Die Information Security Society Switzerland (ISSS) http://www.isss.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	Breiting, Petra	– ISSS Vorstand
	Walder, Dario	– Vizepräsident ISSS
Juristen	Lehmann, Beat	– Jurist, ISSS Vorstand
	Talleri, Rocco	– Jurist Spezialgebiet Cyber Security,
	Zbinden, Reto	– Jurist, Swiss Infosec
Organisationen & Fachexperten	Annino, Umberto	– Infoguard AG (Ex-Präsident ISSS)
	Monika Stucki	– Consultant, Redguard AG
	Rickenbacher, Fridel	– Swiss IT Security AG
	Laube, Annett	– Dozentin, Berner Fachhochschule
	Hassenstein, Gerhard	– Dozent, Berner Fachhochschule

Grundsätzlich sind wir erfreut zu hören, dass sich die e-ID in Richtung einer SSI-Lösung bewegt.[1] Wir glauben, dass damit ein moderner Ansatz verfolgt wird, welcher die Kontrolle weitmöglichst in die Hände des Benutzers selbst legt. Trotzdem möchten wir auf weitere wichtige Security- und Privacy-Aspekte

[1] https://www.tagblatt.ch/schweiz/digitalisierung-die-nutzer-sollen-die-neue-e-id-selber-verwalten-dann-geht-die-post-ab-dann-kann-etwas-grosses-geschehen-ld.2194971

hinweisen, die aus unserer Sicht bei der Umsetzung der e-ID mitberücksichtigt werden sollen.[2]

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.

1.1 Selbstbestimmte elektronische Identitäten (SSI)

Nach der durch Bundesrätin Karin Keller-Sutter am 2. September 2021 gestarteten und am 14. Oktober abgeschlossenen öffentlichen Konsultation zur Ausgestaltung der e-ID, steht nun eine SSI-Lösung im Fokus.[3] Auch von der EU wurde eine SSI als Lösung gewählt. Die SSI-Lösung ist auch für die Schweiz interessant, da sie die Hauptanforderungen der sechs gleichlautenden Motionen für eine "Vertrauenswürdige staatliche E-ID" adressiert. Selbstbestimmte elektronische Identitäten sind ein vielversprechender Lösungsansatz. Wie eine SSI-Lösung im Rahmen einer künftigen staatlichen e-ID-Lösung umgesetzt werden kann, muss noch im Detail geprüft werden und sollte unter anderem die nachfolgenden Aspekte berücksichtigen.

1.2 Dezentrale Datenspeicherung / Privacy by design & default / Datensparsamkeit

In diversen politischen Vorstössen[4] wird der Bundesrat aufgefordert ”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. Dabei sollen insbesondere die Grundsätze "**privacy by design & default, Datensparsamkeit und dezentrale Datenspeicherung"** (wie Speicherung der Ausweisdaten bei den Benutzerinnen und Benutzer) eingehalten werden. Die e-ID darf auf privatwirtschaftlich entwickelten Produkten und Diensten beruhen, wobei aber die anfallenden Daten und Nutzungsprofile keinesfalls kommerziell verwendet werden dürfen. Ausserdem soll bei allfälligen privatrechtlichen Betreibern der e-ID keine zentrale Datenbank erstellt werden dürfen. Einzig die Bundesverwaltung soll über eine zentrale Datenbank verfügen.

1.3 Kompatibilität mit der Entwicklung in der EU

Bei der Entwicklung der neuen e-ID muss auf die **Kompatibilität mit der Entwicklung in der EU** geachtet werden (EU-Kommission ”Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910 / 2014[5] as regards establishing a framework for a European Digital Identity” vom 03.06.2021[6])

1.4 Anwendung auf Drittstaaten

Die Benutzer der in der Schweiz von einer zuständigen Behörde ausgestellten e-ID muss sich damit **gegenüber amtlichen und privaten Stellen im EWR identifizieren** können, wie umgekehrt die Benutzer einer von der Behörde eines EU Landes ausgestellten e-ID in der Schweiz (vgl. den Grundsatz der ”Cross-border reliance on European Digital Identity Wallets“ und dessen Anwendung auf Drittstaaten nach Art. 1 (15) (16) (18) EU Richtlinienvorschlag).

---

[2] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-85476.html

[3] https://www.tagblatt.ch/schweiz/digitalisierung-die-nutzer-sollen-die-neue-e-id-selber-verwalten-dann-geht-die-post-ab-dann-kann-etwas-grosses-geschehen-ld.2194971

[4] Sechs inhaltliche übereinstimmende Motionen (Nr. 21.3124 - 21.3128 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista#k=Vertrauensw%C3%BCrdige%20staatliche%20E-ID

[5] eIDAS Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE

[6] https://op.europa.eu/de/publication-detail/-/publication/5d88943a-c458-11eb-a925-01aa75ed71a1/language-en/format-PDF/source-search

1.5 Berücksichtigung bestehendes Recht über elektronische Dokumente

Die von einer zuständigen Behörde ausgestellten e-IDs sollten in Bezug auf Datenschutz und Datensicherheit auf das **bestehende Recht**[7] über elektronische Dokumente abgestimmt werden.

1.6 Datenschutz und IKT-Sicherheit

Basierend auf datenschutzrechtlichen und sicherheitstechnischen Anforderungen empfehlen wir eine **dezentrale e-ID Lösung**, weil diese

a. keine dem Zugriff von unberechtigten Dritten ausgesetzte zentrale Datenbank mit personenbezogenen Angaben über die ausgegebenen e-IDs und deren Benutzer voraussetzt; und

b. nach dem Grundrecht der informationellen Selbstbestimmung [welches vom Bundesgericht in ständiger Rechtsprechung anerkannt wird, so in BGE 146 I 11 und dort zitierte Entscheidungen sowie deren Besprechung in der Literatur[8]] den Benutzern der e-ID die alleinige Kontrolle über die sie betreffenden Daten ermöglicht. [9]

1.7 Kenntnisse über den Einsatz der e-ID durch den Benutzer

Die für die neue staatliche e-ID gewählte Lösung muss gewährleisten, dass die ausgebende Behörde, die Ausfertigungsstelle oder unberechtigte Dritte auf keinen Fall Informationen, Hinweise und Kenntnisse über den Einsatz der e-ID durch den Benutzer erhalten können (vgl. Art. 1 (7) Ziff. 4 (b) EU-Richtlinienvorschlag).

Des Weiteren sollten **identifizierende Angaben** im Sinne von Art. 2 Abs. 1 AwG auf der e-ID (und allfällige zusätzliche Attribute) **nur von autorisierten staatlichen Stellen** (kantonale Ausweisstelle; Passbüro; Einwohnerkontrolle) festgesellt und in die e-ID übertragen werden dürfen (vgl. Art. 4 ff AwG); sie sollten jedoch auf keinen Fall bei den Ausfertigungsstellen gespeichert werden.

1.8 Voraussetzungen für die Verwendung der AHV und UID Nummer

Zur Gewährleistung der eindeutigen Zuordnung der e-ID an eine bestimmte natürliche Person oder ein Unternehmen kann die **AHV oder UID Nummer** verwendet werden unter der Voraussetzung, dass

a. die Anforderungen an den Mindeststandard bei der systematischen Verwendung der AHV-Versichertennummer ausserhalb der AHV gemäss EDI Verordnung 831.101.4 eingehalten werden[10]; und

---

[7] Dies betrifft namentlich:

a. Datenschutz durch Technik und Datensicherheit nach dem Datenschutzgesetz in der Fassung vom 25. 09. 2020, Art. 7 und 8 (BBl 2020 7639 ff[7] sowie dem ersten Abschnitt der am 23. Juni 2021 veröffentlichten Vernehmlassungsvorlage zur revidierten Datenschutzverordnung[7]

b. Die Gesetzgebung über maschinell lesbare Ausweisschriften für Schweizer Staatsangehörige und für ausländische Personen (AwG - SR Ziff. 143);

c. Die Gesetzgebung über die öffentlichen Personenregister (RHG – SR 431.02);

d. Nachweis der gemäss Art. 9 ZGB in öffentlichen Registern (wie Grundbuch und Handelsregister) im Zivilgesetzbuch (ZGB - SR 210) und im Obligationenrecht (OR - SR 220) bezeugten Tatsachen

e. Die Regelung der Unternehmens-Identifikation (UIDG - SR 431.03);

f. Die Gesetzgebung über die elektronische Signatur (ZertES – SR 943.03);

g. Das elektronische Patientendossier (EPDG - SR 86.1)

[8] http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F146-I-11%3Ade&lang=de&type=show_document

https://forumpoenale.recht.ch/de/artikel/06fp0121auf/zulassigkeit-und-verwertbarkeit-von-polizeilichen-aufzeichnungen-der

[9] https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen--archiv/medienmitteilungen-2006/der-eid-genoessische-datenschutz--und-oeffentlichkeitsbeauftragte.html

[10] https://www.fedlex.admin.ch/eli/cc/2007/749/de

b. die AHV Nummer durch eine Hash-Funktion in nicht rückführbarer Art und Weise verschlüsselt wird [vgl. Art 36 Abs. 4 Bst. c) DSG 1992 und die als Empfehlung ausgestaltete Aufforderung des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten an Bundesrat und Parlament in seinem Tätigkeitsbericht 2016/17)[11]

c. Gemäss Handlungsregister befugte Personen sollen einem Unternehmen eindeutig zugeordnet werden können.

1.9 Ergänzende Attribute

Es wäre zu prüfen, ob und in welchem Umfang **die Benutzer der e-ID die Möglichkeit haben** sollen, die **e-ID um bestimmte Attribute**, wie besondere körperliche Merkmale nach Art. 2 Abs. 4 AwG aber auch um Angaben zu e-Health wie Gesundheits-, Blutungs- oder Medikationsrisiken; besondere Eigenschaften und Fertigkeiten wie Führerausweis Angehöriger von Feuerwehr oder Rettungsdiensten; als Nothelfer; Organspender; berufliche Qualifikationen (Abschluss im tertiären Bildungsbereich) zu ergänzen, wie dies im EU Richtlinienvorschlag Art. 1 (3) (i) (42) ff unter dem Titel "European Digital Identity Wallet" enthalten ist. Als "Attribut" gilt ein "feature, characteristic or quality of a natural or legal person, or of an entity, in electronic form" (EU-Richtlinienvorschlag Art. 3 (i) (43).

Der User der e-ID soll im Prozess einer Identifikation und auf Basis des Systems «anonymus credentials» die Möglichkeit erhalten Attribute wegzulassen bzw. die Informationsdetallierung anwendungsspezifisch anzupassen. So soll beispielsweise die Möglichkeit bestehen anzugeben, dass ein User älter als 16 Jahre ist, ohne aber sein spezifisches Alter angeben zu müssen. Dies würde die Möglichkeit erlauben, dass ein User im B2C Umfeld mit seinem ID-Atavar nach seinen persönlichen spezifischen Datenschutzanforderungen unterwegs sein könnte. Ausserdem soll auch geklärt werden, unter welchen Voraussetzungen (z.B. Datenschutz) diese eingesehen werden können (siehe Abschnitt 1.7).

1.10 Richtigkeit der Angaben

Die **Annahme der Richtigkeit der Angaben** in der von einer zuständigen Behörde erstellten e-ID sollte sich grundsätzlich auf die Identität des Benutzers im Sinne von Art. 2 Abs. 1 AwG beschränken. Insofern geniessen die sich aus öffentlichen Registern ergebenden und von der ausgebenden Stelle geprüften Angaben über die Identität der e-ID Benutzer eine Art von "öffentlichem Glauben" wie die Eintragungen im Grundbuch (Art. 973 Abs. 1 ZGB), was nach Lehre und Gerichtspraxis (BGE 133 III 368 Erw. 2.4.1 S. 375[12]) aufgrund von Art. 931a ff OR iVm Art. 1 HRegV auch für die gemäss Art. 940 OR vom Registerführer zu prüfenden Eintragungen im Handelsregister und deren in Art. 933 OR umschriebenen Wirkungen gilt.

Allenfalls könnte die **Bestätigung der Richtigkeit von Attributen durch eine dafür geschaffene, als "Qualified Trust Service Provider"** (im Sinne von Art. 1 (3) 3 (i) (4), iVm Art. 1 (39) und Annex V EU-Regulierungsvorschlag) qualifizierende, dem öffentlichen oder privaten Recht unterstehende Stelle vorgenommen werden.

Über diese Risiken und Folgen unzutreffender, möglicherweise irreführender Attribute müsste der e-ID Benutzer im Antragsverfahren durch die e-ID ausgebende Stelle unterrichtet werden. Darüber sollte eine Dokumentation vorhanden sein, die auch in Hinweisen über die Verwendung von e-ID's auf einer Webseite bestehen kann. Für die Möglichkeit der Befristung der Gültigkeit der e-ID kann auf Art. 3 AwG verwiesen werden.

[11] https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/24--taetigkeitsbericht-2016-2017/gesetz-zur-elektronischen-identitaet.html

[12] https://www.servat.unibe.ch/dfr/bge/c3133368.html

1.11 Haftung

In Bezug auf die Angaben zur Identität des e-ID Benutzers sollte **das Gemeinwesen eine Haftung** übernehmen. Dies insbesondere betreffend die Eintragungen in öffentlichen Registern sowie für die Handlungen oder Unterlassungen der mit der Ausgabe der e-ID betrauten öffentlichen Stellen gegenüber Dritten. Diese Haftung sollte nach dem anwendbaren Verantwortlichkeitsrecht oder gemäss den bereichsspezifischen Haftungsbestimmungen der e-ID Gesetzgebung übernommen werde (vgl. die Haftbarkeit aus der Führung des Grundbuchs gemäss Art. 955 ZGB, bzw. für Schäden und Verluste aus der Führung des Handelsregisters nach Art 928 OR).

Hingegen können die auf Wunsch eines e-ID Benutzers beigefügten ergänzenden Attribute im ”Digital Wallet“ nach dem EU-Richtlinienvorschlag grundsätzlich keinen ”öffentlichen Glauben” beanspruchen: Für diese zusätzlichen Angaben sollte der Benutzer der e-ID die alleinige Verantwortung und Haftung für unrichtige oder irreführende Angaben im Sinne von Art. 2 und Art 3 Abs. 1 Bst. b) und c) UWG iVm Art. 9 Abs. 3 UWG übernehmen.

Diese Zuweisung der Verantwortung und Haftung, für die auf Wunsch des Benutzers der e-ID beigefügten Attribute, sollte grundsätzlich auch dann gelten, wenn sich die Attribute auf ein Diplom oder Zeugnis im tertiären Bildungsbereich (ETH Zürich/Lausanne; Universitäten; Fachhochschulen) oder den Eintrag in einem öffentlichen Register stützen. Denn es kann nicht Aufgabe der e-ID ausgebenden Behörde sein, die betreffenden Zeugnisse und Registereintragungen zu prüfen.

1.12 Haftung des Benutzers

Haftung des e-ID Benutzers bei Abhandenkommen, Verlust, Missbrauch, Identitätsdiebstahl, Veränderung des Inhalts der e-ID sollte der e-ID Benutzer analog zur Regelung von Art. 59a OR für den Schaden haften, welche Dritte aus Vermögensdispositionen im Vertrauen auf die Angaben in der e-ID erleiden, sofern der e-ID Benutzer die Anwendung angemessener und ihm zumutbarer Sicherheitsmassnahmen unterlassen hat.

Die vom e-ID Benutzer zu treffenden angemessene Sicherheitsmassnahmen sollten namentlich die nach den Umständen raschmöglichste Anzeige [schriftlich; (fern-)mündlich; elektronisch oder in einer anderen Form der Übermittlung, welche im Sinne von Art. 5 Abs. 1 IPRG - SR 291 den Nachweis durch Text ermöglicht] von Verlust, Abhandenkommen oder Preisgabe der e-ID sowie von Anzeichen des möglichen Zugriffs, Veränderung und Missbrauch durch Unberechtigte umfassen (vgl. Art. 8 AwG; Art. 13Abs. 2 VZertES).

Als Empfänger dieser Meldung können die ausgebenden Stellen, die Polizei bzw. das NCSC bezeichnet werden. Angaben übe die Anzeigepflicht und die Kontaktangaben der Mitteilungsempfänger sollten in der Dokumentation zu den ausgegebenen e-ID’s bzw. auf einer öffentlich zugänglichen Webseite aufgeführt sein

Angesichts des mit dem Erwerb und der Nutzung der e-ID verbundenen Risiken sollten die Ausgabestellen die Antragsteller / Erwerber der e-ID über diese Risiken aufklären und geeignete Datenschutz- und Sicherheitsmassnahmen empfehlen (vgl. die Regelung bei Elektronischen Patientendossiers zur Information des Patienten nach Art. 15 Abs. 2 und Art. 25 Abs. 5 EPDV[13])

[13] https://www.fedlex.admin.ch/eli/cc/2017/204/de

1.13 Ermächtigung des Bundesrates

Der Bundesrat sollte ermächtigt und verpflichtet werden, in einer **Verordnung die Anforderungen an die Sicherheit der e-ID, insbesondere vor Fälschung, unerlaubtem Zugriff, Missbrauch und Identitätsdiebstahl festzulegen**, welche die ausgebende Stelle einerseits und die Benutzer der e-ID andererseits zu beachten haben; dabei könnten auch in diesem Punkt Erfahrungen mit dem Covid Zertifikat genutzt werden.

Zur Gewährleistung optimaler Sicherheit sollte - ähnlich wie beim Covid Zertifikat - das Quellenprogramm (”*Source Code*”) der e-ID Lösung öffentlich zugänglich sein und einer öffentlichen Sicherheitsprüfung, z-B. durch ”Ethical Hacking“ und ”Penetration Tests“ unterliegen. Zu einer derartigen öffentlichen e-ID Sicherheitsprüfung könnten - auf Einladung und unter Leitung des Nationalen Zentrums von Cybersicherheit (NCSC[14]) die Abteilungen für Informatiksicherheit der ETH in Zürich (Swiss Support Center for Cybersecurity[15]) und Lausanne, unserer Universitäten und Fachhochschulen aufgefordert werden,

Die ausgebenden Stellen sollte die Sicherheit der e-ID periodisch überprüfen und anpassen, allenfalls durch die Bereitstellung von Korrekturcodes (”*Patches*”) zum Abruf durch die e-ID Benutzer bei der gemäss vorstehender Ziff. 14/15 empfohlenen dezentraler Ausgestaltung der e-ID

1.14 Neue Straftatbestände

Angesichts der Entwicklung der Informationstechnologie wäre zu überprüfen, ob bei der Entwicklung von **bereichsspezifischen Regelungen über die Einführung der staatlichen e-ID oder im StGB** neue Straftatbestände über unerlaubte Eingriffe in die e-ID wie unbefugte Veränderung, Missbrauch, Identitätsdiebstahl einzuführen, bzw. bestehende Straftatbestände zu ergänzen wären (vgl. die Interpellation 13.3726 Jean Christophe Schwaab, vom 18.09. 2013 betreffend ”Identitätsmissbrauch“[16]

Im Namen des ISSS bedanken wir uns bereits im Voraus für die Berücksichtigung unserer Stellungnahme.

[14] https://www.ncsc.admin.ch/ncsc/de/home.html

[15] https://sscc.ethz.ch/

[16] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133726

Information Security Society Switzerland (ISSS) - Kochergasse 6 - 3011 Bern - sekretariat(at)isss.ch - +41 31 311 53 00

Mit freundlichen Grüssen

ARIÉ MALZ
CO-PRÄSIDENT

DARIO WALDER
VIZE-PRÄSIDENT

Information Security Society Switzerland (ISSS)
Kochergasse 6
3011 Bern
E-Mail: president@isss.ch
E-Mail: vicepresident@isss.ch

Stellungnahme NEDIK bezüglich E-ID

Der Bundesrat ist bezüglich E-ID um eine rasche Weiterentwicklung bemüht und möchte rasch die Möglichkeit für eine staatliche digitale Identität schaffen. Bevor er die Eckwerte für die künftige E-ID bestimmt, sollen sich relevante Stellen und auch die breite Öffentlichkeit aktiv in die Diskussion einbringen können.

Nach Absprache mit PTI erachtet auch NEDIK die Anwendungsfelder im Bereich eGovernment (Anzeigeerstattung, Kommunikation mit Bürgern, Anträge sowie Dateneinlieferung und Signierung), Personenkontrollen bzw. Abfragen und eine eventuelle Nutzung durch Polizeimitarbeitende (Login, starke Authentifizierung, interne Zwecke) als Möglichkeiten, die geprüft werden können. Es gilt zu bedenken, dass diese Anwendungsfelder nur dann sinnvoll umgesetzt werden können, wenn die E-ID höchsten Sicherheitsstandards entsprechen kann und eine breite Akzeptanz erfährt. Missbrauchsmöglichkeiten und Fragen des System- sowie Datenschutzes sind in den Entstehungsprozess einzubeziehen.

Im Bereich Cyberbetrug, beispielsweise in Fällen von Nichtliefern auf Kleinanzeigeplattformen (Käufer geschädigt) oder Missbrauchen von Online-Zahlungssyst./Wertkarten oder einer fremden Identität, kann eine E-ID zu mehr Sicherheit beitragen. Dies jedoch nur unter der Voraussetzung einer stark gesicherten Umsetzung. Es ist jedoch auch in diesem Fall davon auszugehen, dass die Täterschaft rasch Möglichkeiten zum Missbrauch ausloten wird, was den Nutzen in diesem Bereich stark reduzieren kann.

Eine hohe Akzeptanz in Politik und Bevölkerung, Unterstützung der eGov und eine flexible An- und Einbindung von eigenen ICT-Anwendungen erscheinen auch NEDIK als relevante Punkte. Besonderen Fokus legen wir darauf, dass mit der E-ID eine verbreitete, sichere und verlässliche Anwendung geschaffen werden muss, um deren Anwendung zukunftsgerichtet gestalten zu können.

NEDIK konnte in den Kantonen eine erste Kurzumfrage zum Thema durchführen. Grundsätzlich sind die Korps gegenüber der E-ID positiv eingestellt und sehen diverse Anwendungsfelder. Gleichzeitig werden aber auch die Limitationen sowie Risiken der E-ID betont und die Rolle von ausschliesslich staatlichen Stellen unterstrichen. Es wird zudem darauf verwiesen, dass die Einführung der E-ID gemäss Abstimmung vom 07.03.2021 abgelehnt wurde.

Ausführlichere Antworten aus den Korps würden eine umfassendere Anfrage und vertiefte Bearbeitung voraussetzen. Die folgenden Punkte möchte NEDIK bezüglich der übermittelten Fragen nach momentanem Stand des Austausches zusätzlich kommentieren.

- *Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?*
  Mit einer E-ID können natürliche Personen ihre Identität bei webbasierten Dienstleistungen (Online-Portalen) sicher und rechtsverbindlich verifizieren. Dies schliesst sowohl behördliche wie auch private Dienstleistungen ein. Eine missbräuchliche Verwendung von Identitäten auf Online-Portalen jeglicher Art, insbesondere privater Dienstleister wie Online-Shops, könnten dadurch reduziert werden. Die Kommunikation mit Behörden und behördlichen webbasierten Dienstleistungen (Abstimmungen, Steuererklärungen, Suisse ePolice etc.) können einfacher zugänglich gemacht werden. Ein Mehrwert für die Polizeiarbeit (beispielsweise in der elektronischen Fallbearbeitungen) und Anwendungen innerhalb der Polizei als Organisation (z.B. Anmelden in den eigenen Systemen) bleiben ebenso zu prüfen wie mögliche Gefahren (missbräuchliche Verwendung etc.).

- *Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?*
  Die E-ID muss vollständig von einer öffentlichen Stelle (Bund und/ oder Kanton) verwaltet werden. Auf keinen Fall sollten private Partner beteiligt werden. Eine staatliche E-ID hat manipulations- und fälschungssicher sowie authentifizierungssicher zu sein und hohen Datenschutzrichtlinien genügen. Sie sollte zudem einfach in der Handhabung und online sowie offline einsetzbar sein. Der Herausgeber Die Nutzungsdaten und die Identifizierungsdaten müssen unabhängig bei verschiedenen Gesellschaften verwaltet werden. Ein E-ID-Herausgeber darf nicht wissen, wie die Besitzer der E-ID diese nutzen (Privacy by Design). Staatliche Stellen dürfen keine Registerdaten an Private liefern, sondern lediglich die Richtigkeit der vom Benutzer selbst gelieferten Daten bestätigen. Der Besitz einer E-ID darf nicht erzwungen werden. Benutzer ohne E-ID dürfen nicht unnötig oder unfair benachteiligt werden. Edierte Daten müssen zeitnah und vollständig (Protokoll, etc.) jederzeit zugänglich gemacht werden können.

- *Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?*
  Idealerweise kann mit einer E-ID eine zentrale Vertrauensstelle (der Staat als Kontrollinstanz) geschaffen, der Verwaltungsaufwand verkleinert, Prozesse beschleunigt, Kosten gesenkt und Synergien genutzt werden (Staat und Private). Die setzt jedoch eine entsprechende Umsetzung voraus. Eine Harmonisierung nationaler Prozesse ergibt schon von sich aus einen Mehrwert für die Endkunden. Die Konsequenz wären nicht nur harmonisierte Dokumente, sondern auch harmonisierte Abläufe zur Erlangung eben dieser, unabhängig von der kantonalen Zugehörigkeit eines Bürgers. Die vereinfachte Überprüfung dieser Dokumente durch Behörden wäre ein weiterer Vorteil einer nationalen Infrastruktur. Im Strafverfahren (bei Editionen von Staatsanwaltschaften) gibt es zudem eine zentrale Auskunftsstelle. Die E-ID könnte zudem zukünftig als Identifikationsmittel für die Ausstellung eines Signiermittels (digitale Signatur) genutzt werden. Mit einer nationalen Infrastruktur können weiter wichtige, aber tatsächlich sehr selten gebrauchte Dokumente (z.B. MA-Ausweis, Ausbildungsnachweis, usw.) zentral aufbewahrt werden und sind im Bedarfsfall jederzeit geordnet abrufbar. Dies in digitaler Form, was eine Implementierung in digitalisierte Systeme von Dritten (Online-Portale usw.) unkompliziert ermöglichen würde. Auch erhöhte Sicherheit und geringere Risiken des Identitätsdiebstahls können erreicht werden. Dies setzt jedoch eine klare Priorisierung des Daten- und Systemschutzes voraus. Wird dies verfehlt, drohen im Gegensatz zusätzliche Risiken.

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail zugestellt an: E-ID@bj.admin.ch

Zürich, 7. Oktober 2021

Öffentliche Anhörung zum Diskussionspapier zum «Zielbild E-ID»

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren,

In dieser Stellungnahme beziehen wir uns auf die am 02. September 2021 eröffnete öffentliche Anhörung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zum Diskussionspapier «Zielbild E-ID». Wir bedanken uns für die Konsultation in dieser wichtigen Angelegenheit.

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. Unsere Arbeitsgruppe Regulations beschäftigt sich mit Gesetzgebung und Regulierung rund um diese Themengebiete.

Unserer Meinung nach wird sich der gesellschaftliche Konsens in Richtung Ambitions-Niveau 3 und Self-Sovereign Identity (SSI) entwickeln. Dies ist gleichbedeutend mit einem umfassenden Ökosystem digitaler Beweise und geht einher mit einer gesamtheitlichen digitalen Integration vieler verschiedenen Dokumente. Unseres Erachtens ist der SSI-Ansatz den anderen vom Bund vorgestellten Ansätzen überlegen.

Die Schweizer Variante sollte grundsätzlich der europäischen Variante der elektronischen ID, der EUid, interoperabel sein. Dies schafft EU-weite Anerkennung und somit europaweite Nutzbarkeit der Schweizer Lösung. Da der Prozess der Überarbeitung der betreffenden eIDAS-Richtlinie noch nicht abgeschlossen ist, ist ein konkreter Bezug auf die EU-Lösung derzeit zwar noch nicht möglich, jedoch sind die Arbeiten zu koordinieren. Darüber hinaus sollte auch die Interoperabilität mit nicht-EU-Ländern, wie beispielsweise UK oder der USA und deren Identitäts-Ökosystemen im Auge behalten werden. Neben Zusammenarbeit und Kooperation innerhalb eines Landes und zwischen den Ländern ist dementsprechend auch die Koordination mit globalen Standards wichtig.

Wir sind überzeugt, dass die E-ID mehrere Vorteile gegenüber den konventionellen Identifizierungs-mechanismen aufweist. Deswegen wollen wir im Folgenden die drei im Diskussionspapier genannten Fragen klären, auf mögliche Vorteile einer staatlich anerkannten Lösung eingehen und Vorschläge einbringen, wie man den offenen Fragen zum SSI-Ansatz begegnen könnte.

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Unser Alltag wird zunehmend digital. Dieser Wandel geschieht nicht stetig, sondern dessen Geschwindigkeit nimmt kontinuierlich zu. In dieser Hinsicht wird es immer wichtiger, dass unser

„digitales Gegenüber“ ausreichend identifiziert ist. Dies muss auf Basis einer gesetzlich anerkannten Lösung möglich sein. Nur eine solche schafft massengeschäftstaugliche Rechtssicherheit. Eine solche "Vertragssicherheit" muss auch im Zeitalter der Digitalisierung gewährleistet werden. Mithilfe der Einführung einer staatlich anerkannten elektronischen Identität könnte im Idealfall eine umfassende Lösung geboten werden. Ziel muss sein, dass sich Schweizer Bürgerinnen und Bürger sowie Firmen eindeutig, sicher und benutzerfreundlich digital ausweisen können.

Mithilfe der E-ID könnten **Behördengänge**, beispielsweise bei der Einholung notwendiger Dokumente zur Gründung einer Firma, die Bestellung des Betreibungsregisterauszugs oder die Durchführung grundbuchlicher Transaktionen effizienter sowohl für die Behörden als auch für einzelne Bürger gestaltet werden. Ferner erhöht sich die **Sicherheit bei Geschäftsbeziehungen**, da Geschäftspartner und Kunden mit hoher Sicherheit identifiziert werden können.

Die Grundlage eines jeden wirtschaftlichen Erfolgs besteht darin, dass die betreffenden Vertragsparteien sich gegenseitig vertrauen. Da sich unsere Prozesse und Dienstleistungen immer stärker in den digitalen Raum verschieben, benötigen wir einen sicheren Zugriff auf unsere Daten. Sowohl Unternehmen als auch deren Kunden würden von einer digitalen Identifikation profitieren. Alltägliche Prozesse wie beispielsweise digitale Vertragsabschlüsse oder Einkäufe, sowie das **KYC («Know-Your-Customer»)** könnten durch die E-ID starke Effizienzsteigerungen erfahren. Des Weiteren sind wir überzeugt, dass die elektronische Identität den Weg für weitere, bisher noch unbekannte, technische Lösungen ebnet.

Aus parlamentarischer Perspektive würde die Schaffung einer E-ID beispielsweise die Umsetzung der folgenden Motionen unterstützen bzw. ermöglichen:

a) Motion 21.3180 Vollständig digitale Unternehmensgründung sicherstellen von NR Andri Silberschmidt (FDP, Zürich) vom 16.3.2021

und

b) Motion 20.4356 Digitaler Fahrzeug- und Führerausweis von NR Franz Grüter (SVP, Luzern); vom 30.11.2020

Vorgenannte Ausprägungen sind nur beispielhaft zu verstehen. Digitale Prozesse sind gegenüber "physischen" generell wesentlich effizienter, rascher und kostengünstiger, was letztlich auch dem Kunden bzw. Konsumenten zu Gute kommt. Eine gesetzlich anerkannte E-ID ist letztlich notwendige Grundlage für jede digital angebotene Dienstleistung des Staates und für jedes digital angebotene Geschäftsmodell der Wirtschaft. Innovation wird insbesondere auch durch Wettbewerb gefördert. Daher halten wir es für wichtig, dass die Möglichkeit besteht, dass sich mehrere ID Anbieter etablieren können, die die staatlichen Vorgaben erfüllen und entsprechend zertifiziert werden. Eine gesetzlich anerkannte E-ID unterstützt damit nachhaltig Innovationskraft und damit auch Attraktivität des Wirtschaftsstandorts Schweiz.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Der **Zugang** zu, der **Zugriff** auf und die **Nutzung** der E-ID muss für die User ohne nennenswerte Schwierigkeiten, möglichst bequem und trotzdem sicher, gewährleistet werden. Die weite Akzeptanz und die einhergehende fortschreitende Digitalisierung unserer Gesellschaft wird nur dann vorhanden sein, wenn die Aspekte der einfachen und raschen Erhältlichkeit, der **Benutzerfreundlichkeit** und der **Transparenz**, insbesondere zur Wahrung des Vertrauens, greifbar sind.

Die drei wichtigsten, hier beschriebenen, Anforderungen sind: **Zugänglichkeit**, **Benutzer-freundlichkeit** und **Transparenz**. Zugänglichkeit und Benutzerfreundlichkeit sind aus unserer Sicht eng miteinander verbunden. Transparenz ist aus unserer Sicht insbesondere auch eine Aufgabe der begleitenden Kommunikation; weniger eine Anforderung an die Lösung selbst.

Ergänzend sehen wir die **Fokussierung auf privatwirtschaftliche Anwendungsbereiche** und die Schaffung allgemeingültiger Richtlinien, die den **Wettbewerb** zulassen und fördern, als wichtige Anforderungen für ein nachhaltiges ID Ökosystem.

Der *erste* Punkt des **einfachen Zugangs, Zugriffs und Nutzung** impliziert, dass die gesamte Schweizer Bevölkerung in der Lage sein muss, auf ein staatlich anerkanntes elektronisches Identifikationsmittel zurückgreifen zu können. Die rasche Durchdringung der Schweizer Bevölkerung in den ersten Monaten der Verfügbarkeit wird sich als unabdinglich erweisen in der erfolgreichen Integration der E-ID.. Die administrativen Prozesse zum Erhalt der E-ID sollten also kurz und unkompliziert gestaltet werden. Das Login sollte so intuitiv und zeiteffizient sein, dass eine grosse Zahl Nutzer innerhalb kürzester Zeit die Plattform der E-ID benützt. Jedoch darf damit unter keinen Umständen ein Minus bei Sicherheit und Integrität der E-ID einhergehen.

Zweitens ist es für die Akzeptanz der E-ID essenziell, dass eine **hohe Benutzerfreundlichkeit** besteht. Das User Interface sowie der Identifikationsprozess müssen übersichtlich sein. Ferner muss ein Ziel der Einführung der E-ID sein, dass es ohne lange Übergangsperiode allfällig notwendige Behördengänge auf Gemeinde- und auf Bundesebene ersetzt. Ferner sollten Unternehmen sowie Privatpersonen nicht durch unnötige Komplexität der einzelnen Funktionen bei der Einführung der E-ID überwältigt werden. Die Abwicklung von Geschäftsprozessen (z.B. Verträge) und alltäglichen Transaktionen (z.B. der Kauf eines ÖV-Tickets oder die Bestellung eines Betreibungsregister-auszugs) muss schnell und unkompliziert vonstattengehen. Des Weiteren wird es wichtig sein, eine Vereinheitlichung und Kompatibilität der E-ID zumindest auf europäischer Ebene anzustreben. Zusätzlich wird die Nutzerakzeptanz durch eine hohe Alltagsrelevanz sichergestellt. Hierzu ist eine breite privatwirtschaftliche Akzeptanz mit Anwendungsfällen über behördliche Anwendung hinaus essenziell.*Drittens* muss der Bund für **Transparenz und Verständnis** der Materie sorgen, denn nur so kann das notwendige Vertrauen der Bevölkerung in die neuartige Identifikationsmöglichkeit entstehen. Dazu gehört auch, die verschiedenen 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 dessen Funktionsweise sollten konsequent aufgezeigt werden. Allfällige Ängste der Bevölkerung, dass eine elektronische Identität in Richtung eines digitalen Überwachungsstaates geht, müssen von Anfang an proaktiv unterbunden werden. Ein wiederverwendbarer digitaler Identitätsservice ist nicht möglich ohne das klare Verständnis, Vertrauen und Engagement eines jeden Benutzer.

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z.B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Die **Sicherheit** vieler Anmeldeverfahren wird oftmals reduziert, indem Passwörter z.B. mehrfach verwendet oder sogar aufgeschrieben werdenMit 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 wie erwähnt 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. **Der elektronische Geschäftsverkehr würde somit sicherer werden und die Privatsphäre eines Einzelnen besser gewahrt werden können** 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 entsprechende EU-Lösungen gesichert ist.

Wie ordnen wir die im Diskussionspapier erwähnten Nachteile zum SSI-Ansatz ein?

Die SSI kann als derzeit komplexeste Entwicklungsstufe digitaler Identitäten gesehen werden. Das Ziel der SSI ist, die Probleme und Herausforderungen der existierenden Identitätsverwaltungssystemen zu lösen. Die Nachteile bei der Umsetzung der SSI-Prinzipien hängen dabei von der konkreten technischen Umsetzung ab. Eine technologie-offene, ergebnisorientierte Definition der Ziele der E-ID ermöglicht die Umsetzung mit den an den besten geeigneten technologischen Lösungen.

Zwar ist der SSI-Ansatz neu und unbekannt. Trotzdem ist zu beachten, dass **der SSI-Ansatz die möglichen Entwicklungsstufen der beiden alternativen Ansätzen (Public-Key-Infrastruktur und zentraler staatlicher Identitätsprovider) vorwegnehmen würde.** Es ist denkbar, dass eine Einführung mit Verzicht auf die Implementierung eines kompletten Ökosystems im Nachhinein als nicht ausreichend betrachtet werden wird. Dies könnte nämlich genau dann geschehen, wenn die umfassenden Vorteile den Usern ersichtlich werden.

Unserer Ansicht nach ist der SSI-Ansatz den anderen vom Bund vorgestellten Ansätzen überlegen. Ferner sind wir überzeugt, dass das Bewusstsein über dessen Fähigkeiten zügig entstehen wird. Die Voraussetzung dafür ist lediglich die lückenlose, unkomplizierte und ganzheitliche Implementierung des Ansatzes. Als ersten Schritt sollten dementsprechend noch offene Grundsatzfragen und Standards geklärt und erläutert werden.

Ein SSI-System basiert auf einem **dezentralen Ansatz.** Die Verantwortung zur Verwaltung der Identität (verified credentials) liegt bei dem einzelnen User und lässt nur wenig Hilfestellung zu. Unter kritischer Betrachtungsweise könnte man meinen, dass dies Unsicherheit auslöse und Wege zur Manipulation eröffne. Dem muss durch eine starke Governance vorgebeugt werden. Durch ein Zertifizierungssystem für Issuer kann beispielsweise Identitätsmissbrauch abgewehrt werden. Zusätzlich können Wallet-Provider dem User Hilfestellung bei der Anwendung der E-ID leisten. Um das Problem der forensischen Aufklärungsschwierigkeiten zu lindern, könnte man auf die bereits bekannte und oftmals verwendete **2-Faktor-Authentifizierung** zurückgreifen.

Offene Fragen zum SSI-Ansatz

Welche Governance-Ebenen gibt es und wer ist dafür zuständig (z. B. Governance-Ebenen nach Trust over IP Framework: Ökosystem, Credentials, Provider, Utility)?

Generell betrachtet, sorgt eine gute Governance für mehr Sicherheit, indem Verfahren und Rechenschaftspflicht vorgesehen werden. Governance ist besonders für die universelle Interoperabilität von entscheidender Bedeutung, da alle Teilnehmer des Netzwerks in der Lage sein müssen, selbst zu entscheiden, wem und was sie vertrauen wollen. Die **vier Ebenen des «Trust-**

over-IP-Frameworks» erscheinen im Zusammenhang mit einer SSI sinnvoll. Auf jeder Ebene bedarf es einer Publikation des erstrebten Governance-Frameworks.

Auf der *ersten Ebene* sollte der Bund und die von ihm zertifizierten Parteien ihre verschiedenen Zuständigkeiten erarbeiten. Bei der Erstellung der Governance des gesamten Ökosystem sollten möglichst viele Parteien involviert werden. Auf der *zweiten Stufe* sollte der Staat nur noch das Registry für staatlich beauftragte Aufgaben übernehmen (Pass, Führerschein etc.) und genügend Raum lassen für externe Ersteller von Registries. Gleichzeitig muss aber sichergestellt werden, dass die verschiedenen Systeme untereinander interagieren und die Governance untereinander abgestimmt wird. Auf der *dritten und vierten Ebene* können ein höherer Grad an Autonomie bestehen. Solange die Funktionsweise nicht beeinträchtigt wird, sollte aktiv dafür gesorgt werden, dass verschiedene Lösungen angeboten werden. Mit Blick auf die grossen Unterschiede zwischen verschiedenen Arten von Dienstleistungen oder Geschäftsmodellen ist dies ebenso sinnvoll wie notwendig. **Das Governance-Framework sollte zwar bestimmte Mindestvorgaben erfüllen, schlussendlich sollen sich aber die Lösungen durchsetzen, die am wettbewerbsfähigsten sind. Zu diesem Zweck muss der Aufbau der Governance nach bewährtem Schweizerischen Ansatz prinzipien- und risikobasiert sowie proportional (verhältnismässig) und überdies wettbewerbs- und technologieneutral erfolgen.** Gestützt darauf können effiziente Dienstleistungs- und Geschäftsmodelle entwickelt werden, welche den konkreten Verhältnissen gerecht werden und z.B. je nach Umfang, Komplexität und Risiko auch unterschiedliche Sicherheitsstandards zum Einsatz bringen können.

Muss der Staat auf gewissen Komponenten das Monopol haben? Müssen Wallets staatlich zertifiziert werden? Wird die Auswahl von Wallet und Institutional Agent dem User überlassen? Gibt es eine Regelung, welche Teile kooperativ, welche in Konkurrenz erstellt und betrieben werden?

Wir sind der Ansicht, dass sich die digitale Identität **nutzerzentriert** gestaltet sein muss. Das bedeutet, dass sie dem Einzelnen gehört, von ihm verwaltet und kontrolliert wird. Damit die digitalen Interaktionen funktionieren, müssen die beteiligten Organisationen die digitale Identität **akzeptieren**.

Deswegen schlagen wir vor, dass **gewisse sicherheitsrelevante Komponenten weiterhin einer monopolistischen Kontrolle des Staates** bedürfen, darunter fallen beispielsweise das Ausstellen von Pässen oder Führerscheinen. Die Delegation dieser Autorität wäre kritisch zu betrachten und sicherlich nicht förderlich für den Aufbau des Vertrauens der User in die E-ID. Hingegen sollten nicht-staatlich angebotene Dienstleistungen nicht zwingend von staatlichen Behörden ausgestellt werden müssen. Es macht keinen Sinn, Kinotickets und Zooeintritte als ähnlich essenziell zu betrachten wie Reisepässe und Führerscheine.. Dementsprechend müsste der Staat nicht als Issuer von jeglichen Dokumenten des gesellschaftlichen Lebens fungieren.

Die E-ID sollte zulassen, dass **mehr als ein Wallet** für digitale Identitäten verwendet werden kann. D.h., dass Wallets **frei wählbar** sein sollten und nicht staatlich zur Verfügung gestellt werden müssen. Die Wallets sollten selbstverständlich interoperabel und somit wettbewerbsfähig sein. Als Folge sollte ein innovativer Markt entstehen, der den Bedürfnissen der Verbraucher am besten gerecht wird. Es erscheint trotzdem sinnvoll, eine **staatliche Zertifizierung** für Wallets anzubieten, um das Vertrauen in das digitale Wallet zu erhöhen. Des Weiteren können einzelne kantonale Behörden die Rolle des Wallet-Anbieters wahrnehmen werden, um ihrer Bevölkerung z.B. massgeschneiderte Services anzubieten.

Die Stufe der einzelnen **Verifier benötigt keine staatliche Autorität** beispielsweise zur Kontrolle der Gültigkeit der einzelnen Dokumente. Ähnlich wie beim Covid-Zertifikat würde lediglich ein Abgleich stattfinden, um die Gültigkeit zu überprüfen.

Wer betreibt die Registry? Ist eine eigene, nationale Registry nötig oder schliesst man sich einem bestehenden, internationalen Ökosystem an? Wollen oder sollen Kantone, Städte oder private Unternehmen Speicher-Knoten (Nodes) betreiben dürfen? Welche Technologie wäre zu bevorzugen? Welche Rolle spielt die Datenmenge? Wie löst man Interoperabilitätsfragen zu anderen Registries? Besteht für den Issuer sogar die Wahlfreiheit der Registry?

Das Covid-Zertifikat zeigt auf, dass eine europaweite Gültigkeit einer Registry möglich ist. Jedes teilnehmende Land sollte also dafür sorgen, dass **mindestens eine staatliche Registry** zur Verfügung steht. Trotzdem sollte man sich nicht auf eine einzelne Registry pro Staat verlassen und **auch weitere, dezentrale Nodes** zulassen. Dies sollte auch dann zutreffen, wenn Länder verschiedene Identifizierungstechnologie verwenden.

Solange die Datensicherheit gewahrt bleibt, sollte **keine Einschränkung bezüglich Anbieter von Registries** bestehen. Diese Anbieter können entweder kantonal, städtisch oder privat finanziert zur Verfügung gestellt werden und sollten zum Ziel haben, das Vertrauen in das Ökosystem zu erhöhen. Des Weiteren sollte das Registry für nicht-staatlich angebotene Dokumente frei wählbar sein. Letzteres impliziert aber, dass **jeder einzelne Node zertifiziert** und gelegentlich überprüft werden sollte.

Wer darf Issuer sein? Bleibt das System völlig offen zum Gewinn zusätzlicher Anwendungsfälle oder werden die Issuer spezifisch ausgewählt oder berechtigt?

Um die Legitimation und Anwendung des digitalen Ausweises zu fördern, sollten die Limitierungen des Systems möglichst gering sein. Eine **Dezentralisierung der Befugnis zur Ausstellung** erscheint sinnvoll. Diesbezüglich sollten die Kontrolle und Übersicht über das Ausstellen von digitalen Dokumenten aber nicht abgegeben werden. Bevor beispielweise eine dezentrale Partei die Lizenz zur Ausstellung eines digitalen Dokuments erhielte, sollte es von einer staatlichen Partei **zertifiziert** werden.

Wie werden Backups und Transfers von Credentials ermöglicht? Wie können zentrale Backups und damit attraktive Hacker-Angriffsziele vermieden werden? Welche Rolle spielt eine mögliche kryptografische Verbindung zwischen Wallet und Verified Credentials?

Wir schlagen vor, dass eine **Verpflichtung** zur kryptografischen Verschlüsselung für alle E-ID-Beteiligten bestehen sollte. Das Vertrauen der User kann nur dann erhalten werden, wenn für eine sichere Handhabung der persönlichen Daten gesorgt wird. Es ist deshalb ratsam, regelmässige Kontrollen zur Verhinderung oder Aufdeckung von Betrug einzurichten.

Welche Sicherheitsmechanismen sind für den Zugriff zur Wallet nötig?

Wie bereits erwähnt könnte man hierbei auf eine **2-Faktor-Authentifizierung oder biometrische Verifizierung** mittels Fingerabdrucks oder Gesichtsscan zurückgreifen.

Wie können Verified Credentials auf mehreren Geräten benutzt werden? Wann wäre dies nötig? Reicht es, wenn mit dem einen Smartphone immer eine Verbindung zum Verifier aufgebaut werden kann, unabhängig davon, auf welchem anderen Gerät man gerade den nach der E-ID-fragenden Prozess initiiert hat?

Die gegenwärtig verfügbaren Möglichkeiten lassen es bereits zu, denselben Account auf mehreren Geräten zu verwenden. So könnte z.B. eine DLT-Lösung für die Protokollierung von **Mehrfach-Verwendungen** eingesetzt werden.

Wer definiert Credential-Schema, braucht es eine ausgewiesene Stelle zur Definition und Koordination (z. B. eCH) oder werden die Definitionen branchenabhängig entwickelt?

Die Definitionen sollten **branchenabhängig** entwickelt werden. Es ist zu empfehlen, diese **zentral zu hinterlegen**. Insbesondere im Falle eines Systemausfalls würde es sich als wichtig erweisen, ein Credential-Schema nicht nur an einem Ort abzuspeichern.

Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll, um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?

Unserer Meinung nach ist die erstmalige Ausstellung einer staatlichen Identität (Führerschein, Pass etc.) die Aufgabe des Staates. Eine Verknüpfung von Ausstellungsprozess und Authentifizierungsfaktoren erscheint sinnvoll. Die Sicherheit könnte dadurch erhöht werden und Manipulationsversuchen vorgebeugt werden.

Gerne stehen wir Ihnen für eine vertiefte Diskussion und für die weitere Zusammenarbeit jederzeit gerne zur Verfügung.

Freundliche Grüsse

Sig. Werner W. Wyss	Sig. Prof. Dr. Cornelia Stengel	Sig. Philipp Rosenauer
Leiter Arbeitsgruppe Regulations	Co-Director/Mitglied Arbeitsgruppe Regulations	Mitglied Arbeitsgruppe Regulations

Swico
Lagerstrasse 33
CH-8004 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Bundesamt für Justiz BJ
Herr Michael Schöll
Bundesrain 20
3003 Bern

Ausschliesslich per Mail an:
E-ID@bj.admin.ch

Zürich, 30. September 2021

Öffentliche Konsultation Zielbild E-ID: Stellungnahme

Sehr geehrter Herr Schöll, 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 650 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 Elektronikaltgeräte.

Gerne beantworten wir nachfolgend die aufgeworfenen Fragen aus dem «Diskussionspapier Zielbild E-ID» und sprechen uns darüber hinaus für Ambitionsniveau 3 im Rahmen der Ökosysteme sowie zu Gunsten des technischen Ansatzes SSI aus.

1. Drei wichtigste Anforderungen an eine staatliche E-ID als digitaler Nachweis (Frage 1 «Zielbild E-ID»)

- *Nutzerseite - Convenience, Akzeptanz und Vertrauen*:
  Für die Endnutzerinnen und Endnutzer muss die E-ID einfach, ohne Hürden und barrierefrei nutzbar sein. Dazu gehört auch, dass die Anwendung für diese kostenfrei ist. Das kürzliche Abstimmungsergebnis hat die Wichtigkeit des Vertrauens in die einzelnen beteiligten Player klar aufgezeigt. Die Einhaltung höchster Sicherheits- und Datenschutzstandards sowie der frühzeitige Einbezug unterschiedlicher Anspruchsgruppen können zum Vertrauensaufbau beitragen.

- *Technische Anforderungen - Privacy by Design, Dezentralität und Datensparsamkeit sowie Integrierbarkeit*:
  Wir befürworten den Wandel vom Prinzip «Privacy by Trust» hin zu «Privacy by Design» und den dezentralen Ansatz: Die E-ID wird somit nicht durch ein zentrales System verwaltet und es besteht keine Abhängigkeit der Nutzung davon. Um das Vertrauen der Nutzerinnen

und Nutzer zu stärken, ist Datensparsamkeit und somit die Übermittlung von ausschliesslich notwendigen Datenpunkten vom Holder an den Verifier sinnvoll. Zusätzlich ist die Möglichkeit der Integrierbarkeit in bestehende oder zukünftige Anwendungen und digitale Identitäten relevant, damit Skaleneffekte erreicht werden können

- *Internationaler Anschluss:* Es ist aus unserer Sicht wichtig, den internationalen Anschluss und eine künftige Kompatibilität mit der EU-Lösung zu erreichen bzw. den Anschluss an den rechtlichen Rahmen der EU offen zu lassen.

2. Anwendungsfälle der E-ID (Frage 2 «Zielbild E-ID»)

Mit dem Perspektivwechsel von einem reinen Log-in zu einem digitalen Ausweis und der Erschaffung einer Basis für eine ganze Infrastruktur hat die E-ID das Potenzial, alle Anwendungsfälle abzudecken, bei denen eine Identifikation nötig ist, so zum Beispiel bei der Bank oder einem Mobilabonnement.

Im Bereich E-Commerce sehen wir Grenzen für die E-ID, da es hier bereits viele niederschwellige Angebote von bestehenden Playern gibt, die beispielsweise mit einer Face-ID als Identifikationsmethode arbeiten. Dies macht es schwierig, eine echte Verbreitung und Anwendungsfälle für die E-ID in diesem Bereich zu finden.

Ein spezifisches Potenzial für den Einsatz der E-ID sehen wir im Bereich Absicherung von Reservationen: In der Schweiz haben wir bei Restaurants, Hotels und sonstige Buchungen das amerikanische Modell, mittels Absicherung durch Kreditkarte, übernommen, welches sowohl für Anbieterinnen und Anbieter als auch für Kundinnen und Kunden umständlich ist.

Wird das Ausrollen der E-ID auf alle E-Government-Transaktionen als Ausgangspunkt genommen, ist dies geeignet, um zunehmend private Anbieter einzubinden, die wiederum weitere Verknüpfungen mit ihren digitalen Identitäten herstellen können. Auch gehen wir davon aus, dass sich weitere E-ID Anwendungen mit der Zeit ergeben werden.

3. Nutzen einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können (Frage 3 «Zielbild E-ID»)

\+ Bei einer nationalen Infrastruktur sehen wir den Vorteil der Diskriminierungsfreiheit: So können beispielsweise alle Geschäfte und Firmen, die eine E-ID einsetzen wollen, dies auch tun. Handelt es sich um privat bereitgestellte Infrastrukturen, könnten die Anbieter den Einsatz der E-ID bewusst beschränken.

\+ Eine nationale Infrastruktur weist den weiteren Vorteil auf, dass der Staat bei vielen als besser geeignet wahrgenommen wird, um Vertrauen in der Zivilgesellschaft zu schaffen: Ihm kommt offenbar bei der Einhaltung Datenschutzrechtlicher Grundsätze, wie z.B. der Datensparsamkeit, eine grössere Glaubwürdigkeit zu.

– Beschränkt sich der Staat auf eine rein nationale Sicht, könnte die maximale Verbreitung und Skalierung der E-ID eingeschränkt werden: Wir erachten eine internationale Sichtweise bzw. Verbreitung als notwendig.

– Wird die technische Entwicklung der E-ID Lösung durch den Staat an Dritte ausgelagert, wird ein Teil der Kontrolle aus der Hand gegeben.

4. Ökosysteme: Ambitionsniveau 3 als stufenweise zu erreichendes Endziel

Wir betrachten das Ambitionsniveau 3 als Ökosystem digitaler Nachweise als zielführend, mit dem grössten betriebswirtschaftlichen und nutzerseitigen Mehrwertpotenzial: Sowohl staatliche als auch private Stellen müssen digitale Nachweise ausstellen können. Für die Nutzerinnen und Nutzer hat dies den Vorteil, dass die Anwendung immer identisch ist und sich damit ein kollektives Verständnis von digitalen Nachweisen etablieren kann. Auch die EU spricht sich für diese Vollvariante aus.

Dabei besteht die Möglichkeit, das Endziel etappenweise, mittels zeitlich gestaffelter Vorgänge, anzugehen, beginnend bei der Ökosystem-Variante 1 (Ausweismöglichkeit als Minimalzweck der E-ID). Darauf aufbauend, und unter Berücksichtigung der technischen Komponenten und der Anliegen der Bevölkerung, kann ein pragmatisches Vorgehen gewählt werden, um schliesslich Ambitionsniveau 3 zu erreichen.

5. Technische Ansätze: Mut zum Einsatz von SSI

Wir sehen im SSI-Ansatz das grösste Potenzial und unterstützen diesen: Diverse schweizerische und ausländische Unternehmen haben bereits darauf beruhende Lösungen entwickelt, ein breiter, skalierfähiger Einsatz steht jedoch noch aus. Obwohl der Ansatz teilweise noch auf unerprobten Technologien beruht, ermöglicht er, dass User die Kontrolle über ihre Daten behalten. Zudem bietet die Lösung einen hohen Datenschutz und die Anbindung mit Drittsystemen kann direkt erfolgen. Die Entwicklung des SSI-Ansatzes hat in den letzten Jahren an Reife gewonnen und es bestehen in diesem Bereich Standardisierungen, auf die abgestützt werden kann, was wiederum zu einer erhöhten Sicherheit beträgt.

Auch die EU verfolgt eine SSI-Lösung. In diesem Zusammenhang befürworten wir eine kompatible Lösung ohne Swiss Finish.

Aus unserer Sicht ist zudem relevant, im vorliegenden Pozess nicht zu früh konkrete, fixe Technologieentscheide, wie z.B. Blockchain, zu stipulieren.

6. Erfolgsfaktoren aus Sicht von Swico

- *Staatliche Führung und klare Governance*: Der Staat sollte den Gesamtüberblick innehaben und die Entwicklung, Ausstellung und den Betrieb des Kernelements E-ID in einem Umfeld von vielen digitalen Nachweisen übernehmen. Zudem sollte eine klare Governance hinsichtlich Arbeitsprozesse, Finanzierung, Compliance und Change-Management definiert werden.

- *Erreichen von Skaleneffekten*: Der Erfolg liegt aus unserer Sicht nicht im Bereitstellen der staatlichen E-ID Infrastruktur, sondern in der Erreichung von Skaleneffekten: Eine Verknüpfung mit weiteren Services, über die E-ID hinaus, trägt auch zu einer Amortisation der Infrastrukturkosten bei.

- *Kommunikation und Einbezug der unterschiedlichen Stakeholder*: Vor allem die Bevölkerung, aber auch Wirtschaft und Wissenschaft sollten möglichst früh einbezogen

und transparent informiert werden, um insbesondere die Unterstützung der ersteren Anspruchsgruppe zu erlangen.

- *Smart Federalism*: Der Bund sollte die Lösung möglichst breit ausrollen, damit keine kantonalen Einzellösungen entstehen. Eine Delegation an die kantonale Stufe sollte nur wo notwendig erfolgen. Je umfangreicher die Erfassung in der Breite durch den Staat, desto interessanter wird die Lösung auch für private Anbieter.

7. Bemerkungen zur Ausgestaltung des neuen Gesetzes

Für Swico ist eine technologieneutrale Ausgestaltung des neuen Gesetzes zentral.

Zudem unterstützen wir eine rasche Einführung der E-ID: Ein vorgezogener, paralleler Dialog zum neuen E-ID-Gesetz könnte den Prozess beschleunigen.

Wir bedanken und bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen zur Verfügung.

Freundliche Grüsse

Andreas Knöpfli
Präsident

Ivette Djonova
Head Legal & Public Affairs

Swiss Data Alliance
Seegartenstrasse 2
Postfach, 8008 Zürich
info@swissdataalliance.ch

Bundesamt für Justiz BJ
Bundesrain 20, 3003 Bern
Einreichung per Mail an: ***E-ID@bj.admin.ch***

Zürich, 29. September 2021

Stellungnahme der Swiss Data Alliance zur öffentlichen Konsultation zum «Zielbild E-ID»

Sehr geehrte Damen und Herren

Die Swiss Data Alliance bedankt sich für die Möglichkeit, im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID» 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.

Obwohl nicht direkt gefordert, ist es uns ein Anliegen, uns zu den vorgeschlagenen Ambitions-Niveaus und Lösungsansätzen zu äussern.

Wir sind der Ansicht, dass nur das «Ambitions-Niveau 3: Ökosystem digitaler Nachweise» zielführend und realistisch ist. Sowohl staatliche als auch private Stellen müssen digitale Nachweise ausstellen können. Für den User hat dies den Vorteil, dass die Anwendung immer identisch ist und sich damit ein kollektives Verständnis von digitalen Nachweisen etablieren kann. Auch die EU spricht sich bei der EUid für die Voll-Variante von Level 3 aus. Für die Swiss Data Alliance ist es absolut notwendig, dass nur eine Europa-kompatible Lösung umgesetzt werden soll.

Damit lässt sich auch die Beantwortung der ersten Frage «Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?» begründen. Der staatlichen E-ID muss man vertrauen können, (d.h. sie muss höchsten Sicherheits- und Datenschutzstandards genügen), sie muss benutzerfreundlich (barrierefrei), kostenfrei und integrierbar mit anderen digitalen Identitäten sein sowie kompatibel zu europäischen Lösungen.

Betreffend Lösungsansätzen unterstützen wir die Variante «E-ID Lösung mittels Self-Sovereign Identity (SSI)». Obwohl dieser Ansatz auf neuen und teilweise noch unerprobten Technologien

beruht, ermöglicht er, dass der User die Kontrolle über seine Daten behalten kann. Für die eigentliche Beurteilung des SSI-Ansatzes berufen wir uns auf die Stellungnahme von DIDAS (Digital Identity and Data Sovereignty Association) und unterstützen diese.

Zur Frage «Welche Anwendungsfälle der E-ID stehen im Vordergrund?» möchten wir nur summarisch Stellung nehmen.[1] Wie in der physischen Welt erfordert die Abwicklung bestimmter Dienstleistungen oder Behördengeschäfte auch in der digitalen Welt die Identifikation der beteiligten User. Deshalb sollten grundsätzlich alle e-Government Transaktionen nur mittels einer digitalen Identität vorgenommen werden können. Je nachdem, wie verbreitet diese Anwendungen dann sind, werden auch zunehmend private Anbieter die E-ID des Staates einbinden und mit ihren digitalen Identitäten verknüpfen wollen.

Die Frage «Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?» lässt sich einfach beantworten: Die Einführung einer E-ID ist die Basis für eine nationale Datenpolitik. Damit ist die E-ID das Rückgrat derselben, was erlaubt, sie als nationale Infrastruktur zu betrachten. Die E-ID ermöglicht Digitalisierung in der Schweiz auf vielfache Weise, wenn sie für die Bevölkerung, die Wirtschaft und die Politik einen Mehrwert mit sich bringt. Der Nutzen besteht darin, dass ein Online-Dienst, der die E-ID als Nachweisinstrument verwendet, viele Menschen in der Schweiz erreicht (hypothetisch: alle, bzw., da die Realität nicht idealtypisch verläuft: eine möglichst grosse Anzahl). Der entsprechende Online-Dienst wird somit weniger in der Verbreitung gebremst[2], was die Digitalisierung in der Schweiz beschleunigt. Ein Dienst, der keine vertrauenswürdigen oder nur weniger vertrauenswürdige Nachweisfunktionen einbindet, wird demgegenüber stärker gebremst.

Eine Dateninfrastruktur hat heute die gleiche Bedeutung wie unser Schienen-, Strassen-, Strom- und Kommunikationsnetz. Bildlich gesprochen kann man auch einen direkten Vergleich zu den genannten Netzen ziehen: Dank der durch die E-ID ermöglichten Identifikationsfunktion wird die Person, die einen Online-Dienst mit Identifikationsbedürfnis nutzen will, von einer Démarche in der physischen Welt befreit (z.B. Behördengang). Der «Nachweiserfolg» (der sonst – im Beispiel – in der Amtsstube hergestellt worden wäre) wird anderswie zum Online-Dienst «transportiert». Diese «Transportfunktion» macht die E-ID klar zu einer Infrastruktur der Digitalisierung.

Grundsätzlich ist es der Swiss Data Alliance wichtig festzuhalten, dass wir das gewählte Vorgehen nur teilweise unterstützen. Einerseits wäre mehr Transparenz über die Kriterien, die zur Zusammensetzung des Beirats geführt haben, angezeigt, andererseits wäre es uns ein Anliegen, bereits jetzt auch eine Diskussion über das neue E-ID Gesetz führen zu können. Dies würde den gesamten Prozess beschleunigen. Es stellen sich uns dabei unter anderem folgende Fragen:

Was ändert sich im neuen Gesetz im Gegensatz zu der vom Volk nicht unterstützten Variante? Es interessiert uns sehr, welche Anpassungen vorgenommen werden.

Wie wird sichergestellt, dass das Gesetz technologieunabhängig bleibt? Wir befürchten, dass mit dem gewählten Vorgehen - zuerst werden ein Ambitionsniveau und ein Lösungsansatz ausgewählt - nicht notwendige Präjudizien geschaffen werden. Einerseits fürchten wir gewisse

[1] Zum Ganzen aber z.B. https://e-idblog.ch/category/use-cases.
[2] Ergänzendes zum Nutzen einer E-ID hier: https://e-idblog.ch/welche-vorteile-dank-der-e-id.

beschaffungsrechtliche Herausforderungen, wenn parallel zum Gesetzgebungsprozess mit der Umsetzungsplanung bzw. der effektiven Umsetzung begonnen wird, andererseits ist es politisch und rechtlich falsch, mit der Umsetzung eines Gesetzes zu beginnen, das noch nicht zu Ende beraten und angenommen ist.

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.

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 in dieser öffentlichen Konsultation zum «Zielbild E-ID» einbringen zu dürfen.

Freundliche Grüsse

André Golliez

Dr. Christian Laux

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Diskussionspapier zum «Zielbild E-ID» - Stellungnahme SWITCH

SWITCH bedankt sich für die Möglichkeit zur Stellungnahme zum «Zielbild E-ID» und begrüsst das vorgeschlagene Vorgehen.

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 mehr als 560'000 Nutzern etabliert und bedient über 1500 Relying Parties (Verifier, unterstützte Applikationen / Ökosystem).

1 Antworten auf die Hauptfragen:

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Im Vordergrund stehen Anwendungsfälle in denen eine hohe Qualität gefordert ist sowohl bei der Identifizierung einer Person als auch bei der Bekanntgabe von persönlichen Attributen an eine Relying Party (Verifier). Analog zum Zeigen eines amtlichen Ausweises, soll der Inhaber einer E-ID gegenüber einer Relying Party seine staatlich geprüften Attribute einfach, sicher, ohne Einschränkungen und möglichst ohne Intermediär weitergeben können. In vielen Fällen ist die hohe Qualität aufgrund von gesetzlichen Vorgaben erforderlich.

In der online Welt lassen sich auf diese Weise Prozesse digitalisieren, die nebst anderen Prozessschritten auch eine zweifelsfreie Feststellung der Identität voraussetzen. Ein Beispiel ist die Identifizierung angehender Studierender im Rahmen der Immatrikulation an einer Hochschule. Der Nutzen ist die nutzerfreundliche, durchgängige Digitalisierung von Prozessen.

In der physischen Welt lassen sich zusätzlich zum amtlichen Ausweis dynamisch weitere Ausweise anderer Aussteller gleichzeitig physisch vorweisen. Ein Beispiel ist die Vorweisung eines Impfzertifikats und der Legitimationskarte einer Hochschule für die Zutrittskontrolle. Übertragen auf die digitale Welt soll es möglich werden, dass nebst der E-ID auch Attribute (Credentials) anderer Aussteller gleichzeitig nutzbar werden. Dies könnte z.B. die Nutzung universitärer Diplome oder die Zugehörigkeit zu Hochschulen umfassen und für den Zugriff auf wissenschaftliche Literatur oder zur Erlangung abgeleiteter Berechtigungen in anderen Lebensbereichen (Gesundheit, ÖV etc.) genutzt werden. Der Nutzen ist die flexible Erweiterung der E-ID im Sinne eines Vertrauensökosystems.

Welche sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

- Benutzerfreundlich mit nutzergesteuerter Datenweitergabe (Privacy by Design), umgesetzt möglichst ohne Intermediäre.
- Offenheit des Systems in den folgenden Dimensionen:

- Basierend auf offenen, gängigen Standards für E-ID-Lösungen, international abgestimmt.
- Maximale Offenheit in der Anwendung, also keine Einschränkungen für Relying Parties (Verifier).
- Offenheit im Einschluss von Attributausstellern (Issuer) unter einer zu definierenden Governance.

- Staatlicher Vertrauensanker (Governance)

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Anwendungsfälle für die lediglich eine E-ID benötigt wird, wie z.B. im e-Government, sind im Alltag einer Person eher selten. Eine Ausweitung der Anwendungen über e-Government hinhaus erlaubt eine regelmässige, alltägliche Nutzung der Infrastruktur.

Dies erhöht die Akzeptanz bei den Nutzern und steigert damit auch den potenziellen Wert für Relying Parties (Verifier). So könnten z.B. Ausbildungsnachweise über diese Infrastruktur nutzergesteuert allen partizipierenden, nachfragenden Relying Parties (Verifier) zugänglich gemacht werden, ohne dass diese Anwendungsfälle erst mit dem Issuer bilateral vereinbart werden müssten. Um solche Szenarien umsetzen zu können, ist der Einbezug von Sektororganisationen zur Standardisierung der Credentials entscheidend.

Letztendlich steigert dies auch der Akzeptanz der E-ID – weg von einer losgelösten, selten genutzten, und somit wenig vertrauten E-ID-Anwendung zu einem selbstverständlichen Teil eines häufig genutzten, durchgängigen Identitäts-Ökosystems.

2 Variantenempfehlung

Die Zielsetzungen der E-ID sind aus Sicht SWITCH am besten mit dem Ansatz SSI zu erreichen.

Insbesondere sind die in den Motionen geforderten Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung, klar am besten mit dem Ansatz SSI erreichbar und die Gründe sind im Zielbild gut dargestellt.

Bei der Abstimmung mit internationalen Entwicklungen, aber auch bei der Beurteilung der Maturität des SSI-Ansatzes und der Vollständigkeit der Standards sind zudem die laufenden Bestrebungen in der EU hin zu einer neuen eID auf SSI-Basis zu berücksichtigen. Diese Bestrebungen sind mitunter ein Grund für die hohen Standardisierungsbestrebungen im SSI-Umfeld und lassen eine schnelle Erhöhung der Maturität der SSI-Produkte im Rahmen des vorgeschlagenen Zeitplanes erwarten.

Deshalb beurteilen wir den SSI-Ansatz als geeignete Basis um ein für alle Marktteilnehmer – sowohl für Inhaberinnen und Inhaber, als auch für Anbieterinnen – attraktives, durchgängig nutzbares Ökosystem entwickeln zu können. Entscheidend für den Erfolg ist, dass die potenziellen Anbieterinnen in geeigneter Weise in den Prozess eingebunden werden.

3 Empfehlungen zu konkreten Elementen im Zielbild

3.1 Klärung der Vision einer E-ID

Wir verstehen die Kernaufgabe der E-ID als Mittel zum Nachweis einer Identität auf digitalem Weg – die Analogie zum physischen Ausweis ist sehr passend. Darauf aufbauende Anwendungen, z.B. für Logins sind für uns klar nicht dieser Aufgabe zuzurechnen – so wie wir ja auch nicht erwarten, dass wir mit Pass oder IDK öffentliche Verkehrsmittel nutzen oder Zutritt zu Gebäuden erhalten. Die E-ID mag uns bei der Beschaffung der entsprechenden Berechtigungen sehr wohl hilfreich sein, bei der Nutzung erwarten wir dies nicht. Wir erwarten sogar explizit, dass die E-ID auf diese Kernaufgabe beschränkt wird und diese staatliche Aufgabe möglichst gut erfüllt.

Bei der Vision der Vertrauensinfrastruktur rund um die E-ID handelt es sich um eine komplementäre Ambition, nämlich der Schaffung eines Umfelds, in dem die E-ID gleichzeitig mit anderen «Ausweisen» in durchgängigen Prozessen eingesetzt werden kann. Die staatliche Aufgabe bei dieser Vision besteht in der Schaffung des Rahmenwerks in enger Zusammenarbeit mit weiteren staatlichen Stellen sowie Dritter.

3.2 Umfang des Ökosystems – Ambitionsniveaus

Für die Kernaufgabe E-ID ist in unserer Einschätzung das Ambitionsniveau 1 anzustreben, und zwar ohne die erweiterte Nutzung im Sinne des Logins.

Beim Aufbau der Vertrauensinfrastruktur ist hingegen klar das Ambitionsniveau 3 anzustreben und als Zielsetzung der Nutzen für die Inhaberinnen und Inhaber zu maximieren.

Eine spezielle Herausforderung besteht darin, dass der Aufbau der E-ID so geschehen soll, dass die Zielsetzung der Vertrauensinfrastruktur maximal unterstützt wird.

4 Unterstützung durch SWITCH

Zusätzlich zu unseren Tätigkeiten im Bereich Identity Management möchten wir darauf hinweisen, dass SWITCH in der Schweiz seit 30 Jahren einen Teil einer globalen, verteilten und föderierten kritischen Infrastruktur für Domain-Namen betreibt und koordiniert und hier viel Erfahrung gewinnen konnte an der Schnittstelle zwischen staatlich und privat betriebenen Diensten unter staatlicher Regulation und Kontrolle. Ergänzt wird dieser Leistungsausweis mit vielfältigen ehrenamtlichen Tätigkeiten im Bereich der Cybersicherheit, insbesondere bei der Zusammenarbeit im Rahmen des Nationalen Zentrums für Cybersicherheit (NCSC), sowie der Wirtschaftlichen Landesversorgung (WL).

SWITCH möchte die umfassende Erfahrung im Identity Management zugunsten der Gesellschaft einbringen. Deshalb empfiehlt sich SWITCH mit aller Erfahrung für das Gelingen einer zukunftsträchtigen E-ID seine Dienste anzubieten.

Zürich, 30. September 2021

Geschäftsstelle
Centre administratif
Centro amministrativo

asa
ASSOCIATION DES SERVICES DES AUTOMOBILES
VEREINIGUNG DER STRASSENVERKEHRSÄMTER
ASSOCIAZIONE DEI SERVIZI DELLA CIRCOLAZIONE

Öffentliche Anhörung zum Diskussionspapier zum "Zielbild E-ID": https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id-d.pdf

Beantwortung der Fragen durch die asa
27. September 2021

· Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Die Strassenverkehrsämter könnten durch die E-ID die Prozesse zum Ausstellen und Halten von Ausweisen digitalisieren. Das daraus abzuleitende Nutzerpotenzial wäre wie folgt: - Lernfahrausweis (300'000 Nutzer) - Führerausweis (6,5 Mio Nutzer) - Fahrzeugausweis (6 Mio Nutzer) - Schiffsführerausweis (300'000 Nutzer) - Schiffsausweis (100'000 Nutzer) Die E-ID ermöglicht uns zudem die Verwaltung einer Vielzahl digitaler Workflows (Berechtigungsmanagement, Identifikation von Partnern und Kunden, ...).

· Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

1. *Technologie welche die An- und Einbindung in weitere Applikationen mit Personenregistrierung ermöglicht, idealerweise kostenfrei für die Leistungserbringer (E-ID verwendender Dienst/Anbieter)*
2. *einfache Handhabung und Beschaffung für den Bürger*
3. *Vertrauenswürdigkeit des Ausstellers > keine Angst vor Missbrauch > Erfasst werden nur die notwendigen Daten, nicht mehr*

· Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?"

Die E-ID ermöglicht zeitgemässe digitale Prozesse ohne Medienbrüche sowie schnellere, aktuellere, komfortable und letztlich günstigere Prozesse für Anbieter und Nutzer.

DIDAS

Stellungnahme DIDAS
zum
Diskussionspapier zum «Zielbild E-ID»

Digital Identity and Data Sovereignty Association
www.didas.swiss
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
Switzerland

Inhalt

Vorwort

Sehr geehrte Damen und Herren

Der Verein Digital Identity and Data Sovereignty (DIDAS) bedankt sich für die Möglichkeit, im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID» Stellung nehmen zu dürfen.

Digital Identity and Data Sovereignty Association (DIDAS) ist ein gemeinnütziger und nicht gewinnorientierter schweizerischer Verein, der mit dem folgenden primären 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.*“

Unsere Vision ist es, die digitale Zukunft einem breiten Spektrum von Branchen und Anwendungsfällen zu ermöglichen, in denen Privatpersonen, Unternehmen, Fachleute, Behörden, Gemeinschaften und sogar angeschlossene Geräte in der Lage sind, auf Basis ihrer Identität und damit zusammenhängende, proprietäre Daten auf elektronischem Wege einfach miteinander auszutauschen und dabei das Dateneigentum und die Privatsphäre zu wahren. Dabei sollen die Rechte an den Informationen und an die Compliance respektiert werden.

Um unsere Vision und Ziele zu erreichen, arbeiten wir mit technologieorientierten Startups, Gesellschaften, Behörden und NGOs zusammen.

Wir freuen uns über die Gelegenheit, hiermit unsere Stellungnahme zum Diskussionspapier «Zielbild E-ID» einreichen zu dürfen und positionieren uns als passionierte Schweizer Expertengruppe, welche für die weiteren Schritte in der E-ID Diskussion und der Entscheidungsfindung nützlich ist. Wir aspirieren Mehrwert zu schaffen, indem wir nach nachhaltigen Prinzipien, entsprechend schweizerischen Governance-Anforderungen, der Einhaltung resp. Etablierung von globalen Standards, ein inkrementell wachsendes Wissens-Ökosystem rund um Self-Sovereign Identity (SSI) ermöglichen. Wir sind auch international in die entstehenden Attribut-Ökosysteme als Experten eingebettet.

Die Stellungnahme ist eine Gemeindsschaftsarbeit 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: SWITCH AG,

AdNovum Informatik AG, Stadt Zug, Swisscom, Procivis, Verein Cardossier, HIN AG, Swiss Data Alliance, Hochschule Luzern, Prof. Tim Weingärtner, der Vorstand und alle Mitglieder des Vereins Digital Identity and Data Sovereignty (DIDAS).

Wir freuen uns, uns in der öffentlichen Diskussion mit unseren Experten und unserem Netzwerk jederzeit einzubringen und bedanken uns noch einmal für die Möglichkeit, uns in dieser öffentlichen Konsultation zum «Zielbild E-ID» einbringen zu dürfen.

Rotkreuz, den 30.09.2021

Vasily Suvorov
Präsident

Daniel Säuberli
Gründungs- und Vorstandsmitglied

Stellungnahme DIDAS
zum
Diskussionspapier zum «Zielbild E-ID»

I. Zusammenfassung unserer Stellungnahme

Wir sind fest davon überzeugt, dass Ökosysteme digitaler Attribute nach den Prinzipen 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 handlungsfähig bleiben.

Unsere Kommentare und Bemerkungen zum Diskussionspapier sind wie folgend aufgeteilt:

1. Antworten und Kommentare zum Kapitel 7 - Öffentliche Diskussion des Zielbilds E-ID
2. Kommentare zur Sektion 5.1.6. des Diskussionspapier „Offene Fragen zum SSI-Ansatz“
3. Kommentare zum Kapitel 5.2 - Warum SSI besser als PKI ist

II. Antworten und Kommentare zum Kapitel 7 - Öffentliche Diskussion des Zielbilds E-ID

1. Frage: Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Das Ambitionslevel bestimmt das Ausschöpfungspotential der digitalen Transformation und somit ganz direkt die Leistungs- und Wettbewerbsfähigkeit der Schweiz in einer zunehmend digitalen Welt. Um mit den Möglichkeiten der Digitalisierung Mehrwerte schaffen zu können, benötigen wir Ökosysteme, in denen über Organisations- und Ländergrenzen hinweg digitale Nachweise sicher und unfälschbar ausgetauscht werden können (z.B. beim Kauf von altersbegrenzen Gütern, der Ausweispflicht im internationalen Reiseverkehr, beim Nachweis einer Versicherungsdeckung, beim Verifizieren eines gültigen COVID-Zertifikats oder beim Sicherstellen von reibungslosen kommerziellen Prozessen zwischen Vertragspartnern).

Anforderungen an digitale Identitätsnachweise von Personen sowie vermehrt von Organisationen und Dingen (IoT) sind dafür die Basis. Qualifikationen und Berechtigungen aller Art (z.B. Ausbildungs- und Gesundheitsnachweise, Herkunftszeugnisse, Mitarbeiter- und Mitgliedschaftsausweise und so weiter) müssen innerhalb der Schweiz und auch mit unseren Internationalen Partnern nachhaltig souverän und anhand von internationalen Standards ausgetauscht werden können.

Die E-ID ist in einem solchen Ökosystem nur ein digitaler Nachweis unter vielen.
In der Zusammenfassung des "Zielbild E-ID" wird die Frage nach der Vision einer zukünftigen E-ID aufgeworfen. Dabei werden zwei unterschiedliche Szenarien sinnbildlich dargestellt:

- E-ID als ein staatlich ausgestellter, digitaler Ausweis (analog dem Schweizer Pass), oder
- E-ID als "Vertrauens-Ökosystem" mit digitalen Nachweisen jeglicher Art, welche sowohl von öffentlicher als auch privater Hand herausgegeben werden können.

Diese beiden Szenarien schliessen sich gegenseitig NICHT aus, umreissen jedoch folgerichtig die Grunddiskussion, welche aktuell in der Schweiz geführt werden sollte: "Was wollen wir mit einer E-ID erreichen -Nicht nur heute oder morgen, sondern auch in Zukunft...".

Es geht also nicht weniger um die Frage, wie sich die Schweiz national und international in Bezug auf das Thema Digitalisierung strategisch aufstellen will.

DIDAS hat hinsichtlich dieser strategischen Frage eine klare Vorstellung. Bezugnehmend auf die in Kapitel 4 erwähnten Ambitionsniveaus erachtet DIDAS das Ambitionsniveau 3 als einzige mögliche Vision, welche genügend Mehrwerte für Nutzer, Unternehmen und öffentliche Hand ermöglicht, die Wettbewerbsposition und digitale Souveränität der Schweiz im In- und Ausland stärkt und eine solide und zukunftsfähige Vertrauensgrundlage für Innovation in der Digitalisierung und Geschäftsprozess-automatisierung schafft. Folgende Überlegungen stützen diese Einschätzung:

- Eine E-ID als Authentifikationsmittel mit dem primären Ziel, Zugang zu Onlinediensten zu gewährleisten ("Login"-Funktionalität) ist u.E. zu kurz gegriffen und entspricht nicht mehr den heutigen Marktbedürfnissen. Es existieren heute schon ausgereifte und am Markt eingeführte Produkte und Dienstleistungen (z.B. Single Sign-On, Social Logins, Identifizierungs- und Identitätsdienstleistungen, Passwort-Manager, passwortlose Authentifizierung), die diese Funktionalität ermöglichen und von Konsumenten akzeptiert werden. Der einzige Mehrwert einer E-ID unter diesem Blickwinkel ist eine höhere Qualität der Identitätsbestätigung resp. eine zusätzlich staatliche Zusicherung, was ausgesprochen wichtig, aber in Hinblick auf den geplanten Realisierungszeitraum (2025 / 26) nicht wirklich die Digitalisierungsherausforderungen adressiert.
- Der Nutzen einer staatlichen E-ID soll darin bestehen, dass schweizweit verlässliche digitale Identitätsnachweise für alle, so zum Beispiel auch für die Akteure im Gesundheits- und Sozialwesen geschaffen werden können, in einem Rechtsrahmen der es erlaubt einen Identitätsnachweis in den entsprechenden Prozessen einfach und sicher einzusetzen. Der Hauptanwendungsfall ist der Identitätsnachweis als Basis für digitale, branchenspezifische Prozesse - die Funktion des Passes, eines Handelsregisternachweises oder der ID wird somit in die digitale Welt transportiert. Analog zum Vorzeigen eines amtlichen Ausweisdokuments, soll der Inhaber einer E-ID gegenüber einem Service seine staatlich geprüften Attribute einfach, sicher und möglichst ohne Intermediär weitergeben können. Die E-ID soll für dieses Ausweisen verwendet werden können - eben als vertrauenswürdige, staatliche Basis-ID, resp. als Vertrauensanker für alle darauf aufbauenden weiteren Attribute oder *Credentials*. Damit können insbesondere Onboarding- und KYC- Prozesse unterstützt werden.
- 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 der von Ihnen aufgegriffene Ansatz „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.

DIDAS begleitet und unterstützt also eine Anzahl von unterschiedlichen Initiativen der öffentlichen und privaten Hand und ist aus diesem Grund der festen Überzeugung, dass ein wichtiger Erfolgsfaktor der Digitalisierung die zweifelsfreie Feststellung der Identitäten der involvierten Parteien ist. Dabei gilt es aber zu berücksichtigen, dass die Anforderung an die «Identifizierung» je nach Kontext unterschiedlich festgelegt wird. Angefangen von einer blossen Feststellung einer Existenz bis hin zum Beweis bestätigter Berechtigungen, ergeben sich unterschiedliche Erwartungen, welche Identitätsattribute und Nachweise in einem digitalen Prozess relevant werden. Eine solche Identitätsdefinition geht über die Bereitstellung von staatlichen Beweisen hinaus und berücksichtig auch verifizierte Informationen aus der Privatwirtschaft.

Digitalisierung bedeutet nicht, bestehende analoge Prozesse in der digitalen Welt «nachzubilden». Digitalisierung bedeutet, die Chancen zu nutzen, um «es anders zu tun» oder «fundamental neu zu denken». D.h., dass eine Nachbildung von komplexen Abläufen aufgrund «physischer» Hürden vermieden werden sollte[1]. In der digitalen Welt werden Prozessschritte automatisiert, verschmelzen oder verschwinden, was wiederum einen positiven Einfluss auf das Kundenerlebnis hat und Abläufe effizienter gestalten lässt.

[1] Beispiel: Bei einem Bewerbungsprozess stellt der Bewerber dem Unternehmen unterschiedliche beweiskräftige Informationen, wie Passdaten, Zertifikate und Arbeitszeugnisse von unterschiedlichen Ausstellern zur Verfügung. Diese Dokumente müssen im Vorfeld dem Bewerber «physisch» zugestellt werden, der Bewerber muss diese Dokumente in einem Dossier zusammenstellen und dann beim neuen Arbeitgeber einreichen. Es gibt heute «digitale» Vereinfachung (bspw. Dokument als PDF oder das Hochladen von Dokumenten), aber nach wie vor ist der Zeitaufwand für alle Beteiligten sehr hoch.

Um dieser Denkweise Rechnung zu tragen, muss die Identifizierung als integraler Bestandteil des Gesamtprozesses gesehen werden und ein zukünftiges «E-ID Ökosystem» sollte so ausgestaltet sein, dass solche Prozessinnovationen realisiert werden können.

DIDAS ERKENNT DIESBEZÜGLICH NUR IM AMBITIONSNIVEAU 3 DIE ERFÜLLUNG DIESER ANFORDERUNG. ES ERSTAUNT AUS DIESEM GRUND AUCH WENIG, DASS DIE EUID GENAU IN DIESE RICHTUNG ABZIELT.

2. **Frage: Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?**

Damit sich digitale Lösungen durchsetzen, müssen diese in puncto Ausgestaltung im Publikum auf Akzeptanz stossen und klare Vorteile für alle beteiligten Akteure mit sich bringen. Aus diesen Zielen lassen sich drei konkrete Anforderungen an eine E-ID ableiten:

a. **Vertrauenswürdigkeit**

Das Vertrauen in elektronische Identifikationslösungen fusst wesentlich auf dem Schutz der Privatsphäre der E-ID-Benutzerinnen und -Benutzer. Dabei stehen datenschutzrechtliche Prinzipien wie "privacy by design" sowie Datensparsamkeit im Brennpunkt. Es darf bei der Verwendung (d.h. konkret bei der Überprüfung) der E-ID keine Kommunikation mit dem Issuer stattfinden [2]. Ebenso soll der Recovationstatus eines einzelnen Credentials nicht getracked werden können. Diese Kriterien lassen sich unseres Erachtens am ehestens mit Konzept SSI verwirklichen, da dieses auf offenen Grundprinzipien beruht.

Unter den diversen datenschutzrechtlichen Vorzügen dieses Ansatzes, ist insbesondere die Reduktion auf die je nach Anwendungsfall notwendigen Attribute bei der Datenübertragung an Dritte und die konsequente Vermeidung unnötiger Datenflüsse und der damit verbundenen Randdaten hervorzuheben.

Die staatlichen E-ID Attribute sollen exklusiv von einer staatlichen Stelle ausgegeben werden. Perspektivisch im gleichen Prozess, bei dem ein(e) Bürger*in den Pass und die ID erhält oder ein(e) Ausländer*in den Aufenthaltsausweis, jedoch in diesem Fall digital in eine kryptografisch geschützte, persönliche Wallet, mit Hilfe einer dezentralen Registry für die Verifizierung.

[2] Wichtig: Kein OCSP. Das Online Certificate Status Protocol (OCSP) ist ein Legacy-Netzwerkprotokoll, das es Clients ermöglicht, den Status von X. 509-Zertifikaten bei einem Validierungsdienst abzufragen.

b. Benutzerfreundlichkeit

Digitale Transaktionen, die den Einsatz der E-ID erfordern, müssen ebenso einfach handhabbar und transparent ausgestaltet sein wie alle übrigen digitalen Geschäftsprozesse, um im Publikum breit akzeptiert zu werden. Die Ermöglichung einer zweifelsfreien Identifizierung einer natürlichen Person in einem digitalen Prozess über unterschiedliche Schnittstellen (API, NFC, QR Code, BLE und Wifi). Diese Identifizierung sollte eineindeutig, staatlich legitimiert und authentifizierbar sein. Die E-ID als Ausweis ist somit das digitale Äquivalent des Schweizerischen Passes, Nukleus / Zuordnungspunkt für weitere Attribute und Nachweise zu dieser Identität (sog. *verifiable Claims*). D.h. dieser E-ID können eineindeutig weitere Informationen, Beziehungen und Delegationsverhältnisse zugeordnet werden, welche wesentlich zur umfassenden Beschreibung der Identität beitragen.

Was von den Benutzerinnen und Benutzern dabei als benutzerfreundlich empfunden wird, bestimmt sich in massgeblicher Weise nach dem jeweils aktuellen Stand der Technik und vorherrschender Trends. War der Einsatz zusätzlicher Geräte oder Karten zwecks Authentisierung beispielsweise noch lange gang und gäbe, dürfte ein entsprechend ausgestaltetes Verfahren heute auf breite Ablehnung stossen.

Demzufolge ist eine hohe Adaptionsfähigkeit an die jeweils aktuellen Ansprüche der Benutzerinnen und Benutzer an die Benutzerfreundlichkeit erforderlich. Der zu schaffende Rechtsrahmen für eine staatliche E-ID-Lösung sollte daher zwar klare Leitplanken setzen ("was"), jedoch namentlich betreffend die benutzerseitigen Systeme weitestgehend technologieneutral, auf offenen, internationalen Standards ausgestaltet sein ("wie"), um eine stetige Weiterentwicklung und Umsetzung von vielmöglichste Anwendungsfälle zu ermöglichen.

Die E-ID kann auch im Ausland (mindestens EU) in digitalen und analogen Prozessen einfach eingesetzt werden.

c. Vertrauensökosystem

Wie Sie in Ihrem Diskussionspapier darlegen, sehen sich Initiativen wie die Einführung nationaler E-IDs regelmässig mit dem "chicken or the egg"-Dilemma konfrontiert: ohne E-ID werden keine Anwendungsfälle geschaffen und ohne Anwendungsfälle wird keine E-ID benötigt.

Vor diesem Hintergrund erachten wir den neuen Anlauf, eine nationale E-ID zu schaffen, als grosse Chance, ein umfassendes Vertrauensökosystem zu etablieren, das einerseits die Anforderungen an eine vertrauenswürdige, staatliche E-ID erfüllt und andererseits den regulatorischen Rahmen für eine Vielzahl von Anwendungsfällen schafft (Staatlicher Vertrauensanker (und Governance) ist hier wichtig), um das grösstmögliche Potential des digitalen Wandels auszuschöpfen. Dabei soll die Offenheit des Systems für die Nutzung durch möglichst viele Diensteanbieter gewährleistet werden.

Das "Ambitions-Niveau 3" im Rahmen des vorgeschlagenen SSI-Ansatzes bietet unseres Erachtens daher den geeigneten Rahmen, um mit den Möglichkeiten der Digitalisierung Mehrwerte für alle beteiligten Akteure zu schaffen. In einem solchen Vertrauensökosystems wird die E-ID schliesslich einen von verschiedenen digitalen Nachweisen darstellen, wobei private und öffentliche Stellen wie Bildungsinstitutionen, Transportunternehmen, Tourismusbetriebe, Telecomprovider, Finanzdienstleister, medizinische Leistungserbringer und Krankenversicherer, Kulturdienstleistende oder dergleichen ebenfalls digitale Nachweise herausgeben können, womit sich der Gesamtnutzen des Vertrauensökosystems entscheidend erhöht und es allen Teilnehmern im Ökosystem ermöglicht, Domain- oder Branchenspezifische oder -übergreifende digitale Prozesse entlang von Interaktionen und Transaktionen neu zu denken sowie intermedär-frei und reibungslos ablaufen zu lassen.

3. **Frage: Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?**

Wir haben in unserer Antwort zu Frage 1 versucht, den Nutzen zu beleuchten, die E-ID nicht nur als digitalen Ausweis, sondern als **nationale Vertrauensinfrastruktur** zu betrachten. DIDAS ist der festen Überzeugung, dass nur unter einer solchen Betrachtungsweise, spürbarer Mehrwert für Zivilbevölkerung, Wirtschaft, öffentliche Hand und Politik entstehen kann. Damit kann der Schweiz ein wesentlicher Schritt in Richtung Teilnahme an den weltweit entstehenden digitalen Ökosystemen und der fortschreitenden Digitalisierung ermöglicht werden, jedoch ohne Kompromisse in Punkto Souveränität, Privatsphäre und Sicherheit einzugehen.

Was die Schienen-, Strassen-, Strom- und Telekomnetze für die industrielle Entwicklung der Schweiz bedeuteten, wird ein digitales Vertrauensnetzwerk (oder digitale Vertrauensinfrastruktur) für die Schweiz im einundzwanzigsten Jahrhundert bedeuten. An dieser Stelle möchten wir, um eine möglichste grosse Entfaltung der nationalen E-ID

Infrastruktur zu erreichen, drei zusätzliche Anforderungen miteinbringen, welche bei der Konzeption und Realisierung zwingend berücksichtigt werden sollten:

a. Schutz der Identität und Privatsphäre jedes einzelnen, Sicherstellung der Datenintegrität

Die Wahrung der Identität, der Schutz der Privatsphäre und die Sicherstellung der Integrität sind die wichtigsten Erfolgsfaktoren und zentral in der Ausgestaltung eines E-ID Ökosystems. Erst wenn die Teilnehmer vertrauen haben, dass sie nicht ausspioniert werden oder zu viele Informationen von sich preisgeben müssen, dass sie geschützt vor unberechtigten Dritten und die ausgetauschten Daten integer und nicht manipuliert sind, dann partizipieren sie aktiv und das Ökosystem beginnt zu leben. Aus diesem Grund erachten wir *Datenschutz und -minimierung, Wahlfreiheit und Kontrolle über die eigene Identitätsdaten, sowie gesicherte Kommunikationsverfahren auf einer zuverlässigen, belastbaren Infrastruktur als die wichtigsten Gestaltungsprinzipien*, die es zwingend zu berücksichtigen gilt.

b. Internationale Interoperabilität

Digitalisierung hört nicht an der Landesgrenze auf. Aus diesem Grund ist DIDAS der Auffassung, dass die internationale Interoperabilität und damit auch die Anlehnung an internationalen Standards (bspw. EUid, eIDAS, W3C) zwingend zu erfolgen hat. Wir sind der festen Überzeugung, dass dies schon von Anfang berücksichtigt, werden sollte. Ein «isoliertes Swiss E-ID Ökosystem» würde u.E. *das Potential massiv beschneiden*. Die Schweiz ist eine kleine, offene Volkswirtschaft, die heute schon rege im wirtschaftlichen und sozialen Austausch mit anderen Ländern steht. *Wir begrüssen, dass der Autor des Diskussionspapieres auf diesen Tatbestand hingewiesen und den Verweis zur EUid gemacht hat. Gerne möchten wir die Wichtigkeit an dieser Stelle nochmals klar unterstreichen.*

c. Ausgestaltung des Ökosystems unter Einbindung der Privatwirtschaft und Zivilgesellschaft, klarer Rollen und nachhaltiger Prinzipien

Der Staat spielt zweifelsohne eine zentrale Rolle in der Definition und Ausgestaltung, sowie im Betrieb digitaler Ökosysteme. DIDAS ist der festen Überzeugung, dass es ohne privatwirtschaftliche Beteiligung nicht gehen wird. Aus diesem Grund ist es von Anfang an wichtig, die unterschiedlichen Rollen präzise zu definieren und entsprechend die unterschiedlichen Kompetenzen und Verantwortlichkeiten gebührend zu berücksichtigten. Ein E-ID Ökosystem ist ein sich entwickelndes Gebilde, *es ist aktuell nicht vorhersehbar, welche Anwendungsfälle in 5 oder 10 Jahren relevant sind,* welche zusätzlichen Innovationen notwendig werden, um diese zu realisieren. Um diese Innovationen zu ermöglichen, ist Wettbewerb wichtig und damit auch die Einbindung von unterschiedlichen privatwirtschaftlichen Akteuren (Herausgeber von Nachweisen,

Integratoren, Technologiepartner, Dienstleistungsanbieter für Privatkunden und Unternehmen, etc.).

U.E. soll der Staat sich auf die Ausgestaltung des Vertrauensrahmen («*Governance Framework*»), die Anerkennung der Teilnehmer und Partner, die Spezifikation der Qualitätslevels, die Zertifizierung der Prozesse und Technologien sowie die Ausstellung der staatlichen Nachweise konzentrieren. Eine derartige Rollendefinition heisst nicht, dass der Staat die Zügel wieder aus den Händen gibt, sondern dass er unter kontrollierter Einbindung der Privatwirtschaft die Entwicklung des E-ID Ökosystems vorantreibt.

Es ist auch wichtig zu bemerken, dass wenn ein Attribut im Ausland verifiziert werden sollte (z.B. ID bei einer Reise, ein Altersattribut oder ein COVID-Zertifikat, etc), die SSI nicht nur ein einzelnes Netzwerk als die Basis für Nationalinfrastruktur ermöglicht, sondern auch sogenannte «Network of Networks» (oder Netzwerk der Netzwerke).

Durch Interoperabilität der Wallets und «*Institutional Agents*» ist es möglich, verschiedene miteinander kompatible SSI Netzwerke zu betreiben. Insbesondere hilft es, das Huhn-Ei-Problem zu lösen, indem hoheitliche Anwendungsfälle des Bundes und der Kantone durch das dafür gestaltete Netzwerk und den dafür geeigneten Vertrauensrahmen (Governance Framework) umgesetzt und betrieben werden können, jedoch falls vom Benutzer gewünscht, seine verfügbaren verifizierbaren Attribute anhand von Standards über weitere (z.B. internationale) Netzwerke verifiziert werden können (z.B. Krankenversicherungsdeckung bei Spitalaufenthalt im Ausland, Gültiger COVID-Immunitätsnachweis im Ausland). Diese «Basisanwendungsfälle» können durch kompatible Wallets[3] und Systeme der kommerziellen und öffentlichen Akteure erweitert werden, ohne dass sie einen direkten Zugriff auf das «hoheitliche Netzwerk» brauchen. Dieser Ansatz wird einerseits helfen, die Aufgaben des Staats bezüglich E-ID und anderen verifizierbaren Attribute unabhängig von ausländischen Akteuren umzusetzen. Andererseits wird er aller Art anderen öffentlichen und kommerziellen Akteuren in der Schweiz und im Ausland es ermöglichen, darauf andere, wertvolle Anwendungsfälle auszubauen. Dies würde für die Schweizer Wirtschaft wie auch für die Behörden einen grossen Nutzen darstellen. So könnten die verschiedensten Ökosysteme entstehen, in denen spezifische Services und Prozesse in einem Vertrauensraum angeboten und abgewickelt werden können.

3 Beim Thema Wallet sehen wir (mind. vorübergehend) einen Nutzen in einer Open-Source Swiss-Wallet, welche erstens in der eigenen Geschwindigkeit weiterentwickelt und zweitens mit unseren Eigenheiten versehen werden könnte. Aber schlussendlich sollte jede (genügend sichere Wallet) verwendet werden können.

III. Kommentare zur Sektion 5.1.6. des Diskussionspapier „Offene Fragen zum SSI-Ansatz“

1. Welche Governance-Ebenen gibt es und wer ist dafür zuständig (z. B. Governance Ebenen nach Trust over IP Framework: Ökosystem, Credentials, Provider, Utility)?

Das ToIP-Framework bildet einen guten Rahmen zu den Governance-Überlegungen und sollte u.A. als Basis verwendet werden. Sobald der Richtungsentscheid für eine zukünftige Schweizer E-ID zu Gunsten SSI ausfällt, sollte der Bundesrat die Gremien bestimmen, welche in Zusammenarbeit mit den europäischen Initiativen zur Errichtung eines digitalen Vertrauensnetzwerkes die technischen Standards festlegt. Dabei kann weitestgehend auf die W3C-Standards zurückgegriffen werden, die laufend weiterentwickelt werden.

Was die einzelnen Ökosysteme (Mobilität, Gesundheit, Ausbildung, Finanzwesen, Verwaltung, Justiz u.a.) betrifft, soll auf die bestehenden Netzwerke, Strukturen und Verbände aufgebaut werden. Wenn der Richtungsentscheid einmal gefällt ist, können auf dieser Basis die verschiedenen organisationübergreifenden Prozesse neu gedacht und entwickelt werden.

Wir erachten es als wichtig, wenn schon frühzeitig die Privatwirtschaft sowie weitere Institute in die Definition des Governance-Frameworks miteinbezogen werden. Insbesondere bei Ambitionsniveau 3, welches nicht nur staatliche Beweise, sondern auch Nachweise von weiteren autoritativen Stellen herausgegeben werden, ist die Zusammenarbeit und gemeinsame Akzeptanz essentiell.

2. Muss der Staat auf gewissen Komponenten das Monopol haben? Müssen Wallets staatlich zertifiziert werden? Wird die Auswahl von Wallet und Institutional Agent dem User überlassen? Gibt es eine Regelung, welche Teile kooperativ, welche in Konkurrenz erstellt und betrieben werden?

Nein, ein Monopol irgendeines Akteurs im Rahmen von SSI widerspricht dem Kerngedanken von SSI. Der Staat verfolgt in einem SSI-Ansatz die vertrauensbildenden Massnahmen, mit anderen Worten, er ermöglicht den "Human Trust". Dies bedeutet, dass er die Gesamtverantwortung für das Governance Framework trägt, Standards vorgibt, die Qualitätslevels und -regeln definiert, sowie Prozesse, Technologien und Infrastrukturen zertifiziert[4]. U.E. wird aber vom Staat nicht erwartet, dass er die Technologie bereitstellen

[4] Wie schon erwähnt, betrachten wir das Konzept von «Network of Networks» als den besten Ansatz, die Vertrauensinfrastruktur für SSI Ökosystem aufzubauen.

muss. Die Wahlfreiheit bei allen Komponenten, die nicht zwingend staatlich betrieben werden müssen, soll maximiert werden. Zur Einhaltung der Mindestanforderungen gemäss Governance-Framework kann eine Zertifizierung der Wallets zielführend sein.

3. **Wer betreibt die Registry? Ist eine eigene, nationale Registry nötig oder schliesst man sich einem bestehenden, internationalen Ökosystem an? Wollen oder sollen Kantone, Städte oder private Unternehmen Speicher-Knoten (Nodes) betreiben dürfen? Welche Technologie wäre zu bevorzugen? Welche Rolle spielt die Datenmenge? Wie löst man Interoperabilitätsfragen zu anderen Registries? Besteht für den Issuer sogar die Wahlfreiheit der Registry?**

Der Entscheid über die Technologie, den Aufbau und Betrieb des Registry soll an den Kriterien der Performanz, der Resilienz, der internationalen Interoperabilität und der Effizienz gemessen werden.

Aufgabe des Bundes ist es obige Kriterien zu definieren und deren Einhaltung durchzusetzen. Der Betrieb des Registry kann in Eigenregie oder im Auftrag des Bundes erfolgen. Kein Kriterium soll die Einbindung der verschiedenen politischen Verwaltungsebenen sein.

Der Aufbau und der Betrieb des Registry ist eine Infrastrukturaufgabe zu Gunsten der gesamten Volkswirtschaft und soll demzufolge auch von der Allgemeinheit finanziert werden. Nichtsdestotrotz schlagen wir vor, dass der „Network of Networks“ Ansatz bei der Umsetzung der SSI -Infrastruktur als wichtiger Bestandteil der detaillierten Ausarbeitung des Designs berücksichtigt werden soll, sodass NoN ermöglicht werden können und die Skalierung von Anwendungsfällen nicht behindert wird. Die Wahl der Registry soll also primär einen sicheren, stabilen Rahmen für den staatlichen Vertrauensanker liefern. Den Issuern sollen die Freiheit zur Wahl einer Registry belassen werden.

4. **Wer darf Issuer sein? Bleibt das System völlig offen zum Gewinn zusätzlicher Anwendungsfälle oder werden die Issuer spezifisch ausgewählt oder berechtigt?**

Bei Ambitionsniveau 3 gehen wir von einem offenen System aus. Eine SSI-basierte E-ID ist der Eckstein des gesamten SSI-Ökosytems, worauf sich öffentliche und private Issuer stützen können, um ihre eigene Verifiable Credential herauszugeben. Der Rolle

des Staats soll sich auf die Herausgabe der E-ID fokussieren. Das Issuing von weiteren staatlichen, institutionellen und privaten Issuer soll möglich sein. Es sollte ein Trust-Level geben, damit hochprioritäre Dienste stärker gesichert sind. Analog der Domain-Name Vergabe im Internet sollte es eine geringe Gebühr als "Spam-Schutz" geben.

Dies lässt sich mit dem „Networks of Networks“ Ansatz einfach umzusetzen, wobei das für z.B. Staatliche Issuers gestaltete SSI-Netzwerk (oder Registry) besondere Regeln (Governance Framework) hat.

5. **Wie werden Backups und Transfers von Credentials ermöglicht? Wie können zentrale Backups und damit attraktive Hacker-Angriffsziele vermieden werden? Welche Rolle spielt eine mögliche kryptografische Verbindung zwischen Wallet und Verified Credentials?**

Das Backup soll beim Bürger dezentral erfolgen, um einen zentralen Angriffspunkt zu vermeiden. Die Mindestanforderungen an Backups von Wallets inklusive damit verknüpfter Credentials soll im Governance-Framework geregelt werden. Wir empfehlen, sich an den aktuellen Stand der internationalen Entwicklungen anzulehnen. Wir sehen heute schon Ansätze, die die wichtigsten Antworten auf diese Fragen geben. Des weiteren verweisen wir auf die aktuell laufenden Arbeiten innerhalb der EU («Toolbox for a EU Digital Identity Framework»).

6. **Welche Sicherheitsmechanismen sind für den Zugriff zur Wallet nötig?**

Dies soll auf Basis gängiger Standards für die geforderten Sicherheitsniveaus im Governance-Framework geregelt werden. Bei den Anwendungsfällen, die vom Staat definiert und geregelt sind (e.g. KYC, Auszüge aus dem Strafregister usw.), sollen die Wallets zertifiziert werden und entsprechend die höchste Sicherheitsmechanismen verwenden (z.B. Einsatz von *Secure-Elements* (TPM, HSM, SIM, etc.) und Biometrie). Es braucht aber auch die Möglichkeit, gewisse Credentials (z.B. E-ID) an das Device zu binden, damit es nicht kopiert werden kann.

7. **Wie können Verified Credentials auf mehreren Geräten benutzt werden? Wann wäre dies nötig? Reicht es, wenn mit dem einen Smartphone immer eine Verbindung zum Verifier aufgebaut werden kann, unabhängig davon, auf welchem anderen Gerät man gerade den nach der E-ID-fragenden Prozess initiiert hat?**

Man will seine Credential von den verschiedensten Geräten aus verwenden können. Aber es sollten keine Schlüssel kopiert/dupliziert werden, sondern immer eine Delegation von Rechten (mit abgeleiteten Schlüsseln) vorgenommen werden. In Zukunft, wenn mehr Apps und Dienste nativ SSI (resp. *DIDComm*) implementieren, wird das Abscannen eines QR-Codes immer seltener werden und die Apps kommunizieren mittels DIDComm mit dem lokalen Wallet.
Dies soll im Governance-Framework geregelt werden.

8. **Wer definiert Credential-Schema, braucht es eine ausgewiesene Stelle zur Definition und Koordination (z. B. eCH) oder werden die Definitionen branchenabhängig entwickelt?**

Wie bei aller Kommunikation muss sich die Standardisierung an der Grösse des Ökosystems (resp. Subsystems) ausrichten. Je mehr Stakeholder involviert, desto wichtiger, schwieriger und langwieriger wird die Standardisierung. Aber sie ist zentral für eine Verbreitung und Interoperabilität. Der Bund kann mitgestalten und schlussendlich das Schema für die E-ID festlegen. Aber die Schemata (und Name) der einzelnen Claims (Attribute) muss international abgestimmt sein. Wir erwarten also, dass Branchenorganisationen die Schemadefinitionen der in der Branche autoritativ herausgegebenen Verifiable Credentials in eigener Regie entwickeln und verwalten werden. Der Einsatz dieser Credentials kann in der Folge aber durchaus branchenübergreifend erfolgen (z.B. Befähigungen, Atteste, Diplome, etc.).

9. **Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll, um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?**

Spezifisch für die Herausgabe von verifizierbaren Attributen oder «Verifiable Credentials» der Basisidentität (E-ID-Attribute) an Wallets des Nutzers könnte ein solcher

Authentifizierungsdienst sinnvoll sein. Beim Einsatz des Wallets, hingegen, wird kein solcher Authentifizierungsdienst[5] benötigt.

[5] Es braucht keinen staatlichen IdP (der würde viel zu viel mitbekommen). Aber eine lauffähige Komponente (Docker-Image) für Kantone und Gemeinden würde sicher Sinn machen, natürlich OpenSource (ist eh er nur Packaging und Config, analog VON Images)

IV. Kommentare zum Kapitel 5.1.4. - „Nachteile des SSI-Ansatzes“

1. Relativ junger Ansatz, einige Grundsatzfragen sind noch nicht abschliessend geklärt und Standards sind noch nicht komplett.

Ja, der Ansatz ist noch jung, einige Fragen müssen noch geklärt werden. Unseres Erachtens soll dies aber aus zweierlei Gründen den Bund nicht hindern, diesen Ansatz weiterzuverfolgen:

1) Der Ansatz baut auf erprobte kryptographische Verfahren und bewährten Technologien auf, die heute schon in unterschiedlichen Anwendungsfällen genutzt werden.

2) Seit dem Aufkommen des Ansatzes (2015) haben wir eine rasante Entwicklung von Innovation und Verbesserungen gesehen. Ein Richtungsentscheid der Europäischen Gemeinschaft mit ihrer globalen regulatorischen Reichweite und der Schweiz als führende Nation in der Blockchaintechnologie, deren skalierbare Anwendungen allesamt auf ein digitales Vertrauensnetzwerk angewiesen sind, wird die weitere Entwicklung und damit die Lösung der noch offenen Fragen sehr positiv beeinflussen. Wir sind zuversichtlich, auch in Hinblick auf den geplanten Einführungszeitraum der neuen E-ID (2025/26), dass für die heute noch nicht abschliessend geklärten Themen praktikable Lösungsvorschläge vorliegen. Aber SSI funktioniert und kann bereits jetzt verwendet werden. Mit dem Aufbau des Ökosystems resp. der Anwendungen wird das System (und die Bevölkerung) erst erwachsen. Warten ist keine Option.

2. Das breite Bewusstsein für die Möglichkeit dieses ganzheitlichen Ansatzes (im Vergleich zu einem Login) muss zuerst entstehen.

Dies ist Richtig. Dies hat aber weniger mit SSI als vielmehr mit der Digitalisierungskompetenz der Schweizer Bevölkerung und der schweizer Unternehmen zu tun. Hier ist es zwingend notwendig an der Kommunikation zu arbeiten sowie relevante, für die Anwender attraktive Anwendungsfälle zu ermöglichen, respektive zur Verfügung zu stellen.

Momentan werden konkrete Anwendungsfälle mit institutionellen und privaten Akteuren umgesetzt. Dabei wird die kaskadierte Nutzung von Verifiable Credential innerhalb eines Ökosystem demonstriert. Sie zeigen gut das Potential eines SSI-basierten Ökosystems auf. Durch solche Beispiele wird das Bewusstsein gesteigert.

Sofern der Bundesrat in absehbarer Zukunft einen Richtungsentscheid fällt, entsteht bei vielen Firmen in der Schweiz die notwendige Investitionssicherheit und sie werden beginnen, schon vor Inkrafttreten des neuen E-ID Gesetzes, Pilotprojekte und vereinzelte Anwendungsfälle gemäss den SSI-Prinzipen umzusetzen.

Somit hätte die öffentliche und private Hand bereits ab heute die Möglichkeit, einen wesentlichen Beitrag zu einer erfolgreichen Einführung in fünf Jahren zu leisten und ihre Kunden und Kundinnen auf diesen ganzheitlichen Ansatz vorzubereiten.

3. **Die Verantwortung zur Verwaltung von Verified Credentials wird vollständig dem User übergeben, was Hilfeleistungen durch den Issuer praktisch verunmöglicht.**

Die Issuer haben grundsätzlich gewisse, aber begrenzte Möglichkeiten, der Verwaltung der Verified Credentials durchzuführen (sie geben die Verified Credentials heraus und widerrufen sie). Das ist ein Grundsatz im SSI-Ansatz. Die Verwaltung (oder besser gesagt die Nutzung) der Verified Credentials geschieht im Wallet oder durch den Walletanbieter. Abhängig von den individuellen Bedürfnissen bezüglich Sicherheit, Convenience und Privatsphäre werden die User unter verschiedenen Walletanbietern und Wallets wählen können.

Es gibt aber noch eine wenig beachtete vierte Rolle neben Issuer, Holder und Verifier - nämlich die der Agency. D.h. eine Dienstleistung welche ein User/Holder (resp. sein Wallet) nutzt um z.B. Backups, Social Recovery sicherzustellen, oder um eine gewisse Offline-Fähigkeit zu ermöglichen, sprich, dass in seinem Namen (mit delegierten Credentials) gewisse Aktionen durchgeführt werden, auch wenn der User resp. sein (Haupt) Wallet nicht online ist. Die Agency kann auch gleich der Mediator sein, welche sowieso jedes Mobile-Wallet braucht.

Zu berücksichtigen ist jedoch, dass die forensische Auswertbarkeit schwierig ist, da das System dezentral und kryptografisch gut geschützt ist. Dies kann beim Missbrauchsfall der E-ID oder anderen Nachweisen dazu führen, dass es schwierig wird nachzuweisen, dass man etwas «nicht gewesen» ist. Nichtsdestotrotz hilft das kryptografisch gut geschützte und dezentrale System gerade die missbräuchliche Verwendung digitaler Nachweise zu minimieren. Wo es die Sicherheitsanforderungen verlangen, können Verifyingsprozesse auditierbar und datensparsam aufgezeichnet werden. Die grösste Missbrauchsgefahr liegt in der Zugriffskotrolle des Wallets,

weswegen Mindestanforderungen an Hard- und Software (e.g. Biometrics, Secure Element, etc.) zwingend sind.

4. **Hochsichere Wallets für spezielle Anwendungen müssten auf Secure Elements in Smartphones aufbauen. Derzeit sind aber noch nicht alle Smartphones damit ausgestattet und die dazu benötigten Entwicklerwerkzeuge sind noch nicht vollständig und einfach verfügbar.**

Auf jeden Fall braucht eine E-ID ein Wallet mit Secure-Element, ansonsten ist sie beliebig auf andere Devices kopierbar (siehe DE ID-Wallet). Damit sich die digitalen Signaturen (QES) endlich durchsetzen, braucht es die neueste Generation von Smartphones sowieso, welche ein FIPS zertifiziertes Element haben (aktuell etwa 65% der aktuell benutzten Mobiltelefone in der Schweiz).

Die Entwicklung ist aber in vollem Gange und wird nie abgeschlossen sein. Zudem werden die meisten Anwendungen in einem zukünftigen digitalen Vertrauensnetzwerk nicht Hochsicherheitsanwendungen sein. Risikobasierte Mindestanforderungen für Hard- und Software von Wallets, Verifying und Issueing agents und andere Systemkomponenten können höchstmögliche Sicherheit garantieren. Benchmark soll nicht die maximale Sicherheit sein, sondern eine Verbesserung des heute real existierenden Sicherheitsniveaus (Beispiele: Altersverifikation mittels ID eines älteren Geschwisters, Papierdokumente als Ausbildungszeugnisse).

Kommentar zum Kapitel 5.2 - Warum SSI besser als PKI ist

Im Gegensatz zu PKI können bei SSI einzelne Attribute eines Verified Credential präsentiert werden sowie Zero-Knowledge-Proofs. Dies ermöglicht es, den in den Motionen geforderten Datensparsamkeit-Ansatz optimal gerecht zu werden.

Zudem ermöglicht SSI im Gegensatz zu PKI die kombinierte Abfragen aus verschiedenen Verified Credential durchzuführen (z.B. Basis-Identität und Delta-Verified Credential). Somit vermeidet man das Duplizieren von Attributen und erhöht die Aktualität/Qualität der Daten (z.B. Name, Adresse, etc.)

Ein ganz zentraler und wichtiger Punkt ist die sogenannte *Revocation*. Bei der PKI ist das ein zentraler Dienst, welche eine Liste von revozierten Zertifikaten veröffentlicht. Um ihn zu verwenden, braucht es eine Kommunikation mit dem Dienst (OCSP) oder mit der Liste kann ein einmal gesehenes Zertifikat anhand seiner SerialNum getracked werden. Z.B. kann man einmal pro Tag abfragen, ob ein bestimmtes Mitarbeiter-Cert (z.B. CEO) revoziert wird. Im Falle von Sovrin wird dafür ein sog. Kryptographischer-Akkumulator verwendet, welcher im Ledger gespeichert ist. Dieser ist Privacy-Preserving. Und der Proof, dass ein Credential (noch) gültig ist, macht der Holder beim Erstellen eines Proof, und ist auch nur für genau diesen Zeitpunkt gültig.

Die internationale Gemeindschaft (e.g. EU, WHO, IATA, weitere) orientiert sich an souveränen und offenen digitalen Identitätsökosystemen. Somit wäre eine PKI-basierte Lösung eine Schweizer Insellösung.Diese ist im Sinne von Datensparsamkeit, Interoperabilität, Portabilität, der Nutzung von globalen Standards, sowie der nachhaltigen Etablierung einer lokalen Governance auch als Brückenlösung NICHT zu bevorzugen.

Per Mail (E-ID@bj.admin.ch)
Bundesamt für Justiz BJ
Herr Michael Schöll, Direktor
3003 Bern

Bern, 14. Oktober 2021

Stellungnahme IG eHealth zu «Zielbild E-ID

Sehr geehrter Herr Schöll

Die IG eHealth bedankt sich für die Möglichkeit zum «Zielbild E-ID» Stellung beziehen zu können.

Die IG eHealth ist der einzige Fachverband mit Expertise in den Bereichen Gesundheitspolitik, Organisation, ICT, Semantik und Technik. Sie unterstützt die digitale Transformation im Gesundheitswesen in der Schweiz proaktiv, damit Qualitäts- und Sicherheitslücken in der Behandlung abgebaut und administrative Prozesse verbessert werden.

Die IG eHealth hat im 2021 zusammen mit interessierten Verbänden die Allianz «digitale Transformation im Gesundheitswesen» gegründet. Sie vertritt die Industrie im «Beirat der Umsetzer und User» von eHealthSuisse und steht im Kontakt mit allen relevanten Stakeholdern im Gesundheitswesen.

Antworten zu den Hauptfragen:

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Mit einer staatlichen E-ID werden schweizweit rechtsgültige, digitale Identitätsnachweise geschaffen, die auch im Gesundheitswesen zum Einsatz kommen sollen. Es soll eine Rechtsgrundlage für Identitätsnachweise geschaffen werden, die in die bei Prozessen im öffentlichen und privaten Umfeld von allen Schweizer Einwohner*innen und Behörden einfach und sicher eingesetzt werden kann.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

- **Benutzerfreundlichkeit:** Die E-ID wird sich schnell und reibungslos durchsetzen, wenn diese in zahlreichen Anwendungsfällen einfach, sicher und interoperabel eingesetzt werden kann.
- **Datenschutz, Datenhoheit und Datensparsamkeit:** Die Klärung des Datenschutzes, des Umgangs mit den Daten und der Schutz der Privatsphäre sind zentral für die Akzeptanz der Lösung. Für die IG eHealth steht die SSI-Lösung im Vordergrund, weil (a) die Holder/User selbstbestimmte Entscheide fällen und (b) die Lösung aufgrund der dezentralen Datenhaltung sicher ist und dadurch Vertrauen schafft.
- **Technologieneutralität:** Die E-ID soll auf offenen, internationalen Standards basieren. Damit kann sichergestellt werden, dass diese ebenfalls international einsetzbar ist und weiterentwickelt werden kann.

Interessengemeinschaft eHealth, Amthausgasse 18, 3011 Bern
Tel. 031 560 00 24, Fax 031 560 00 25, info@ig-ehealth.ch

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Der Staat hat die technologieneutrale Rechtsgrundlage zu schaffen für eine sichere technische Infrastruktur für digitale Ökosysteme. Im Fokus steht die Herausgabe der Identitäten und auch Credentials. Credentials sollen hoheitlich vom Staat, aber auch von Dritten, z.B. Universitäten, Spitäler, Verbände oder Firmen, herausgegeben werden können. Dazu braucht es keine Bundes-PKI.

Empfehlung IG eHealth: «E-ID-Lösung mittels Self-Sovereign Identity»

Für die digitale Transformation ist es zentral, dass Gesundheitsdatenökosysteme geschaffen werden, was u.a. eindeutige Identitäten voraussetzt. Die E-ID und SSI sind Hilfsmittel, die für das Funktionieren dieser Ökosysteme unerlässlich sind.

Empfehlung bezüglich Ambitionsniveau:

Die Rolle des Staates beschränkt sich auf die Aufgabe, die er in der physischen Welt übernimmt. Er gibt amtliche Dokumente heraus und schafft den Rechtsrahmen für deren Anwendung. Diese Aufgabe muss nun in die digitale Welt übertragen werden.

Ziel ist es, das Ambitionisniveau 3 zu erreichen. Es ist allerdings ein Balanceakt zwischen notwendiger Regulierung, die Vertrauen schafft, und flexibler Lösung, welche den Aufbau und die dynamische Entwicklung von privaten und öffentlichen Ökosystemen zulässt.

Freundliche Grüsse

Freundliche Grüsse
Im Namen des Vorstands

Anna Hitz
Präsidentin IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Stiftung für Konsumentenschutz
Nordring 4
Postfach
3001 Bern

Bundesamt für Justiz
Bundesrain 20
3003 Bern
Per E-Mail: E-ID@bj.admin.ch

Rückfragen:
Lucien Jucker, Leiter Datenschutz / Digitalisierung / IT
l.jucker@konsumentenschutz.ch

Bern, 30. September 2021

Stellungnahme zur öffentlichen Konsultation zum «Zielbild E-ID»

Sehr geehrter Herr Schöll
Sehr geehrte Damen und Herren

Vielen Dank für die Möglichkeit, an der öffentlichen Konsultation zum «Zielbild E-ID» 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 zu den Fragen und ausgewählten Aspekten wie folgt Stellung:

Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?
Die staatliche E-ID soll mindestens so **sicher** wie die physische Identitätskarte sein. Damit ist einerseits die Manipulations- und Fälschungssicherheit gemeint. Gleichzeitig muss die Bevölkerung die Möglichkeit haben, die Authentizität einer E-ID zu überprüfen.
Die staatlich herausgegebene E-ID soll den Nutzerinnen und Nutzern einen **Mehrwert bieten**, z.B. das Bestellen eines digitalen Registerauszugs. Ein wichtiger Mehrwert im Vergleich zur bestehenden physischen Lösung wäre die Datensparsamkeit.
Die **Datensparsamkeit** ist in Art. 7 Abs. 3 des neuen Datenschutzgesetzes verankert. Die staatlich herausgegebene E-ID soll nur so viel Daten übermitteln, wie für den konkreten Anwendungsfall notwendig sind. Wenn also überprüft wird, ob eine Person volljährig ist, soll nicht das gesamte Geburtsdatum abgefragt werden. Stattdessen soll die E-ID nur die Frage nach der Volljährigkeit im Überprüfungszeitpunkt beantworten. Bei einer Abfrage der Informationen sollen die Inhaberinnen und Inhaber der E-ID zudem die Möglichkeit haben, nicht alle angefragten Daten zu übermitteln, damit nicht willkürlich Daten abgefragt werden. Schliesslich können einmal übermittelte Daten nicht zurückgeholt werden.
Für uns ist klar, dass eine staatliche E-ID nur dann eine ist, wenn der Staat sie herausgibt. Eine E-ID der immer weiter privatisierten Post (SwissSign) ist schon deshalb keine Lösung.

Aber auch die zahlreichen Tracking- und Analyselösungen (Google, Facebook, Amazon usw.) auf der Post-Webseite zeigen deutlich, dass Datensparsamkeit der Post kein Anliegen ist. Die fehlende Ablehnungsmöglichkeit für Besucherinnen bestätigt diesen Eindruck.

Welche Anwendungsfälle der E-ID stehen im Vordergrund?
Im Grundsatz soll die E-ID ein digitaler Ausweis sein, mit dem z.B. Alter, Krankenversicherung, Führerschein oder Covid-Zertifikat nachgewiesen werden kann. Auch der Bezug und das Vorweisen von Registerauszügen (z.B. Betreibungsregister) soll einfach und digital möglich werden. Weitere E-Government-Anwendungen sind denkbar.
Die E-ID soll als qualifizierte elektronische Unterschrift im In- und Ausland verwendet werden können. Zudem könnte die E-ID das rechtsgültige elektronische Unterzeichnen von Initiativen und Referenden (E-Collecting) ermöglichen. Wenn die E-ID die Stimmberechtigung enthielte, könnten ungültige elektronische Unterschriften sogar vollständig verhindert werden.
Die E-ID soll keine Login-Möglichkeit für Online-Shopping oder andere Online-Dienste von Privaten sein. Das ist letztendlich auch im Interesse einer breiten Akzeptanz der E-ID in der Bevölkerung. Die Verwendung als ein solches Login würde zu Bedenken in der Bevölkerung führen und womöglich das Vertrauen in die E-ID erodieren.

Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z.B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?
Die Konsumentinnen und Konsumenten würden davon je nach Ausgestaltung und Ambitionsniveau unterschiedlich stark profitieren. Je mehr physische Ausweise von einer einzigen E-ID abgelöst werden, desto grösser wird der Einsatzbereich und damit der Nutzen für die Inhaberinnen. Aufgrund der staatlichen Herausgabe der E-ID wird sie grosses Vertrauen in der Bevölkerung geniessen, solange dieses nicht mit Anliegen wie der Nutzung als Online-Shopping-Login torpediert wird.

Kein Abbau bestehender staatlicher Services
Dem Konsumentenschutz ist es ein grosses Anliegen, dass das Einführen der E-ID für Personen, die sich gegen die E-ID entscheiden (oder keine erhalten können), keine Service-Verschlechterung bedeutet. Da die E-ID ihren Inhaberinnen ab Ambitionsniveau 2 teilweise den Gang zum Amt erspart, könnte die Folge sein, dass noch kürzere Öffnungszeiten angeboten oder Preise erhöht werden. Schon jetzt gibt es Ämter, die nur einige Stunden pro Woche offen haben – dieses Problem soll durch die E-ID nicht weiter verschärft werden. Ein Abbau oder gar eine Verteuerung von bestehenden staatlichen Services darf nicht erfolgen.

Weitere Bemerkungen
Die Bewertung der technischen Detailfragen der vorgestellten Lösungsansätze überlassen wir anderen Organisationen. Aufgrund unseres Grundanliegens einer datensparsamen E-ID eignet sich wohl die Self-Sovereign Identity (SSI) am besten. Das IdP-Modell ist durch das gescheiterte E-ID-Gesetz stark vorbelastet und sollte schon deshalb nicht verfolgt werden.

Wir danken Ihnen für die Kenntnisnahme unserer Antworten und Bemerkungen und stehen Ihnen bei Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Sig. Sara Stalder
Geschäftsleiterin

Sig. Lucien Jucker
Leiter Datenschutz

Stiftung für Konsumentenschutz, Nordring 4, Postfach, 3001 Bern, Tel. 031 370 24 24, Bestellungen: Tel. 031 370 24 34
info@konsumentenschutz.ch, konsumentenschutz.ch, CHE-107.809.718 MWST, BIC POFICHBEXXX, IBAN CH37 0900 0000 3002 4251 3

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Bundesamt für Justiz
3003 Bern

per E-Mail:
E-ID@bj.admin.ch

Bern, den 07. Oktober 2021

Diskussionspapier «Zielbild E-ID»
Stellungnahme

Sehr geehrte Damen und Herren

privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, hat u.a. zum Zweck, den Anliegen des Datenschutzes Nachdruck zu verschaffen. In diesem Sinne äussert sich privatim zu Rechtsetzungsentwürfen und Projekten, die für den Datenschutz erheblich sind.

Gerne nehmen wir zum Diskussionspapier «Zielbild E-ID» wie folgt Stellung, verzichten dabei aber auf eine Bewertung der skizzierten (technischen) Lösungsansätze. Eine Auswahl und Bewertung der Lösungsansätze müsste u.E. erst in einem zweiten Schritt erfolgen, nachdem im ersten Schritt Anforderungen und Priorisierung geklärt worden sind.

Eine zuverlässige, sichere und datenschutzfreundliche E-ID ist sehr zu begrüssen und bildet eine wichtige Grundlage für weitere Digitalisierungsvorhaben im öffentlichen und privaten Bereich. Auch wenn beim Zweck nachvollziehbar und sinnvoll festgehalten ist: «*Das «Zielbild E-ID» verzichtet bewusst auf die Beschreibung und Bewertung einer endgültigen Lösung*» (Diskussionspapier, S. 7) erscheint eine Gewichtung der Kriterien, welche mit der E-ID erfüllt werden sollen, unabdingbar. Diesem Umstand trägt auch Kapitel 2.4 im Diskussionspapier Rechnung und führt aus, dass einige Anforderungen im Widerspruch zueinander stehen oder zumindest ein Spannungsfeld bergen. Wird diese Gewichtung nicht vorgenommen, besteht die erhebliche Gefahr, dass nicht vereinbare Anforderungen umgesetzt werden sollen und am Ende erneut keine taugliche Lösung zur Verfügung steht. Die Auswahl der technischen Lösung (inkl. Architektur des Systems) und Umsetzung muss den Anforderungen und der Gewichtung der Kriterien folgen. Es kann u.E. nicht pauschal davon ausgegangen werden, dass ein zentraler oder dezentraler Ansatz per se besser oder sicherer wäre. Entscheidend erscheint für eine taugliche E-ID zudem, dass soweit wie möglich auf bereits etablierte Lösungsansätze und Technologien gesetzt wird.

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, CH-3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

Das Fehlen einer praxistauglichen, datenschutzfreundlichen und sicheren E-ID ist aktuell ein grosses Hemmnis bei Digitalisierungsvorhaben. Es kann festgestellt werden, dass Prozesse, die a) eine eindeutige und zuverlässige Identifikation voraussetzen, b) eine rechtsverbindliche Unterschrift erfordern und c) ein hohes Mass an Integrität (Unveränderbarkeit des Inhalts) voraussetzen, schwierig bis nicht umgesetzt werden können. In der Umsetzung kommt derzeit hinzu, dass jeder (öffentliche und private) Anbieter aufgrund des Fehlens einer tauglichen zentralen Lösung eine eigene, proprietäre Lösung aufbauen und betreiben muss.

Aus dieser Betrachtung folgt u.E. folgende Priorisierung der Anforderungen:

- Verhinderung von Identitätsdiebstahl;
- Gleichwertigkeit zum analogen Ausweis und somit staatliche Aufgabe;
- Ermöglichung rechtsverbindlicher Unterschriften.

Bezüglich der Datenminimierung und des Datenschutzes sollten folgende zusätzliche Aspekte hoch gewichtet werden:

- Vom System soll nur ein Minimum an «Stammdaten» erfasst werden, die gegebenenfalls vom Benutzer ergänzt werden können.
- Es braucht klare gesetzliche Vorgaben, wie Anbieter mit den Informationen umzugehen haben, inklusive Löschvorgaben und harten Sanktionierungsmassnahmen bei Verstössen.

Bei den gesetzlichen Vorgaben sollte zudem sichergestellt werden, dass die E-ID nur bei Prozessen verlangt werden darf, bei welchen eine solche notwendig ist. Es erscheint sinnvoll, private Identitätsprovider (IdP) zuzulassen für Anwendungsfälle, welche tiefere Anforderungen an eine Zuverlässigkeit und Nachvollziehbarkeit der Identifikation voraussetzen. Diese müssten in der Folge klare Vorgaben zum Umgang mit den Informationen befolgen und staatlich kontrolliert werden.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim

SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Bundesamt für Justiz
Herrn Michael Schöll
Direktor
Bundesrain 20
3003 Bern

BSG/RR/lm 312 Bern, den 11. Oktober 2021

Öffentliche Konsultation zum «Zielbild E-ID»

Sehr geehrter Herr Schöll

Der Schweizerische Anwaltsverband (SAV) dankt Ihnen für die Gelegenheit in der obgenannten öffentlichen Konsultation Stellung nehmen zu können.

1. Vorbemerkungen

Der SAV begrüsst, dass mit der Einführung einer E-ID die Voraussetzungen zur Vereinfachung des elektronischen Rechtsverkehrs in der Schweiz geschaffen werden. Die Frage der elektronischen Identität steht in engem Zusammenhang mit dem Projekt Justitia 4.0, bei dem der Zugang zur Plattform vom Vorhandensein einer solchen Identität abhängt, die es derzeit für Anwälte nicht gibt (im Gegensatz z. B. zu Justizbehörden). Ohne E-ID ist somit der Zugang der professionellen Benutzerinnen und Benutzer, insbesondere der Anwaltschaft, auf die künftige Plattform zum elektronischen Rechtsverkehr gefährdet. In diesem Zusammenhang verweist der SAV auf seine Stellungnahme vom 26. Februar 2021 zum neuen Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ).

Die E-ID soll einer Person erlauben, sich über ihre Identität auszuweisen. Mittels Schnittstellen können so beliebige Ausweise (z.B. Führerausweise aber auch private Ausweise wie Mitarbeiterausweise) einer Person sicher zugeordnet werden. Grundsätzlich sollte bei der E-ID an einen Identitätsausweis des Staates und nicht an ein Login gedacht werden. Selbstverständlich kann die E-ID auch von einem Login-Dienst verwendet werden, um ein Benutzerkonto einer identifizierten Perso

zuzuordnen – es handelt sich bei Login und Identitätsnachweis aber um systemisch unterschiedliche Dienste.

Nach Ansicht des SAV ist im idealfall Ambitionslevel 3 anzustreben. Nicht nur sollten staatliche Stellen (Gerichte und Behörden) auf allen Ebenen eingebunden werden, sondern soweit möglich auch Private (z.B. Mitarbeiterausweise). Darüber hinaus muss die E-ID für eine qualifizierte elektronische Signatur eingesetzt werden können. Nur eine möglichst weite Verbreitung und breite Verwendungsmöglichkeiten werden der E-ID zum Erfolg verhelfen können.

Entgegen der im Diskussionspapier vertretenen Ansicht, scheint es dem SAV durchaus möglich auch mit einer Public Key Infrastruktur ("PKI") den Anforderungen an Datensparsamkeit zu genügen. Zu denken ist an hierarchisch abhängige Zertifikate, bei welchem Attribute in einzelne Tochter-Zertifikate eingeschlossen werden und der Holder jeweils diejenigen auswählen kann, die in einem spezifischen Fall notwendig sind. So könnte der Holder jeweils auf der E-ID App wählen, welche Attribute er preisgeben will (z.B. beim Disco Eingang : Bild und Alter 18 +, aber eben nicht das Geburtsdatum und ohne Namen oder Adresse; bei der Polizeikontrolle kann der volle Führerausweis gezeigt und vorgewiesen werden etc.).

Eine rein kartenbasierte PKI Lösung sollte – wie im Diskussionspapier ausführlich erörtert – nicht gewählt werden. Für eine möglichst einfache Installation oder Wiederherstellung der E-ID können physische Ausweise aber sinnvoll kombiniert werden. Hier könnte beispielsweise auf der physischen ID ein "Vater-Zertifikat" hinterlegt werden, welches dem Inhaber erlauben würde eine "verlorene" E-ID (z.B. ein defektes Smartphone) wieder herzustellen, ohne dass eine erneute physische Identifikation notwendig ist. Der Holder könnte mittels der E-ID App, dem "Vater Zertifikat" sowie der PIN die E-ID wieder neu installieren. Es ist dem SAV bewusst, dass die heutige Karten ID nicht über einen NFC-Chip verfügt. Aber dies sollte jedenfalls anlässlich der Ausschreibung neuer physischer Ausweisdokumente berücksichtigt werden.

Eine SSI Lösung bietet sich nach Ansicht des SAV nicht an, zumindest soweit das Registry auf der Blockchain / DLT sein soll. Verteiltes, anonymes Vertrauen, d.h. die Prüfung eines anonymen oder unbekannten Issuers, ist im vorliegenden Fall eben gerade nicht notwendig, da der Verifier immer wissen wird, wer der Herausgeber des zu überprüfenden Ausweises ist. In jedem Fall abzulehnen ist sodann eine Lösung mittels zentralem staatlichen Identitätsprovider. Ein solcher Ansatz scheitert an den im Diskussionspapier genannten Nachteilen.

Weiter ist sicherzustellen, dass die E-ID international akzeptiert und in grössere Systeme, wie z.B. Systeme der EU, eingebunden werden kann. Es ist deshalb wünschenswert, dass diesbezüglich das Vorgehen abgestimmt wird.

Ihre Fragen können wir danach gerne wie folgt beantworten:

2. Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Wir sehen die folgenden drei Anforderungen als besonders wichtig an:

a) **Komplette Kontrolle muss beim Nutzer liegen**: Die Daten müssen dezentral, d.h. beim *Holder* selbst gespeichert sein und dieser muss die Möglichkeit haben, diese datensparsam weiterzugeben.

b) **Einfachheit**: Die Verwendung (offene, standardisierte Protokolle) und Handhabung (Unabhängigkeit von einer spezifischen App) der E-ID sollte möglichst einfach gestaltet werden. Auch der Prozess für den Erhalt der E-ID sollte möglichst einfach sein.

c) **Sicherheit und hohe Verfügbarkeit**: Nur mit einem hohen Sicherheitsniveau kann Vertrauen geschaffen und erhalten werden. Die Systeme, auf welchen die E-ID basiert, müssen zudem eine hohe Verfügbarkeit aufweisen und möglichst unterbruchslos funktionieren.

3. Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Für den SAV steht hier die einfache Identifikation von Personen im digitalen Raum im Vordergrund. Ein grosser Teil der anwaltlichen Tätigkeit beinhaltet Kommunikation mit Dritten, insbesondere Behörden (auf allen staatlichen Ebenen, d.h. Gemeinden, Kantonen und Staat, sowie Gerichten aber auch mit Privaten). Die Kommunikation mit Privaten verlagert sich mehr und mehr in den digitalen Raum. Eine klare Identifikation der Beteiligten ist hier von besonderer Bedeutung und ist bisher noch nicht einheitlich möglich. Es wäre wünschenswert, wenn auch die Kommunikation mit Behörden von diesem Schub profitieren würde.

Identifikation wird auch im Rahmen von Justitia 4.0 ein grosses Thema darstellen, insbesondere um die Rechtsanwälte und Rechtsanwältinnen gegenüber den Gerichten und Behörden zu identifizieren. Der Vorentwurf zum Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) sieht hier lediglich die E-ID als Identifikationsmittel vor. Sollte die E-ID nicht kommen, müsste ein Identifikationssystem lediglich für diesen Zweck geschaffen werden.

4. Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z.B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsausweise) auszustellen und überprüfen zu können?

Der Hauptnutzen wäre sicherlich eine Vereinfachung des Verkehrs im digitalen Raum bei gleichzeitigem Gewinn von Sicherheit im Verkehr mit den staatlichen Behörden, sprich eGovernment in sämtlichen Ausprägungen. Hinzu kommt aber auch die Verwendung als alternatives und datensparsames Ausweisdokument bei der physischen Verwendung.

Im privaten Raum steht insbesondere die elektronische Signatur im Vordergrund. Heute ist eine aufwendige Identifizierung notwendig, die entsprechend wegfallen könnte bzw. durch die E-ID ersetzt werden könnte.

Mit dem nochmaligen Dank für die Einräumung der Gelegenheit zur Stellungnahme verbleibe wir namens des Schweizerischen Anwaltsverbandes

mit freundlichen Grüssen

Präsidentin SAV

Birgit Sambeth Glasner

Generalsekretär SAV

René Rall

Swiss Banking

Bundesamt für Justiz BJ
Herr Michael Schöll
Direktor
Bundesrain 20
3003 Bern

Per Mail zugestellt an: E-ID@bj.admin.ch

8. Oktober 2021

Stellungnahme zur öffentlichen Konsultation zum «Zielbild E-ID»

Sehr geehrter Herr Schöll
Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 2. September 2021 eröffnete öffentliche Konsultation des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zum «Zielbild E-ID». Wir bedanken uns für die Möglichkeit, uns in dieser wichtigen Angelegenheit äussern zu können. Gerne nehmen wir die Gelegenheit zur Stellungahme wahr und unterbreiten Ihnen nachfolgend, entlang Ihrer drei Leitfragen, unsere wichtigsten Anliegen.

Zusammenfassung

Eine staatlich anerkannte elektronische Identität (E-ID) stellt eine zentrale Basisinfrastruktur für die weitere Digitalisierung der Schweizer Wirtschaft, der Behörden und der Gesellschaft und damit der Wettbewerbsfähigkeit des Wirtschafts- und Finanzplatzes Schweiz dar. Sie bringt Nutzerfreundlichkeit und erhöht die Sicherheit für die Anwenderinnen und Anwender.

Für eine politisch mehrheitsfähige Lösung im Spannungsfeld von rascher, breiter und einfacher Anwendung sowie effektivem Persönlichkeits- und Datenschutz sind aus Sicht der SBVg folgende Anforderungen ausschlaggebend:

- **Sicherheit und Vertrauen**, indem mittels einer dezentralen und datensparsamen Architektur Datenschutz und die Datenhoheit der Nutzenden gewährleistet werden.
- **Benutzerfreundlichkeit und Verbreitung**, indem die E-ID sowohl einfach zu nutzen und zu erhalten ist als auch schnell eine breite Akzeptanz und Verbreitung findet, sowohl national wie auch international.
- **Kosteneffizienz und Zukunftsfähigkeit,** indem die E-ID ohne signifikanten Aufwand für die Wirtschaft implementiert und mit Blick auf zukünftige Entwicklungen flexibel um zusätzliche Funktionen in unterschiedlichen Anwendungsbereichen erweitert werden kann.

Nachfolgend nehmen wir Bezug auf die von Ihnen gestellten Fragen im Rahmen der öffentlichen Konsultation zum «Zielbild E-ID».

1. Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

a. Sicherheit und Vertrauen, indem mittels einer dezentralen und datensparsamen Architektur Datenschutz und die Datenhoheit der Nutzenden gewährleistet werden.

Eine dezentrale und datensparsame Architektur, die sich am Grundsatz «Privacy by Design» orientiert, ist entscheidend, um das Vertrauen der Nutzerinnen und Nutzer in die E-ID sicherstellen zu können. Dafür muss das wirtschaftlich zugrunde liegende Modell der E-ID bzw. der beteiligten Parteien transparent und vertrauenswürdig sein. Nur wenn die Nutzerinnen und Nutzer diesem Aspekt Vertrauen schenken, werden sie die E-ID auch einsetzen. Obschon der Lösungsansatz mittels einer Public-Key-Infrastruktur viele dieser Anforderungen ebenfalls erfüllen könnte, scheint aus Sicht der SBVg die technische Umsetzung mittels einer selbstverwalteten Identität bzw. Self-Sovereign Identity (SSI) die Anforderungen am besten abzudecken und sollte daher bei den weiteren Überlegungen zum Zielbild E-ID im Vordergrund stehen. Zwar ist dieser Ansatz neu und komplex und mit teilweise offenen Fragen verbunden, jedoch scheinen die zukünftigen Ausbaumöglichkeiten dieses Lösungsansatzes um zusätzliche Anwendungsfälle bei gleichzeitiger Wahrung von Datensparsamkeit und Datenhoheit der Nutzerinnen und Nutzer am vielversprechendsten. Dafür sind die offenen Fragen zu diesem Ansatz, unter anderem zu Governance, Zertifizierung von Walltes und Grad der Offenheit des Systems, zwingend frühzeitig zu klären. Zudem sollte die schweizerische Lösung so angelegt sein, dass die Interoperabilität mit der europäischen eIDAS gewährleistet ist.

b. Benutzerfreundlichkeit und Verbreitung, indem die E-ID sowohl einfach zu nutzen und zu erhalten ist als auch schnell eine breite Akzeptanz und Verbreitung findet, sowohl national wie auch international.

Damit eine staatlich anerkannte elektronische Identität auch rasch in der Breite angewandt wird, muss sie aus unserer Sicht benutzerfreundlich ausgestaltet sein. Dafür muss sie einfach erhältlich, sowie weit verbreitet und akzeptiert sein. Nur wenn diese Punkte erfüllt sind, kann ein solches Identifikationsmittel nachhaltig und zufriedenstellend in den Alltag der Bürgerinnen und Bürger Einzug finden.

Die gesamte Schweizer Bevölkerung sollte die Möglichkeit haben, nach der Einführung rasch und einfach auf ein staatlich anerkanntes elektronisches Identifikationsmittel zurückgreifen zu können. Dabei sollte die zügige und niederschwellige Verbreitung der E-ID im Vordergrund stehen und nicht durch komplizierte und langwierige administrative Prozesse erschwert werden. Denn nur wenn eine grosse Anzahl Nutzerinnen und Nutzer rasch eine staatlich anerkannte E-ID besitzt und diese konsequent auch verwendet werden kann, erfüllt die E-ID ihren Zweck.

Weiter muss die E-ID nicht nur einfach erhältlich, sondern auch weit verbreitet und akzeptiert sein. Dies gilt einerseits für die unterschiedlichen Unternehmen und deren Geschäftsprozesse, aber auch für die verschiedenen alltäglichen Einsatzmöglichkeiten aus Bürgersicht, namentlich auch als präferiertes Mittel für Behördengänge, von der Gemeinde- bis zur Bundesebene, nach dem Prinzip «Digital ID First». In diesem Zusammenhang ist es zentral, dass zumindest die Nutzung der E-ID für die Anwendenden analog zu anderen Identifikationsmitteln kostenlos bleibt. Weitere Überlegungen zum wirtschaftlich zugrunde liegenden Modell sind frühzeitig im Gesetzgebungsprozess zu berücksichtigen. Nicht zuletzt muss sichergestellt werden, dass die E-ID auch mit einer allfällig existierenden europäischen Lösung interoperabel ist und auch dort problemlos zur Anwendung kommen kann.

c. *Kosteneffizienz und Zukunftsfähigkeit, indem die E-ID ohne signifikanten Aufwand für die Wirtschaft implementiert und mit Blick auf zukünftige Entwicklungen flexibel um zusätzliche Funktionen in unterschiedlichen Anwendungsbereichen erweitert werden kann.*

Aus Sicht der SBVg ist es wichtig, dass die E-ID in der Schweiz vollumfänglich als rechtlich und regulatorisch gleichwertig zur physischen Identitätskarte und zum physischen Pass im Umfeld «Bank» eingesetzt werden kann. Insbesondere soll mit der E-ID eine VSB-konforme Identifikation ermöglicht werden, wie auch die Erfüllung der damit zusammenhängenden Wiederholungspflichten. Wir wünschen uns, dass mit Hilfe der E-ID der Prozess bei Video- und Online-Identifizierungen nach FINMA-RS 2016/7 massgeblich vereinfacht werden kann. In diesem Zusammenhang wäre hilfreich, wenn die E-ID elektronisch (z. B. per E-Mail) übermittelt werden könnte. Denkbar wäre eine Lösung analog «Elektronische Ausweiskopie mit qualifizierter elektronischer Signatur» nach FINMA-RS 2016/7 Rz. 38 f. Allenfalls würde es in diesem Bereich Sinn machen, die FINMA frühzeitig einzubeziehen. Sie könnte jene Anforderungen beisteuern, die ihrer Ansicht nach erfüllt sein müssen, damit im Rahmen der Video- und Online-Identifikation möglichst einfache und unkomplizierte Identifikationen möglich werden.

Die Anforderungen an die E-ID, die Identifikation unter VSB und die qualifizierte elektronische Signatur müssen unseres Erachtens ohnehin harmonisiert und aufeinander abgestimmt sein. Wer eine E-ID löst, muss die qualifizierte elektronische Signatur nach ZertEs und die Identifikation nach VSB praktisch in einem Paket erhalten, ohne dafür noch zusätzlich etwas tun zu müssen.

Mit Blick auf zukünftige technologische Entwicklungen, Bedürfnisse der Nutzenden und Bedürfnisse der Wirtschaft sollte die E-ID so ausgestaltet sein, dass sie ohne signifikanten Mehraufwand an die aktuellen technologischen Möglichkeiten angepasst und flexibel um zusätzliche Funktionen für den Einsatz in unterschiedlichen privatwirtschaftlichen und auch behördlichen Anwendungsbereichen erweitert werden kann. Wie bereits erläutert, scheint der SSI-Ansatz aus Sicht der SBVg in dieser Hinsicht den anderen im Diskussionspapier vorgestellten Ansätzen überlegen zu sein und sollte daher bei der weiteren Konkretisierung des «Zielbilds E-ID» im Vordergrund stehen.

2. Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Aus Sicht der SBVg ist das Ambitions-Niveau 3 mit der Schaffung eines Ökosystems mit digitalen Nachweisen anzustreben. Damit würde die E-ID verschiedenen Anbietern geöffnet werden und zusätzlich ein breites Publikum erreichen. Es ist zentral, dass die E-ID von Anfang an bei einer breiten Palette an privaten und staatlichen Anbietern eingesetzt werden kann. Der Fokus einer tragfähigen Lösung sollte daher beim Aufbau eines solchen Ökosystems liegen. Das bedingt aber auch, dass private Marktteilnehmer eigene Attribute mit der E-ID verknüpfen können.

Auch wenn als Nutzer der E-ID bisher primär natürliche Personen im Fokus standen, wäre es ein Anliegen der Wirtschaft, auch für juristische Personen E-ID Lösungen bereitzustellen. Entsprechende Überlegungen sollten daher ebenfalls getätigt, evaluiert und vorgeschlagen werden.

Von einem staatlich anerkannten Identifikationsmittel profitieren sowohl Bankkundinnen und Bankkunden als auch Banken. Durch die fortschreitende technologische Entwicklung verlagern Banken ihre Geschäftsprozesse immer mehr in die digitale Welt. Dabei liegt die Priorität seit jeher auf dem sicheren Zugriff auf die notwendigen Daten. Die Abwicklung elektronischer Transaktionen und der Austausch von

sensiblen bzw. schützenswerten Informationen erfordert dabei jederzeit Vertrauen in die Identität und Authentizität des Gegenübers.

Mit der E-ID wird idealerweise ein staatlich anerkanntes Identifikationsmittel geschaffen, welches den Nutzerinnen und Nutzern eine eindeutige, sichere sowie benutzerfreundliche Identifizierung ermöglicht, mit der sowohl grundlegende Finanzdienstleistungen als auch weitere Dienstleistungen aus einem breiteren Ökosystem abgedeckt werden können. Die soweit wichtigsten Anwendungsfälle aus Sicht der Banken sind nachfolgend aufgeführt:

- Onboarding von Neukunden: Für Schweizer Banken bietet eine E-ID grundsätzlich die Möglichkeit, Prozesse kundenfreundlicher und gleichzeitig effizienter auszugestalten. Als primärer Anwendungsfall steht das Onboarding von Neukunden im Zentrum. So können zum Beispiel mittels einer staatlich anerkannten E-ID Nutzen und Aufwand im Zusammenhang mit «Know-Your-Customer»-Prozessen wesentlich reduziert werden. Der Nutzen entsteht hierbei insbesondere durch eine höhere Kundenzufriedenheit (wenige Schritte bis zur Kontoeröffnung), einer Aufwandsreduktion für die Bank (geringere IT-Kosten durch verkürztes Onboarding, weniger Aufwand in der Qualitätskontrolle etc.) und durch eine höhere Datenqualität und -sicherheit.
- Elektronische Signatur: Idealerweise unterstützt eine E-ID den Einsatz von elektronischen Signaturen, welche im privaten und geschäftlichen Umfeld zu einer noch breiteren Anwendung kommen könnten. Diese erlauben eine medienbruchfreie digitale Unterzeichnung von Verträgen mit Schriftlichkeitserfordernis, beispielsweise Kredit- oder komplexere Arbeitsverträge.
- Innovative Anwendungsfälle in Ökosystemen: Nicht zuletzt würde eine staatlich anerkannte und breit verfügbare E-ID, insbesondere in Form einer SSI, den Weg für die weitere Umsetzung von innovativen Geschäftsmodellen weit über die traditionellen Finanzdienstleistungen ebnen und den nutzerzentrierten und sektorübergreifenden Datenaustausch unterstützen. So könnten Nutzerinnen und Nutzer mittels ihrer digitalen Wallet einfach und transparent ihre Einwilligung zum Austausch ihrer personenbezogenen Daten erteilen und dabei stets informiert sein, für welche Dienste und unter welchen Bedingungen ihre personenbezogenen Daten verwendet werden.

Unabhängig von den Anwendungsfällen ist es wichtig, dass ein neu konzipiertes Identifikationsmittel die Entwicklung von neuen Technologien nicht hindert, sondern diese vielmehr fördert. Dabei sollten unterschiedliche Sicherheitsstufen, mit welchen ein solches Mittel ausgestattet wird, in Betracht gezogen werden. Denn nicht jeder Geschäftsprozess benötigt notwendigerweise dieselben Sicherheitsanforderungen. Zudem muss eine neue Lösung technologieneutral sein und heute noch unbekannte künftige Anwendungsmöglichkeiten ermöglichen.

3. Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise auszustellen und überprüfen zu können?

Der Ansatz, eine nationale Infrastruktur aufzubauen, entspricht dem Bedürfnis von Staat und Wirtschaft nach einer breiten Anwendbarkeit von digitalen Nachweisen, reduzierten Kosten, Gewährleistung der Interoperabilität sowie der allgemeinen Verfügbarkeit der Daten. Zudem entspricht dieses Vorgehen auch demjenigen der EU. Dieses zielt darauf ab, dass sich Individuen und Unternehmen EU-weit ausweisen und bestimmte Informationen nachweisen können. Sowohl online und offline als auch für öffentliche oder private Dienstleistungen.

Mit einer nationalen Infrastruktur hätten Nutzerinnen und Nutzer alle persönlichen Unterlagen in einer digitalen Brieftasche (Wallet) abgespeichert und könnten diese je nach Bedarf zur Überprüfung einer Drittperson vorweisen oder auf digitalem Wege übermitteln. So könnten zum Beispiel in Zukunft Bankkredite vereinfacht beantragt und bewilligt werden. Wichtig dabei ist, dass im Sinne der Datenhoheit jede Person selbst bestimmen kann, welche Daten zu welchem Zweck an wen weitergegeben werden. Mit einem solchen Vorgehen würde man den Bürgerinnen und Bürgern einen Service zur Verfügung stellen, welcher eine einfache und sichere Identifikation im elektronischen Geschäftsverkehr garantiert und gleichzeitig die Wettbewerbsfähigkeit erhöht.

Wir danken Ihnen für die Kenntnisnahme unserer Stellungnahme und die Berücksichtigung unserer Überlegungen in Ihren weiteren Arbeiten. Wir erachten den Dialog zwischen den Behörden und der Wirtschaft in diesem wichtigen Thema als erfolgsentscheidend und stehen gerne bereit, die weitere Ausarbeitung des «Zielbilds E-ID» aktiv zu unterstützen. Gerne stehen wir Ihnen für ergänzende Auskünfte zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

August Benz
Stv. CEO, Leiter Private Banking & Asset Management

Richard Hess
Leiter Digitalisierung
Mitglied des Kaders

swiss
clinical
trial
organisation

Electronic mail
Bundesamt für Justiz
Urs Paul Holenstein
Bundesrain 20
CH-3003 Bern

Bern, 06.10.2021

Position of the Swiss Clinical Trial Organisation (SCTO)
on a governmental, electronic identity (e-ID):

To whom it may concern

The Swiss Clinical Trial Organisation (SCTO) is a research infrastructure committed to high quality, patient-oriented clinical research in Switzerland. An independent, not-for-profit organisation funded by Switzerland's State Secretariat for Education, Research and Innovation (SERI) and the Swiss National Science Foundation (SNSF). Its mission is to advance academic clinical research in Switzerland as a nationwide cooperation platform and international networking partner.

The interfaces of clinical research (= all research covered by the Swiss Human Research Act and its ordinances[1]) with e-ID are manifold. However, we consider the following two issues paramount:

1. **E-signature** applicable in compliance with the law
2. **Legal basis and digital trust infrastructure** / ecosystem **allowing secure linkage** of (sensitive) data from different sources

E-signature applicable in compliance with the law

In most cases, a consent from potential participants is needed prior to including them in clinical research projects. E-consents are digital tools to inform potential participants, however, as per current law, participants may be informed via e-consent, but still have to provide a wet ink signature if willing to participate[2]. For the future, e-consent **including e-signature** (without the need for wet ink signature anymore) is key (as has been recently shown during the pandemic). E-consent including e-signature could serve different purposes. It could be applicable to the General Consent (for the re-use of medical data and biological samples for research), clinical care as well as clinical trials. Therefore, a future e-ID must cover the needs of both, clinical care, and research, keeping in mind the sensitive nature of health data. See "**Discussion paper on the target vision for an e-ID"** (hereafter referred to as "discussion paper"), use case section 4.3.5 Electronic signatures.

[1] https://www.fedlex.admin.ch/eli/cc/2013/617/en
[2] https://swissethics.ch/en/themen/positionspapiere-leitfaden see "Conception and application of an electronic informed consent (eIC)

swiss
clinical
trial
organisation

Legal basis for data linkage and digital trust infrastructure

Furthermore, healthcare and research would benefit from the larger vision of a "a state-operated digital trust infrastructure which enables and promotes secure processes without media discontinuity" ("Discussion paper", section 2.3). The development of a digital trust infrastructure and ecosystem (as described in the "Discussion paper") **including** the necessary adaptation of various legal bases should allow linking various information sources and thus, facilitate research for the sake of better health for the Swiss society. Technically, such linkage is already possible today.

Taking these issues into account, please find our written comments on the points mentioned in the "**Discussion paper on the target vision for an e-ID",** section 7:

Where do you see the particular benefit of an e-ID, and which use cases are most important to you?

As mentioned above: **E-consent including e-signature** (without the need for wet ink signature anymore) is most important. Furthermore, a legal basis, allowing the linkage of various medical information sources under the overarching vision of a "a state-operated digital trust infrastructure which enables and promotes secure processes without media discontinuity" could have a major positive impact on biomedical research and finally on public health.

In your view, what are the three most important requirements for a governmental e-ID as a digital identity card?

Transparency: Citizen-centered and citizen involvement
Security: Data protection and security
Trust: Digital trust infrastructure solution

What benefits do you see in a national infrastructure that enables the state and private parties to issue and verify digital proofs (e.g. e-ID, digital driving licence, employee identity cards, training certificates)?

Empowerment of patients and citizens to (proactively) take informed decisions to participate or not to participate in clinical research. In the context of publicly funded clinical research: easier access to and generation of patient-relevant research results with an impact on public health and a more efficient use of public money.

The SCTO appreciates the open consultation on a governmental, electronic identity (e-ID). We are open to provide expertise and know-how for the future discussion about the two main issues raised above. Please do not hesitate to contact us.

Best regards
Swiss Clinical Trial Organisation

Prof. Christiane Pauli-Magnus
President

Annette Magnin
Managing Director

Universitäre Medizin Schweiz
Médecine Universitaire Suisse

Bundesamt für Justiz
Urs Paul Holenstein
Bundesrain 20
CH-3003 Bern

Per mail versandt an: E-ID@bj.admin.ch

Ort, Datum:	Bern, 14.10.2021	Direktwahl:	031 306 93 85
Ansprechpartnerin:	Agnes Nienhaus	E-Mail:	agnes.nienhaus@unimedsuisse.ch

Stellungnahme unimedsuisse in der Anhörung zum Zielbild der E-ID

Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, zum Entwurf des Zielbilds einer E-ID für die Schweiz Stellung nehmen zu können. Gerne möchte der Verband Universitäre Medizin Schweiz (unimedsuisse) diese Möglichkeit wahrnehmen und sich im Namen seiner Mitglieder zur Vorlage äussern.

Generelle Bemerkungen zum Nutzen einer E-ID

Im Gesundheitsbereich sind zahlreiche Bereiche vorhanden, wo die E-ID nicht nur nützlich, sondern einen wichtigen Bestandteil darstellen werden, um die Kommunikation zwischen Gesundheitsversorgern und Patinetinnen und Patienten zu ermöglichen und zu vereinfachen. Wichtig ist dazu, dass die E-ID eine E-Signatur beinhaltet, welche sicher und rechtlich gültig ist, sodass keine «wet ink signature» mehr notwendig ist, um den Willen von Individuen festzuhalten und zu dokumentieren. Eine E-ID mit E-Signatur ermöglicht dabei nicht nur eine vereinfachte Dokumentation des Willens von Patientinnen und Patienten sondern stärkt auch deren Möglichkeit, informierte Entscheide zu treffen im Hinblick auf ihre Behandlung, die gesundheitliche Vorausplanung und ihre Beteiligung an der medizinischen Forschung. Die technischen Möglichkeiten werden es in Zukunft einfacher machen, dass die Entscheide von Individuen betreffend ihre medizinischen Behandlungen oder betreffend eine Forschungseinwilligung dynamisch festgehalten werden können, sodass die Dokumentation der Willensbekundungen der Betroffenen laufend an neue Situationen anpasst und so aktuell gehalten werden kann.

Eine E-ID erleichtert es damit, dass die Fachpersonen im Gesundheitswesen den Willen des Patienten oder der Patientin eindeutig erfassen und berücksichtigen können. Mit der E-ID wird ausserdem die Forschung administrativ vereinfacht und werden neue Forschungsprojekte zum Nutzen von Betroffenen wie auch des gesamten Gesundheitssystems möglich.

Breite Anwendungsmöglichkeiten

Die Anwendungsmöglichkeiten sind breit und umfassen unter anderem:

- Die Dokumentation der Kommunikation und der von Arzt und Patient/in vereinbarten Behandlungen innerhalb des Behandlungsprozesses (z.b. in Bezug auf die Aufklärung vor Untersuchungen und Eingriffen) und Eingabe von vertraulichen, behandlungsrelevanten Daten durch den Patient oder die Patientin selbst in ein digitales Instrument zur Unterstützung der Therapie (digital health care).
- Dokumentation des Patientenwillens im Rahmen einer gesundheitlichen Vorausplanung etwa durch eine (elektronischen) Patientenverfügung, im Rahmen der ärztlichen Notfallanordnung ÄNO (u.a. betr. Reanimation im Notfall) oder der Willensbekundung betreffend eine Organspende.

- Elektronisches Patientendossier: Eine E-ID würde es die Eröffnung eines EPD durch Patientinnen und Patienten erleichtern und es ist zu hoffen, dass so mehr Personen sich zu einem solchen Schritt entscheiden. Damit würde die E-ID auch den digitalen Austausch zwischen verschiedenen Leistungserbringern des Gesundheitswesens fördern.
- Identifikation und Einbezug weiterer Personen, die wichtige Rollen wahrnehmen wie z.B. betreuende Angehörige, gesetzliche/r Vertreter/in bei nicht urteilsfähigen Personen oder therapeutische Personen ausserhalb der eigenen Institution. Diese könnten über eine E-ID besser identifiziert und mit den behandelten Personen verknüpft werden.
- Forschung: Die E-ID erleichtert die Einwilligung von Patientinnen und Patienten zur Nutzung ihrer Daten und Proben zur Forschung gemäss Humanforschungsgesetz – dem sogenannten Konsent. Dies betrifft sowohl den Generalkonsent (Einwilligung zur Forschung mit Routinedaten) wie auch die Teilnahme und Einwilligung zur Forschung bei spezifischen klinischen Studien oder im Rahmen von Registern. Ausserdem bietet die E-ID die Möglichkeit, dass Patientinnen und Patienten sich selbst mit Daten einbringen (citizen science).

Zentrale Aspekte, die bei einer E-ID zu beachten sind

unimedsuisse unterstützt die Einführung einer E-ID durch den Bund als einen «vom Staat ausgestellter digitaler Ausweis, um die eigene Identität nachweisen zu können». Die Einführung einer solchen staatlich gestützten E-ID wird für die Dokumentation des Willens der Personen im Behandlungsprozess und in der Forschung in Zukunft elementar sein. Dazu sind folgende Punkte zu beachten.

- Es braucht zwingend eine rechtlich gültige E-Signatur.
- Im Gesundheitswesen wird die gesamte Bevölkerung behandelt. Es ist deshalb elementar, dass das System von E-ID und E-Signatur ein hohes Vertrauen der Bevölkerung besitzt und einfach angewendet werden kann – die Anwendung muss sehr niederschwellig ausgestaltet sein.

Im Bericht wird ausserdem darauf hingewiesen, dass eine E-ID beinhalten kann, dass in der Schweiz eine «staatlich betriebene digitale Vertrauensinfrastruktur» umgesetzt wird, welche sichere, medienbruchfreie Prozesse ermöglicht und fördert. unimedsuisse unterstützt die Entwicklung einer derartigen «Vertrauensinfrastruktur» explizit. Sie sollte eine vereinfachte Verlinkung von medizinischen Datenquellen ermöglichen und so die medizinische Forschung und Versorgungsforschung fördern. Es ist wichtig, dass bei der weiteren Bearbeitung der Vorlage der E-ID diese Perspektive einer übergeordneten Vertrauensinfrastruktur weiter bearbeitet wird.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen bei der weiteren Bearbeitung der Vorlage und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

A. Nienhaus

Agnes Nienhaus
Geschäftsführerin unimedsuisse

eID 2.0

Document de travail eID concernant le projet d'identité électronique (eID)

Prise de position sur le document

Product	Version	Date	Author	Status
TrustID	V1.0	07.09.21	PKB, RPO, CFR	Published

Table des matières

1 Introduction

La Confédération a mandaté l'Office Fédéral de la Justice pour préparer une étude sur une future identité électronique se basant sur les résultats du référendum du 7 mars 2021 et sur les motions qui ont été déposées entre temps au Parlement. C'est le « Document de travail eID concernant le projet d'identité électronique (eID) »[1].

Afin de maintenir une lecture fluide et pertinente de celui-ci, nous avons établi notre regard en tant qu'acteur actif et doté d'une longue expérience sur ce marché par rapport aux idées forces du document de l'OFJ.

[1] https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id-f.pdf

2 Regard de CloudTrust sur le document eID OFJ

2.1 Facteurs de succès

ELCA et CloudTrust ont déjà une longue expérience de mise en place de solutions dépendantes de lois fédérales comme le Dossier Electronique du Patient (DEP), l'identité électronique dudit DEP, tout comme de participation aux consultations sur la mise en œuvre de la LSIE.

Notre expérience nous montre que des standards techniques bien établis ne sont pas une garantie de succès pour la mise en œuvre d'une loi. De nombreux autres facteurs sont à considérer pour assurer son succès :

1. **Un leadership au niveau fédéral**
   Les parties prenantes doivent pouvoir compter sur un sponsor avec une vision à long-terme et le pouvoir de la mener à bien
2. **Une vision financière à long-terme**
   Le modèle de coût et de financement doit être posé dès le départ
3. **La communication et l'implication de la population**
   Comme partie prenante principale, la population doit être informée et intégrée en toute transparence pour s'assurer de son adhésion à la vision
4. **Un fédéralisme intelligent**
   Ne déléguer que ce qui est nécessaire et raisonnable de déléguer pour minimiser la complexité du système
5. **Une gouvernance claire**
   Les opérations, le financement, l'arbitrage, la compliance, la gestion des évolutions doivent être clairement définies
6. **Une protection des investissements**
   L'écosystème doit aussi garantir une protection des investissements déjà consentis par les cantons et les entreprises privées qui auront mis en place des solutions avant l'entrée en vigueur de la loi eID 2.0.
7. **Bâtir sur l'expérience**
   Partir des expériences réussies existantes en Suisse et en Europe en les faisant fructifier pour ne pas perdre du temps en partant d'une feuille blanche

La mise en œuvre de cette loi ne fait pas exception à la règle. Les mises en œuvre citées plus haut ont soit échoué, soit atteint des résultats loin des attentes initiales pour avoir manqué de clarifier l'un ou l'autre des facteurs de succès.

2.2 Niveau d'ambition

La loi européenne eIDAS est en vigueur depuis 2016 avec les premières identités émises dans les années qui ont suivi au niveau d'ambition 1. L'UE révise la loi en 2021 (EUid[2]) en ambitionnant le niveau 3, se basant sur une adoption réussie du niveau 1.

En parallèle la Suisse n'est pas encore au niveau 1 et n'a pas encore réussi à convaincre sa population de sa nécessité.

Dans ce contexte, créer un écosystème ambitieux au niveau 3 comme l'Union Européenne sans l'expérience d'un déploiement réussi au niveau 1 nous semble difficile. A contrario plus une solution est utile et présente dans le quotidien des citoyens, plus elle aura de chances d'être adoptée.

C'est pourquoi nous recommandons de viser au départ une ambition de niveau 2 : une identité électronique opérée et garantie par l'Etat, une infrastructure PKI pour la signature de documents émanant de l'Etat, combinée à des services disponibles au démarrage.

2.3 Cadre légal

La nouvelle loi eID 2.0 doit remplacer l'entrelac de lois suisses existantes : ZertES, LDEP et FINMA par exemple. En particulier, cette nouvelle loi doit remplacer la réglementation eID contenue dans la LDEP[3] qui a montré ses limites.

Ceci pour éviter un grand nombre de certifications concurrentes et coûteuses pour les différentes fournisseurs de systèmes. Et surtout pour éviter des identifications similaires et multiples selon des lois différentes pour les citoyens.

Cette loi doit aussi être compatible avec eIDAS et la future loi EUid pour permettre aux citoyens suisses d'interagir sans encombre avec des institutions européennes et vice-versa.

La loi ne doit pas donner de précisions techniques et doit se contenter de préciser la gouvernance de cette eID 2.0.

Ainsi une identité eID 2.0 permettra de s'identifier dans tous les domaines d'applications (santé, financier, cyberadministration) sans nécessiter de nouvelle certification coûteuse et évitera à un citoyen de devoir se faire identifier plusieurs fois régulièrement. Que ce soit en Suisse ou en Europe.

[2] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid

[3] https://www.bag.admin.ch/dam/bag/fr/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/anhang_8_epdv_edi_ausgabe_2.1.pdf.download.pdf/EPDV-EDI_Anhang_8_FR_Ausgabe_2.1.pdf

2.4 Infrastructure

Le modèle de l'identité souveraine (SSI) est le plus séduisant sur le long-terme et celui qui répond le plus aux exigences politiques. Plusieurs entreprises en Suisse et dans le monde se sont déjà attaqués à la réalisation d'une telle solution, mais à notre connaissance aucune n'a encore d'implémentation à large échelle utilisable par un gouvernement pour ses citoyens.

De plus, l'architecture SSI contient encore de nombreux éléments de standardisation et réglementaires qui ne sont pas clairs et risquent d'augmenter la durée de la mise en œuvre dans un environnement fédéral aussi complexe que la Suisse.

Bien que nous croyions fermement à cette solution pour le long-terme, nous sommes d'avis que la Suisse n'est pas encore mûre pour une mise en œuvre rapide du SSI dans le cadre la future loi eID. Il y a trop de risques annexes existants pour prendre celui de la technologie en plus.

En parallèle, l'architecture PKI fonctionne bien pour les documents émis par l'Etat mais ne permet pas une utilisation comme système de login simple.

L'architecture IDP est bien maîtrisée. Toutefois une centralisation de l'IDP va à l'encontre des projets cantonaux actuels et de la culture politique fédérale de la Confédération.

CloudTrust soutient donc la variante IDP en combinaison avec une infrastructure PKI, complétée par des applications de base au démarrage car c'est celle qui est la plus ouverte et la plus flexible pour le futur tout en permettant à l'économie suisse de bénéficier d'un écosystème de confiance innovant sans lourdeur administrative.

L'architecture proposée fournira une base d'expérience et de confiance qui sera très utile pour passer à une infrastructure SSI pour une eID 3.0, plus difficile à expliquer à la population.

Nous soutenons aussi une compatibilité maximale avec les standards européens (EUid, eIDAS) pour pouvoir exporter notre savoir-faire et notre capacité d'innovation sans entraves en Europe. Le « Swiss Finish » qui entrave la compatibilité avec le reste du continent est à proscrire absolument. La souveraineté de la solution (opérations, distribution) doit cependant absolument rester en Suisse pour obtenir la confiance de la population.

Une approche Open Source de la solution est aussi un autre moyen de garantir la transparence de l'infrastructure et garantir la confiance de la population et des experts en sécurité.

2.5 Ecosystème de base

CloudTrust est d'avis que l'infrastructure intermédiaire avant le SSI devrait comporter les éléments suivants, basé sur des recettes éprouvées plus facilement compréhensibles par la population suisse.

1. **Des IdP décentralisés et fédérés au niveau suisse**
    - Chaque canton ou groupement de cantons opère un IdP sous le contrôle de la Confédération pour une compliance nationale des processus
    - La base technologique peut être fédérale ou non
    - L'exigence de décentralisation est ainsi en partie remplie
    - Un modèle de fédération ou de brokering permet à chaque citoyen d'utiliser son identité dans toute la Suisse et en Europe
2. **Une infrastructure à clés publiques (PKI) décentralisée et fédérée pour les cantons et la Confédération**
    - La base technologique peut être fédérale ou non
    - Chaque organisme qui doit approuver des documents obtient une clé privée qui permet de signer des attestations ou des légitimations
    - Le point d'accès doit être unique pour en faciliter les opérations
    - Cette infrastructure est intégrée à l'IdP fédéré et permet de lier les attestations et légitimation à l'identité du sujet au moment de la signature du document
    - Infrastructure limitée à l'Etat dans un premier temps pour gagner la confiance des citoyens (ambition niveau 2 avant niveau 3)
    - Annuaire centralisé des clés publiques pour permettre une vérification facile des attestations et légitimations
3. **Des services associés dès le démarrage**
    - **Une intégration des services d'authentification** avec le plus de portails de cyberadministration possibles.
    - **Un service de signature électronique qualifié personnelle** convivial lié à l'IdP fédéré permet à tout un chacun de signer des documents électroniquement au niveau qualifié dès l'obtention d'une eID.
    - **Des applications « wallet »** développés par la Confédération ou des privés contenant les identités, les attestations et les légitimations.
    - **Une application de vérification unique** pour les identités, les attestations et les légitimations

3 Autres thèmes ouverts

3.1 Identités multiples

L'usage actuel des identités non régulées montre que les citoyens sont habitués à gérer plusieurs identités en parallèle, qu'elles soient liées entre elles ou non.

Imaginer qu'un citoyen puisse s'authentifier auprès d'un grand nombre de fournisseurs de services avec une seule identité est irréaliste.

Un citoyen est appelé à évoluer dans plusieurs contextes et avec plusieurs rôles qui peuvent se chevaucher. Ces rôles et contextes peuvent évoluer au cours du temps.

Quelques exemple de rôles, contextes et applications :

- Citoyen : interactions avec l'administration, eVoting
- Privé : relations bancaires, eCommerce
- Entreprise : registre du commerce, signature électronique comme fondé de pouvoir, signature d'offres
- Professionnel : Légitimation de médecin, accès à eJustice, expertises comme garagiste
- Privé discret : sites santé et DEP, sites « adultes »

Toutes ces identités ont des exigences d'identification différentes et nécessitent parfois une étanchéité en termes de suivi des utilisations entre les domaines.

De ce fait nous pensons que la future identité électronique fédérale doit pouvoir coexister avec d'autres identités étatiques, semi-étatiques et privées. Et que l'identification au niveau de l'eID fédérale doit pouvoir être portée à d'autres identités du citoyen si celui-ci le désire pour une meilleure expérience utilisateur et devoir lui éviter de faire identifier selon le même processus de multiples fois.

3.2 Accréditations

Un même individu peut donc avoir plusieurs identités distinctes et indépendantes. Cependant elles sont toutes rattachées à la même personne qui doit être identifiée formellement selon des processus de KYC (Know Your Customer).

Une mise en œuvre idéale doit pouvoir réutiliser une identification réussie pour la propager aux autres identités de la même personne, augmentant ainsi la valeur ajoutée du KYC initial et amenant une facilité d'utilisation de ces identités au citoyen par une identification unique.

3.3 Décentralisation

La décentralisation des données est un élément clé du mandat politique donné aux concepteurs de la nouvelle loi eID 2.0.

Tout d'abord il faut voir ce que l'on entend par décentralisation. Pour notre part nous voyons deux types de décentralisation :

1. **Stockage des données d'identité**
   Auprès de l'utilisateur ; dans une infrastructure publique (base de données, blockchain) régionale ou nationale
2. **Regroupement des identités**
   Wallet, fournisseurs d'identité séparés

Cette décentralisation doit non seulement couvrir les attributs des identités (point 1) et les documents associés, mais aussi les informations de connexion aux différents fournisseurs de services (point 2). Ceci pour garantir un respect maximal de la vie privée.

3.4 Ecosystème

Une solution n'est utile que si elle répond à des besoins connus ou sous-jacents des utilisateurs. C'est pourquoi l'eID du futur ne doit pas être conçue uniquement sous forme de loi, mais comme une offre complète immédiatement utilisable avec un nombre minimal de services universels présents.

Les besoins en transformation numérique de la Suisse sont énormes. L'eID et les services associés contribueront à combler le fossé qui sépare la Suisse de la modernité et initier un cercle vertueux de modernisation des services à la population.

Nous pensons donc que les services suivants doivent être disponibles au démarrage:

eID

1. **eID de base comme identification numérique**
   Brique de base pour une intégration des services d'authentification (login) avec le plus de portails de cyberadministration ou privés possibles.
2. **eID de base avec photo comme identification physique**
   Plus besoin de montrer sa carte d'identité, une image des attributs avec la photo peut être montrée depuis le smartphone.

eDocs

3. **Légitimations d'Etat et similaires**
   Légitimation pour une fonction, un rôle ou une appartenance délivré par une organisation étatique ou non. Elle peut avoir une durée de validité limitée ou exiger une vérification dynamique, mais est prévue pour une longue durée.

   Quelques exemples : permis de conduire, carte d'assurance maladie, diplôme scolaire ou

4. **Attestations numériques d'Etat réutilisables avec durée de validité**
   Attestation pour un statut ou un fait. Document à durée de vie limitée qui se présente sous forme d'un document lié à l'identité du porteur. Il a une durée de vie limitée et est valable au moment de son émission.

   Quelques exemples : attestation de domicile, extrait des poursuites, livret de famille, certificat d'Etat Civil.

eSignature

5. **eSignature liée à l'eID**
   Signature électronique avancée et qualifiée personnelle, conviviale et liée à l'eID selon eIDAS et SCSE (ZertES en allemand). Cela permettra à tout citoyen de signer des documents électroniquement dès l'obtention d'une eID.

eApps

6. **Portefeuille citoyen « Citizen Wallet »**
   Des applications « wallet » contenant les identités, les attestations et les légitimations.
7. **Application de vérification universelle**
   Une application de vérification unique pour les identités, les attestations et les légitimations qui permette à toute autorité ou institution autorisée de vérifier la légitimité et la cohérence de ces informations

3.5 Succès rapides

L'établissement de cette nouvelle loi eID 2.0 prendra du temps, comme tout processus législatif. Nous pouvons saisir cette opportunité pour préparer le terrain et être prêts à lancer l'eID 2.0 rapidement dès que la loi sera en vigueur en réalisant quelques tâches de préparation.

Nous vous proposons d'entamer les chantiers suivants.

eID

- Définition des champs de base et des champs facultatifs de la future eID

eDocuments

- Spécification des formats numériques des documents les plus courants. Suivant lesquels des standards internationaux ou nationaux existent déjà et il n'est évidemment pas nécessaire de réinventer la roue
  - Carte d'identité
  - Passeport
  - Permis de conduire
  - Certificat des poursuites
  - Certificat d'Etat Civil

4 Questions de l'OFJ

Quelles sont les trois principales exigences auxquelles doit satisfaire une e-ID étatique comme moyen d'identification numérique ?

1. La comptabilité avec les standards européens eIDAS et EUid
2. La confiance de la population
3. La facilité de compréhension et d'utilisation

Quels sont les principaux domaines d'utilisation de l'e-ID ?

1. Identité numérique pour l'authentification auprès de services étatiques et privés
2. Identité équivalente à la carte d'identité pour l'identification physique
3. Signature électronique de niveau qualifiée
4. Emission, stockage, transmission et contrôle de eDocuments (légitimations et attestations)

Quels sont les avantages d'une infrastructure nationale permettant à l'État et aux particuliers de prouver et de contrôler électroniquement l'identité (par ex. e-ID, permis de conduire, pièce de légitimation de collaborateur ou carte d'étudiant numériques) ?

1. Permettre des flux d'informations entièrement numériques avec authentification de l'émetteur et de l'identité sans passage par des médias analogiques
2. Faciliter la transition numérique de processus administratifs et privés
3. Augmenter la sécurité de l'authentification de personnes, à la fois en ligne et physiquement
4. Lier une identité avec un émetteur dans un eDocument pour une vérification facilitée de la validité complète d'un tel document

Partisia Blockchain

Disclamer : *Ce document a été préparé et écrit par la société DuoKey active en cybersecurité et présente en Suisse. DuoKey est aussi membre de la foundation Suisse Partisia Blockchain (www.partisiablockchain.com). Ceci propose notre vision d'un système eID qui respecte la protection des données et la privacy de nos citoyens basés sur une blockchain permettant les* transaction Zero-Knowledge Proofs ; contact : Mr Nagib Aouini, CEO et fondateur de DuoKey – email : nagib.aouini@duokey.ch

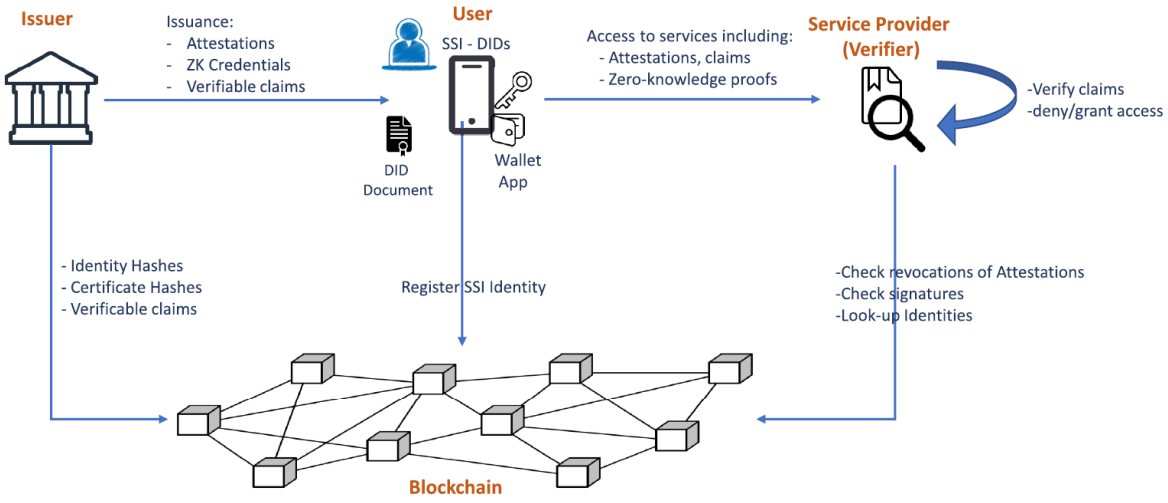
Une solution SSI qui respecte la protection des données personnelles pour l'e-ID Suisse : quels sont les avantages ?

Le terme SSI (Self Sovereign Identity) se réfère à un système de gestion d'identifiant digital qui permet à un individu ou à une entité d'avoir le contrôle exclusif de son identité numérique. Contrairement aux méthodes d'authentifications actuelles, un système SSI respecte la sphère privée de l'utilisateur et ne dépend pas de partis tiers (i.e. les données personnelles ne sont jamais stockées autre part que dans le portefeuille digital de l'utilisateur, local à son téléphone).

A l'heure actuelle, le stockage de donnée est centralisé. Les communes stockent toutes les données personnelles de ses citoyens (liens familiaux, dates de naissances, casiers judiciaires, etc.). Différents prestataires de services tels que les hôpitaux, Swisscom, SBB-CFF, Migros, Coop, Le Shop etc. stockent une variété de données personnelles sur lesquelles les sujets n'ont finalement que très peu de contrôle. Ces bases de données centrales constituent des SPO (Single point of Failure) contre les cyberattaques et nuisent à la sphère privée des individus (i.e. les données peuvent être utilisées par des partis tiers sans que les sujets puissent s'y objecter). Ceci nuit à la démocratie de notre pays.

Le potentiel de l'administration en ligne avec une SSI-eID est le scénario selon lequel les identités des citoyens sont enregistrées dans la blockchain, ce qui ajoute un nouveau champ d'application où le modèle SSI pourrait être exploité pour faire face aux aspects de la vie privée. En effet, l'intégration des technologies blockchain dans les services administratifs a suscité l'intérêt des gouvernements de différents pays, comme la Suisse, la Finlande (pour les services d'immigration) ou l'Estonie, qui est devenue le premier pays à utiliser la blockchain pour les soins de santé à l'échelle nationale, et à permettre aux personnes de n'importe où de devenir un e-résident. L'identité numérique

délivrée par l'administration estonienne permet de mener des activités commerciales, ainsi que des activités gouvernementales. Dans ce scénario, il est nécessaire de garantir la vie privée des citoyens en adoptant des approches de divulgation minimale lors de l'accès aux services correspondants.



La blockchain matérialise le système SSI, elle permet de construire une base de données d'identifiant (DID) distribuée qui respecte les principes d'accès (les utilisateurs doivent avoir accès à leur données), de transparence (projet Open Source), de consentement (l'utilisateur doit approuver l'utilisation de ses données), de portabilité et d'interopérabilité (les identifiants doivent être utilisables aussi largement que possible). Afin de garder l'anonymité de l'utilisateur aucune donnée personnelle (même encryptée) est stockée sur la blockchain, ceci grâce à l'utilisations de DIDs (Decentralized Identifiers) et de techniques cryptographiques conçues pour protéger la vie privée tels que les ZKP (Zero Knowledge Proof) et la SMPC (Secure Multiple Party Computation). Alors que les meilleures pratiques actuelles fournissent les premiers candidats importants pour une infrastructure de blockchain sécurisée, l'un des compromis les plus critiques est le manque de confidentialité.

Sans confidentialité, la perturbation potentielle des tiers existants sera limitée par le manque de conformité, l'adoption réduite et le transfert réel du pouvoir et du contrôle des données. C'est ce que reconnaissent de nombreux acteurs centraux de l'industrie de la blockchain. Un indicateur clé est l'importance croissante accordée aux preuves ZK proofs. Les preuves ZK sont une première étape importante pour ajouter la confidentialité à une infrastructure décentralisée viable et sécurisée.

Le bénéfice d'un système blockchain supportant les ZKP et la SMPC pour du SSI

L'absence de confidentialité et de respect de la vie privée sur les blockchains est évidente et entrave leur adoption et leur utilisation. Bien que des tentatives initiales aient été faites pour remédier à cette faiblesse, une blockchaine « privacy-by-design » devrait fournir une plateforme complète pour orchestrer et offrir des calculs Zero-Knowledge (ZK) sur la chaîne, hors chaîne et entre les blockchains (inter-chaîne).

Une solution innovante pour générer la fonctionnalité d'une base de données partagée sans avoir à révéler les données est le calcul multipartite sécurisé (MPC). Le MPC est une "boîte à outils" de techniques cryptographiques qui permet à plusieurs parties différentes de calculer conjointement des données, comme si elles disposaient d'une base de données partagée. Les techniques cryptographiques sont utilisées pour protéger les données, afin qu'elles puissent être analysées d'une manière qui empêche les parties concernées de pouvoir consulter les données des autres. Les parties participantes déterminent qui est autorisé à voir le résultat du calcul.

Dans un concept SSI avec ZKP, nous proposons une approche complètement différente en utilisant une communauté fédérale de nœuds de calcul ZK (qui peuvent être hébergés par des universités suisses et des écoles EPF, EPFL, ETH ... comme l'infrastructure SWITCH AAI). Chaque canton gérera et exploitera son propre nœud de calcul ZK pour valider toute transaction et vérification d'un citoyen suisse qui souhaite prouver son identité à un fournisseur de services tout en préservant la confidentialité et la traçabilité de ses demandes.

Prenons un simple scénario de preuve d'âge. En Suisse, par exemple, vous devez avoir 18 ans pour acheter de l'alcool fort. Et si vous pouviez prouver que vous avez au moins 18 ans au site ou au commerçant sans révéler votre date de naissance réelle ? Au lieu de leur remettre votre permis de conduire ou carte d'identité (qui comprend votre date de naissance et d'autres informations personnelles telles que votre adresse), un ZKP vous permettrait d'envoyer une preuve numérique indiquant simplement que vous avez 18 ans ou plus.

Voici d'autres cas d'utilisation potentiels des ZKP :

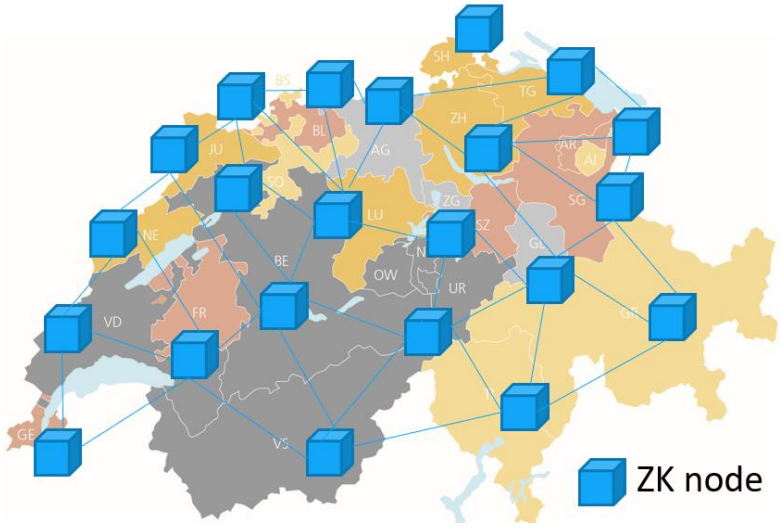
- **Qualification pour un prêt** : au lieu de refaire un processus complet KYC à la banque, vous pouvez utiliser un ZKP pour prouver que KYC et votre risque est inférieur à un certain nombre. La banque peut être sûre que votre crédit est supérieur à un certain seuil qu'elle définit, et vous n'avez pas besoin de révéler plus que nécessaire.

- **Preuve d'adresse** : si vous devez prouver que vous habitez dans une certaine circonscription électorale, vous pouvez utiliser un ZKP pour prouver que vous habitez dans la bonne zone, sans divulguer votre adresse.
- **Prouvez que vous n'êtes pas un robot / bot** : En utilisant des ZKP, vous pourriez prouver que vous êtes une personne vérifiée dans n'importe quel flux d'affaires, sans divulguer aucune information sur vous-même.

Ces scénarios sont centrés sur les caractéristiques humaines, mais il existe également de nombreux cas d'utilisation intéressants dans les domaines industriel, médical, automobile et autres. Les ZKP sont utiles chaque fois que la confidentialité ou la minimisation des données est une priorité.

Quels niveaux de gouvernance existe-t-il et qui est compétent en la matière ?

Le niveau de gouvernance est déterminé au niveau du registre de la blockchain, les nœuds seront par exemple gérés par les cantons ainsi que les universités qui sont des établissements publics ou banques avec les capacités d'hébergement des nœuds de validation des preuves ZKP.



L'État doit-il avoir le monopole sur certains éléments? Doit-il certifier les portefeuilles électroniques? Le choix du portefeuille et de l'agent institutionnel est-il laissé à l'utilisateur? Une réglementation distingue-t-elle les parties qui doivent être conçues et exploitées de manière coopérative ou plutôt concurrentielle ?

Les portefeuilles électroniques sont un maillon essentiel de l'e-ID et la chaîne de confiance. Ils doivent bien entendu être revu et certifiés (pour éviter des failles majeures

de sécurité) sur la protection des données des citoyens et éviter que des plugins et librairies tierces accumulent des données sur les utilisations du wallet.

Dans tous les cas le portefeuille utilisé doit être du développement Open Source. L'Etat aura toujours le monopole sur l'émission des passeports et de carte d'identités, il est *l'issuer* de certificat. Nous pensons qu'une approche similaire au passeport covid devra être adopté par la confédération pour guarantir une transparence totale sur la gestion des « Verifiable Credentials » et assurer qu'il n'y ait aucun partage des données avec des tiers (même pour des utilisations statistiques de l'app). Nous avons étudié les acteurs majeurs proposant des wallets SSI-eID et nous ne sommes pas convaincu qu'ils respectent les bonnes pratiques en terme de protection de la sphère privée et ait une approche « Privacy by design ». Nous pensons que l'aspect concurrentielle sera important afin d'avoir plusieurs acteurs qui peuvent se positionner sur le portefeuille. Dès lors il s'agit de définir un standard d'interface que les portefeuilles devront implémenter pour écrire et effecturer des preuves ZK au sein de la blockchain.

Chaque fournisseur de « wallet » devrait fournir son code source à une entité « de vérification / certification » pour s'assurer qu'il collecte pas de données et méta-données les transactions de vérification d'identité.

Qui exploite le registre?

Les institutions publiques de l'Etat Suisse, les banque, les universités, ainsi qu'un écosystème international. La Blockchain doit à notre avis être une *permissioned* blockchain, c'est-à-dire que les nœuds qui souhaitent rejoindre la blockchain doivent être certifiés avant de devenir proprement des nœuds de la blockchain (pour des raisons de confiance).

La Blockchain devra de notre point de vue régie par une fondation similaire aux fondations qui régissent des projets tels que Ethereum, Cardano, Dfinity et de nombreux d'autres projets de blockchain ainsi que des mécanismes décentralisés.

Par exemple comme idée de gouvernance

- Les opérateurs de nœuds sont approuvés et inscrits sur une liste blanche pour exploiter un nœud par le biais d'un processus de vérification automatisé. La licence d'exploitation ne peut être révoquée que par l'opérateur du nœud lui-même ou par un vote soigneusement conçu.
- Des mécanismes incitatifs garantissent que les nœuds les plus fiables exploitent la blockchain .Cela comprend l'attribution de notes aux nœuds, des mécanismes de sélection des nœuds pour l'exécution des calculs ZK et des mécanismes d'incitation.
- Les nouvelles versions du logiciel qui constitue la Blockchain sont initialement approuvées implicitement par les opérateurs de nœuds exécutant la blockchain.

Les futures versions de la blockchain comprendront des règles de vote plus détaillées, garantissant que les opérateurs de nœuds décident de l'utilisation de la blockchain.

Comment résout-on les questions d'interopérabilité avec les autres registres? L'émetteur est-il même libre de choisir un registre?

Au sein des écosystème SSI, nous observons une convergence autour du standard W3C sur DID. Par exemple, récemment Microsoft Azure implémente le concept DID sur Azure via le registre ION. La blockchain SSI doit être compatible avec d'autres blockchains.

Comment rendre possibles les sauvegardes et les transferts de justificatifs d'identité? Comment éviter les sauvegardes centrales et donc les cibles privilégiées des pirates? Quel rôle joue la possibilité d'une liaison cryptographique entre le portefeuille électronique et les données vérifiées ?

Une blockchain qui utilise le MPC et les ZKP, sécurisant ainsi la transmission des données stockées sur les portefeuille électroniques (il est difficile de compromettre la clé qui est distribuée à plusieurs partis, grâce au ZKP l'utilisateur dévoile un minimum de données). Les données propres à l'utilisateur sont stockées dans le portefeuille de l'utilisateur, les vérificateurs demandent un accès ou une preuve temporaire, il n'y a donc pas de sauvegardes centrales. La blockchain stockerait plutôt un DID qui est un pointeur vers le DID document (contient les données relatives à l'utilisateur) qui est stocké est dans le portefeuille de l'utilisateur, similaire au DNS.

Quels mécanismes de sécurité faut-il pour accéder au portefeuille électronique ?

Les mécanismes de cryptographies utilisés par une blockchain « privacy-by-design » permettent à l'utilisateur de divulguer ses informations personnelles selon son envie (e.g. il peut envoyer une preuve « J'ai 18 ans » sans devoir montrer une date de naissance etc.). De plus afin de partager les données, plusieurs partis sont nécessaires (MPC) permettant ainsi de ne pas mettre en jeu une seule clé privée qui pourrait être corrompue. Ces parties pourrait bien entendu être des cantons hébergeant des nœuds ZK voire même des universités, banques … Sans aucune des parties n'ait en sa possession la clé privée du citoyen.

Comment utiliser les données vérifiées sur plusieurs appareils? Quand serait-ce nécessaire? Suffit-il de toujours établir une liaison avec le vérificateur sur un

smartphone, même si l'on vient de lancer le processus demandant l'e-ID sur un autre appareil ?

Le système peut être construit de manière flexible selon les besoins, un utilisateur pourrait se connecter avec le même portefeuille sur plusieurs appareils simultanément. De plus l'utilisateur peut créer différents DID documents dans son portefeuille tels des cartes de visites pour différents services.

Qui définit le système d'identification ? Faut-il qu'une instance reconnue se charge de la définition et de la coordination (par ex. eCH) ou les définitions sont-elles développées en fonction de la branche concernée ?

Plusieurs partis participent à la définition et à plusieurs niveau (politique, technique, social), l'important est que la solution se base sur les standards actuels, que le système soit Open Source et auditable. Oui nous pensons que eCH pourrait contribuer à établir un standard tel que eGOV pour effectuer un « bridge » entre les DID et les service providers afin d'intégrer plus facilement une authentification eID – SSI à des portails eGOV.

Präambel

Der Schweizer Bundesrat hat am 26. Mai 2021 das Eidgenössische Justiz- und Polizeidepartement (EJPD) mit der Umsetzung der Arbeiten zur Schaffung einer staatlichen elektronischen Identität – kurz E-ID – beauftragt. Im Zuge dessen wurde am 2. September 2021 eine öffentliche Konsultation zum Diskussionspapier zum «Zielbild E-ID» eröffnet. Das Konsultationsverfahren wird durch das Bundesamt für Justiz (BJ) des EJPD durchgeführt. Die öffentliche Konsultation schließt am 14. Oktober 2021 mit einer öffentlichen Diskussion an einer Konferenz.

Eine „digitale Identität" ist ein Hilfsmittel für den Menschen, mit einem Computersystem zu interagieren. Für den Computer müssen Menschen, besonders in der vernetzten Welt, erreichbar und wiedererkennbar sein. Eine digitale Identität wird meist angereichert mit Informationen über die Nutzer:innen. Im „klassischen" Identitätsmanagement verwaltet eine digitale Identität eine Drittpartei, der grundsätzliches Vertrauen entgegengebracht werden muss. Self-Sovereign Identity, kurz SSI, stellt diesen Ansatz infrage und proklamiert, dass Nutzer:innen ihr digitale Identität selbst verwalten und kontrollieren, ein fundamentales Prinzip von „echtem" SSI. Fakten über Nutzer:innen stellen weiterhin Drittparteien aus. Diese liegen in einem von ihnen kontrollierten eigenen Datenspeicher, oft als „digitale Brieftasche" – englisch „Wallet" – bezeichnet. Nutzer:innen entscheiden, wer auf Anfrage welche Daten bekommt, unter ihrer vollständigen Kontrolle, datensparsam und die Privatsphäre wahrend.

Die esatus AG beteiligt sich als langjährig international aktiver und vernetzter Stakeholder im Innovationsbereich SSI am schweizerischen Konsultationsverfahren. Die esatus AG engagiert sich seit 2015 in Sachen „Decentralized Identity", da sie dieses Paradigma als unverzichtbar für eine hypervernetzte digitale Welt einstuft. Demzufolge vertritt sie die grundsätzliche Position, dass eine SSI-basierte E-ID für die Schweiz und ihre Bürger:innen zukunftsweisend und nachhaltig vorteilhaft wäre. Die esatus AG empfiehlt, einen SSI-basierten Ansatz für das schweizerische Identitätsökosystem zu verfolgen. Über die eingereichte Position bringt sie Erfahrungen ein, die sie seit der Prägung des Begriffs SSI im Jahr 2016 und in konkreten Projektaktivitäten der letzten beiden Jahre sammeln konnte. Dabei wird zu den folgenden gewünschten Fragen konkret Position bezogen:

- Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?
- Welche Anwendungsfälle der E-ID stehen im Vordergrund?
- Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Wichtigste Anforderungen

1 – Vertrauen. Oberste Priorität für jedes Identitätsökosystem ist, bei allen beteiligten Stakeholdern, diese beinhalten

- die Nutzer:innen (bei SSI sind dies „Holder"),
- die staatlichen und privatwirtschaftlichen Akteure,
- in ihrer jeweiligen Rolle als Infrastrukturbetreiber und -dienstleister,
- Diensteanbieter und Anwender (bei SSI „Issuer" und „Verifier"),

das erforderliche Vertrauen aufzubauen,

- in den verfolgten **Ansatz** an sich,
- die zugrundeliegende **Technik**, sowie
- die übergreifende **Governance**.

Ein SSI-basiertes Identitätsökosystem stellt einen gänzlich neuen **Ansatz** dar, der gegenüber allen Stakeholdern erklärungs- und gewöhnungsbedürftig ist. Nutzer:innen haben erfahrungsbasiert häufig das Verständnis, dass sie keine echte Kontrolle über ihre Daten haben und dass immer eine verantwortliche Drittpartei existiert, an die man sich im Fehlerfall wenden kann (bspw. „Passwort-Reset" über den Support eines Online-Dienstes). Bei SSI gehen Kontrolle und Verantwortung an die Nutzer:innen über. Das müssen sie verstehen, daran müssen sie sich gewöhnen. Auch die anderen Akteure im Ökosystem müssen ein tiefgehendes Verständnis über die grundlegenden SSI-Prinzipien, technische Möglichkeiten (und Unmöglichkeiten) sowie ihre Rechte und Pflichten aufbauen. Oft fällt es Datenkonsumenten schwer, ihre „Sammelwut" zu zügeln und tatsächlich nur die Daten von Nutzer:innen anzufragen, die im konkreten Anwendungsfall benötigt werden. Alle müssen Vertrauen in das Prinzip der fließenden Daten, eigenständig gesteuert durch Nutzer:innen, fassen und ihre Verantwortung verinnerlichen.

Für die zugrundeliegende **Technik** besteht ein mehrjähriger aber im Produktivbetrieb limitierter Erfahrungshorizont. Für SSI typische kryptografische Verfahren (bspw. „Zero-Knowledge Proof") sind zwar akademisch validiert, aber eine detaillierte Prüfung und ggf. Zertifizierung der technischen Implementierung in den gängigen Open Source Technology Stacks ist erforderlich. Die Skalierungsfähigkeit ist zu berücksichtigen und sicherzustellen, da die zu erwartende Größenordnung von Nutzerzahlen im hohen Millionenbereich liegt. Es ist grundsätzlich davon auszugehen, dass ein Identitätsökosystem ein hochrangiges Ziel für gutwillige Sicherheitsforscher:innen sowie Datendiebe und Störer aus der organisierten Kriminalität, terroristischen Kreisen oder böswilligen Staaten und deren Geheimdiensten darstellt. Höchste Sicherheitsanforderungen an ein System zu stellen, das eine elektronische Vertrauensinfrastruktur für eine vollständig digitalisierte Welt liefert, ist zwingend angeraten. Damit ist auch die regulatorische Konformität leichter zu belegen, bis zu einem gewissen Grad ist sie dann ein Nebenprodukt.

Das Identitätsökosystem muss sich in die durch Gesetze und Verordnungen geregelte Welt der relevanten Jurisdiktion integrieren. Dies lässt keinen Ambivalenzen zu. Es ist daher grundlegend, dass die Notwendigkeit für eine **Governance** des Identitätsökosystems erkannt wird und diese bereits in der Konzeptionsphase zu bedenken ist. Die Diskussion und Definition von Rechten und Pflichten aller Akteure im Identitätsökosystem und vollständige Transparenz sind elementar für die Vertrauensbildung. Die Vertrauensniveaus im regulatorischen Sinne, die das Identitätsökosystem unterstützen soll, sind festzulegen. Bspw. wird es in gewissen Anwendungsfällen zwingend erforderlich sein, dass sich Datenkonsumenten gegenüber Nutzer:innen authentifizieren. Klare Anforderungen an das Identitätsökosystem, in Konzeption, (Weiter-)Entwicklung und Betrieb, sowie ein verständlicher, für die interessierte Öffentlichkeit partizipativer Prozess für deren Erhebung und Bewertung sind unerlässlich.

2 – Relevanz. Ein Identitätsökosystem wird nur dann erfolgreich sein, wenn es für alle beteiligten Akteure nützlich ist, d. h. es viele Anwendungsfälle im täglichen Gebrauch gibt, die es verwenden. Staatlich motivierte bzw. lancierte Identitätsökosysteme sind unterschiedlich erfolgreich. Bei zu hohen – bspw. technischen oder regulatorischen – Einstiegshürden für Issuer und Verifier werden diese das System nicht in ihre Anwendungsfälle integrieren. Nutzer:innen haben dann keine Incentivierung, ihre Rolle als Holder im System einzunehmen, da sie ihnen nichts nutzt. Entsprechend hohe Durchdringung

und Reichweite im öffentlichen und privatwirtschaftlichen Sektor sind daher anzustreben und durch geeignete Maßnahmen wie eine modulare Gesamtarchitektur, offene, frei verfügbare Softwarekomponenten und Integrationsunterstützung zu motivieren. Nutzer:innen sind heute in mehrfacher Hinsicht mobil: In ihrem privaten und beruflichen Alltag sind sie die Verfügbarkeit von digitalen Diensten praktisch an jedem beliebigen Ort gewohnt und wünschen sich die mobile Nutzung für eine E-ID. Die Mobilität geht eindeutig auch über Landesgrenzen hinweg. Ein ideales Identitätsökosystem hat daher für Nutzer:innen leichtgängig interoperabel mit Identitätsökosystemen anderer Jurisdiktionen zu sein. Zwingend zu berücksichtigen ist, dass Nutzer:innen schon von den quasi omnipräsenten und maximal nützlichen Identitätsökosystemen der „Big Techs" aus West und Ost geprägt („verwöhnt") sind. Eine gleichwertige Relevanz muss das erklärte Ziel für ein neues Identitätsökosystem sein.

3 – Nutzerfreundlichkeit. Ein Identitätsökosystem wird nur dann akzeptiert werden, wenn es insbesondere für Nutzer:innen einfach zu handhaben und gefällig in der Anmutung ist. Die technischen Komponenten, mit denen Nutzer:innen interagieren, müssen für optimale „User Experience" („UX") designt und implementiert sein. Dies betrifft insb. die Wallet App auf den Smartphones von Nutzer:innen und die von Diensteanbietern bereitgestellten Anwendungsfälle bzw. deren Abläufe. Wesentlich ist, dass das Identitätsökosystem für alle offen ist und die Anforderungen auf Nutzer:innenseite so gering wie möglich sind. Im Ökosystem nutzbare Wallet Apps sollten auf möglichst vielen Smartphone-Modellen und -Betriebssystemversionen nutzbar sein, Barrierefreiheit maximal unterstützen und kostenfrei zur Verfügung stehen.

Anwendungsfälle

Von der Verfügbarkeit eines einfach handhabbaren elektronischen Identifikationsmittel können die Anbieter von Anwendungsfällen, die eine Personenidentifikation erfordern, unmittelbar profitieren. Die esatus AG teilt daher die im *Diskussionspapier zum «Zielbild E-ID»* vertretene Grundannahme, dass eine E-ID einen Befähiger („Enabler") für öffentliche und privatwirtschaftliche Anwendungsfälle („Use Cases") darstellt. Die genannten Beispiele Altersnachweis, Bankwesen, Bonitätsauskunft, Login und Signatur sind als ein sinnvoller Einstieg zu werten. In weiteren unzähligen Anwendungsfällen des täglichen Lebens besteht die Notwendigkeit für eine Identitätsprüfung, bspw.

- im Bildungswesen bei Ausstellung von Zeugnissen, Diplomen und Weiterbildungszertifikaten;
- im Gesundheitssektor bei Attesten und Rezepten für Patient:innen und Befähigungsnachweisen oder Zutrittsberechtigungen für Ärzt:innen;
- im Telekommunikationssektor beim Abschluss eines Mobilfunkvertrages;
- im Bauwesen beim Nachweis der legalen Beschäftigung auf Baustellen sowie Befähigungsnachweisen oder Zutrittsberechtigungen für Arbeiter:innen;
- in der Automobilindustrie bei Fahrzeugfinanzierung und -zulassung;
- in der Luftfahrtindustrie bei Lizenzen für Pilot:innen.

Aber: Nicht überall ist eine Identifikation erforderlich. Zu berücksichtigen sind daher auch die Anwendungsfälle, in denen eine anonyme Verwendung von Nachweisen gewährleistet werden muss. Nicht bei jedem Online-Dienst müssen sich Nutzer:innen ausweisen, damit sie den Dienst nutzen können, oftmals präferieren diese eine (Quasi-)Anonymität. In solchen Fällen wäre es ausreichend, wenn Nutzer:innen ein beliebiges Verifiable Credential zur Wiedererkennung bei der Rückkehr zum Dienst

verwenden könnten. Ein vollständiges Identitätsökosystem hat derartige Anwendungsfälle zwingend zu unterstützen und zu ermöglichen.

Grundsätzlich ist festzuhalten, dass die Mehrwerte eines Identitätsökosystems erst dann voll zur Geltung kommen, wenn Anwendungsfälle über Organisations- oder Ländergrenzen hinweg gedacht, konzipiert und realisiert werden.

Nutzen

Die Nutzungsszenarien für ein Identitätsökosystem sind in den gängigen Anwendungsfällen spezifiziert und die erzielten Nutzwerte sind leicht ersichtlich und verständlich. Issuer – Holder – Verifier Beziehungen gibt es aber in praktisch unzähligen Anwendungsfällen. Die Erfahrung zeigt, dass SSI-Briefings mit verständigen Interessenten aus allen Branchen nahezu immer dazu führen, dass den Brancheninsidern eine Flut von Möglichkeiten einfällt, wie SSI in ihrem Kontext nutzenstiftend eingesetzt werden könnte. Die esatus AG ist daher zu der Erkenntnis gelangt, dass SSI einen idealen Enabler für jegliche Digitalisierungsvorhaben darstellt. Tatsächlich wird der Bedarf für ein Identitätsökosystem, das Vertrauen digital abbildet und Nutzer:innen in die Lage versetzt, sie betreffende Daten kontrolliert fließen zu lassen, täglich mehr evident. Dieses zu erschaffen ist eine globale Herausforderung in einer hypervernetzten digitalen Welt. Jeder Staat, dessen Bürger:innen und politische Entscheidungsträger:innen dies erkennen, sollten aktiv ihren Beitrag dazu leisten.

Flughafen Zürich

Bundesamt für Justiz
Herr Urs Paul Holenstein
Bundesrain 20
CH-3003 Bern

Per mail an E-ID@bj.admin.ch

Zürich-Flughafen, 11. Oktober 2021

Diskussionspapier zum «Zielbild E-ID» - Stellungnahme

Sehr geehrter Herr Holenstein

Mit Schreiben vom 2. September 2021 hat Frau Bundesrätin Keller-Sutter interessierte Kreise zur Teilnahme am im Titel erwähnten Diskussionspapier eingeladen. Gerne nehmen wir die Gelegenheit wahr, uns zum geplanten Zielbild E-ID zu äussern und die diesbezüglichen Anliegen der Flughafen Zürich AG als Eigentümerin und Betreiberin des grössten Landesflughafens mit über 30 Millionen Passagieren im Jahr (pre-Covid) und rund 25'000 Angestellten bei über 280 Unternehmen zu platzieren.

Wir begrüssen die Stossrichtung des Bundesrats nach der Volksabstimmung im März nun rasch die Möglichkeit für eine staatliche digitale Identität zu schaffen. Eine E-ID, die das gesamte digitale Ökosystem umfasst und verschiedene Funktionalitäten mitbringt, die in verschiedenen Bereichen eingesetzt werden können, ermöglicht grosse Vorteile für Nutzer, Kunden und Unternehmen. Insbesondere bietet eine E-ID vielfältige Nutzungs- und Anwendungsbereiche, wenn das Kunden- und Reiseerlebnis einfach, zugänglich und digital möglich ist. Die Covid-19-Pandemie hat gezeigt, dass sich die Menschen zunehmend digitaler verhalten und sich bereits jetzt viele Vorteile für Anbieter und Kunden ergeben. Als bestes Beispiel, dass die Handhabung und Anwendung digitaler Identitäten funktioniert, dient das Covid-Zertifikat. Auf diesen erzielten Erfolgen sollte aufgebaut und die nächsten Schritte in Angriff genommen werden.

Die folgenden Antworten beziehen sich auf die im Diskussionspapier auf Seite 33 gestellten Fragen.

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Der Nutzen einer E-ID ist überall da gegeben, wo sie als «enabling feature» eingesetzt werden und dienen kann und das Kundenerlebnis ermöglicht und verbessert. Es sind vielfältige Anwendungsmöglichkeiten denkbar, die von einfachen Logins bis zu kompletten digitalen «customer

andrew.karim@zurich-airport.com | T +41 43 816 71 29 | M +41 77 529 13 93
Flughafen Zürich AG | Postfach | CH-8058 Zürich-Flughafen | flughafen-zuerich.ch

journeys» reichen. In Anlehnung auf die in Kapitel 4.2 vorgestellten Ambitionsniveaus ergeben sich für jedes Niveau vielfältige Einsatzmöglichkeiten, die im Folgenden auch mit Blick auf das Flughafenumfeld aufgeführt werden:

- Niveau 1: Eine E-ID kann als Login für die WiFi-Nutzung an öffentlichen Orten genutzt werden. Ebenso könnte eine E-ID für Logins zu sensiblen Systemen von Mitarbeitenden fungieren. Sofern eine E-ID Protokolle wie OpenID Connect unterstützen würde, könnte diese als Schweizer Lösung für herkömmliche Logins verwendet und als Single-Entry-Solution für verschiedene Systeme genutzt werden.
- Niveau 2: Die Verknüpfung der E-ID mit weiteren staatlich regulierten Beweisen 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. Die mögliche Nutzung einer E-ID ist damit fast 1 Million mal pro Monat, bei der Schaffung von verschiedenen Touchpoints während der Reise noch höher. Damit einher geht eine Effizienz- und Komfortsteigerung für Passagiere und beteiligte Unternehmen.
- Niveau 3: Wird die E-ID zum Ökosystem digitaler Beweise ausgebaut, ergeben sich weitere Anwendungsmöglichkeiten wie beispielsweise ein komplettes digitales und vereinfachtes Reiseerlebnis auf der Basis eines Kundenprofils und biometrischer Daten. 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.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Für die regelmässige Nutzung und Anwendung einer E-ID ist erstens eine einfache, schnelle und zugängliche Erstellung einer E-ID von grossem Vorteil. Diese könnte zum Beispiel an stark frequentierten Orten wie Bahnhöfen, Flughäfen etc. erfolgen. Zweitens sollte die E-ID über «Kommunikationsmöglichkeiten» mit verschiedenen digitalen sowie öffentlichen und privaten Plattformen verfügen. Und drittens soll der Datenschutz auf dem Datenschutzgesetz basieren und grundsätzlich dem Schweizer Ansatz folgen. Eine Abstufung der Datensichtbarkeit muss gewährleistet und das Opt-In konsequent angewandt werden mit dem Ziel, dass die Schweizer Bevölkerung dem System vertraut und es nutzt. Eine E-ID sollte auf den Schlagworten Seriosität, Vertraulichkeit und Verantwortlichkeit basieren.

andrew.karim@zurich-airport.com | T +41 43 816 71 29 | M +41 77 529 13 93
Flughafen Zürich AG | Postfach | CH-8058 Zürich-Flughafen | flughafen-zuerich.ch

Flughafen Zürich

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Am Flughafen Zürich tragen mehr als 25‘000 Angestellte einen Flughafenausweis im Sinne eines Mitarbeiterausweises, davon werden jährlich 5'000 – 7'000 Ausweise neu erstellt oder erneuert. Für dessen Ausstellung sind zum Teil vielfältige Sicherheitsüberprüfungen notwendig, darunter fallen können unter anderem Führerausweis, Ausbildungsnachweis, Betreibungs- und Strafregisterauszug. Eine nationale Infrastruktur einer E-ID, die die benötigten Informationen digital zur Verfügung stellt, würde den administrativen Aufwand enorm reduzieren und die Fehlerquellen minimieren.

Ebenfalls ist die Möglichkeit einer Ausstellung von digitalen Nachweisen durch Private zu prüfen und die dafür notwendigen Kriterien zu erstellen.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme sowie für die Berücksichtigung unserer Anliegen. Gerne stehen wir für die Beantwortung allfälliger Fragen zur Verfügung.

Freundliche Grüsse

David Karrer
Head Public Affairs

Andrew Karim
Stv. Leiter Public Affairs

andrew.karim@zurich-airport.com | T +41 43 816 71 29 | M +41 77 529 13 93
Flughafen Zürich AG | Postfach | CH-8058 Zürich-Flughafen | flughafen-zuerich.ch

Bundesamt für Justiz BJ
Michael Schöll
Direktor

zugestellt per Mail an E-ID@bj.admin.ch

Wallisellen, 12. Oktober 2021

Stellungnahme Health Info Net AG zu «Zielbild E-ID»

Sehr geehrter Herr Schöll

HIN bedankt sich für die Möglichkeit der Stellungnahme und begrüsst das gewählte Vorgehen.

HIN vertritt die Branche Gesundheits- und Sozialwesen und insbesondere die Gesundheitsfachpersonen (GFP) und deren Einrichtungen. HIN betrachtet schon heute das Gesundheitswesen als Ökosystem. HIN bietet in diesem Ökosystem den Akteuren verschiedene Dienstleistungen an. Der Zugriff auf HIN-eigene Services sowie Angebote von Dritten basiert auf der HIN ID und den damit verbundenen Attributen. Die Grundlage der HIN ID bildet die Personenidentität und basiert auf amtlichen Ausweisdokumenten (Pass, ID) der Teilnehmer. Der Identitätsnachweis wird aktuell über Video-Identifikation erbracht und ist EPDG-konform zertifiziert. Die Attribute stammen aus verschiedenen Quellen, unter anderem aus amtlichen Registern.

Antworten zu den Hauptfragen:

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Der Nutzen einer staatlichen E-ID besteht darin, dass schweizweit verlässliche digitale Identitätsnachweise für alle, so auch für die Akteure im Gesundheits- und Sozialwesen, vorhanden sind. Sowie einem Rechtsrahmen, der es erlaubt den Identitätsnachweis in den entsprechenden Prozessen einfach und sicher einzusetzen.
Der Hauptanwendungsfall ist der Identitätsnachweis als Basis für digitale, branchenspezifische Prozesse - die Funktion des Passes oder der ID wird in die digitale Welt transformiert.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

- Benutzerfreundlichkeit – Die Nutzer sollen die E-ID einfach in den von ihnen gewählten Anwendungsfällen einsetzen können. Die Nutzer sollen analog zur physischen ID / Pass in den unterschiedlichsten Szenarien den Identitätsnachweis erbringen können. Entsprechend müssen die Identitätsnachweise von den unterschiedlichen Stellen einfach überprüft werden können
- Interoperabilität – Die E-ID soll universell eingesetzt werden können und nicht an spezifische Anwendungsfälle gebunden sein
- Technologieneutralität – Die E-ID soll auf offenen, internationalen Standards basieren und eine flexible Weiterentwicklung und Adaption an neue Technologien erlauben

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Die Infrastruktur sollte eine flächendeckende und stabile, rechtsichere Grundlage für digitale Ökosysteme bilden. Das heisst, sie sollte sich auf die Funktionalitäten «Herausgabe von Identitätsnachweisen (Credential Issuing)» und die Gewährleistung eines «Rechtsrahmen – Trustanker» konzentrieren. Dies würde für die Schweizer Wirtschaft wie auch für die Behörden einen grossen Nutzen darstellen. So könnten die verschiedensten Ökosysteme entstehen, in denen spezifische Services und Prozesse in einem Vertrauensraum angeboten und abgewickelt werden können.

Aus der Beantwortung der Hauptfragen leiten wir unsere Varianten-Empfehlung ab:

«E-ID-Lösung mittels Self-Sovereign Identity»

HIN beschäftigt sich schon seit einiger Zeit mit SSI und betreibt auch eine entsprechende Infrastruktur für Testapplikationen.
Dies basiert auf der Überzeugung, dass die Umsetzung der SSI-Prinzipien am besten die Bedürfnisse der Marktteilnehmer abdecken:

- Einfachheit, Sicherheit, Usability
- Selbstbestimmung
- Privacy by Design

Die Umsetzung der SSI-Prinzipien decken auch die zentralen Forderungen der sechs Motionen am besten ab:

- Staatliches elektronisches Identifikationsmittel vergleichbar mit Pass
- Datensparsamkeit und «privacy by design»
- Dezentrale Datenspeicherung
- Verantwortung für den Ausstellungsprozess und den Gesamtbetrieb bei staatlichen Behörden

Um eine schnelle Verbreitung und Nutzung zu erreichen, muss eine E-ID die Bedürfnisse **aller** Marktteilnehmer abdecken: Die der Inhaberinnen und Inhaber (Holder) **und** der Service-Anbieter (Issuer / Verifier). Dies wäre, nach Meinung der HIN, mit dem vorgeschlagenen Ansatz möglich.

HIN schlägt vor, mit der neuen E-ID die Chance zu ergreifen, die Basis für digitale Ökosysteme in er Schweiz zu schaffen. Dies kann nicht mit «einem grossen Wurf» durch den Staat geschehen. Die Schaffung von digitalen Ökosystemen ist ein Prozess über Jahre, der durch den Staat ermöglicht und

begleitet werden muss. Dies sollte durch Bereitstellung von Rahmenbedingungen und Hilfsmitteln erfolgen und keinesfalls zu enge Vorgaben, Definitionen und Restriktionen beinhalten, die eine flexible Weiterentwicklung verhindern.

Unter diesen Aspekten kann die vorgeschlagene Vision durch HIN mitgetragen werden:
«Die Schweiz hat eine staatlich betriebene digitale Vertrauensinfrastruktur, welche sichere, medienbruchfreie Prozesse ermöglicht und fördert.»

Empfehlung bezüglich Ambitionsniveau:
Der Bund beschränkt sich auf Ambitionsniveau 1 basierend auf den Grundsätzen der Umsetzungsvariante SSI und konzentriert sich auf die Herausgabe von digitalen Identitätsnachweisen sowie der Schaffung des Rechtsrahmens.
Darauf basierend, kann die Entwicklung der Ökosysteme im Privaten wie auch im Öffentlichen Sektor hin zu Ambitionsniveau 3 erfolgen und durch den Staat begleitet werden (siehe als Beispiel dazu auch https://findy.fi/en/).

Dies entspricht der Rolle, die der Staat in der physischen Welt schon heute wahrnimmt: Er stellt amtliche Dokumente aus, die zu treuen Händen den einzelnen Personen zur Verfügung gestellt werden und schafft den Rechtsrahmen für deren Verwendung.

Für die Umsetzung der E-ID im empfohlenen Rahmen, rät HIN dringend von einem «Swiss Finish» ab.

Die Adaption und Weiterentwicklung der noch neuen Technologie soll ermöglicht und begleitet werden, damit die sich daraus ergebenden Chancen und Möglichkeiten genutzt werden können.

Die Schweiz sollte den Schritt wagen, als Enabler von digitalen Ökosystemen aufzutreten und auf eine E-ID-Lösung mit Potential setzen und die Entwicklung der Details begleiten.

Freundliche Grüsse

HEALTH INFO NET AG

Marco Zimmer Leiter IT (CIO)	Peer Hostettler Leiter Vertieb	Urs Fischer Leiter BD & Innovation

THE SWISS
INFORMATION GOVERNANCE
COMPETENCE CENTER

Kompetenzzentrum Records Management AG | Hegnaustr. 60 | 8602 Wangen

Bundesamt für Justiz (BJ)

E-ID@bj.admin.ch

Zürich, 28. September 2021

Stellungnahme zur „Konsultation E-ID“

Sehr geehrte Damen und Herren

Als langjährige Experten im Bereich der Digitalen Identität teilen wir Ihnen hiermit unsere Einschätzung zum Thema „E-ID“ gemäss Ihrer Anfrage mit.

Freundliche Grüsse
Kompetenzzentrum Records Management AG

Dr. Bruno Wildhaber
Managing Partner

Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

1. Priorität: 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. Der Verfasser hat im Jahr 1996 (sic!) das damalige EJPD kontaktiert und sich erkundigt, wann man mit der Einführung einer elektronischen Identität rechnen dürfe! In der aktuellen Situation kam es nur noch um Schadensbegrenzung gehen. Die von Ihnen angesprochenen Detailfragen zur Umsetzung sind nur am Rande interessant und behindern die Diskussion um die Grundsatzfrage «Digitale Identität: JA oder NEIN» nur. Diese Frage muss dem Gesetzgeber vorgelegt werden. Das zu schaffende Gesetz muss möglichst schlank und ohne unnötige Detailregelungen entworfen und im Eilverfahren umgesetzt werden.
2. 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 E-ID Gesetz verloren gegangen ist.
3. Die Umsetzung der digitalen Identität muss möglichst einfach und auf etablierten Technologien erfolgen. Dazu am besten geeignet und weil 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-Technologie.

Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Wie oben bereits erfasst, geht es bei der Schaffung der E-ID nicht um deren Anwendung. Es ist nicht Aufgabe des Staates, dafür zu sorgen, dass die digitale Identität eingesetzt werden kann. Ebensowenig, wie der Staat Autos gebaut hat, um Autobahnen zu nutzen, muss er Anwendungen für die E-ID 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 im Diskussionspapier erwähnten Anwendungsfälle sind altbekannt und teilweise bereits umgesetzt.
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 ist ein Föderalismus, welcher die E-ID verunmöglichen würde. Wie erwähnt, die E-ID das Pendant zum physischen Identifikationsdokument sein. Andere Nutzer sollen darauf aufbauen, aber auf keinen Fall Parallellösungen bauen.

Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Die alleinige Kernaufgabe des Staates damit des Bundes ist es, den digitalen Ausweis zu erstellen. Es ist nicht seine Aufgabe, Anwendungen direkt zu lancieren, ausser sie liegen in der alleinigen Kompetenz des Bundes und sind damit bereits zentralistisch organisiert. Beispiel dazu wären unter anderem Strafregisterauszüge, welche bereits heute schon digital abgefragt werden können. Die Identifikation hat nichts mit der Nutzung bzw. mit dem Authentifizierungsprozess zu

tun. 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 E-ID nicht einmischen. Über die Zeit werden heute isolierte Lösungen die E-ID als Identifikationsanker nutzen, weil der Aufwand für die Weiterführung eigener Identifikationslösungen zu gross werden wird.

procivis
AN ORELL FÜSSLI COMPANY

Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

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

4. Oktober 2021

Stellungnahme Procivis zum Diskussionspapier «Zielbild E-ID»

Sehr geehrte Damen und Herren

Am 2. September 2021 hat das Bundesamt für Justiz das Diskussionspapier «Zielbild E-ID» veröffentlicht und alle interessierten Parteien eingeladen, zu dessen Inhalt Stellung zu nehmen. Procivis begrüsst diesen transparenten und partizipativen Ansatz und ist überzeugt, dass dieser eine wichtige Grundlage für eine breit akzeptierte und vertrauenswürdige staatliche E-ID ist, welche aktuellen und zukünftigen Bedürfnissen der Nutzer*innen Rechnung trägt.

Die Umsetzung der gesetzlichen, technischen und wirtschaftlichen Aspekte der zukünftigen staatlichen E-ID wird – auch abhängig vom gewählten Ambitions-Niveau und Lösungsansatz – einige Jahre in Anspruch nehmen und sollte ganzheitlich angegangen werden, um den vollen Nutzen einer staatlichen E-ID auszuschöpfen. Das Potential der bestehenden kantonalen E-ID Lösungen, sowie die Erfahrung und das Wissen, welches auf kantonaler und kommunaler Ebene besteht, sollte in diesem Prozess unbedingt genutzt werden.

Im Anhang 1 finden Sie unsere Positionen zu den drei von ihnen gestellten Fragen sowie zu weiteren Punkten des Zielpapiers, welche wir als relevant erachten. Zusätzlich fügen wir diesem Schreiben im Anhang 2 unsere eigene Vision für die Entwicklung der zukünftigen nationalen E-ID in Form meines Gastbeitrages in der Neuen Zürcher Zeitung vom 27. September 2021 bei.

Wir danken für die Berücksichtigung unserer Anliegen und freuen uns ebenfalls in den weiteren Etappen der Ausarbeitung und Umsetzung des neuen E-ID Gesetzes unseren Betrag zu leisten.

Mit freundlichen Grüssen

Daniel Gasteiger

CEO und Mitgründer Procivis AG

Anhänge wie erwähnt

Anhang 1 – Stellungnahme Procivis zu «Zielbild E-ID»

Die Stellungnahme ist wie folgt strukturiert:

1. Procivis Position zu den drei Fragen des Diskussionspapiers
2. Beurteilung der drei Ambitionsniveaus
3. Beurteilung der drei Lösungsansätze

1. Procivis Position zu drei Fragen des Diskussionspapiers

Frage 1: Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Eine E-ID ist für die meisten Anwendungsfälle nur der Schlüssel, mit welchem Nutzer*innen Zugang zu einem Anwendungsfall erhalten. Deshalb ist der Nutzen einer E-ID direkt abhängig von den verfügbaren Anwendungsfällen. Eine E-ID kann ihre volle Wirkung auch nur entfalten, wenn die mit der E-ID angestossenen Anwendungsfälle ebenfalls vollständig digital (medienbruchfrei) und in Echtzeit abgewickelt werden können. Dies ist z.B. nicht der Fall, wenn eine Nutzer*in sich mit einer E-ID auf einem Behördenportal anmelden und eine Wohnsitzbestätigung bestellen kann – dann aber einige Stunden oder gar Tage warten muss, bis Mitarbeitende der Verwaltung die Bestätigung aus der Fachapplikation heraus als PDF erstellt und versandt haben.

Die Erfahrung in EU-Ländern (und mit unseren Kunden Kanton Schaffhausen und Stadt Zug) zeigt ebenfalls, dass eine E-ID ihren Nutzen nur entfalten kann, wenn diese sowohl für Transaktionen mit Behörden als auch im Privatsektor eingesetzt werden kann – deshalb muss zumindest langfristig (je nach Entscheid im Zusammenhang mit den erwähnten Ambitionsniveaus und Lösungsansätzen) nach der Einführung der E-ID im Jahr 2026 ein offenes Ökosystem etabliert werden, bei welchem der Privatsektor auf die staatliche E-ID und deren Vertrauensinfrastruktur zugreifen kann. Weiter sollte die Nutzung der E-ID von Anbeginn sowohl bei ausschliesslich digitalen (Transaktionen im Internet) wie auch in analogen Situationen (zum Beispiel bei einer Alterskontrolle in einem Lebensmittelgeschäft) möglich sein.

Eine zentraler, wenn nicht sogar der wichtigste Anwendungsfall für eine staatliche E-ID ist, wie im Zielpapier unter 4.3.5. erwähnt, der einfache Zugang zu qualifizierten elektronischen Signaturen. Der im Zielpapier beschriebene Anwendungsfall beschränkt sich jedoch nur auf die Signatur von PDFs. Bei der Ausgestaltung einer zukünftigen staatlichen E-ID sollten idealerweise die technischen Möglichkeiten genutzt werden, welche die staatliche E-ID mit der gegenwärtig noch separat geregelten digitalen Signatur (ZertES) zusammenführt und neue Anwendungsfälle, welche über die Signatur von PDFs hinausgehen, ermöglicht.

Weitere Anwendungsfälle einer staatlichen E-ID, welche Procivis als wichtig erachtet, sind:

- **Automatisierte Online-Authentifizierung und Autorisierung**
  Wie im Zielpapier unter 4.3.4 erwähnt, sollte die E-ID als sicheres Login für E-Government Portale und Dienstleistungen dienen. Darüber hinaus sollte sie aber auch - dank einer auf PKI/QR Codes aufbauenden E-ID Walletlösung - als automatisierter und passwortloser Zugang zu Onlineportalen und -prozessen des Privatsektors dienen können. Weiter können mit einer solchen E-ID Walletlösung dank Credential-basierter

Autorisierung ebenfalls signifikante Verbesserungen beim Nutzererlebnis ermöglicht werden.

- **Medienbruchfreier Bezug digitaler Behördennachweise (Zertifikate resp. Credentials)**
  Neben dem unter Kapitel 4.3.3. erwähnten Anwendungsfall «Betreibungsregisterauszug» wäre es wünschenswert, wenn sämtliche Behördennachweise dank der nationalen E-ID medienbruchfrei bezogen werden könnten - in der Stadt Zug ist es bereits heute möglich, medienbruchfrei eine Wohnsitzbestätigung zu bestellen, zu bezahlen und diese als PDF mit einen Organisationszertifikat signiert praktisch in Echtzeit wieder auf die «eZug» App zugestellt zu erhalten. Weiter sollte als Endziel eine nahtlose und standardisierte Übermittlung von digitalen Nachweisen (Credentials) von einer Behörde zu einer anderen (oder auch in den Privatsektor) unter der alleinigen Kontrolle des Bürgers ermöglicht werden.

- **Anwendungsfälle des Privatsektors**
  Um der E-ID zum Durchbruch zu verhelfen, sollte zwingend darauf geachtet werden, dass Anwendungsfälle des Privatsektors (wie z.B. unter 4.3.2 erwähnt) mittels der staatlichen E-ID mittel- bis langfristig einfach und sicher umgesetzt werden können. Nur so wird sichergestellt, dass die E-ID eine breite Akzeptanz erfährt.

Frage 2: Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Procivis erachtet die folgenden drei Anforderung an eine staatliche E-ID als prioritär:

- **Höchstmögliche Vertrauenswürdigkeit**
  Um die zukünftige staatliche E-ID bei den Bürgern erfolgreich zu etablieren, ist das Vertrauen in die E-ID von zentraler Bedeutung. Dies zu erreichen erfordert folgende Elemente:
  - Betrieb der E-ID Infrastruktur durch den Staat in der Schweiz inkl. transparenter Governance Strukturen im Zusammenhang mit dem Betrieb und dem Aufbau des E-ID Ökosystems (Zertifizierungskriterien /-stellen)
  - Absoluter Fokus auf Datenschutz, Datensparsamkeit, Sicherheit und «Privacy by Design» inkl. offenem Quellcode der E-ID Technologiekomponenten (z.B. E-ID Wallets)

- **Benutzerfreundlichkeit**
  Eine einfache, für sämtliche Alters- und Anspruchsgruppen der Schweizer Bevölkerung zugängliche E-ID Lösung ist zentral für den Erfolg der zukünftigen nationalen E-ID. Ein starker Fokus sollte daher auf ein benutzerzentriertes Design mit eingängigen, medienbruchfreien und selbsterklärenden E-ID Anwendungen gelegt werden. Die naheliegende Umsetzung einer E-ID ist daher eine Smartphone-basierte Wallet-Lösung, welche von Anbeginn die relevanten Anwendungen (siehe Frage 1) unterstützt. Zudem muss sichergestellt werden, dass bei Verlust des Smartphones einfache Back-up/Recovery Möglichkeiten bestehen.

- **Interoperabilität**
  Um die Schweizer E-ID mittelfristig auch international einsetzen zu können, ist es zwingend, dass bei der Entwicklung der Lösung auf die bestehenden und sich entwickelnden internationalen Standards gesetzt wird. Hier sind besonders Entwicklungen in der EU (EUid/eIDAS v2, EBSI, ESSIF) und die Standards der World Wide Web Consortiums (W3C) zu berücksichtigen. Weiter sollten bereits bestehende technische Standards für die einfache Einsetzung der E-ID berücksichtigt werden (z.B. ISO 18013-5, OpenID).

Frage 3: Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z.B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Der anfallende Nutzen lässt sich in vier grossen Themenblöcken zusammenfassen:

- **Eine nationale Vertrauens-Basisinfrastruktur für die öffentliche Hand und den Privatsektor**
  Staatliche und private Akteure betreiben heute eine Vielzahl von isolierten und unterschiedlich weit entwickelten 'IAM- und Login-Lösungen'. Dies führt dazu, dass bestehende finanzielle Mittel (u.a. Steuergelder) oft für die Finanzierung von Doppelspurigkeiten und nicht für Innovation eingesetzt werden. Eine geteilte nationale E-ID Infrastruktur, welche von allen staatlichen und auch privaten Akteuren benutzt werden kann, würde es erlauben Doppelspurigkeiten abzubauen, die bestehenden finanziellen Mittel zu bündeln und zielgerichtet für die Weiterentwicklung der Infrastruktur einzusetzen.

- **Reduktion von Transaktionskosten**
  Medienbruchfreie Prozesse dank der Verfügbarkeit von digitalen Zertifikaten und Nachweisen und des effizienten Einsatzes von digitalen Signaturen zwischen Behörden, E-ID Nutzer*innen und dem Privatsektor können viele manuelle Prozesse ersetzen und somit Kosten einsparen.

  Beispiele solcher Prozessoptimierungen sind:
  - Automatisierte, medienbruchfreie Vertragsabwicklungen dank weit verbreiteter digitaler Signaturen auf Basis der E-ID
  - Wegfall von visuellen Inspektionen bei digital eingereichten Nachweisen (z.B. Betreibungsregisterauszüge, Universitätsdiplome, Wohnsitzbestätigungen, Führerschein, etc.)
  - Automatisierter Altersnachweis beim Bezug von Produkten mit Altersbeschränkung im Internet oder bei Self-Check Out.

  Eine Berechnung der Einsparungen für solche Transaktionskostenoptimierungen ist schwierig. Als Vergleich können Schätzungen aus Estland herangezogen werden: Hier führt allein der flächendeckende Gebrauch der elektronischen Signatur jährlich zu Einsparungen in der Höhe von 2% des BIP (Quelle: e-Estonia).

- **Innovationsschub und Standortpositionierung**
  Der Aufbau einer nationalen E-ID Vertrauensinfrastruktur wird zu neuen spezialisierten Technologie-Anwendungen führen, welche durch innovative Schweizer Start-ups und Firmen umgesetzt werden, was wiederum zu neuen Arbeitsplätzen führen wird. Als neutrales Land, welches höchstes Vertrauen geniesst und der Demokratie und dem Rechtsstaat verpflichtet ist, könnte die Schweiz mit Lösungen im Bereich von staatlichen E-ID Vertrauensinfrastrukturen einen neuen Technologiesektor etablieren, welcher weltweit führend ist und ein hohes Ansehen geniesst, ähnlich der Positionierung unseres Landes als führende Nation im Bereich Blockchain und Digital Assets.

- **Ermöglichung neuer Geschäftsprozesse / -modelle**
  Durch die Möglichkeit der Verknüpfung von bislang unabhängigen digitalen Nachweisen, welche aber gleichzeitig durch die Nutzer*innen vollständig kontrolliert werden können (Stichwort Datenminimierung beim Teilen solcher digitaler Nachweise in Kombination mit neuen Verschlüsselungstechniken wie ZKP), können neue innovative und vor allem benutzerfreundliche Geschäftsprozesse und -modelle entstehen (Bsp. «One-Click

Vertragsabschlüsse» bei Verträgen, welche Bonitäts- oder andere Hintergrundprüfungen bedingen, z.B. bei Mietwohnungen, Arbeitsverträgen usw.). Die Möglichkeiten für die Umsetzung solch neuer Geschäftsprozesse sind beinahe unbegrenzt und werden automatisch Innovationen in allen Sektoren mit sich bringen.

2. Beurteilung der drei Ambitionsniveaus

Aus unserer Sicht – und mit Blick auf die internationalen Entwicklungen – ist das **Ambitions-Niveau 1 (E-ID) nicht mehr zeitgemäss** und würde auch die mittelfristige Wettbewerbsfähigkeit der Schweiz in Frage stellen. Sollte dieses Ambitions-Niveau aus Gründen einer nötigen stufenweisen Einführung (Time-to-Market) der staatlichen E-ID gewählt werden, ist es zwingend erforderlich, dass parallel zu der Entwicklung des gesetzlichen Rahmens für einer solchen E-ID des Ambitions-Niveaus 1 die höheren Ambitionsniveaus mitberücksichtigt werden, insbesondere was zukünftige Governance-, Technologie- und Ökosystemfragen angeht, um eine zukünftige Erweiterung des Gesetzes einfach zu ermöglichen. Weiter wäre eine E-ID auf Ambitionsniveau 1 insbesondere in Kombination mit dem klassischen IdP Ansatz (wie im Zielpapier zur Diskussion gestellt) schon heute nicht mehr zeitgemäss und könnte den vom Parlament und Volk verlangten Minimumanforderungen bezüglich «Privacy by Design», Datenminimierung und dezentraler Datenhaltung nicht gerecht werden.

Procivis erachtet das **Ambitions-Niveau 2 (E-ID mit Verknüpfung weiterer staatlich regulierter Beweise) als Minimumziel**. Es gibt bereits heute technische Lösungen im Markt, welche E-IDs auf kantonaler und kommunaler Ebene inklusive staatlich regulierter Nachweise (Auszügen aus Behördenregistern) und digitalen Signaturen ermöglichen und deshalb sollte dieses Ambitionsniveau auch das Minimumziel für die nationale E-ID sein. Auch hat gerade das Beispiel mit dem Covid-Zertifikat gezeigt, dass solche digitale Nachweise einfach und schnell umgesetzt und zukünftig auch einfach in eine nationale E-ID Wallet integriert werden können.

Der Aufbau eines nachhaltig funktionierenden **Ökosystems digitaler Beweise (Ambitionsniveau 3) sollte das eigentliche Ziel** der Entwicklung der zukünftigen Schweizer E-ID darstellen. Um dieses Ziel möglichst schnell zu erreichen, sollten bei der Entwicklung des E-ID Gesetzes keine Hürden eingebaut werden, welche das Entstehen eines solchen Ökosystems in der Zukunft beeinträchtigen könnte. Neben der Entwicklung des Gesetzes und der technologischen Grundlagen sollte ebenfalls begonnen werden, alle Stakeholder eines solchen Ökosystems (Behörden aller Ebenen, Privatwirtschaft, Politiker, Bürger*innen) von den Vorteilen dieses Ansatzes mittels einer konsequenten Kommunikations- und Ausbildungsstratgie zu überzeugen.

3. Beurteilung der Lösungsansätze

Procivis beurteilt die drei vorgeschlagenen Lösungsansätze folgendermassen:

Self-Sovereign Identity ist der von Procivis klar präferierte Ansatz. Die Umsetzung der E-ID auf Basis der Self-Sovereign Identity Philosophie/Technologie wird jedoch Zeit in Anspruch nehmen, da noch eine Vielzahl an regulatorischen, technischen und auch wirtschaftlichen Fragen geklärt werden müssen. Nichtsdestotrotz sollte mit dem Aufbau der benötigten Infrastruktur (nationale Vertrauensinfrastruktur), der Klärung der Governance im Zusammenhang mit dem Betrieb dieser Infrastruktur und der Etablierung des Ökosystems (staatliche und privatwirtschaftliche Akteure sowie Akkreditierungsstellen für Technologieanbieter) baldmöglichst begonnen werden. Parallel dazu können die

bestehenden kantonalen und kommunalen E-ID Lösungen, welche bereits auf dezentrale E-ID Wallet-Lösung aufbauen, weiterentwickelt werden. Das Ziel des E-ID Gesetzes muss sein, diese bestehenden Lösungen zu gegebener Zeit mit der nationalen SSI-Infrastruktur nahtlos zusammenführen zu können. Das «Zielbild E-ID» identifiziert unter 5.1.6 wichtige offene Fragen zum SSI-Ansatz. Mittels SSI Pilotprojekten sollten solche Fragen in einer praktischen Herangehensweise geklärt werden.

Für vertiefte Lösungsansätze zu den offenen Fragen verweist Procivis zusätzlich auf die Stellungnahme vom Verein «DIDAS» - Procivis ist ein Gründungsmitglied von «DIDAS» und hat seine SSI Expertise in die DIDAS Stellungnahme einfliessen lassen.

Der **PKI - Public-Key-Infrastruktur** Ansatz basiert auf bewährten Prinzipen und Technologien und hat unter anderem Vorteile im Bereich von Offline-Transaktionen, welche auch international bereits gut standardisiert sind (Bsp. ISO Standard für digitale Führerscheine). Aus unserer Sicht ist der PKI Ansatz jedoch nicht mehr zeitgemäss und hat gerade gegenüber dem SSI Ansatz gewichtige Nachteile. Zudem wäre dieser Ansatz auch nur bedingt kompatibel mit dem Ambitions-Niveau 3, da individuelle Attribute vom E-ID Nutzer*innen nur limitiert eingesetzt werden können und wichtige neue kryptographische Verfahren (ZKP usw.) zur Erreichung des Ziels der Datenminimierung gar nicht eingesetzt werden könnten. Damit wären die Weiterentwicklungsmöglichkeiten in der Zukunft begrenzt und der Investitionsschutz der Lösung auf lange Sicht nicht gegeben. Weiter gehen die internationalen Entwicklungen weg von PKI hin zu SSI Lösungen.

NB: Bei einer PKI Lösung in Kombination mit einer physischen Karte als Träger des Zertifikats wären wir zurück bei der vom SECO im Jahr 2010 eingeführten E-ID Lösung («Suisse ID») resp. bei dem Ansatz des deutschen Personalausweises mit E-ID Chipfunktionalität. Beide dieser Lösungen konnten sich auf Grund der umständlichen Anwendung der E-ID (zusätzlich benötigte Hardware / Software für den Einsatz am PC) nicht durchsetzen.

Die bereits im «Zielbild E-ID» erwähnten Nachteile zum **IdP - staatlicher Identitätsprovider** Ansatz sind aus Sicht Procivis so gewichtig, dass man diesen Ansatz ebenfalls nicht weiterverfolgen sollte. Gleichwohl möchte wir hier nochmals auf die wichtigsten Nachteile eingehen: Mit einer zentralen E-ID lassen sich die wichtigsten Forderungen der sechs Motionen «Vertrauenswürdige, staatliche E-ID» vom 10. März 2021 – namentlich «Privacy by Design», Datensparsamkeit und dezentrale Datenspeicherung, nur limitiert umsetzen.

Zusätzlich wäre bei einem Ausfall des zentralen IdPs das ganze E-ID Ökosystem betroffen und würde kurzerhand nicht mehr funktionieren. Weiter ist eine zentrale IdP basierte E-ID limitiert ausbaufähig und eine spätere Überführung in eine SSI-Ökosystem wäre nicht möglich, da es sich um diametral entgegengesetzte Lösungsansätze handelt. Die Attraktivität eines zentralen IdPs für Hacker ist ein weiteres Kriterium, welches gegen diesen Ansatz spricht. Und letztlich geht die Diskussion in der EU klar Richtung «SSI». Mit einer zentralen IdP Insellösung würde die Schweiz riskieren, dass der staatenübergreifende Einsatz der Schweizer E-ID nicht möglich sein wird.

Anhang 2 - NZZ Gastkommentar "Die Zukunft der E-ID muss in der Selbstbestimmung liegen"

Print-Ausgabe: 27. September 2021
Weblink: https://www.nzz.ch/meinung/die-zukunft-der-e-id-muss-selbstbestimmt-sein-ld.1643642

Nach dem Nein zur E-ID sind sich praktisch alle über die Grundsätze für eine Neuauflage einig: datensparsam, dezentral und vom Staat herausgegeben. Doch für eine nachhaltige Lösung reicht das allein noch nicht.

Daniel Gasteiger

Das wuchtige Nein zum E-ID-Gesetz vom März 2021 hat die Möglichkeit geschaffen, das Thema elektronische Identität von Grund auf neu zu denken und damit den Forderungen des Stimmvolks Rechnung zu tragen: Die E-ID soll vom Staat herausgegeben werden und höchsten Ansprüchen an den Datenschutz genügen.

«Privacy by Design»
Parteiübergreifend fordern deshalb mehrere Motionen im Parlament, dass die E-ID nach dem Grundsatz «Privacy by Design» entwickelt wird und Daten dezentral gehalten sowie sparsam geteilt werden. Äusserungen des Bundesrats deuten ebenfalls darauf hin, dass das Zielbild für die E-ID weitgehend klar ist. Die Diskussionen drehen sich derzeit vor allem darum, wie dieses erreicht werden kann. Im Raum stehen weiterhin klassische E-ID-Ansätze, wie sie auch im verworfenen E-ID-Gesetz vorgesehen waren. Dabei würde neu der Staat die Rolle des alleinigen Identitätsproviders übernehmen. So können zwei Forderungen des Stimmvolks erfüllt werden: Es handelt sich um eine staatliche E-ID, und Transaktionen können dank einem einzigen Herausgeber datensparsamer abgewickelt werden. Eine chipbasierte Lösung auf der Identitätskarte ist ebenfalls den klassischen Ansätzen zuzurechnen, wobei hier verschiedene negative Erfahrungen, unter anderem in Deutschland, hoffentlich als abschreckende Beispiele dienen.

Den klassischen Ansätzen ist eines gemein: dass sie eine E-ID als digitales Dokument verstehen, das einen eng begrenzten Satz von persönlichen Attributen – wie Name, Geburtsdatum und Nationalität – enthält und von einer einzigen Institution – dem Passbüro – herausgegeben wird. Dem gegenüber stehen selbstbestimmte digitale Identitäten, auf Englisch «self-sovereign identities» oder kurz SSI. Diese verstehen eine E-ID als hochsicheres, erweiterbares Set von persönlichen Attributen und basieren auf einer dezentralen Netzwerkarchitektur. Gehalten wird die «self-sovereign identity» in einem digitalen Portemonnaie, dem sogenannten Wallet, das sich zum Beispiel auf dem Smartphone befindet. Dieser Ansatz erlaubt das Führen einer Vielzahl von Attributen, die jeweils durch vertrauenswürdige Organisationen bestätigt werden, zum Beispiel Einwohnerämter, Strassenverkehrsämter oder Bildungsinstitute. In meinem Wallet findet sich also neben den Angaben zu meinem Namen und meinem Geburtsdatum auch Platz für meinen Fahrausweis, mein Universitätsdiplom und weitere Attribute. Mit wem ich diese Informationen teile, entscheide allein ich – genau wie es heute bei physischen Dokumenten der Fall ist.

Beträchtliche Vorarbeit
Die Möglichkeiten des SSI-Ansatzes sorgen derzeit vielerorts für Euphorie. Das ist angesichts der Vorteile verständlich. Doch muss bedacht werden, dass sowohl bei der technischen Infrastruktur als auch bei der Standardisierung und dem Aufbau des nötigen Ökosystems noch beträchtliche Vorarbeit geleistet werden muss. Erfreulicherweise laufen dazu international bereits verschiedene Bestrebungen. An denen sollten wir uns orientieren, um für unser Land frühzeitig das erforderliche Know-how aufzubauen. Für die Schweiz gilt es jetzt, die Zeichen der Zeit zu erkennen und die E-ID-Technologie von Beginn weg so auszugestalten, dass sie mit künftigen SSI-Standards zusammenspielt. So stellen wir sicher, dass die regulatorischen,

organisatorischen und technologischen Investitionen in unsere E-ID-Infrastruktur einen nachhaltigen Nutzen erzielen. Dass das Zeitalter selbstbestimmter Identitäten bereits eingeläutet wurde, zeigen nicht zuletzt der Kanton Schaffhausen und die Stadt Zug, die ihrer Bevölkerung bereits heute eine auf SSI-Prinzipien beruhende E-ID anbieten, die in naher Zukunft auch interkantonal eingesetzt werden kann.

Daniel Gasteiger ist Gründer und CEO der Procivis AG, welche die technische Lösung für die E-ID im Kanton Schaffhausen und in der Stadt Zug entwickelt hat.

SBB CFF FFS

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, 1. Oktober 2021

Öffentliche Konsultation zum «Zielbild E-ID»

Sehr geehrte Damen und Herren

Die SBB begrüsst die Diskussion zum Zielbild E-ID. Die Thematik ist für die SBB sowohl als Mobilitätsanbieter als auch Industrieunternehmen von zentraler Bedeutung. Vor allem aber eröffnet sie hohe Nutzenpotentiale für unsere Kund:innen. Zu diesem frühen Zeitpunkt tragen wir deshalb gerne erste Überlegungen zu den Schlüsselfragen der Diskussion bei.

Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Anwendungsfälle für die Mobilitätskund:innen: Der Zugang zu Mobilität als millionenfacher täglicher Vorgang wird zunehmend digitalisiert. Die flexible Wahl verschiedener Mobilitätsformen wird dabei immer wichtiger. Die E-ID kann helfen, diesen Zugang einfach, intuitiv, medienbruchfrei und sicher zu gestalten. So erspart ein Ökosystem digitaler Nachweise den Kund:innen beispielsweise das mehrfache Erfassen von Personalien und Nachweisen und unterstützt die Verwendung von Zugangsschlüsseln und Berechtigungen aus einer einzigen digitalen Brieftasche.

Anwendungsfälle für die Prozessintegration: Auch aus Sicht der SBB als Industriebetrieb ergeben sich vielfältige Anwendungsfälle. Qualifikationsnachweise (Ausbildungen, Maschinenbedienausweise usw.) und Zutrittsberechtigungen für Mitarbeitende und Beauftragte sind heute aufwändig zu erbringen. Unternehmensübergreifend einsetzbare digitale Nachweise können die Prozesseffizienz erheblich verbessern. Im Geschäftsverkehr steht beispielsweise die Anwendung der digitalen Signatur und der sicheren Digitalen Vernetzung mit Partnerunternehmen im Vordergrund.

SBB AG
Public Affairs und Regulation
Hilfikerstrasse 1 · 3000 Bern 65 · Schweiz
luca.arnold@sbb.ch / www.sbb.ch

SBB CFF FFS

Welches sind die wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Die E-ID soll in digitalen Prozessen medienbruchfrei, einfach, sicher und für die Nutzer:innen kostenlos und vertrauenswürdig eingesetzt werden können. Gerade mit Blick auf die Anwendung im Mobilitätsbereich ist dabei die europäische Interoperabilität von zentraler Bedeutung.

Eine wichtige Anforderung besteht überdies darin, dass die vom Bund gewährleistete Vertrauensinfrastruktur einen Wettbewerb innovativer Kundenlösungen im Ökosystem digitaler Nachweise erlaubt.

Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise auszustellen und überprüfen zu können?

Der Nutzen der E-ID entsteht bei deren Anwendung. Die erwähnten Anwendungsfälle vereinfachen den Zugang zur Mobilität für die Kund:innen, unterstützen nachhaltige integrierte Mobilität und tragen damit auch zur Kosteneffizienz des Systems Bahn bei.

Den Anwendungen im Mobilitätsbereich gemeinsam ist, dass sie eine anbieterunabhängige Service-Public-Infrastruktur für digitale Identität und weitere Nachweise voraussetzen. Wir begrüssen deshalb die Stossrichtung eines offen gestalteten digitalen Ökosystems digitaler Nachweise, denn hier ergibt sich für die Bevölkerung und die Unternehmen der wesentliche Nutzen.

Wir freuen uns, uns in die weitere Diskussion einzubringen. Für Fragen steht Ihnen Matthieu Boillat (matthieu.boillat@sbb.ch) zur Verfügung.

Freundliche Grüsse

Marcus Griesser
Chief Information Security Officer

Luca Arnold
Leiter Regulation und Internationales

Die Schweizerische Post AG
Stab CEO
Wankdorfallee 4
3030 Bern

Telefon +41 58 341 15 64
Fax +41 58 667 33 73
www.post.ch

Stab CEO, Wankdorfallee 4, 3030 Bern

Bundesamt für Justiz
Herr Michael Schöll
Direktor
Bundesrain 20
3003 Bern

Als PDF/Word an: E-ID@bj.admin.ch

Datum 4. Oktober 2021
Ihre Nachricht

Kontaktperson Franziska Heer
E-Mail franziska.heer@post.ch
Direktwahl +41 58 341 15 64

Stellungnahme der Schweizerischen Post zum Diskussionspapier zum «Zielbild E-ID»

Sehr geehrter Herr Schöll
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zum «Diskussionspapier zum Zielbild E-ID» Stellung nehmen zu können.

1. Ausgangslage für die Schweizerische Post

Die Post sieht in der digitalen Transformation eine Notwendigkeit für die Schweiz und will sie mit ihren Kompetenzen fördern. Sie versteht sich als Motor für eine moderne Schweiz und will heutige und zukünftige Bedürfnisse ihrer Kundinnen und Kunden erfüllen, ganz gleich ob physisch oder digital. IT ist seit Langem Teil des Postalltags: einerseits ermöglichen die sicheren und stabilen digitalen Systeme den reibungslosen Ablauf des physischen Kerngeschäfts. Andererseits schaffen sie die Voraussetzung dafür, dass die Post ihre Kernkompetenz, sensible Informationen sicher und vertrauensvoll zu transportieren, auch in der virtuellen Welt umsetzen kann. Die Post hat in den letzten Jahren ihre Kompetenzen und Ressourcen in der IT und Verschlüsselungstechnologie ausgebaut und bietet heute digitale Lösungen für Behörden, Geschäfts- und Privatkunden an. Eine sichere Identität für Akteure im digitalen Raum erachten wir als Schlüsselelement für den Erfolg der digitalen Transformation der Schweiz**.** Die Post hat diese Tastsache sehr früh erkannt. Sie ist einer der Pioniere in Sachen elektronische Identität und elektronische Signatur. Sie hat die vom SECO geförderte frühere Identitäts- und Signaturlösung SuisseID entwickelt, vermarktet und verbreitet. Als Mitglied des Joint Ventures SwissSign hat die Post den Aufbau der SwissID – Nachfolge Lösung gefördert. Mit der vollständigen Übernahme der SwissSign AG per 1. Oktober 2021 fahren wir auf diesem Pfad fort.

Die Post will rasch eine elektronische Identität: Die Post begrüsst die Initiative des Bundes, nach der Ablehnung des Bundesgesetzes über die E-ID, rasch eine neue Gesetzesvorlage aufzugleisen und eine gemeinsame Vision einer staatlichen elektronischen Identität zu diskutieren, denn für die Post ist die elektronische Identität in vielerlei Hinsicht von zentraler Bedeutung.

Die Post steht bereit als mögliche E ID-Partnerin des Bundes: Die Post als bundesnahes Unternehmen mit langjähriger Erfahrung in der Bereitstellung von sicheren digitalen Diensten ist bereit, als Bindeglied zwischen Bund, Kantonen und Wirtschaft einen Beitrag zu einer Lösungsfindung für eine rechtlich, politisch und unternehmerisch tragfähige und von der Gesellschaft (Bürger/-innen) akzeptierte elektronische Identität zu leisten. Am 1. Oktober 2021 hat die Post vollumfänglich die SwissSign AG übernommen. Die SwissSign bietet digitale Dienstleistungen an wie die SwissID, Zertifikats- und Signaturlösungen. Die Post stellt mit der Übernahme sicher, dass die in der Schweiz entwickelte und in der Bevölkerung weit verbreitete und bei Schweizer Unternehmen und öffentlichen Verwaltungen etablierte SwissID in Schweizer Händen bleibt. Als staatsnahes Unternehmen schafft sie damit auch die Voraussetzungen, um bei Bedarf der Schweiz, den Kantonen und den Bürgerinnen und Bürgern eine digitale Identität anbieten zu können. Die Post gehört für viele Schweizerinnen und Schweizer zur Identität unseres Landes. Sie geniesst grosses Vertrauen, ist in allen Landesteilen stark präsent und verfügt mit den Postfilialen über ein dichtes Infrastrukturnetz. Dieses schweizweite Netz an Zugangspunkten ist die ideale Voraussetzung dafür, dass für jeden Bürger und jede Bürgerin der physische Zugang zu einer E-ID-Ausgabestelle gewährleistet werden kann. Realistischerweise ist davon auszugehen, dass es diese physischen Kontaktpunkte für die Nutzerinnen und Nutzer nachwievor brauchen wird. Die Post kann dabei als vertrauenswürdige Identitätsprüferin gegenüber dem Staat und allen Bürgerinnen und Bürgern agieren.

2. Im Einzelnen

Zu den im «Zielbild E-ID» aufgeworfenen Fragen, nehmen wir wie folgt Stellung:

1. Wo sehen Sie den besonderen Nutzen der E-ID?

- **Die elektronische Identität ist ein Schlüssel für eine erfolgreiche digitale Transformation unseres Landes:** Die Schweiz weist im internationalen Vergleich beim Einsatz moderner Technologien einen Rückstand auf. Dies ist nicht zuletzt aus volkswirtschaftlicher Sicht kritisch zu beurteilen. Eine E-ID ist ein wesentliches Schlüsselelement, damit die Schweiz diesen Rückstand aufholen kann. Sie ermöglicht uns, viele Besorgungen und Dienstleistungen des täglichen Lebens im digitalen Raum zu erledigen. Unternehmen und den Behörden können ihre Kundinnen und Kunden und Dienstleistungsempfänger generell auch in der virtuellen Welt erkennen und einfach und vertrauensvoll in ihre digitalen Prozesse einbinden.

- **Indem der Staat beglaubigte Identitäten herausgibt, schafft er die nötige Rechtssicherheit und Vertrauen in der virtuellen Welt:** Dies fördert insbesondere die Digitalisierung in den Bereichen E-Commerce, E-Government, E-Health und weiterer wichtiger Anwendungsfälle hin zum Erreichen eines Ökosystems digitaler Nachweise. Das Vertrauen in die Digitalisierung steigt mit der E-ID. Behörden und private Unternehmen können ihren Kundinnen und Kunden Online-Services auf noch höherer Sicherheitsstufe anbieten, da sie auf einer vertrauensvollen und standardisierten E-ID basieren. Mit einer E-ID steigt das Vertrauen, dass persönliche Daten in einer Anwendung sicher und vor dem Zugriff Unbefugter geschützt sind.

- **Die Sicherheit wird entscheidend erhöht:** Weder Kundinnen und Kunden noch Anbieter von Online-Dienstleistungen sind vor Cyberkriminalität und -betrug gefeit. Auch die digitalen Prozesse der Post gewinnen durch die E-ID weiter an Sicherheit.

2. Welche Anwendungsfälle stehen für Sie im Vordergrund?

Alleine die Bereitstellung einer E-ID wird noch nicht zu einer breiten Adoption führen. Sie muss mit einem entsprechenden Angebot von nutzenstiftenden Anwendungsfällen und ergänzenden Services einhergehen. Als nutzenstiftend erachten wir insbesondere alle Anwendungsfälle, die oft genutzte Prozesse vereinfachen, zeitlich effizienter gestalten, die Transparenz und Nachvollziehbarkeit erhöhen und diese (rechts)verbindlicher machen. Folgende Anwendungsgebiete stehen hier aus unserer Sicht im Vordergrund:

- **Bereich E-Commerce**: Anwendungen, welche Nachweise für die Abschlüsse und Absicherung von Geschäften benötigen. Beispiele für solche Nachweise sind Altersnachweise oder bestätigte Lieferadressen für den Kauf und die Lieferung von Gütern, welche mit der Fähigkeit digitaler Unterschriften, Eintragungen von Eigentumsvorbehalten, dem Übergang von Nutzen und Gefahr oder anderen Handelsklauseln ergänzt werden.
- **Bereich der Gesundheitsversorgung:** Anwendungen wie der Bezug von Medikamenten aufgrund ausgestellter Arztrezepte, welche nur einmalig oder zeitlich begrenzt bezogen werden dürfen. Weiter bei der Ausstellung und der vertraulichen Weitergabe von medizinischen Attesten, in welchem Zero-Knowledge und Need to Know-Aspekte wichtig sind.
- **Bereich der Geschäfte zwischen Bürgern, staatlichen Entitäten und privaten Organisationen:** Anwendungen wie der Bezug und die Weiterleitung von Straf- oder Betreibungsregisterauszügen, der Ausstellung oder Änderung von Fahrzeugausweisen, Anwendungen im Bereich der Handänderungen von Immobilien (Grundbucheintragungen, Nachweise zu Finanzierungen oder Versicherungsdeckungen) oder allgemein Anwendungen welche Nachweise zu Qualifikationen und Berechtigungen erfordern.
- **Bereich der Erstellung, Anpassung oder Kündigung von rechtsverbindlichen Verträgen:** Anwendungen wie der Anpassung von Krankenkassenpolicen oder dem Abschluss von Mietverträgen welche entsprechende Nachweise aus Authorativen Quellen erfordern und mit rechtsverbindlichen qualifizierten digitalen Signaturen ergänzt werden.
- **Anwendungen und Prozesse welche Echtheits-, Qualitäts-, Herkunfts- oder Eigentumsnachweise** als Grundlage benötigen wie beispielsweise im Bereich von end-to-end-Lieferketten in der Lebensmittel- und Pharmaherstellung oder dem Handel wertvoller Güter.
- **Kombination mit physischen Anwendungen:** Aus unserer Sicht sollte die E-ID in erster Linie in der digitalen Welt breit zur Anwendung kommen. Nichtsdestotrotz kann die E-ID auch in der analogen Welt wichtige Funktionen übernehmen. Ein Beispiel hierfür ist die Ausweismöglichkeit mit dem Covid-Zertifikat oder die Wahrung der Privatsphäre beim Alkoholkauf mit Ausweispflicht, indem nur die absolut zwingend notwendigen Daten freigegeben werden.

3. Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Sicherheit als Basis für das notwendige Vertrauen: Privacy and Security by Design: Sicherheit und hoher Schutz der Daten sind der Schlüssel für die Akzeptanz des Systems in der Bevölkerung. Wichtige Anforderung an eine staatliche E-ID als digitaler Ausweis sind daher die Ansätze «Privacy by Design» und «Security by Design». Zudem soll eine künftige Lösung die Grundsätze Datensparsamkeit und dezentrale Datenspeicherung befolgen und damit sicherstellen, dass die Bürgerinnen und Bürger die Hoheit über ihre Daten behalten. Eine Gesetzesvorlage, welche auf diesen Elementen basiert, trägt den von der Bevölkerung und der Politik geäusserten Anliegen Rechnung. Der Staat sollte in diesem Kontext entsprechende Vorgaben bezüglich der einzusetzenden Standards, insbesondere im Bereich der Verschlüsselung, der Kommunikationsprotokolle und der Datennutzung und Haltung (GDPR, Recht auf Vergessen) festlegen.

Benutzerfreundlich und nutzenstiftend: Die Handhabung der elektronischen Identität muss für die Bürgerinnen und Bürger gut verständlich und einfach nutzbar sein. Sowohl der Erwerb wie auch der Einsatz der E-ID sollten darum so einfach wie möglich ausgestaltet sein. Nur wenn die Bevölkerung und die Unternehmen die E-ID effektiv im Alltag verwenden, kann sie ihren vollen Nutzen entfalten und den erwünschten Mehrwert liefern.

Möglichst grosses Anwendungsfeld (inkl. Interoperabilität) mit einheitlichen Standards: Damit die künftige E-ID einen wichtigen Beitrag zur digitalen Transformation unseres Landes leisten wird, muss ihr Anwendungsfeld möglichst grosse sein. Je mehr Anwendungen für die elektronische Identität zur Verfügung stehen, desto höher ist der effektive Nutzen und der Mehrwert für jeden einzelnen und desto grösser ist auch der Nutzerkreis der E-ID. Ein grosses Ökosystem digitaler Belege

von persönlichen Daten, Ausweisen, Diplomen, etc. als langfristige Zielsetzung birgt daher das grösste Potenzial für eine breite Nutzung der E-ID. Der Gesetzgeber muss deshalb die Erweiterbarkeit und die Anschlussmöglichkeit des Systems garantieren. Konkret müssen unbedingt zentrale Standards festgelegt werden, damit in allen Branchen und Lebensbereichen (Gesundheit, Bildung, Freizeit, Arbeitswelt, Finanzwelt usw.) dieselbe E-ID verwendet werden kann. Entsprechend sollten hier durch den Staat bezüglich der Interoperabilität und der Kommunikationsprotokolle Mindeststandards für die Sicherstellung eines offenen, auch international interoperablen Netzwerkes festgelegt werden.

4. Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Wir verstehen den Begriff 'nationale Infrastruktur' dahingehend, dass es sich um eine schweizweite einheitliche Infrastruktur handelt, die auch von einem privaten Unternehmen genutzt werden kann. Dies würde auch den Privaten erlauben, nach einheitlichen, nationalen Standards digitale Nachweise auszustellen. Damit wären neben E-Government dem Anwendungsspektrum keine Grenzen gesetzt. Wir sind daher der Ansicht, dass langfristig ein grosses digitales Ökosystem mit einem Ambitionsniveau 3 angestrebt werden sollte, damit das Potenzial der E-ID bestmöglich ausgeschöpft werden kann. Wir sind überzeugt, dass in einem breit gedachten Ökosystem die Chance am höchsten ist, aufwändige und kostspielige Medienbrüche gänzlich zu vermeiden.

Ambitionsniveau 3 mit einem Ökosystem digitaler Beweise als Zielsetzung: Die Frage, ob es die Schweiz wagen soll, auf eine E-ID-Lösung mit Potenzial zu setzen, ohne die genauen Details zu kennen, beantworten wir klar mit ja. Ein rein staatlich genutzter, digitaler Ausweis als Minimalvariante erscheint uns nicht zweckdienlich und wird nicht ausreichen, um die Digitalisierung in der Schweiz voranzutreiben und deren wertvolles wirtschaftliches Potenzial gänzlich auszuschöpfen. In Ambitionsniveau 1 ist der Anreiz für den Nutzer eine E-ID zu erwerben, nicht genügend hoch, weil deren Anwendungsmöglichkeiten sehr beschränkt sind. Der volkswirtschaftliche Beitrag einer E-ID mit Blick auf eine Beschleunigung der Digitalisierung bliebe sehr beschränkt.

Das Zielbild E-ID geht aus Sicht der Post daher klar in Richtung Ambitionsniveau 3, das es am besten erlaubt, sowohl die Zahl der Nutzerinnen und Nutzer als auch der Anwendungen, die mit der E-ID zugänglich sind, zu steigern und damit das Huhn-Ei-Problem zu überwinden. Ambitionsniveau 3 ermöglicht integrierte und somit sehr einfache Interaktionen zwischen Privaten, Unternehmen und Behörden. Die gemeinsame Basis der Marktteilnehmer reduziert die Komplexität auf der Nutzen- und der Aufwandseite.

5. Bewertung der technologischen Umsetzungsvarianten

Die zu wählende technische Umsetzungsvariante muss folgenden Anforderungen genügen:

- **Dezentralität:** In der Abstimmung über das E-ID Gesetzes ist die klare Abneigung gegenüber zentralistischer Ansätze in der Datenhaltung – sei dies staatlich oder privat – zum Ausdruck gekommen. Wenn das neue Bundesgesetz politisch mehrheitsfähig sein soll, dann muss die Forderung nach einer dezentralen Lösung im Zentrum der technologischen Lösung stehen.
- **Interoperabilität:** Eine solche Lösung sollte interoperabel und kompatibel mit Schweizer Recht und mit Lösungen aus Ländern der Europäischen Union sein. Entsprechende Initiativen innerhalb der EU werden derzeit stark gefördert.

Die Schweizerische Post kann sich bei allen drei zur Diskussion stehenden technischen Umsetzungsvarianten vorstellen, tragende Rollen in der Umsetzung und dem Betrieb einzunehmen und die entsprechende Verantwortung zu tragen. Wir sehen jedoch eine klare Priorisierung der Varianten:

- **«Selbst-kontrollierte Identität» (SSI):** Aus unserer Sicht unterstützt die technologische Umsetzungsvariante der «Selbst-kontrollierten Identität», der sogenannten SSI-Lösung diese Anforderungen am besten. Wir sehen eine konzeptionell hohe Ähnlichkeit der SSI- und PKI-Varianten. Für die Erreichung des Ambitionslevel 3 bietet die SSI-Lösung aus Sicht der Post aber eine höhere Flexibilität insbesondere im Ausbau der Möglichkeiten z.B. mit der Verwendung anderer identitätsnaher Attribute für Firmen und Individuen.
- **Zentraler staatlicher ID-Provider:** Unserer Einschätzung nach, wird sich mittel- und langfristig sowieso eine dezentrale Lösung durchsetzen. Darum erachten wir die Investition in eine Lösung mittels zentralem staatlichen Identitätsprovider als nicht zielführend. Weiter glauben wir auch, dass eine solche neue Lösung von den Bürgerinnen und Bürgern und der Wirtschaft kaum akzeptiert werden wird.

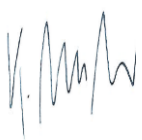
Der Aufbau einer dezentralen Lösung, die die Erreichung des Ambitionsniveau 3 ermöglicht, stellt eine Herausforderung dar. Als Basis hierfür braucht es eine Gesetzgebung, welche die Grundzüge der technischen Standards sowie aller rechtlichen, kommerziellen und User Experience-Aspekten regelt. Dabei ist eine stufengerechte Regulierung unabdingbare Voraussetzung, welche die Grundzüge und die wesentlichen Anforderungen im Bundesgesetz verankert, die technologischen Umsetzungsdetails jedoch in dynamischeren Erlassen regelt. Dies ermöglicht dem Gesetzgeber auf Basis stabiler Prinzipien im Gesetz, rasch auf technologische Entwicklungen reagieren zu können. Im Fokus der politischen Diskussion sollen ebendiese Prinzipien stehen.

Das bestehende Angebot der Post bietet die Möglichkeit, auf eine funktionierende Lösung für die Bürgerinnen und Bürger und die Wirtschaft unter der alleinigen Kontrolle einer bundesnahen Unternehmung zugreifen zu können. Diese Lösung könnte als Startpunkt für den Übergang in die dezentrale Lösung genutzt werden, von welcher aus die Nutzer über die Zeit ihre Identitätsinformationen in eine selbst-kontrollierte Lösung portieren und entsprechend erweitern können. Beide Lösungen werden deshalb für eine bestimmte Übergangszeit von mehreren Jahren parallel existieren. Die Post arbeitet derzeit an einer konzeptionellen Lösung für diese Übergangszeit. Mit dieser Lösung soll es möglich sein, dass User in persönlichen Wallets (Device oder Web basiert) ihre bereits bestehenden Credentials aus ihren IdP Accounts in ihre Wallet mittels bestehenden Flows portieren und in der SSI Registry (Blockchain) registrieren können. Die IdP's würden so bereits als Issuers agieren und die User als Holder im Sinne des SSI Konzeptes. Relying Parties können dann aufgrund ihrer eigenen technischen Roadmaps als Veryfier entsprechende Credentials vom Holder direkt anfordern und auf der SSI Registry verifizieren. Neue Issuer von Identitäts-Credentails (E-Ids) oder identitätsnahen Credentials können diese dann bereits direkt dem Holder in seine persönliche Wallet übergeben.

Wir bedanken uns für Ihre Kenntnisnahme und die Berücksichtigung unserer Ausführungen in den aktuellen Arbeiten.

Freundliche Grüsse

Die Schweizerische Post AG



Katrin Nussbaumer
Co-Leiterin Stab

Matthias Dietrich
Co-Leiter Stab

EID EN SUISSE

LA VISION DE SICPA

Octobre 2021

PRESENTED BY:
SICPA SA
AV DE FLORISSANT 41,
1008 PRILLY
SWITZERLAND

SICPA

Enabling trust

TABLE DES MATIÈRES

OBJECTIF DE CE DOCUMENT

L'objectif de ce document est d'apporter la vision de SICPA concernant l'implémentation de l'identité numérique (eID) en Suisse. Cette vision se base sur l'expertise de spécialistes du domaine de l'identité numérique et particulièrement dans l'approche dite « Self-Sovereign Identity » (SSI). Cette vision est également basée sur une constante veille technologique et conceptuelle d'initiatives similaires dans le monde. Ceci nous permet de fournir une vue globale et consolidée des expériences passées et des enseignements à tirer pour mettre en perspective les tendances futures et des enjeux liés à ce domaine.

1 TENDANCES DU MARCHÉ

Avec l'avènement d'internet sur le téléphone mobile, l'identité numérique est devenue un élément critique pour de nombreuses industries et dans nos interactions de tous les jours. Les citoyens ont aujourd'hui accès à de plus en plus de services en ligne. Dû à la multiplicité des fournisseurs de service en ligne (notamment des banques, du e-Commerce ou de gouvernements), les utilisateurs ont besoin de s'identifier numériquement de multiple fois par jour. De plus, la fragmentation des marchés, des applications, des technologies, des standards et des régulations est telle que l'émergence d'une identité numérique unique et simple n'était tout simplement pas envisageable jusqu'à présent. De ce fait, l'expérience utilisateur est restée très pauvre à cause de nombreux enregistrements à effectuer en ligne, avec des centaines de mots de passe/logins ou encore des contraintes administratives multiples …

Pour les fournisseurs de service en ligne, les coûts d'implémentation et la maintenance de systèmes d'identité numérique pour leurs opérations augmentent d'année en année. En effet, les besoins en sécurité et la conformité aux nombreuses réglementations sont devenus de plus en plus complexes (des dizaines voire des centaines de millions[1] chaque année pour le e-KYC dans l'industrie bancaire). Les nombreuses complications liées à l'enregistrement en ligne est un facteur prépondérant dans l'augmentation du taux d'abandon (56%) pour les clients de banques (en très forte hausse depuis deux ans). Les clients renoncent par exemple à l'ouverture d'un nouveau compte dès qu'il s'agit de passer dans une filiale pour une vérification en présentiel avec notamment leurs documents d'identité voire leur facture d'électricité. Comme la plus jeune génération commence à se tourner vers des banques alternatives qui fournissent des interfaces harmonieuses grâce à des applications mobiles intégrées, les banques traditionnelles doivent s'adapter sous peine de perdre cette nouvelle clientèle. L'identité numérique est devenue un aspect clé dans les opérations de nombreuses compagnies. De même pour l'industrie de la gestion des données comme Google ou Facebook, l'identité numérique est devenue au centre de leur système de création de valeur, ce qui représente des milliards de revenus chaque année. Finalement et jusqu'à présent, peu de gouvernements ont réellement pris l'initiative de fournir une identité numérique qui serait le pendant d'un document physique. L'organisation internationale de l'aviation civile (OACI) est l'instance de référence concernant tous les documents d'identité comme les passeports ou les cartes d'identité. Les e-Passeports qui contiennent une puce RFID et qui sont liés au système de PKD de l'OACI peuvent être utilisés comme facteur d'authentification pour des transactions en ligne. En effet,

[1] https://thepaypers.com/digital-identity-security-online-fraud/kyc-compliance-costs-banks-eur-50-million-a-year--780502

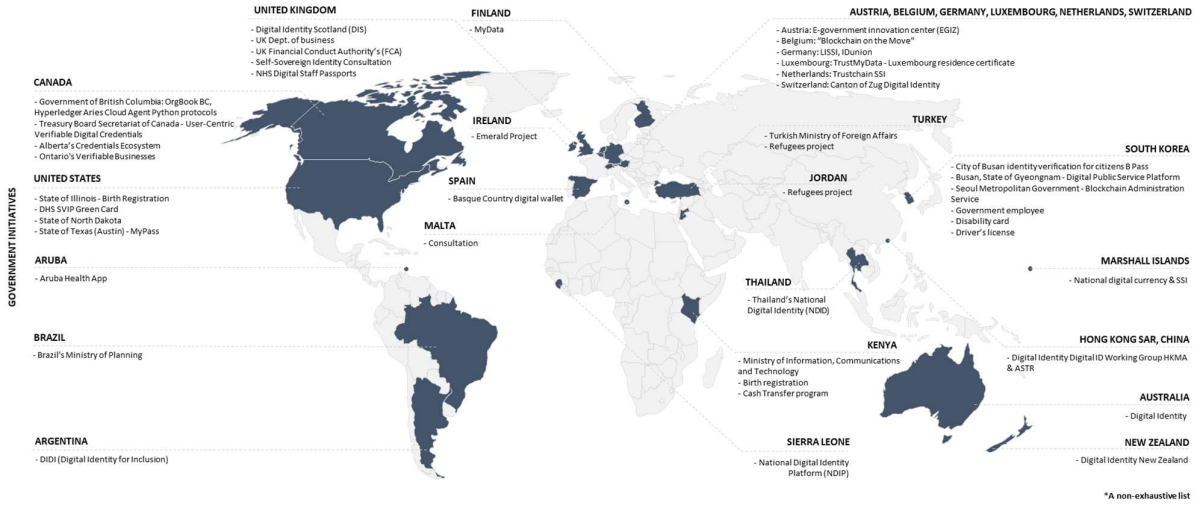
beaucoup de smartphones peuvent lire ces puces et peuvent vérifier l'authenticité du document présenté de manière cryptographique. Cependant, en 2021, seuls 78 pays sont émetteurs de ce type de passeports selon l'OACI[2]. De plus, dans de nombreux pays, les passeports restent très onéreux et seulement une infime part de la société peut se permettre d'acquérir un tel document de voyage. Finalement, le fait de devoir recourir à un document physique externe au smartphone n'est pas satisfaisant du point de vue de l'expérience utilisateur. De ce fait, les e-Passeports ne peuvent pas être considérés comme des identités numériques en tant que tel.

De tous les faits exposés ci-dessus, il en résulte l'émergence de nombreuses initiatives du secteur privé qui ont comme objectif de construire un système d'identité accepté et reconnu de manière globale. Jusqu'à aujourd'hui, des acteurs économiques tels que les banques ou des opérateurs de télécommunication ont pris et joué le rôle de fournisseurs d'identité à un niveau national ou même régional. Ces initiatives ont souvent connu des taux d'adoption limités et ont été confrontés à des contraintes d'interopérabilité avec d'autres systèmes similaires. De ce fait, c'est sans surprise qu'une initiative telle que Global Assured Identity Network (GAIN)[3] a vu le jour très récemment. Une coalition de banques, d'opérateurs de télécommunication et des acteurs « GAFAM » imaginent utiliser leur infrastructure e-KYC et leur capacité d'authentification de leurs clients pour offrir des services de confiance numériques via des « Application Programming Interfaces » (APIs). Ils ont publié ce « white paper » qu'ils ont nommé du même nom (GAIN). Leurs objectifs sont de développer des relations de proximité avec leurs clients, des revenus supplémentaires et des coûts de fonctionnement inférieurs. Un projet suédois illustre bien ce qu'il peut advenir aux gouvernements et aux citoyens avec une initiative comme GAIN. Bank-id (trademark BankID) est de loin le système d'identification numérique le plus utilisé en Suède avec un taux d'adoption de 94% parmi les utilisateurs de smartphones. BankID est administré par by Finansiell ID-Teknik BID AB qui est détenu par plusieurs banques suédoises et scandinaves. En mars 2018, BankID comptait environ 6.5 millions d'utilisateurs actifs et était accepté par 600 services en ligne[4] créant de fait une situation de monopole. En 2017, pour mettre fin à cette situation de monopole, Verisec lança sur le marché la solution d'eID qui se nomme Freja eID[5]. Jusqu'à présent, ce système a connu un succès très relatif malgré des fonctionnalités supérieures.

Même si une solution comme GAIN se montre techniquement interopérable au-delà des frontières et des secteurs de marché, cela amène des questions qui sont résumées par l'histoire de l'identité numérique en Suède[6]. Par exemple, est-ce que des clients qui ne feraient pas partie du réseau GAIN pourraient tout de même obtenir une identité numérique ? Si ce n'est pas le cas ou que des contraintes trop restrictives limitaient cet accès à une identité numérique, certaines personnes pourraient se retrouver exclues de beaucoup d'activités de la société dans le monde digital et même physique. Un autre sujet d'importance est la régulation. Que va-t-il se passer lorsque des pays voudront imposer certaines régulations (comme le GDPR[7] ou similaire) et que GAIN refusera ou ne sera pas en mesure de se soumettre à ces directives ? Concernant la gouvernance de ce type d'organisation, les considérations financières primeront très souvent sur les intérêts des utilisateurs. Le risque pour les gouvernements est une perte substantielle de leur attributs régaliens et limitation

[2] https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx
[3] https://www.iif.com/Publications/ID/4573/Global-Assured-Identity-Network-White-Paper
[4] https://www.bankid.com/om-oss/statistik
[5] https://frejaeid.com/en/home/
[6] https://www.diva-portal.org/smash/get/diva2:1236665/FULLTEXT01.pdf
[7] https://gdpr-info.eu/

de leur capacité à réguler des systèmes de-facto tels que ceux-ci. De ce fait, il devient urgent que les gouvernements analysent et décident de quel type de société numériques ils désirent pour leur propre pays. C'est exactement ce qu'il se passe dans de nombreux pays à travers le monde. Certains gouvernements sont en train de tester et de construire un cadre de confiance (trust framework) pour permettre l'émergence de la prochaine génération d'internet basée sur l'approche Self-Sovereign Identity (SSI). Ci-dessous se trouve une liste non-exhaustive des initiatives à travers le monde :



Des gouvernements tels que les Etats-Unis, le Canada, la Corée du sud, l'Australie, la Nouvelle Zélande ou la communauté Européenne travaillent sur des façons d'échanger de l'information de manière harmonieuse et simple pour favoriser leurs économies numériques, ce qui donnera aux citoyens et aux acteurs du secteur privé de solides fondations pour des interactions sûres et respectant la vie privée. De tels systèmes bénéficieront au final au tant aux gouvernements, aux citoyens et au secteur privé.

Par exemple, l'Union européenne a financé un projet dont le but est de faire avancer l'adoption à large échelle du concept de Self-sovereign Identity pour la prochaine génération d'identité numérique de confiance qui permettrait des transactions plus rapides et sécurisées via internet et dans la vie réelle. L'UE a exprimé un intérêt à prendre part au développement de « l'internet des identités » [8]. Ainsi, en 2016, l'UE a lancé l'initiative qui se nomme « Next Generation Internet » [9] qui doit favoriser les échanges d'informations liés à l'identité entre pays membres de l'UE et ainsi qu'au Canada et aux Etats-unis, en toute conformité avec les législations sur la protection des données. Le but est de développer le futur internet de manière à le rendre interopérable afin de promouvoir les valeurs qui sont chères à l'Europe : l'ouverture, l'inclusivité, la transparence, la protection de la vie privée, la coopération et la protection des données.

Toutes ces initiatives sont basées sur des standards[10,11] dits « open » et recommandés par l'organisation W3C. L'activité première de la W3C est de développer des protocoles et des directives qui assurent la croissance à long terme de l'internet. Les standards de la W3C définissent les éléments clé qui permettent au World Wide Web de fonctionner. Ainsi, la conformité avec de tels standards est essentielle afin de garantir une interopérabilité avec des initiatives similaires à travers le monde et de manière à garantir la viabilité à long terme.

[8] The EU has coined its initiative the "Internet of humans": https://www.ngi.eu/about/
[9] https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative
[10] https://www.w3.org/TR/vc-data-model/
[11] https://www.w3.org/TR/did-core/

2 EID EN SUISSE

Dans cet environnement complexe et en constante évolution, les questions soulevées par la population Suisse suite au vote sur la loi concernant l'identité numérique nationale sont cruciales[12]. Notamment, la peur de la dépendance vis-à-vis de systèmes d'identité numérique gouverné par des acteurs privés est symptomatique du manque de confiance dans les solutions fournies par le marché. De ce fait, la demande faite au gouvernement peut se traduire comme le besoin de fournir à la population une identité fondationnelle sûre (par rapport aux identités qui seraient dérivées) et qui agirait comme base de confiance pour toutes les transactions digitales en Suisse.

Si la discussion sur le niveau d'ambition est importante, elle peut difficilement être décorrélée et isolée de ce qui se passe sur le marché. Fournir une solution qui ne serait utilisable qu'en Suisse adressera forcément qu'un cadre limité de cas d'usage et ainsi l'adoption risque de rester faible. C'est la raison pour laquelle les interfaces entre la future eID Suisse et le reste du monde sont très importantes pour garantir une interopérabilité des systèmes.

Comme première étape, il s'agirait d'assurer que la solution d'eID Suisse couvre correctement les besoins des autorités communales, cantonales et fédérales et qu'elle facilite toutes les interactions avec les multiples services étatiques. L'objectif serait de proposer des moyens d'authentification pour accéder à différents services étatiques comme les prestations sociales ou les impôts et d'émettre des équivalents digitaux des documents officiels sous forme papier comme les permis de circulation, les extraits de casier judicaires, les actes civils, les permis de travail, les permis de séjour, etc … . Si l'eID peut servir comme base solide d'identité foundationnelle, les identités dérivées (comptes bancaires, abonnements mobiles, …) seraient beaucoup plus faciles à émettre et à gérer. Dans un deuxième temps, les interactions avec des acteurs sur le marché local seraient importantes et bénéficieraient à l'ensemble de la collectivité comme les citoyens, le secteur privé et le gouvernement. La promesse de cette approche est multiple : pour le citoyen de simplifier sa vie et d'accélérer les processus administratifs, pour le secteur privé de diminuer les coûts liés à la vérification de documents d'identité et finalement pour les départements étatiques de faciliter les processus d'émission et ainsi fournir de meilleurs services à la population.

Même si ce système pourrait fonctionner uniquement en Suisse, cette approche atteindrait rapidement ses limites car confrontée aux contraintes du marché et de ce qui est implémenté ailleurs dans le monde. En effet, comme décrit au chapitre1, beaucoup d'initiatives similaires sont en ce moment testées dans d'autres pays. L'interopérabilité avec des initiatives est donc clé pour construire un système d'identité numérique pérenne dans le temps et qui permettra les interactions au-delà des frontières et de s'interfacer aisément par rapport à des initiatives globales comme GAIN.

Comme demandé, cette vision pour une eID en Suisse doit être une base de débat pour la discussion publique. Ci-après, notre vision :

[12] https://www.admin.ch/gov/fr/accueil/documentation/votations/20210307/loi-federale-sur-les-services-d-identification-electronique.html

Quelles sont les trois principales exigences auxquelles doit satisfaire une e-ID ?

1. **Interoperabilité au-delà des silos**

   Comme mentionné auparavant dans ce document, l'interopérabilité est la clé, afin de garantir une large adoption de l'identité numérique en Suisse et de maximiser les impacts positifs pour la société. Comme d'autres pays implémentent des écosystèmes similaires, les bénéfices seront autant pour les citoyens Suisses qui voyageront à l'étranger que pour les étrangers qui voudraient résider dans notre pays. Beaucoup de processus seront simplifiés dû au fait que la vérification des identités et certificats pourra être faite de manière instantanée et au-delà des frontières, grâce à une base et des standards communs. Cela bénéficiera également aux acteurs du secteur privé qui opèrent à une échelle globale comme les banques, car les interfaces qu'elles vont mettre en place en Suisse pourront être largement réutilisées dans d'autres pays au lieu d'adapter leurs technologies et leurs processus spécifiquement pour la Suisse.

2. **Securité et confiance**

   La confiance dans le système débute par la phase d'enregistrement des personnes et la sécurisation du lien entre le porteur légitime, les certificats et le terminal (mobile). Le recours aux centres biométriques établis pour les passeports et les cartes d'identité en Suisse semble donc critique de ce point de vue, afin d'assurer la fiabilité de la phase d'enregistrement. Concernant la technologie, des mesures et des moyens dans l'état de l'art devraient être mis en place afin d'éviter tout risque lié à la modification des certificats ou à l'usurpation d'identité. De même, des scenarios de menaces et de failles globales du système devraient être mis en place pour minimiser les impacts de toutes sortes. Par exemple, l'Estonie a vécu péniblement une telle vulnérabilité et a dû résoudre rapidement un problème de sécurité avant de créer des dommages considérables dans la société[13][14]. En plus de l'Estonie, la Slovaquie, l'Autriche et l'Espagne ont fait face à des vulnérabilités similaires[15][16]. Finalement, la confiance se gagne grâce à un cadre de confiance (trust framework) qui est développé et partagé publiquement comme au Canada au travers du Digital Identification and Authentication Council of Canada (DIACC) par exemple[17]. Le DIACC Trust Framework Expert Committee (TFEC) représente une diversité d'acteurs publics et privés qui collaborent ensemble de manière à délivrer des ressources qui contribuent à une identité numérique de confiance comme : la validation de cas d'usage, des standards, des partenariats, des alignements au niveau international et le développement des réglementations.

3. **Inclusivité, équivalence légale et viabilité opérationnelle**

   Tout le monde devrait être éligible pour obtenir une identité digitale en Suisse. Ceci est une partie vitale de la souveraineté dans notre pays et garanti à chacun la possibilité de faire partie de la société numérique sans discrimination. La question sensible de l'âge devrait être abordée et débattue car cela pose des questions pratiques à propos de l'authentification grâce à des systèmes biométriques. Facebook par exemple défini la majorité numérique à 13 ans[18]. De même, certains aspects pratiques liés à la validité et la révocation de l'identité numérique (lié par exemple à un décès) devraient être abordés dès le début. Concernant les certificats comme la carte grise, le permis de circulation, les actes civils etc… l'équivalence

[13] https://magicofsecurity.com/estonia-hits-gemalto-again-insecure-eid-cards/
[14] https://e-estonia.com/card-security-risk/
[15] Electronic Government and the Information Systems Perspective
[16] Electronic Government and the Information Systems Perspective: 7th ... - Google Livres
[17] https://diacc.ca/
[18] https://m.facebook.com/help/157793540954833

de la forme digitale devrait être reconnue légalement à travers tout le pays. Autant la version physique que la version digitale des documents devrait être reconnue dans les processus administratifs. Cependant, autant que possible, la forme digitale devrait être privilégiée de manière à pouvoir simplifier les processus grâce à des transactions en ligne plutôt qu'en présentiel. Finalement, l'identité et les certificats numériques devraient être opérationnellement viables. Ceci signifie qu'ils devraient être vérifiables autant en ligne que hors réseau (c'est-à-dire sans connectivité). Une vérification en présentiel reste très importante dans la vie de tous les jours et si les deux formes doivent être équivalentes, ce cas d'usage devrait être couvert également.

Quels sont les principaux domaines d'utilisation de l'e-ID ?

1. La réutilisation de certificats pour obtenir d'autres certificats (carte grise, extraits de casier judiciaires, actes civils, permis de travail, permis de séjour …). Dans de nombreux processus administratifs, différents documents sont nécessaires. Pour bénéficier de tous les avantages liés à transformation numérique de la société, la réutilisation des certificats est essentielle car elle permet d'assurer un effet boule de neige qui garantir une large adoption par la population.

2. C'est bien la multiplicité des cas d'usage et la généralisation du système de certificats qui va garantir une adoption à large échelle et non-pas un cas d'usage spécifique. Ceci va également faciliter l'expérience utilisateur car les citoyens ne devront comprendre qu'une fois comment interagir en ligne et feront face à la même interface dans toutes leurs transactions numériques.

3. L'authentification en ligne pour accéder à des services communaux, cantonaux ou fédéraux sera très importante. Un cas d'usage typique est l'accès au portail des impôts, aux prestations sociales ou au contrôle des habitants.

Quels sont les avantages d'une infrastructure nationale permettant à l'État et aux particuliers de prouver et de contrôler électroniquement l'identité (par ex. e-ID, permis de conduire, pièce de légitimation de collaborateur ou carte d'étudiant numériques) ?

Détenir et contrôler une infrastructure nationale d'identité est important à plusieurs égards. Premièrement, les données seraient stockées et sécurisées en Suisse. Même si cela ne permet pas de se prémunir entièrement contre des vulnérabilités ou des pertes de données, cela permettrait au moins au gouvernement de mettre en place les mesures et les moyens dans l'état de l'art nécessaires pour minimiser de potentiels risques. De plus, le gouvernement devrait assurer à long-terme l'accessibilité des données car souvent les données liées à l'identité sont de nature sensible et doivent être accessibles pendant des dizaines d'années. Troisièmement, il est important que les autorités Suisses restent indépendantes de toutes législation et régulation concernant le stockage de donnée (par exemple le Cloud Act[19]). D'autres pays comme le Luxembourg par exemple ont récemment décidé de se diriger dans cette direction[20]. En 2019, le Ministère de la Digitalisation a annoncé la création de la première blockchain du secteur publique. Cette technologie offre à tous les acteurs du domaine publique au Luxembourg l'opportunité d'améliorer la transparence, la fiabilité et la sécurité des systèmes et des processus d'information numériques du secteur publique.

[19] https://en.wikipedia.org/wiki/CLOUD_Act
[20] https://luxembourg.public.lu/en/invest/innovation/blockchain.html

3 CONCLUSION

De par sa configuration, la Suisse a toujours su tirer profit de ses multiples interactions tant au niveau communal, cantonal ou fédéral qu'international. Alliant différentes langues et la précision qui la caractérisent, cette diversité relationnelle à différents degrés, doublé de son sens de l'innovation, du respect de la privauté, a permis à la Confédération Helvétique de pérenniser son excellente réputation internationale et d'en faire un acteur important dans les échanges globaux.

L'approche dite « Self-sovereign Identity » (SSI) est issue de ces mêmes principes fondamentaux, et a été reconnu par de nombreux protagonistes publiques et privés comme étant l'approche de choix pour une transition vers l'identité digitale. 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 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'UE mènent actuellement des projets pilotes pour évaluer les impacts sur leur infrastructure existante et leurs processus existants, la Suisse pourrait également faire partie des pionniers du SSI qui façonnent les transactions numériques de demain. Nous serions heureux de partager davantage notre vision d'une mise en œuvre réussie et harmonieuse de l'identité numérique en Suisse

4 ABBREVIATIONS ET ACRONYMES

Acronym	Definition
API	Application Programming Interfaces
DIACC	Digital Identification and Authentication Council of Canada
eKYC	Electronic Know Your Customer
GAFAM	Google Amazon Facebook Apple Microsoft
GAIN	Global Assured Identity Network
GDPR	General Data Protection Regulation
OACI	Organisation de l'aviation civile internationale
IIF	Institute of International Finance
NGI	Next generation Internet
PKD	Public Key Directory
SSI	Self-sovereign Identity
W3C	World Wide Web consortium

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

swisscom

C1 - Public

Per E-Mail an E-ID@bj.admin.ch
Herr Urs Paul Hollenstein
Fachbereich Rechtsinformatik
Bundesamt für Justiz

Worblaufen und Zürich, 30.9.2021

Zielbild E-ID, öffentliche Konsultation

Sehr geehrter Herr Hollenstein

Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der öffentlichen Konsultation zum "Zielbild E-ID" Stellung zu nehmen.

1 Grundsätzliches zum Zielbild E-ID

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 der von Ihnen aufgegriffene Ansatz „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, bedacht 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 das elektronische Patientendossier, E-Collecting und -Votingsysteme, die Bestellung von Registerauszügen aller Art sowie in übergeordneter Weise die digitale Willenskundgabe mittels der elektronischen Signatur.

Vor diesem Hintergrund begrüssen wir die von Ihnen vorgelegte, sehr fundierte und breite Auslegeordnung zum "Zielbild E-ID".

2 Zu den einzelnen Fragestellungen

2.1 Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Damit sich digitale Lösungen durchsetzen, müssen diese in puncto Ausgestaltung im Publikum auf Akzeptanz stossen und klare Vorteile für alle beteiligten Akteure mit sich bringen. Aus diesen Zielen lassen sich drei konkrete Anforderungen an eine E-ID ableiten:

Vertrauenswürdigkeit

Das Vertrauen in elektronische Identifikationslösungen fusst wesentlich auf dem Schutz der Privatsphäre der E-ID-Benutzerinnen und -Benutzer. Dabei stehen datenschutzrechtliche Prinzipien wie "privacy by design" sowie Datensparsamkeit im Brennpunkt.

Diese Kriterien lassen sich unseres Erachtens am ehestens mit dem von Ihnen zur Diskussion gestellten Konzept "SSI" verwirklichen, da dieses auf ebendiesen Grundprinzipien beruht.

Unter den diversen datenschutzrechtlichen Vorzügen dieses Ansatzes ist namentlich die Reduktion auf die je nach Anwendungsfall notwendigen Attribute bei der Datenübertragung an Dritte und die konsequente Vermeidung unnötiger Datenflüsse und der damit verbundenen Randdaten hervorzuheben.

Benutzerfreundlichkeit

Digitale Transaktionen, die den Einsatz der E-ID erfordern, müssen ebenso einfach handhabbar und transparent ausgestaltet sein, wie alle übrigen digitalen Geschäftsprozesse, um im Publikum breit akzeptiert zu werden.

Was von den Benutzerinnen und Benutzern dabei als benutzerfreundlich empfunden wird, bestimmt sich in massgeblicher Weise nach dem jeweils aktuellen Stand der Technik und vorherrschender Trends. War der Einsatz zusätzlicher Geräte oder Karten zwecks Authentisierung beispielsweise noch lange gang und gäbe, dürfte ein entsprechend ausgestaltetes Verfahren heute auf breite Ablehnung stossen. Auf der anderen Seite ist es ebenso wichtig, weniger technologieaffine Benutzerinnen und Benutzer nicht zu überfordern (z.B. beim Verwalten der Verifiable Credentials).

Demzufolge ist eine hohe Adaptionsfähigkeit an die jeweils aktuellen Ansprüche der Benutzerinnen und Benutzer an die Benutzerfreundlichkeit erforderlich. Der zu schaffende Rechtsrahmen für eine staatliche E-ID-Lösung und das damit einhergehende Vertrauensökosystem sollte daher zwar klare Leitplanken setzen (*"was"*), jedoch insbesondere betreffend die benutzerseitigen Systeme weitestgehend technologieneutral ausgestaltet sein (*"wie"*), um eine stetige Weiterentwicklung zu ermöglichen.

Vertrauensökosystem

Wie Sie in Ihrem Diskussionspapier darlegen, sehen sich Initiativen wie die Einführung nationaler E-IDs regelmässig mit dem Huhn-Ei-Problem konfrontiert: ohne E-ID werden keine Anwendungsfälle geschaffen und ohne Anwendungsfälle wird keine E-ID benötigt. Unserer Ansicht nach wird eine Kombination aus bewusst geförderter (Verwaltungsdienste) und freier Nutzung (private Dienste) nötig sein, um einen ausreichenden Verbreitungsgrad zu erreichen.

Vor diesem Hintergrund erachten wir den neuen Anlauf, eine nationale E-ID zu schaffen, als grosse Chance, ein umfassendes Vertrauensökosystem zu etablieren, das einerseits die Anforderungen an eine vertrauenswürdige, staatlich herausgegebene E-ID erfüllt und andererseits den regulatorischen Rahmen für eine Vielzahl von Anwendungsfällen schafft, um das grösstmögliche Potential des digitalen Wandels auszuschöpfen.

Daher bietet das "Ambitions-Niveau 3", im Rahmen des vorgeschlagenen SSI-Ansatzes, unseres Erachtens den geeigneten Rahmen, um mit den Möglichkeiten der Digitalisierung Mehrwerte für alle beteiligten Akteure zu schaffen.

In einem solchen Vertrauensökosystems wird die E-ID schliesslich einen von verschiedenen digitalen Nachweisen darstellen. Die E-ID ist namentlich der staatlich herausgegebene Identitätsnachweis, welcher nutzerseitig in einem (allenfalls zertifizierten) Wallet eigebettet werden kann. Basierend auf dieser Identifikation können dann beliebig weitere Nachweise in diesem Wallet hinterlegt werden. Private Stellen wie Bildungsinstitutionen, Transportunternehmen, Tourismusbetriebe, Kulturdienstleistende oder dergleichen sind dadurch in der Lage, ihrerseits digitale Nachweise herauszugeben. Ebenso andere staatliche Stellen wie beispielsweise Strassenverkehrsämter. Dadurch erhöht sich der Gesamtnutzen des Vertrauensökosystems entscheidend.

In einem offenen Vertrauensökosystem, das Raum für Innovation bietet und den Benutzerinnen und Benutzern gleichzeitig die vollständige Kontrolle über ihre Daten belässt, sehen wir schliesslich die Zukunft digitaler Vertrauensdienste.

2.2 Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Neben einer Vielzahl möglicher Nachweise von Merkmalen wie Qualifikationen und Berechtigungen in einem Vertrauensökosystem sehen wir in der staatlichen E-ID eine einfachere Zugangsmöglichkeit zur digitalen Willensäusserung mittels qualifizierter elektronischer Signaturen. Konkret könnte insbesondere ein sicherer Zugang zu digitalen Vertragsabschlüssen ermöglicht werden.

Dadurch sparen Benutzerinnen und Benutzer bei unterschiedlichsten Anwendungsfällen Zeit und Kosten bei unverändert hoher Rechtssicherheit und erzielen dadurch einen unmittelbaren Nutzen. Entsprechend erleben wir in der Praxis ein stetig wachsendes Bedürfnis nach hochwertigen elektronischen Signaturen und erachten diese als wichtiges Element des digitalen Wandels.

2.3 Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Gemäss Erhebung des Bundesamtes für Statistik (BFS) zur Internetnutzung in den Schweizer Haushalten nahm der Anteil der Internetnutzerinnen und -nutzer in der erwachsenen Bevölkerung der Schweiz weiter zu. Von 84% im Jahr 2014 ist er auf 90% im Jahr 2017 und 93% im Jahr 2019 gestiegen. Nach Alter betrachtet nutzen demnach nahezu alle Personen zwischen 15 und 55 Jahren das Internet, 95% davon täglich. Der grösste Zuwachs ist bei den höchsten Altersgruppen festzustellen. 88% der 65- bis 74-Jährigen verwenden 2019 das Internet (+11 Prozentpunkte gegenüber 2017).

Noch eindrücklicher sind die Zahlen zur Internetnutzung in beruflichem Kontext: 87% der Erwerbstätigen in der Schweiz verwenden bei der Arbeit einen Computer oder eine andere elektronische Ausstattung. 57% arbeiten mit einer fachspezifischen Software und nahezu 40% erhalten ihre Aufgaben oder Anweisungen über eine Fachanwendung.

Dabei ergeben sich heute überall dort Medienbrüche, wo Formerfordernisse den digitalen Weg versperren und kein Zugang zu einer rechtssicheren digitalen Alternative besteht oder wenn Nachweise nur physisch zur Verfügung stehen. Eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können, bildet daher eine notwendige Komponente, um das

Wertschöpfungspotenzial der Digitalisierung zu nutzen und das standortrelevante, hohe Mass an Rechtssicherheit mittel- und langfristig zu erhalten.

Schliesslich ist festzuhalten, dass gerade bei Anwendungsfällen hoher Bedeutung wie Behördengeschäften oder Justizverfahren regelmässig (Identitäts-)Nachweise erforderlich sind. In Anbetracht des hohen Nutzungsgrads des Internets über alle Bevölkerungsgruppen hinweg bewirkt das heutige Fehlen einer digitaler Vertrauensinfrastruktur de facto auch eine Erschwerung des Zugangs zu essenziellen öffentlichen Angeboten.

Zusammenfassend kann festgehalten werden, dass die Schaffung eines verlässlichen digitalen Vertrauensökosystems eine zentrale Lücke schliesst, denn fehlende Vertrauenselemente bei digitalen Transaktionen stellen heute das grösste Hemmnis der Digitalisierung dar. Die Beseitigung dieses Defizits schafft einen soliden Nährboden für die künftige digitale Ökonomie sowie hochwertiges e-Government.

Wir bedanken uns für Ihre Kenntnisnahme und die Prüfung unserer Eingabe. Sehr gerne unterstützen wir Sie im Rahmen des weiteren Prozesses und bieten eine Mitarbeit beispielsweise in einer vom Bund einzusetzenden Begleitgruppe ausdrücklich an.

Freundliche Grüsse

Stellungnahme der Threema GmbH zum «Zielbild E-ID»

Vielen Dank für die Gelegenheit zur Stellungnahme. Gerne beziehen wir nachfolgend zu den Fragen Position:

Wichtigste Anforderungen an eine staatliche E-ID

- **Datensparsame Architektur / Privacy by Design**: der Herausgeber soll nicht erfahren, wann/wo die E-ID eingesetzt wird. Möglichkeit zur Selbstbestimmung, welche Daten bei der Präsentation der E-ID an den Verifier weitergegeben werden. Daten sollten möglichst durch technische und nicht nur durch rechtliche Massnahmen geschützt werden.
- **Die E-ID soll primär eine digitale Identität sein, kein Login à la «Bürger-Single-Sign-On».** Die E-ID soll also nicht ein «Login für alles» werden, sondern nur dort eingesetzt werden, wo es wirklich nötig ist. Beispiel: eine Online-Shop-Bestellung braucht keine E-ID (ausser vielleicht für eine Altersprüfung). Zum Eröffnen eines Bankkontos ist eine E-ID notwendig, aber nicht für das spätere Login im e-Banking.
- **Alle benötigten Software-Komponenten sind Open Source** (als vertrauensbildende Massnahme und zur Erhöhung der Sicherheit). Kommunikationskanäle und Prozesse zum Melden und Beheben von Sicherheitslücken sind definiert.

Anwendungsfälle

Die wichtigsten Anwendungsfälle für eine E-ID sind aus unserer Sicht:

- Identitätsbeweis für Vertragsabschluss (Handyvertrag, Bankkonto etc.)
- Identifikation bei Behördengängen (Steuererklärung, Betreibungsregisterauszug, Handelsregister etc.)
- Verträge rechtsgültig digital signieren (um die unsägliche Praktik des «drucken – unterschreiben – scannen» zeitgemäss zu ersetzen)
- Altersprüfung mit der Möglichkeit, nur die Identität und ein Mindestalter ohne genaues Geburtsdatum zu beweisen. Beim Szenario Eintrittskontrolle (Disco o.ä.) wäre es ein Mehrwert, nur ein Bild und ein Mindestalter ohne Details wie Name oder Geburtsdatum präsentieren zu können.

Nutzen einer nationalen Infrastruktur für digitale Beweise

Den Nutzen einer nationalen Infrastruktur für digitale Beweise sehen wir primär darin, die unzähligen analogen Plastikkarten/Papierausweise in die digitale Welt zu bringen und den Anbietern die Ausstellung und Erneuerung langfristig zu vereinfachen.

Wir würden empfehlen, diesen Weg in die Zukunft bei der Konzeption der E-ID zu berücksichtigen. Es ist aber unseres Erachtens wichtig dass die E-ID nicht gleich zu Beginn mit solchen Möglichkeiten überladen und damit die technische Komplexität erhöht wird. Dies würde sonst die Akzeptanz gefährden.

Je mehr solche (auch privat ausgestellte) Beweise genutzt werden, desto mehr muss auf das Risiko der Verknüpfbarkeit von Aktivitäten der Nutzer über verschiedene Dienste/Anbieter hinweg geachtet werden.

Allgemeine Überlegungen

Nach unserer Praxis-Erfahrung (Threema-ID, Aufbewahrung von Private-Keys, Verlust von Handys, Backup-Thematik) führt für eine sichere E-ID kaum ein Weg an einem physischen Token als Private-Key-Storage vorbei. Das Token speichert den privaten Schlüssel so, dass dieser nicht ausgelesen werden kann, ähnlich wie dies bei Cryptocurrency-Wallets umgesetzt wird. Der Schlüssel kann anschliessend genutzt werden, um eine E-ID auf ein Smartphone oder einen PC zu übertragen, ohne dass der private Schlüssel selbst übertragen werden muss.

22.9.2021

Threema GmbH

Für Rückfragen: Manuel Kasper (manuel.kasper@threema.ch)

Stellungnahme ti&m zum Diskussionspaper «Zielbild E-ID» des Eidgenössischen Justiz und Polizeidepartements EJPD

(https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/ziel-bild-e-id.html)

Als führender Anbieter von Dienstleistungen und Produkten zur digitalen Transformation in vielen Bereichen der Schweizer Wirtschaft erachten wir die digitale Identität als ein ganz zentrales Thema. Viele digitale Prozesse, ob in der Wirtschaft, der Administration aber auch im sozialen Miteinander (Stichwort: Social Networks) leiden heute darunter, dass im digitalen Raum die Identifizierung des Gegenüber ein komplizierter und fehleranfälliger Prozess ist. Neben unseren Produktentwicklungen zur benutzerfreundlichen 2-Faktor Authentisierung oder zur schnellen und sichereren Online Identifikation haben wir auch bereits seit mehreren Jahren nach Lösungen gesucht, die Identität des Einzelnen sicher, flexibel und vertraulich zu verwalten. Mit der digitalen Identität für die Bürger der Stadt Zug haben wir die ersten grössere Pilotinstallation als Self Sovereign Identity Lösung realisiert, und dieses Prinzip in mehreren weiteren Anwendungen erprobt. Auf diesen Erfahrungen basiert diese Stellungnahme zum interessanten und erhellenden Diskussionspapier.

Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Die aus Sicht des Staates wichtigste Anforderung an einen staatliche e-ID als digitaler Ausweis ist sicherlich die, dass die Hoheit des Staates als Herausgeber der Identität seiner Bürger gewahrt bleibt. Wem wird für wie lange eine Identität gewährt, welche Attribute sind es genau, die den Bürger dem Staat gegenüber identifizieren? Dabei muss der Konflikt «Bürger Souveränität» vs. «Staats Souveränität» sinnvoll gelöst werden.

Die Anforderung des Bürgers an eine staatliche Identität ist etwas anders gelagert: er muss sich sicher sein, dass seine digitale Identität ihn als Person und Bürger wirklich eindeutig identifiziert, und dass niemand sich gegenüber dem Staat oder Dritten als er selbst ausgeben kann. Weiterhin muss der Bürger darauf vertrauen können, dass das Vorweisen einer digitalen Identität keine Auswirkungen auf seine Rechte als autonomer Bürger hat, sprich, dass keine Nachverfolgung aufgrund übermittelter Daten stattfinden kann.

Und – last but not least – gibt es noch eine Anforderung. Die digitale Identität muss der herausragenden Rolle, die sie im wirtschaftlichen und gesellschaftlichen Kontext spielt – sowohl digital als auch «analog» - gerecht werden. Sie muss im Zentrum jeglicher Berechtigung, Bestätigung oder auch Eigenschaft stehen, die der Besitzer im Verlaufe seines Lebens erhält, erwirbt oder sich aneignet. Das heisst, sie muss mit dem Besitzer wachsen können und damit das Abbild seiner aktuellen wirtschaftlichen und gesellschaftlichen Rolle darstellen.

Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Die Identifizierung von Personen und in immer höherem Masse auch von «Dingen», stellt den grundlegenden Anwendungsfall einer E-ID dar. Jede dieser Personen oder auch Dinge besitzt jedoch im Kontext seiner wirtschaftlichen, gesellschaftlichen oder persönlichen Aktivitäten auch zusätzliche Berechtigungen,

Fähigkeitsnachweise oder Eigenschaften, die ihm (mit seiner spezifischen Identität) verliehen wurden, oder die sie auf sonstige Art und Weise erworben hat. Diese Attribute erweitern die Identität der Person und sind alle potenzielle Anwendungsfälle für eine digitale Identität. Beispiele sind der Führerschein, ein Arztrezept, ein Schlüssel für ein elektronisches Schloss, eine Bestätigung der Kreditwürdigkeit, ein Schul- oder Universitätszeugnis und Hunderte weitere Attribute, die den Besitzer als Berechtigten oder Befähigten ausweisen und ihm so die Teilnahme oder den Zutritt zu speziellen Prozessen und Tätigkeiten ermöglichen.

Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Eine nationale Infrastruktur im Sinne eines «Trust Networks», die sowohl von staatlichen Institutionen als auch von Wirtschafts- und Forschungseinrichtungen der Schweiz betrieben wird und allen Schweizer Bürgern offensteht, bietet ein hohes Innovations- und Entwicklungspotenzial für den Wirtschaftsstandort Schweiz. Eingebettet und interoperabel mit vergleichbaren europäischen und internationalen Initiativen würde eine solche Infrastruktur die Digitalisierung der Wirtschaft und der Gesellschaft in nachhaltiger und vertrauenswürdiger Art und Weise fördern. Die Lasten von “datensparsamem Onboardings” und “Beweisführungen”, die heute Fall-spezifisch (und unterschiedlich) von Bürgern und Anbietern zu tragen sind, können massiv reduziert werden.

Fazit und Empfehlung

Von den im Diskussionspaper dargestellten Lösungsansätzen kann nach unserer Erfahrung nur der Ansatz der Self-Sovereign Identity alle vorgenannten Anforderungen erfüllen und kann aufgrund seiner Flexibilität, Erweiterbarkeit und Einfachheit im Handling das Potenzial einer modernen digitalen Identität voll ausschöpfen. Unsere Erfahrungen zeigen, dass dieser Lösungsansatz sowohl von den technischen Voraussetzungen als auch von den Anforderungen an eine Governance her heute bereits produktiv umsetzbar ist.

Kontakt ti&m: Martin Fabini, Principal, martin.fabini@ti8m.ch, +41 44 497 7525

Vereign

Vereign AG · Kolinplatz 10 · CH-6300 Zug

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail zugestellt an: E-ID@bj.admin.ch

15. October 2021

Öffentliche Anhörung zum Diskussionspapier zum «Zielbild E-ID»

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren,

wir beziehen uns auf die am 02. September 2021 eröffnete öffentliche Anhörung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zum Diskussionspapier «Zielbild E-ID» und die Online-Konferenz am 14. Oktober 2021, welche wir mit grossem Interesse verfolgt haben. Wir begrüssen die Initiative und den offenen Dialog um eine langfristig tragfähige Lösung für die Schweiz zu finden.

Leider kommen wir erst jetzt zur Rückmeldung, da wir intern mit Hochdruck an den letzten Details unserer Lösung für Verifizierbare Credentials für Email gearbeitet haben, welche das klassische Einschreiben mit erheblichen Mehrwerten ablösen können. Wir hoffen, dass Sie unseren Beitrag dennoch hilfreich finden.

Vereign AG ist ein Schweizer Startup aus dem Cryptovalley in Zug. Unser Name setzt sich zusammen aus den Begriffen “Verifiable” und “Sovereign”. Verifizierbare (Credentials) und (Selbst-) Souveräne (Identität) sind bei uns im Namen und Selbstverständnis verankert. Wir sind mit der Mission angetreten, Selbst-Souveräne Identität nützlich und nutzbar zu machen.

Aus unserer Erfahrung sind insbesondere im Bereich der Usability und User Experience klassische wie auch moderne Identitätssysteme den meisten Menschen nicht zumutbar. Die Schlüsselverwaltung bei digitalen Signaturen ist auf einem noch schlechteren Stand. In der Praxis finden sich daher aktuell eigentlich nur Lösungen welche die Schlüsselverwaltung in den Händen eines zentralen Intermediärs legen. Diese Intermediäre werden mithin zum digitalen und oft auch de-fakto juristischen Stellvertreter der Anwenderinnen.

Die Nutzer haben dabei keine Kontrolle über und auch keine Einsicht in die beteiligten Systeme. Mithin fehlen ihnen die Mittel, bei einem allfälligen Missbrauchsfall zu beweisen, dass sie es nicht gewesen sind. Sie sind vielmehr auch für diese Funktion auf den zentralen Intermediär angewiesen, der den allfällig selber ausgeführten Missbrauch – sei es vorsätzlich oder fahrlässig durch mangelhafte interne Prozesse oder Technologie – nun auch selber untersuchen und verfolgen muss.

Dieser ins System eingebaute Interessenkonflikt ist ein inhärenter Nachteil aller zentralisierten Lösungen, unabhängig davon, welche Partei diese bereit stellt. Tatsächlich fehlt diesen Systemen meist auch die Transparenz – und daher auch das Vertrauen von insbesondere technisch versierten Nutzern. Viele andere Nutzer können technisch vermutlich nur begrenzt nachvollziehen in welchem Masse sie hier von einem Anbieter abhängig sind, scheinen aber intuitiv zu realisieren, dass dies nicht wirklich “ihre” Identität ist, sondern vielmehr ihr digitales Abbild in den Händen einer dritten Partei.

Das Referendum vom März 2021 hat diese Bedenken sichtbar gemacht und gezeigt, dass der Grossteil der Bevölkerung sich eine E-ID wünscht, welche datensparsam ist, die Privatsphäre bewahrt und unter Kontrolle des Nutzers steht. Aus unserer Sicht erfüllt nur Self-Sovereign Identity (SSI) diese für eine breite Akzeptanz notwendigen zentralen Anforderungen.

Darüberhinaus ist SSI der sich zunehmend etablierende Standard weltweit. Die Europäische Union ist mit ihrer GAIA-X Initiative bereits dabei, entsprechende Technologien zu fördern während gleichzeitig die Aktualisierung der eIDAS-Verordnung zur Unterstützung von SSI bereits in vollem Gang ist.

Wir haben zum Teil über 20 Jahre Erfahrung in traditionellen Technologien, insbesondere den verbreiteten Ansätzen für Identity- & Access-Management (IAM), Schlüsselverwaltung, sowie Public Key Infrastructures (PKI). Unsere Erfahrungen mit diesen Technologien war der Grund warum wir uns 2017 dafür entschieden haben, voll auf SSI Technologien zu setzen.

Im Jahr 2018 haben wir begonnen, einen Proof of Concept für eine nutzbare SSI Lösung zu entwickeln, welche viele der im Diskussionspapier angesprochenen Themen vorweg nimmt und bereits Lösungswege aufzeigt. Wir haben dabei bewusst bei der User Experience begonnen weil wir davon ausgehen, dass die einfache Nutzung für die tatsächliche Adaption zentral sein wird.

Als Anwendungsziele für unseren SSI POC haben wir dabei Email und Dokumentensignatur auf Basis der in ZertES und eIDAS vorgegebenen Technologien gewählt, da Email den wohl wichtigsten Kommunikationskanal darstellt und Dokumentensignatur einen offensichtlichen und zentralen Anwendungsfall für die geschäftliche Nutzung darstellt.

In Partnerschaft mit dem Kanton Zug haben wir dabei auch bereits das Onboarding über den bestehenden Zuglogin oder die Verknüpfung einer Vereign SSI mit dem Zuglogin implementiert und haben entsprechende Erfahrungen darin gesammelt, bestehende Systeme im Rahmen einer modernen SSI Anwendung zu verknüpfen.

Aufgrund dieser langjährigen Erfahrungen würden wir daher gerne zu den von Ihnen angesprochenen Nachteilen von SSI ein paar Rückmeldungen anbringen.

Dass die Nutzer die Verantwortung für eigene Verified Credentials trägt ist korrekt. Die Verwaltung derartiger Credentials ist dabei eine Kernfunktion der entsprechenden “Wallet”, eine Hilfestellung durch die Anwendung, durch entsprechende Selbsthilfe-Ressourcen und allenfalls auch durch den Hersteller der Wallet sind jedoch durchaus möglich und werden wohl zumindest am Anfang durchaus notwendig sein. Am Ende übersetzt sich dieser “Nachteil” also in die Anforderung, nutzbare Software zu schreiben.

Der Erfahrung nach stösst auch die nutzbarste Software teilweise an ihre Grenzen, insbesondere wenn es sich um Konzepte und Ideen handelt mit denen die meisten Menschen noch nicht vertraut sind. Dies ist insbesondere bei SSI bisher der Fall. Den Nachteil, dass viele Menschen bisher noch keine Berührungspunkte mit SSI hatten und allenfalls auch noch nicht verstehen, welcher Mehrwert Ihnen durch SSI entsteht, können wir aus eigener Erfahrung bestätigen. SSI ist im Moment noch recht komplex für den durchschnittlichen Anwender.

Wir haben daher in unserem POC einen Weg gewählt bei dem die Persistierung der Daten über foderierte Instanzen erfolgte, welche im Zweifelsfall sogar im Selbsthosting betrieben werden können. Wer dies nicht will oder dazu nicht in der Lage ist hat noch immer die Wahl zwischen verschiedenen Betreibergesellschaften, welche verschiedene Gesellschaftsformen haben können, u.A. auch Genossenschaften und andere, den Nutzern verpflichtete Strukturen.

Dieser Aufbau erlaubt es, die Prinzipien und Grundlagen von SSI zu bewahren, jedoch gleichzeitig einen höheren Grad an Hilfestellung zu gewährleisten. Die Nutzer haben in diesem Modell, welches zu allen internationalen SSI Ansätzen kompatibel ist, die Wahlfreiheit zwischen vollständiger Autonomie und einer teilweisen Autonomie mit Unterstützung einer durch sie selbst bestimmten Partei.

Aus unserer Sicht ist ein derartiger Ansatz zumindest für eine schnelle Einführung ein guter Weg, da er die vertrauten Prinzipien mit der neuen Welt von SSI so verknüpft, dass dem Nutzer eine Handreichung gegeben wird. Gleichzeitig entspricht ein derartig föderierter Ansatz auch ideell den bewährten Prinzipien der Schweizer Eidgenossenschaft,

Dies ist im Sicherheitsbereich bereits lange eine Anforderung, und es gibt zunehmend Erfahrung damit, wie dies gelingen kann. Funktionen wie Zahlungen per Mobiltelefon sind mittlerweile im Mainstream angekommen, und auch wenn die Sicherheitselemente von modernen Smartphones nicht standardisiert sind, so würde mit einer Unterstützung der beiden dominanten Anbieter sicherlich der grösste Teil der Anwender abgedeckt.

Für alle anderen Nutzer und die Nutzer von alten Smartphones liessen sich Lösungen finden bei denen ein ausgelagertes Sicherheitselement einen Teil beiträgt, u.A. durch geeignete Schlüsselaufteilung. Absolute Sicherheit kann jedoch keiner der beschriebenen Ansätze jemals erreichen, da die Sicherheit immer auch eine Funktion von physischer Sicherheit des Nutzers, verwendeten Endgeräten und ganz besonders der Nutzergewohnheiten ist.

Wir haben daher in unserem POC einen Weg gewählt bei dem wir hohe Sicherheit mit hoher Transparenz kombinieren und jede Aktion der Identität sich immer auch in einem ebenfalls via Blockchain gesicherten Audit-Trail unter Kontrolle des Nutzers niederschlägt. In Kombination mit automatischer Generation von Schlüsseln zur einmaligen Verwendung kann so auch der bei den Nachteilen angesprochene Nachweis abgedeckt werden: Ein Nutzer kann durch Offenlegung des jeweiligen Eintrags aus seinem Audit Trail beweisen, eine gewisse Aktion nicht durchgeführt zu haben.

Sollte das Endgerät selber kompromittiert sein, so hat der Nutzer auf seinen anderen Geräten Sichtbarkeit auf die Handlungen dieser Wallet, kann darauf entsprechend reagieren, und das kompromittierte Gerät deaktivieren. Selbst bei Totalverlust aller Zugangsmöglichkeiten haben wir einen gut nutzbaren Weg implementiert bei dem via Social Recovery dafür gesorgt werden

kann, dass die eigene Identität und die entsprechenden Credentials allenfalls auch ohne zentralen Intermediär wiederhergestellt werden können.

Uns ist bewusst, dass diese Detailebene zum jetzigen Zeitpunkt bereits zu tief ist. Wir wollten Ihnen aber auf jeden Fall einmal darlegen, dass es für die angesprochenen Nachteile bereits funktionale Lösungen gibt welche demonstriert werden können und wir bieten uns dafür sehr gerne an.

Die Vision eines heterogenen SSI Ökosystems von Anbietern und Anwendungen unter Beteiligung des Staates für die Herausgabe von staatlichen Dokumenten ist aus unserer Sicht der einzige Ansatz welcher den Prinzipien der Schweiz gerecht wird und dem über das Referendum vom März 2021 ausgedrückten Bürgerwillen gerecht wird.

Wir hoffen daher, dass eine entsprechende Grundsatzentscheidung bald getroffen werden kann und bieten allenfalls gerne unsere Kompetenz bei der Strukturierung und Umsetzung an.

Mit besten Grüssen,

Georg Greve
Verwaltungsratspräsident und Head of Product Development

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Bundesamt für Justiz
Bundesrain 20
3003 Bern

PER E-MAIL AN e-id@bj.admin.ch

30. September 2021

Stellungnahme zur öffentlichen Konsultation zum «Zielbild E-ID»

Sehr geehrte Damen und Herren

Am 2. September 2021 eröffnete der Bundesrat die öffentliche Konsultation zum Diskussionspapier zum «Zielbild E-ID». Für die Einladung zum Austausch mit Bundesrätin Karin Keller-Sutter gemeinsam mit Bundeskanzler Walter Thurnherr sowie mit ausgewählten Vertreter:innen aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft zur künftigen Schweizer E-ID-Lösung sowie zur schriftlichen Stellungnahme danken wir Ihnen bestens.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Unsere Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Unser Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir im Rahmen der öffentlichen Konsultation wie folgt Stellung:

Vorbemerkungen

Die Digitale Gesellschaft war massgeblich am erfolgreichen Referendum gegen das E-ID-Gesetz beteiligt und brachte sich aktiv in die Abstimmungsdebatte ein. Dabei war es uns immer wichtig, weder die E-ID noch die Digitalisierung per se zu verhindern. Vielmehr muss die Frage gestellt werden, wem der technologische Fortschritt dient. Als zivilgesellschaftliche Organisation setzen wir uns dafür ein, dass (auch) die Ausstellung des digitalen Ausweises eine staatliche Aufgabe bleibt. Im Zentrum müssen der Nutzen für die Inhaber:innen der E-ID sowie die Sicherheit und der Datenschutz stehen.

Zu den einzelnen Fragen

Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Die E-ID muss den datenschutzrechtlichen Grundprinzipien **«Privacy by Design» und «Privacy by Default»** strikt folgen, wie es auch das neue Datenschutzgesetz explizit fordert**.** Dies bedeutet, dass eine möglichst dezentrale Architektur gewählt wird, bei der die beglaubigten Attribute (wie Name, Geburtsdatum, Wohnort oder Berechtigung zum Führen eines Fahrzeuges) lokal und sicher bei den Benutzer:innen als elektronischer Ausweis (beispielsweise in einem «Wallet») gespeichert werden und direkt einer prüfenden Instanz (wie ein Portal zur Einreichung der Steuererklärung) vorgewiesen werden können. Eine solche Nutzung muss möglichst anonym bzw. datensparsam möglich sein, so dass beispielsweise bei der Überprüfung des Alters weder das genaue Geburtsdatum noch bei der Überprüfung des Covid-Zertifikates der Name bekannt gegeben werden müssen. Für die höchste Sicherheitsstufe muss ein Hardwaretoken (Karte, Stick oder auch Chip) zum Einsatz kommen können.

Neben dem Datenschutz muss der **Nutzen für die Inhaber:innen** im Zentrum stehen. Eine E-ID muss flexibel verwendbar sein und sollte nicht allein als digitale Identitätskarte dienen. Eine Nutzung muss auf mehreren, verschiedenen Geräten (Smartphone, Tablet, Notebook, Smart Watch, Desktop-Computer) möglich sein. Sie muss international einsetzbar und daher möglichst EU-kompatibel sein. Die Ausstellung und die Verwendung müssen gratis sowie die Implementierung mit möglichst geringen Kosten verbunden sein.

Um die Kosten gering zu halten, das nötige Vertrauen zu schaffen und für die notwendige Verbreitung zu sorgen, müssen die Software sowie Beispiel-Implementierungen unter einer **Open-Source-Lizenz** entwickelt und veröffentlicht werden und ausnahmslos auf offenen Schnittstellen (APIs) und Standards basieren.

Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Die E-ID ist in erster Linie ein digitaler Ausweis, der für die Identifikation und zur Bestätigung verschiedener Tatsachen (Alter, Aufenthaltsstatus, Covid-Status, Krankenversicherung) verwendet werden kann. Die Identifikation kann auch zum Onboarding für weitere, unabhängige Identitätsdienste verwendet werden. Es geht bei der E-ID aber nicht darum, ein allgemeines Login für alltägliche Online-Dienste (wie Webshops) zu schaffen.

Die E-ID soll zudem ein gesichertes Login (Zwei- oder Multi-Faktor-Authentisierung) ermöglichen. Und sie soll zur (qualifizierten) elektronischen Unterschrift in der Schweiz und im Ausland verwendet werden können.

Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Ein flexibler und breiter Anwendungsbereich sorgt für einen grösseren Nutzen bei den Anwender:innen und führt zu einer schnelleren Akzeptanz sowie einer grösseren Verbreitung.

Eine staatliche Infrastruktur schafft die Voraussetzung für Kontinuität und Vertrauen, gerade auch mit Blick auf das Ambitionsniveau 3. Die Infrastruktur muss sich aber auf das technisch Notwendige beschränken und kryptografisch so gestaltet sein, dass ein Rückschluss auf den Zeitpunkt, den Ort oder den Verwendungszweck – also das Sammeln von Randdaten – verunmöglicht wird. Die staatliche Infrastruktur (im weiteren Sinne) soll sich möglichst auf die Ausstellung von Beweisen (beglaubigte Attribute) und die Bereitstellung auf offenen Standards basierender Schnittstellen sowie entsprechender Beispiel-Implementierungen beschränken, die auch eine einfachere Vernetzung mit E-ID-Infrastruktur(en) im Ausland ermöglichen.

Schlussbemerkungen

Die im Diskussionspapier vorgestellten Lösungsansätze (Self-Sovereign Identity, Public Key Infrastruktur, Zentraler staatlicher Identitätsprovider) schliessen sich nicht zwingend aus, sondern können sich (auch) ergänzen. So könnte eine Public Key Infrastrukur beispielsweise als Übergangstechnologie zur Self-Sovereign Identity dienen. Da die internationale Entwicklung und die wissenschaftliche Forschung hin zur Self-Sovereign Identity tendieren, sollte dieser Lösungsansatz stark im Fokus stehen, da er insbesondere auch die Forderungen der sechs gleichlautenden Motionen erfüllt.

Datensparsamkeit, «Privacy by Design» und dezentrale Datenspeicherung sind bei einem zentralen, staatlichen Identitätsprovider hingegen nicht gegeben (oder nur sehr umständlich zu erreichen). Das Konzept der Identitätsprovider (IdP) aus dem gescheiterten E-ID-Gesetz, basierend auf Protokollen wie SAML oder OpenID Connect, steht daher im Widerspruch zur Idee einer selbstbestimmten Identität und sollte daher verworfen werden.

Mit freundlichen Grüssen

Erik Schönenberger
Geschäftsleiter

Stellungnahme zum EID-Zielbild

Annett Laube
Gerhard Hassenstein

Forschungsgruppe IAM des Instituts IDAS
Berner Fachhochschule – Technik & Informatik

Die vorliegende Stellungnahme behandelt folgende Themen:

- Varianten, welche im Diskussionspapier behandelt werden
- Einsatz der E-ID im analogen und digitalen Umfeld
- Einbettung der E-ID in die Wirtschaft der Schweiz
- Vision einer E-ID
- Antworten zu den Fragen des BJ
- Anforderungen an den Staat

1. Vorab einige Gedanken

Die Fragen, welche in diesem Diskussionspapier gestellt wurden, erachten wir als richtig.
Ein erneuter Anlauf, eine nachhaltige nationale E-ID zu schaffen, ist der richtige Weg und bietet eine grosse Chance. Es muss ein neues Vertrauen beim Benutzer wie auch bei den vertrauenden Dritten geschaffen werden. Darüber hinaus muss geklärt werden, welches die Anforderungen an eine vertrauenswürdige, staatliche E-ID sind, welche Rolle der Staat und welche die vertrauenden Parteien übernehmen sollen. Damit können eine Vielzahl von Anwendungsfällen geschaffen werden, ohne diese auf einer Liste zu führen.
Der Bürger hat in den letzten Jahren grosse Fortschritte gemacht. Sein Alltag ist digitaler geworden. Er ist den «Techies» etwas nähergekommen. Jetzt sprechen aber diese «Techies» wieder von einem neuen Ansatz «privacy by design», «benutzerzentriert», «selbst-kontrollierte Identitäten», «Blockchains», usw. Wie soll der Bürger damit umgehen?

Ein «benutzerzentrierter» Ansatz ist der einzig richtige, denn er ist dem altbekannten physischen Prozess nachempfunden: *Ausstellen-Erhalten-Besitzen-Vorzeigen-Verifizieren*, und deshalb einfach nachzuvollziehen - nur eben jetzt in digitaler Form. Ein Paradigmenwechsel – weg von einem zentralen System muss aber erst von der Bevölkerung verstanden werden. Dieser zentrale Dienst war eine Zwischenlösung, mit welcher man möglichst einfach alles an einer Stelle gespeichert hat. Dieser Ansatz ist nicht mehr zeitgemäss, da der Schutz der Privatsphäre neu ins Spiel gekommen ist, denn diesem zentralen Dienst muss vollumfänglich vertraut werden - und damit haben viele Kreise ein berechtigtes Problem.
Die E-ID soll ein vom Staat ausgestellter digitaler Ausweis für jedwelche Art von Subjekten sein. Der Staat soll eine Basis-Identität dem Inhaber übergeben (benutzerzentrierter Ansatz). Diese Basis-Identität beinhaltet einen eineindeutigen Identifikator und geprüfte Attribute, für welche der Staat zuständig ist. Damit dies alles zum Fliegen kommt, soll der Staat eine Basis-Infrastruktur zur Verfügung stellen bzw. diese definieren.

2. Zu den Varianten

Aus unserer Sicht ist die Variantendiskussion unabhängig von Ambitionsniveaus zu betrachten. Ambitionsniveaus sind für uns Entwicklungsschritte, welche für jede dieser Varianten Gültigkeit haben.

Variante 1 (SSI):

Aufgrund von Forderungen nach hohem Datenschutz und dezentraler Datenspeicherung stellt eine «benutzerzentrierte» Variante die einzig sinnvolle Lösung dar. Parlamentarische Vorstösse und Entwicklungen in der EU in diese Richtung verstärken diesen Anspruch.

Variante 2 (PKI):

Ein X.509 Certificate basierender Ansatz (PKI) hat gegenüber der Variante 1 klare Nachteile, da diese Lösungsvariante auf «Verifiable Credentials» (VC) beruht.

- X.509 Certificates sind gegenüber VCs viel weniger flexibel. Ein Zertifikat ist zwar auch eine Art VC. Beide werden von einem Herausgeber signiert. Im Gegensatz zu VCs können X.509 Certificates nur bestimmte Informationen beinhalten. Eine Erweiterung von Identitätszertifikaten mit Attributzertifikaten wurde zwar von IETF standardisiert, aber nie wirklich umgesetzt. Es existieren auch Vorstösse X.509 Certificates als DID einzusetzen: https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/X.509-DID-Method.md.
- X.509 Zertifikate werden von einer zentralen Instanz herausgegeben. Dieser zentralen Instanz muss vom Benutzer vollständig vertraut werden. Damit ist der Grundsatz «privacy by design» nicht mehr gegeben. Für eine schnelle und unkomplizierte Herausgabe von Covid-Zertifikaten ist dieser Ansatz naheliegend, aber man kann dasselbe Ziel auch mit VCs erreichen.

Variante 3 (staatlicher IdP):

Diese Variante ist nicht zeitgemäss und nicht «privacy» konform. Falls ein online Dienst aus Kompatibilitätsgründen diese Variante - die Delegation an einen vertrauenswürdigen zentralen IdP wünscht, könnte er dieselbe Funktionalität auch mit Variante 1 erreichen. Diese Variante wäre zukunftsträchtiger, aber sie bedingt, dass der online Dienst die Überprüfung der Identität selbst vornimmt. → Ausbau der RP als Verifier. (siehe weitere Kommentare dazu in Kapitel: 7 - Anforderungen an den Staat: Authentifizierungsservice).

3. Soll die E-ID in der analogen wie auch der digitalen Welt genutzt werden können?

Die E-ID sollte zunächst nur in der digitalen Welt verwendet werden. Die analoge Welt wird wie bisher von einem physischen Ausweis abgedeckt (→ Identitätskarte).
In einer weiteren Ausbaustufe wäre es aber wünschenswert, dass diese digitale Identität auch in der analogen Welt zum Einsatz kommt und auf Dauer die Identitätskarte ablöst. Dazu braucht es aber noch weitere Infrastrukturkomponenten, die im Diskussionspapier nicht aufgeführt sind. Zum einen muss das Wallet erlauben, die digitale Identitätskarte (inkl. Lichtbild) vorzuweisen und es muss für jeden möglich sein, die Echtheit dieser digitalen Identitätskarte, z.B. mit einer Prüf-App, zu verifizieren.

4. Einbettung der E-ID

Die E-ID soll von verschiedenen Organisationen verwendet werden können. Dies können private Unternehmungen, Behörden, KMUs oder grössere Ökosysteme sein. Die Art der Verwendung der E-ID soll eine Entscheidung dieser Institutionen bleiben.
Wenn wir von Variante 1 ausgehen, so kann eine Organisation selbst digitale Nachweise in Form von VC liefern und damit einen Mehrwert für eine Inhaberin oder einen Inhaber darstellen.
Es gilt aber zu unterscheiden, für welche Identität die digitalen Nachweise herausgeben werden. Ist die E-ID ein gemeinsamer Nenner oder eine spezifische Identität, welche innerhalb der Organisation

Gültigkeit hat. Wenn der Kundenstamm der Organisation mit dem der E-ID 100% deckungsgleich ist, kann die E-ID voll verwendet werden. Ist der Kundenstamm hingegen grösser, so stellen Identitäten der E-ID nur ein Subset dar. Betroffene Institutionen sind also gezwungen selbst eigene Identitäten herauszugeben und zu verwalten und werden daher die E-ID nur für das «Onboarding» ihrer Kunden nutzen. Dies trifft für eine Vielzahl von nutzenden Institutionen zu, insbesondere für grössere Ökosysteme, da diese bereits ihre eigenen Identifikatoren haben und nutzen wollen (Kundenbindung und -kontrolle).

5. Vision der E-ID

Wenn der Staat eine Basis-Infrastruktur (Registry und Wallets, inkl. Agents) reguliert und evtl. auch zur Verfügung stellt, so können grössere Ökosysteme diese Infrastruktur nutzen, um Referenzen zu eigenen VCs darauf abzulegen. Diese privaten VCs referenzieren entweder die Basis-Identität der E-ID oder eine Identität, die nur innerhalb des Ökosystems Gültigkeit hat. Unabhängig davon können damit VCs auch von fremden Ökosystem genutzt werden, da ihr Format standardisiert ist. Das fremde Ökosystem muss aber die Identität kennen und den Inhalt der VC interpretieren können.

6. Standardfragen des BJ zum Diskussionspapier

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

- *Nutzen der E-ID:* Analog zur physischen Welt, in welcher man bei Bedarf einen amtlichen Ausweis zeigen muss, soll dasselbe in der digitalen Welt möglich sein → Transformation.
    - *Anwendungsfälle* gibt es viele. Es macht zurzeit keinen Sinn die Anwendungsfälle einzeln aufzulisten. Wie das E-ID Leitbild mehrmals aufführt (Huhn-Ei Problem) wird es ohne E-ID keine Anwendungsfälle geben (jeder wurstelt selbst etwas) und ohne Anwendungsfälle wird keine E-ID benötigt. Der Staat muss eine bestimmte Vorarbeit leisten, um dann zuzuwarten und den Markt spielen zu lassen.
    - Anwendungsfälle können grob in drei Kategorien zusammengefasst werden:
        - *Authentisierung* (In verschiedenen Fällen sind Identität und Merkmale das einzig geforderte z.B. beim Login → Autorisation)
        - *Willensäusserung* (digitale Signatur).
        - *Dezentrale Datenablage:* Eine sichere, möglichst dezentrale Ablage von Daten (z.B. Solid - Social Linked Data) wo die Inhaberin/Inhaber die Hoheit über die eigenen Daten hat und damit der Grundsatz «privacy by design» eingehalten wird.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

- *Vertrauen:* Der Inhaber einer E-ID muss seinen digitalen Ausweis einem anfragenden Dienst unabhängig vom Herausgeber glaubwürdig präsentieren können. Das heisst: Ein Online-Dienst muss sich überzeugen können (ohne den Herausgeber kontaktieren zu müssen - also offline), dass die Identität des Inhabers und dazugehörigen staatlich geprüften Attribute echt sind und zu diesem Inhaber gehören. Dies beinhaltet auch den aktuellen Status der behaupteten Identität → Aktualisierung und Revokation.
- *Privacy:* Eine weitere Anforderung an die E-ID ist der Schutz der Privatsphäre. Eine Zuwiderhandlung wäre in der heutigen Zeit fatal und auch nicht zielführend. Es würde unnötig Gegner einer solchen Infrastruktur auf das Tapet locken. Viele Benutzer werden aber diese Features nicht oder nur sehr wenig nutzen. Dennoch muss man ihnen gebührend Rechnung tragen.

- *Usability:* Eine digitale Transformation in Form einer E-ID muss einfach handhabbar sein. Digitale Behördengänge oder Geschäftsprozesse müssen jederzeit, einfach, sicher und von überall her durchgeführt werden können, um vom Publikum akzeptiert zu werden. Soziale Medien haben es vorgemacht. Eine Willensäusserung hingegen benötigt je nach Prozess mehr Bewusstsein des Inhabers.

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

- Der Nutzen wäre gross, wenn der Staat sich auf die Aufgaben konzentriert, für welche er zuständig ist. Herausgabe von Identitäten und digitalen Nachweisen seiner Bürger. Zudem eine Berechtigung von Diensten in einer Form, welche von Behörden und Privaten genutzt werden kann. Dies muss der Hauptfokus des Staates sein. Der Markt macht dann das Übrige, seinen Bedürfnissen entsprechend, wenn die zur Verfügung gestellten Dienste des Staates nutzbar sind. Dies wird in der physischen Welt schon seit geraumer Zeit erfolgreich gemacht. Warum also nicht dieselben Prozesse beibehalten, nur eben in digitaler Form anbieten.

7. Anforderungen an den Staat

Dies führt zu den Aufgaben des Staates:

- *Authentifizierungsdienst:* Der Staat sollte keinen Authentifizierungsdienst (IdP) anbieten. Ein solcher Dienst macht sowieso nur dann Sinn, wenn der Benutzerkreis der vertrauenden Dienste deckungsgleich mit den E-ID-Benutzern ist. Da die E-ID freiwillig ist (und es somit eine Anzahl von Bürgern ohne E-ID geben wird), käme die Verwendung eines solches Dienstes einem E-ID-Zwang gleich. Zudem ist die Anzahl von vertrauenden Diensten, die ausschliesslich Schweizer Bürgern und Ausländern mit Ausländerausweis vorbehalten sind, sicher begrenzt.
- *Basis-Identität:* Der Staat muss über den Inhaber einer E-ID in Form eines digitalen Ausweises (VC in Variante 1) grundsätzlich eine Aussage machen, für die er zuständig ist. Diese Aussage beinhaltet die Identität des Inhabers und staatlich geprüfte Attribute. Onlinedienste können ihren Prozessen folgend diese Information konsumieren (für das «Onboarding», oder als Login für Dienstleistungen, die sie anbieten).
- *Berechtigung von Diensten:* Aussagen des Staates sollen sich aber nicht nur auf die Inhaberin bzw. Inhaber (Holder) beschränken, sondern auch auf Anbieter von online Diensten (Verifier). Diese sollen vom Staat eine Berechtigung erhalten, dass sie in dieser Funktion auftreten können. Ein Holder soll für jede Nachricht eines Dienstes eine Verifikationskette erstellen können, welche beim Staat endet. Webserverzertifikate dienen nur zur Absicherung der Transportstrecke.
- *Basis-Infrastruktur:* Der Staat soll die Komponenten der Basis-Infrastruktur regulieren, bei Bedarf zertifizieren und idealerweise auch selbst zur Verfügung stellen. Ansonsten laufen wir Gefahr von Inkompatibilitäten. Insbesondere soll der Staat folgende Komponenten regulieren:
    - Persönliche Brieftasche (Wallet, inkl. Agents) → Herausgabe, Nutzung und Überprüfung
    - Verifiable Credentials der *Basis-Identität*.
    - Registry bzw. Ablage von Daten (z.B. private Blockchain oder DB). Im Rahmen der Basis-Infrastruktur muss eine Registry spezifiziert bzw. zur Verfügung gestellt werden, welche einen Link zu persönlichen VCs beinhaltet. Dienstleister jeglicher Art müssen diesem Link folgen können.

    - Revokations- und Überprüfungsverfahren einer Identität.
- *EU-Kompatibilität:* Der Staat muss dafür sorgen, dass die Basis-Infrastruktur der CH (Wallet, VC) auch in der EU nutzbar ist, und umgekehrt, dass auch die EU-Lösung (Ambition Level 3) in der CH akzeptiert wird (Analog zu den heutigen Covid-Zertifikaten).

per E-Mail an: E-ID@bj.admin.ch
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Zürich, 6. Oktober 2021

Stellungnahme zum Diskussionspapier «Zielbild E-ID»: Wir brauchen ein digitales Staatsverständnis

Sehr geehrte Damen und Herren

Gerne nehme ich hiermit Stellung zum Diskussionspapier «Zielbild E-ID», das am 2. September von Ihnen veröffentlicht wurde. Ich erachte es als richtigen und wichtigen Schritt, vor der aufwändigen Erarbeitung eines Gesetzesentwurfs und der Botschaft mit diesem offenen Verfahren eine grundsätzliche Debatte in Gang zu setzen.

Die drei Fragen nach Anwendungsfällen, Anforderungen und Nutzen, die Sie als Richtlinie für Stellungnahmen vorschlagen, erachte ich als berechtigt. Allerdings verzichte ich darauf, auf diese im Detail einzugehen. Ich verweise auf andere Stellungnahmen, insbesondere auf jene meiner Arbeitgeberin Procivis AG vom 4. Oktober 2021.

Mein Beitrag hat zum Ziel aufzuzeigen, welcher fundamentale Wandel mit der Einführung einer staatlichen E-ID einhergeht. Dies aus der Überzeugung, dass jenseits utilitaristischer Abwägungen unser Staatsverständnis unter digitalen Bedingungen neu geklärt werden muss. Erst auf dieser Grundlage wird es gelingen, die E-ID umfassend zu beurteilen – und ebenso umfassend in die digitalen Lebenswelten – private wie staatliche – zu integrieren.

Identitäten – individuelle, kollektive, analoge, digitale – sind schillernde Phänomene, auch wenn sie nur profane Nachweise für einen Namen oder ein Geburtsdatum erbringen sollen. So sehr sich der Mensch nach einer klaren Identität sehnt, so ambivalent sind reale Identitätserfahrungen. Die Ambivalenz ist keineswegs erst der Moderne geschuldet. Bereits die Volkszählung Davids – die biblische Vorläuferin der E-ID – wurde als Frevel erachtet. Mit Lösegeldern an das Heiligtum sollte verhindert werden, dass böse Mächte die auf Listen erfassten Namen mit magischen Flüchen belegen können.

Der Sprung zum gläsernen Bürger von heute ist gross, aber die Spannung, die auch diesem Bild innewohnt, kann mit Verweisen auf Datenschutz und Cyber-Security nicht grundsätzlich entschärft werden. Dies gelingt nur, wenn dem digitalen Bürger ein digitaler Staat gegenübergestellt werden kann, der Identifikationspotential aufweist.

Die Frage, was den digitalen Staat vom analogen unterscheidet, ist aus zwei Gründen schwierig zu beantworten. Erstens, weil unser herkömmliches Staatsverständnis so selbstverständlich ist, dass seine Definition schwerfällt. Zweitens, weil es den analogen Staat schon lange gar nicht mehr gibt. Der scheinbar schleichende Prozess der Digitalisierung hat bereits viele unserer Lebenswelten unverkennbar verändert und erfasst nun auch den Staat. Die Proliferation von Sensoren und Systemen, deren Vernetzung, die daraus ergebenden Datenmengen und die wiederum darauf basierenden Analysen und Dienstleistungen befördern einen sprunghaften Verlauf der weiteren Entwicklung.

Aus diesem Grund greifen für mich die Fragen nach Anwendungsfällen und Nutzen, die von der analogen Welt inspiriert sind, zu kurz. Die neuen technologischen Möglichkeiten verändern den öffentlichen Raum, und zwar zweifach: Erstens verliert die analoge Version an relativer Bedeutung; zweitens weist die digitale Variante neue Eigenschaften auf wie nahezu totale Transparenz, Simultanität etc. Damit rütteln wir an den Grundfesten des Staats als formale Organisation, welche die Voraussetzungen und Bedingungen unseres Zusammenlebens im öffentlichen Raum herstellt. Mit anderen Worten: Wir müssen klären, welche Art von öffentlichem Raum erforderlich ist, um Prinzipien wie Demokratie, Rechtsstaat und Föderalismus unter digitalen Bedingungen weiterentwickeln zu können. Konkreter: Welche öffentlichen Güter – analoge und digitale, Güter, Dienstleistungen und Infrastrukturen – muss der Staat bereitstellen, um ein freies und zugleich solidarisches Zusammenleben zu ermöglichen? Von diesen Antworten ist abzuleiten, wie in Zukunft politische Entscheidungen zustande kommen sollen, wie die öffentliche Verwaltung zu konzipieren ist und richterliche Sanktionen ausgesprochen werden können. Die Übersetzung dieser Antworten in konkrete Massnahmen ist ohne Verfassungsänderung nicht zu haben. Ob eine Teilrevision ausreicht, wie sie im Zusammenhang der Digitalen Verwaltung Schweiz in Erwägung gezogen wird, ist offen. Ich gehe davon aus, dass eine Totalrevision, einschliesslich Gebietsreformen auf kantonaler und kommunaler Ebene unumgänglich sind. Erst vor diesem Hintergrund kann eine E-ID auf politische Akzeptanz hoffen und Eingang in den Alltag von Bevölkerung, Verwaltung und Wirtschaft finden.

Dabei kommt erschwerend hinzu, dass nicht nur geklärt werden muss, wie die Technologie genutzt werden soll. Bei allem technologischen Fortschritt, der bereits erzielt worden ist, stehen wir erst am Anfang. Das «Internet» von heute erinnert an Röntgengeräte, die während langer Zeit in jedem besseren Schuhgeschäft zur Überprüfung der Passform von Schuhen im Einsatz waren.

Es liegt auf der Hand: Will die Schweiz ihren Wohlstand erhalten und ihrem ideengeschichtlichen und technologischen Selbstansprüchen gerecht werden, liegt noch viel Arbeit vor uns. Den bereits heute digitalen Bürgerinnen und Bürgern muss ein digitaler Staat mit Identifikationspotential gegenübergestellt werden. Eine Self Sovereign Identity mit Anspruchsniveau 3 wäre ein erster Schritt in diese Richtung.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf die weitere Debatte.

Mit besten Grüssen

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

Per Mail an E-ID@bj.admin.ch

Campus Zug-Rotkreuz
Suurstoffi 1, CH-6343 Rotkreuz
T +41 41 757 68 11
www.hslu.ch

Prof. Dr. René Hüsler
Prof. Ursula Sury
Prof. Dr. Tim Weingärtner

Rotkreuz, 29. September 2021

Öffentliche Konsultation zum «Zielbild E-ID»

Sehr geehrte Damen und Herren

Herzlichen Dank für Ihre Einladung zur Mitwirkung am Zielbild E-ID.

Die Hochschule Luzern – Informatik ist mit über 1'000 Studierenden, 6 Bachelor- und 4 Master-programmen sowie mit über 60 Weiterbildungsangeboten im digitalen Bereich die zentrale Adresse für Digitalisierung in der Zentralschweiz. Mit unserer Beteiligung in namhaften Vereinigungen, u.a. auch bei DIDAS, liegt uns die Mitgestaltung der digitalen Zukunft der Schweiz am Herzen.

Wir beziehen betreffend der drei Fragen aus Ihrem Konsultationspapier wie folgt Stellung:

1. *Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?*
    a. **Vertrauen**. Die E-ID muss durch die technologischen Grundlagen (Privacy by Design), Basisinfrastruktur und die administrativen Prozesse so ausgestaltet sein, dass die Bürger*innen uneingeschränktes Vertrauen in die Identität und deren Verwendung haben.
    b. **Interoperabilität**. Die E-ID muss sowohl national als auch international mit dortigen Systemen interoperabel / kompatibel sein. Dies schliesst auch eine möglichst hohe Offenheit und Technologieneutralität ein.
    c. **Benutzerfreundlichkeit**. Die E-ID muss in Bezug auf Ausstellung, Handhabung und Sicherheit maximal benutzerfreundlich sein. Dabei dürfen keine Personengruppen ausgeschlossen werden.
2. *Welche Anwendungsfälle der E-ID stehen im Vordergrund?*
   Die E-ID ist die Basis für sehr viele Geschäftsfälle, vor allem in der digitalen Kommunikation. Dabei ist wichtig, dass die E-ID meist mit anderen Identitäten in Kombination funktionieren muss.
3. *Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können?*
   Eine E-ID auf Basis einer nationalen Infrastruktur bietet den Bürger*innen die Grundlage am digitalen Leben teilzunehmen, ohne auf internationale oder kommerzielle Infrastrukturen angewiesen zu sein. Dies sichert Datenschutz, Neutralität und gibt Rechtssicherheit.

Wir empfehlen die E-ID-Lösung mittels Self-Sovereign Identity und die Konzeption auf Ambitions-Niveau 3: Ökosystem digitaler Nachweise.

Self-Sovereign Identity entspricht von ihrer Handhabung und Flexibilität dem physischen Portemonnaie. Die Bürger*innen sind im Besitz ihrer Identität und ihrer Daten. Sie entscheiden, wem sie Informationen zeigen. Darüber hinaus besitzt die Technologie Vorteile, wie die selektive

Veröffentlichung von einzelnen Daten, die Nutzung des Zero-Knowledge Proofs zur informationsfreien Bestätigung sowie die einfache Weitergabe von Zertifikaten und Bestätigungen z.B. mittels QR-Codes. Gegenüber der PKI (Public-Key-Infrastruktur) Lösung besitzt die Self-Sovereign Identity, neben den bereits oben aufgeführten, weitere entscheidende Vorteile: Die Kombination mit anderen Identitäts-informationen, die Interoperabilität mit den Initiativen auf EU-Ebene oder die einfache Revokation.

Aus Sicht der Hochschule Luzern ist der Entscheid für Self-Sovereign Identity und das gezielte Umsetzen erster Schritte hin zum Ambitions-Niveau 3 essenziell. Wir sehen die Wichtigkeit einer E-ID in vielen unserer Projekte, die eine Identität der Benutzer*innen voraussetzen. Dabei ist zentral, dass die staatliche Identität Teil eines Ökosystems mit vielen anderen Identitäten, Zertifikaten, Rollen, Berechtigungen und Informationen ist. Die internationale Forschungsgemeinschaft arbeitet an Lösungen und wir haben jetzt die Chance an der Weltspitze mitzuwirken. Gleichzeitig sehen wir es als unseren Auftrag als Hochschule in der Aus- und Weiterbildung «die digitale Zukunft mitzugestalten». Die Digitalisierung birgt die Gefahr, dass Personenkreise ausgeschlossen werden. Die Geschichte hat uns gezeigt, dass dies nicht durch die Verzögerung des Einsatzes von modernen Technologien verhindert werden kann. Vielmehr sind Bund, Bildung und Wissenschaft gefordert, diese Lücke zu schliessen und die Bürger*innen der Schweiz zu befähigen, verantwortungsbewusst mir ihren Daten und den modernen Technologien umzugehen. Gerne leisten wir unseren Beitrag in diesem Bereich.

Bezüglich Abbildung 3 (S. 21) des Diskussionspapiers möchten wir zu bedenken geben, dass der Bund nicht alle der dort aufgeführten Komponenten entwickeln oder zur Verfügung stellen muss. Ein Grundsatzentscheid und damit eine Rechtssicherheit wird automatisch Investitionen und Weiterentwicklungen der Wirtschaft auslösen. Zum Beispiel ist die Entwicklung geeigneter und benutzerfreundlicher Wallets aktuell im Gange und muss nicht durch den Bund beauftragt werden. Hier ist ein auditierende und zertifizierende Rolle des Bundes zu empfehlen. Gerne nehmen wir im Laufe der öffentlichen Diskussion, der Vernehmlassung und der weiteren Ausgestaltung der Schweizer E-ID zu den aufgeführten Fragestellungen und Kritikpunkten zur Self-Sovereign Identity Stellung und unterstützen bei der Konzeption einer modernen, zukunftsweisenden und sicheren Identitätslösung.

Freundliche Grüsse

Prof. Dr. René Hüsler
Direktor Departement Informatik

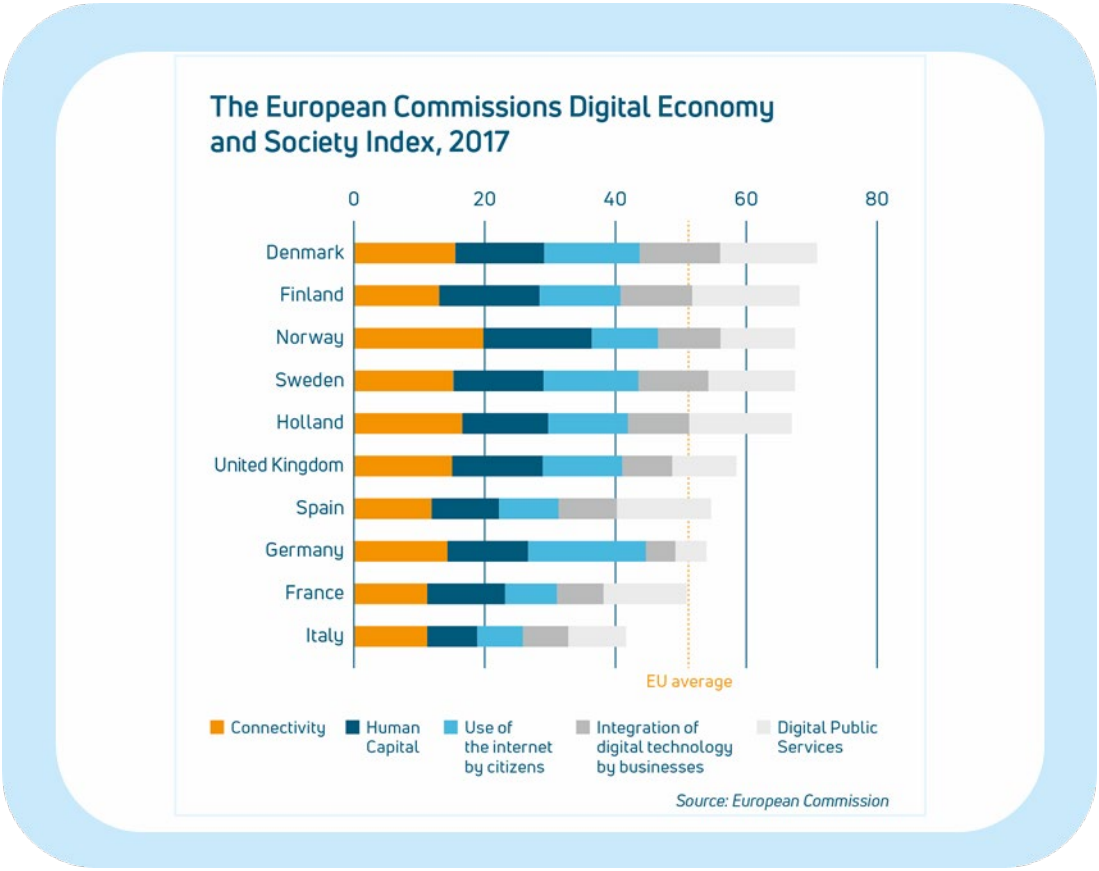
Prof. Ursula Sury
Vizedirektorin Weiterbildung

Prof. Dr. Tim Weingärtner
Dozent Blockchain

29 September 2021

Response to the Discussion paper on the target vision for an e-ID I Switzerland

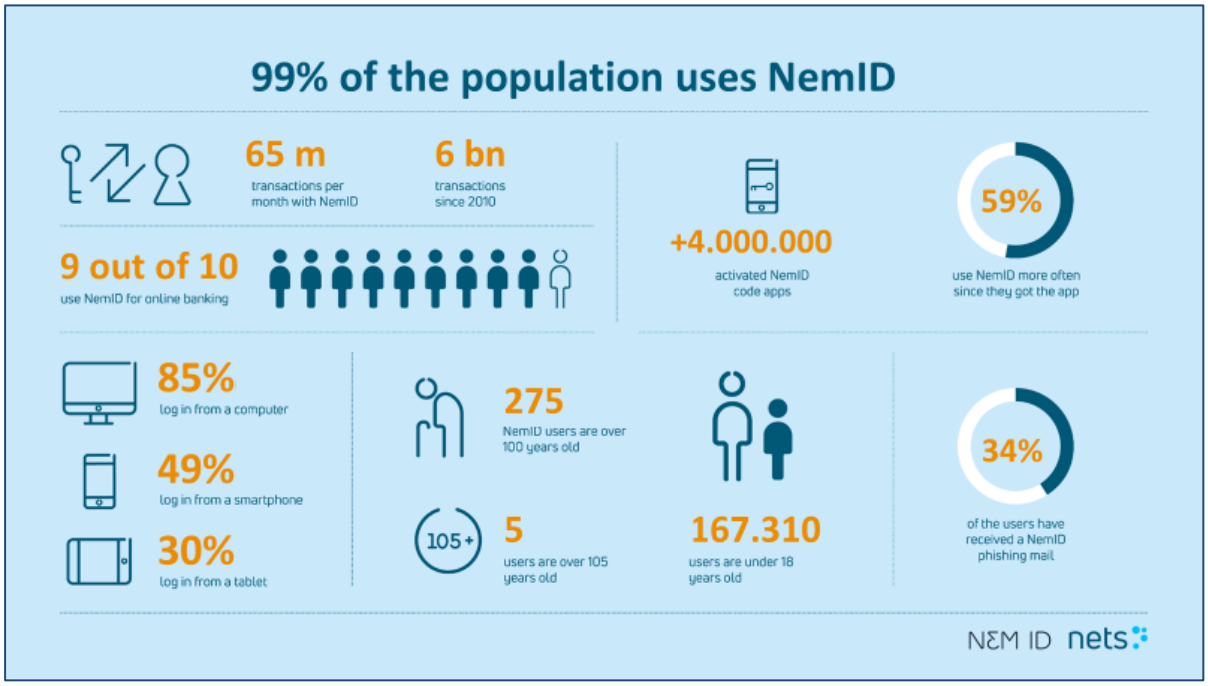
As mentioned in the description of Nets competences Nets has been the leading provider of eID solutions in the Nordic countries Norway and Denmark for the last 20 years. The Nordic countries are in front when it comes to digitalization and widespread usage of eID solutions. With this background we have obtained a substantial knowledge in development, maintenance, and operation of national eID solution in large scale by processing more than 700 m. transactions pr year (140 transaction/user/year) in NemID in Denmark.



The Nordic country is in front when it comes to digitalization in the society

As mentioned in the discussion paper the chicken-egg issue is fundamental to get a success in the eID area. A well-functioning eID is crucial to get success in the digitalization of the governmental sector. However, it is not enough, the Governmental sector needs also to develop modern portals that allows citizen to contact and interact in every aspect of their daily life, when applying for services in the governmental sector. That would include health care, pension, national e-box, building permits, education, family matters etc. The use cases are there plenty of if they are developed. So, what is the fundamental problem? The problem is that the ordinary citizen in the beginning of this digitalize journey does not have a regular interaction with the governmental sector. Before introducing NemID to the Danish society the estimate was, that the average citizen did only have 1,2 interaction with the governmental sector during a year. For a population of the size of Denmark with 5,6 m. people that will never justify an expense to advanced eID solutions. The governmental

sector could neither reduce cost to manual processing of inquiries from citizen, because the digitalization is to low. After 10 year of operation with NemID the number of interactions with the government with NemID for an average citizen is 36 transactions pr. Year.



The success story of NemID in Denmark

Building a full digitalized governmental sector takes many years and is costly, so the strategy that have been proven by the Nordic countries is to establish a well-functioning eID solution that's user-friendly meaning based on app's and smart phones but also support people with physical or cognitive disabilities. Nets has now built the third generation of this kind of eID called MitID, that is state of the art build on microservices, modular design principles and API's that allows new customer to get their own look and feel. It is fully compliant with eIDAS and GDPR.

Nets has been involved in the eID area for the last two decades and have been involved supporting the government to overcome the different obstacles that hinder the development of a well-functioning eID in Denmark.

involvement of the private sector especial the banks from the outset will strength the development. Getting critical mass of users up and running that uses the system regularly in the private sector allows the governmental sector to develop and build digital services along this path.

In our opinion, suggesting implementation of an eID solution based on self-sovereign identity ref. chapter 5.1 could be a very expensive experiment. The technology has not been proven in any large scale production environment and there are plenty of unanswered question not only technical but also legal and business wise, e.g. how will the business model look like when the ordinary payer in the eID infrastructure normally is the relying party, but now the relaying party is also a provider of proof. Trying to build a critical mass of users on the foundation of very new and unproven technology will come with a substantial risk. As mentioned previously, there are lot of use cases already present there could be developed in the governmental sector.

As a last statement is, that both NemID and also the successor MitID is fully GDPR compliant. Only very limited information of the citizen is collected, and the citizen is in full control whenever the social security number collected and distributed.

Nets

Nets Issuer & eSecurity Services provides processing services for more than 250 issuers of payment cards and banks in Europe, as well as complementary services such as Consumer Management Services and Fraud & Dispute Services.

Our vision in Issuer & eSecurity Services is to make our customers more successful by delivering card payments, consumer management and e-security easier, smarter and faster with innovative solutions. Issuer & eSecurity Services also delivers strengthened fraud prevention services to a number of its financial services customers.

Merchant Services

We provide our merchant customers with payment acceptance solutions across channels (in-store, online and mobile) and with a broad range of payment methods in Europe.
Our offerings for merchants are brought to market by our merchant services in the Nordic region and in mainland Europe respectively.

Together, we offer best-in-class payment solutions tailored to meet our customers' needs.
Our complementary product portfolios empower merchants to benefit from the digitisation of payments with, for example, state-of-the-art e-commerce gateways, merchant portals and invoicing solutions for e-commerce merchants.

OPEN BANKING PROJECT.CH

coordinated by BEI Business Engineering Institute St. Gallen

Stellungnahme des OpenBankingProject.ch zum «Zielbild E-ID»: Ambitionsniveau 3 für einen kundenzentrierten, branchenübergreifenden Servicebezug

Das OpenBankingProject.ch (OBP) gestaltet zusammen mit seinen Partnern, Membern und der Community Bausteine für Open Banking in der Schweiz und begrüsst das «Zielbild E-ID» des Bundes. OBP ist überzeugt, dass bei der Ausgestaltung einer staatlichen E-ID folgende Punkte essenziell sind:

- Die **Bedürfnisse des Kunden** resp. E-ID-User, seine Customer Journey sowie der selbstbestimmte Umgang mit seinen Daten sollen im Zentrum stehen.
- Ein medienbruchfreier und **effizienter Servicebezug** sowohl unternehmens- als auch branchenübergreifend bringt für alle Marktteilnehmenden enorme Mehrwerte (z. B. Bank B kann von Person Y sämtliche Daten im Zusammenhang mit einer Bankkontoeröffnung abrufen, welche bereits durch Dritte gesammelt und verifiziert wurden). Das Ambitionsniveau 3 schafft die entsprechenden Grundlagen und fördert die Entwicklung von unternehmensübergreifenden Kollaborationen in Ecosystemen.
- Der **Schutz der Privatsphäre** des Kunden resp. E-ID-User hat höchste Priorität. Daher sollen Unternehmen nur jene Informationen beziehen, welche für die Leistungserbringung notwendig sind (z. B. Apotheke kann nur spezifisches Rezept für Medikament X abrufen).
- Bei der Entwicklung der E-ID soll auf die **internationale Interoperabilität** geachtet werden und auf vorhanden technischen wie auch fachlichen Standards aufgebaut werden.
- Die Entwicklung der E-ID sowie die in diesem Zusammenhang entstehende Bausteine sollen den **«Open Source»**-Ansatz folgen und öffentlich publiziert werden.
- Die Arbeitsergebnisse sollen unter **Einbezug aller relevanter Parteien** transparent und ausgewogen erarbeitet werden.

Für die Partner des OpenBankingProject.ch:

St. Gallen, 30.09.2021

Thomas Zerndt
Business Engineering Institute St. Gallen
CEO

Über OpenBankingProject.ch (www.obp.ch)

OpenBankingProject.ch ist im Februar 2019 als organisationsübergreifendes Konsortium zur Förderung der Open-Banking-Entwicklung in der Schweiz gegründet worden. OBP steht dabei für eine Öffnung der Bank im Sinne des Kunden und umfasst heute 9 Partner und 15 Member. Die Initiative fokussiert im Rahmen von Open Banking auf die Nutzbarmachung von Standards (z. B. API, Tokens), die Sichtbarmachung der relevanten Akteure, die Aufbereitung von Wissen sowie die Vernetzung von Unternehmen.

Was ist Open Banking?

Nach dem Open-Banking-Konzept können Endkunden ihre persönlichen Finanzdaten über offene Schnittstellen verschiedenen Banken bzw. Finanzdienstleistern oder FinTech-Unternehmen zugänglich machen. Grundlagen von Open Banking bilden technische Schnittstellen (API, SOA) sowie regulatorische Vorgaben (PSD2). Open Banking erleichtert die Bildung digitaler Ökosysteme und reduziert die Eintrittsbarrieren für Startup- und Nichtbank-Unternehmen.

avaloq DXC TECHNOLOGY ergon finnova FINSTAR inventx netcetera UNIVERSITÄT BERN

swimag GmbH
Mattenstrasse 14
CH-5436 Würenlos

swimag GmbH · Mattenstrasse 14 · CH-5436 Würenlos

Würenlos, 30.09.2021

Einschreiben

Herr
Urs Paul Holenstein

Bundesamt für Justiz
Bundesrain 20
CH-3003 Bern

Vorab per Mail: E-ID@bj.admin.ch,rechtsinformatik@bj.admin.ch

Stellungnahme zur E-ID insbesondere bzgl.:

- **Zielbild und**
- **Diskussionspapier.**

Sehr geehrter Herr Holenstein
Sehr geehrte Damen und Herren

Vielen Dank für die Gelegenheit und Einladung zur Stellungnahme in vorgefassten Angelegenheiten.

Dürfen wir Sie von daher höflich als Zugehörige fachlich interessierter Kreise um Kenntnisnahme und geneigte Berücksichtigung der folgenden Ausführungen und gesondert herausgestellten Änderungsvorschläge speziell unter Rückbezug des Diskussionspapiers zum «Zielbild E-ID» und dessen Gliederung bzw. Bezifferung ersuchen:

0 Zusammenfassung

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 bei der Ausgestaltung der Gesetzesvorlagen für die E-ID wesentliches

Schwergewicht auf genau diese Punkte zu richten, da ansonsten nicht ganz zu Unrecht ein wiederholtes Nein zur E-ID zu befürchten steht mit all den dann nicht unerheblichen persönlichen, rechtlichen, gesellschaftlichen und wirtschaftlichen Nachteilen auch gegenüber der Umwelt und der internationalen Staatengemeinschaft.

2.3 Klären der E-ID Vision

Wie schon einleitend im vorausgegangenen Abschnitt angedeutet, gilt es das Einsatzfeld der E-ID nicht unnötig einzuschränken, sondern auf alle denkbaren Bereiche zu erstrecken, wo es um den Aus- wie Nachweis der Identität von natürlichen Personen und um Wahrung derer Rechte geht, was sich im Übrigen bereits heute mit der Vergabe und der Anwendbarkeit bzw. Akzeptanz von qualifiziert zertifizierten elektronischen Signaturen selbst vor den höchsten Bundesbehörden in der Praxis im gewissen Rahmen bestens vollziehen lässt, aber sich bedauerlicherweise in der Breite nicht durchzusetzen vermochte u.a. wegen der teilweise schwierigen bis unmöglichen Portierung auf bestimmte Betriebssysteme sowie erlebter rechtswidriger Zurückweisung des Identitätssignets durch private und öffentliche Institutionen, die es dann mittels aufsichtsführender Stellen ins Recht zu weisen galt.

Von daher laufen alle Interessen des Einzelnen wie auch der Gesellschaft darauf hinaus, die E-ID bei allen Stellen des öffentlichen und privatwirtschaftlichen Lebens als Zugang und Identitätsnachweis, sei es digital oder physisch, zur Eröffnung der jeweils für die betreffende Person zugriffsberechtigten Vorgänge als auch zur Erlangung und Wahrung derer Rechte und Sicherheiten einzusetzen, ohne unnötige, ungerechtfertigte oder rechtswidrige Einschränkungen, Hindernisse, Weigerungen einschliesslich zusätzliche wie willkürliche Auflagen erleben bzw. befürchten zu müssen.

Eine ganz entscheidende Bedeutung kommt dabei dem Datenschutz und der Transparenz über die Datenflüsse zu. Sämtliche mit der E-ID verbundenen Vorgänge und Prozesse bedürfen der Protokollierung und der direkten Abrufbarkeit durch den betreffenden E-ID-Inhaber einschliesslich der Anrufmöglichkeit höherer Stellen im Falle des Verdachtes von Datenschutzverletzungen ganz im Sinne der rechtsstaatlich zu realisierenden Garantien zur Durchsetzung der informationellen Selbstbestimmung u.a. nach den EMRK und der DSGVO auf europäischer sowie der Bundesverfassung, dem Verwaltungsrecht und den Datenschutzgesetzen auf nationaler Ebene.

Dazu gehört ganz konkret, sich als Inhaber einer E-ID jederzeit Kenntnis in einer präzis abgefassten lückenlosen Aufstellung der kontinuierlich bzw. chronologisch durchzunummerierenden Prozessvorgänge wie Datensammlungen verschaffen zu können, welche Person oder Personen zu welchem Zeitpunkt [Datum] nach welcher gesetzlichen Vorgabe bzw. rechtlichen Bestimmung zu welchem Zweck unter welchen Massgaben, Folgerungen und Feststellungen den jeweiligen Datenverarbeitungsprozessschritt vornahm etwa nach dem Schema:

Prozess-schritt	bearbeitet v. Frau/Herrn	am Datum/Zeit	zwecks bzw. nach Recht	Folgerungen und Bemerkungen

Nur so lässt sich überhaupt von einer "digitalen Vertrauensinfrastruktur" sprechen, die zwingend wie dringend einer diesbezüglichen gesetzlichen Regelung bzw. Anpassung gerade im Hinblick auf den Einsatz der E-ID bedarf, zumal der Begriff selber, also

die "digitale Vertrauensinfrastruktur", gegenwärtig keiner gesetzlichen oder sonstigen rechtlichen Regelung wie Relevanz und insoweit auch nicht dem Legalitätsprinzip unterliegt, also damit keinerlei Rechtsfolge, -wirkung und -bindung entfaltet.

2.4 Ansprüche an die Digitalisierung

Entgegen der unter diesem Titel im Diskussionspapiers zum «Zielbild E-ID» gefassten Ausführungen und dargestellten Schwierigkeiten in Zusammenhang mit den unterschiedlichen Erwartungen an eine E-ID darf an dieser Stelle der Hinweis nicht fehlen, dass sich schon heute mit vergleichsweise einfachen Mitteln und deren Möglichkeiten eine Vielzahl bestehender und selbst für die Zukunft absehbarer Ansprüche absolut zufriedenstellend decken lassen, speziell auf der Basis äusserst bewährter, effizienter, leistungsstarker und dazu noch höchst sicherer ständig aktualisierter Open-Source-Lösungen.

3.1 Technische Entwicklungen im Bereich digitaler Identitäten

Gestützt auf eigene Erfahrungen in Zusammenhang mit der digitale Identität hat sich in der Tat der Umgang mit der Public-Key-Kryptografie und darauf abgestimmten Systemen bewährt sowohl hinsichtlich Zuverlässigkeit, Flexibilität und Anpassungsfähigkeit bzw. Integration in bestehende Entwicklungs- und Verarbeitungsumgebungen. Hingegen zukünftig dem gegenwärtigen Trend allein in Richtung Smartphone zu folgen, verbietet sich allein schon wegen der dann kaum bis gar nicht umsetzbaren Barrierefreiheit und dieses ganz besonders in der Schweiz aufgrund der geltenden Gesetze und Verordnungen zur Beseitigung von Benachteiligungen. Menschen fortgeschrittenen Alters und/oder solche mit Einschränkungen, beispielsweise im Sehvermögen, Leseschwäche oder im manuellen Umgang mit Touchscreen, erfahren dann mit einer allein oder weitgehend an das Smartphone geknüpften E-ID eine unzulässige Ausgrenzung bzw. Diskriminierung. Von daher gilt es unbedingt sämtliche Möglichkeiten der E-ID als vollumfänglich einrichtbar vorzusehen auf freien u.a. die Barrierefreiheit unterstützenden bzw. linuxbasierten Betriebssystemen, die sich noch dazu auf sämtlichen Hardwareplattformen, ungeachtet weniger eher exotisch anmutender Ausnahmen, installieren lassen, was insofern kein Problem darzustellen vermag, da Android als sicherlich marktanteilmässig häufigst verwendete Applikation bzw. Software-Plattform auch über einen Linux-Kernel verfügt.

3.2 Entwicklung im EU-Recht bzgl. der digitalen Identitäten

Es versteht sich eigentlich selbstredend, dass das Ausgestalten der E-ID sogleich mit dem Erfüllen sämtlicher diesbezüglicher EU-Normen einhergeht und damit die E-ID im europäischen Rechtsraum ohne Einschränkung und in voller Gänze zur Anwendung gelangen darf und kann.

4 E-ID-Ökosystem

Die E-ID möge sich nicht über Ambitions-Niveaus definieren, sondern sich generell, wie anfänglich kurz erläutert, zur Aufgabe machen, in allen Bereichen, wo es um den Auswie Nachweis der Identität von natürlichen Personen und um Wahrung derer Rechte geht, verlässliche Wirksamkeit zu entfalten. Dieses gilt natürlich auch für die mit und nach der Identifizierung ablaufenden Vorgänge und Prozesse. Durch Vorlage der E-ID-Identifizierung bzw. eines entsprechenden Logins und der Deklaration des konkreten Anliegen, sei es ein bestimmtes Gesuch, eine Eingabe oder ein Geschäft, findet der entsprechende Informations- oder Materialaustauch im vereinbarten und/oder gesetzlich geregelten Rahmen statt. Für den Anbieter einer Leistung bedeutet das, auf Verlangen jederzeit Auskunft gegenüber dem E-ID-Inhaber zu geben über den jeweiligen das eigentliche Anliegen betreffenden Verfahrensstand und den zwischenzeitlich erhobenen Daten.

Unter dieser Prämisse erscheinen die bislang im Diskussionspapier «Zielbild E-ID» vorgebrachten Anwendungsfälle eher minimalistisch und wenig gegenüber bisherigen bzw. konventionellem Vorgehen animierend insbesondere gemessen an den vielfältigen und ausgezeichneten Möglichkeiten, die die E-ID schon heute realisierbar mit einfachen und überaus ansprechenden technischen Mitteln bieten könnte. Zudem darf die E-ID unter allen zu diskutierenden Punkten eine zusätzliche Weitung der qualifiziert zertifizierten elektronischen Signatur sowohl national als auch europaweit mit sich bringen.

5 *Verschiedene E-ID-Lösungsansätze*

Grundlegende Entscheide über die Auswahl geeigneter E-ID-Lösungsansätze verlangen für gewöhnlich ein vertieftes technisches Verständnis gepaart mit entsprechendem Praxiswissen. Ggf. gibt es aber noch weitere im Diskussionspapier «Zielbild E-ID» nicht berücksichtigte bzw. ausgelassene Alternativen oder es lassen sich die vorgestellten Varianten in günstigerer Art und Weise kombinieren.

Im Endeffekt kommt es darauf an, dass sämtliche potentiellen Nutzer wie Anwenderkreise den vollumfänglichen und technisch gut beherrschbaren wie barrierefreien Zugang zur E-ID unter einem Maximum an bereits geforderter umzusetzender Transparenz wie Sicherheit erhalten. In dieses Umfeld gehören selbstverständlich die unbedingt zu berücksichtigenden Menschen fortgeschrittenen Alters und/oder solche mit Einschränkungen, beispielsweise im Sehvermögen, Leseschwäche oder im manuellen Umgang mit Touchscreens. Im Übrigen hilft gerade das Einbeziehen dieser Gruppe und die zur Realisierung der Barrierefreiheit verbundenen besonderen Herausforderungen den Entwicklern beim Implementieren besonders nutzerfreundlicher Systeme und Schnittstellen bzw. User-Interfaces als auch beim gänzlichen Eliminieren von Systemfehlern, was zudem erfahrungsgemäss regelmässig und nachhaltig erheblich zur finanziellen Kostenneutralität von Gesamtlösungen beizutragen weiss.

Zürich, 30th September 2021

Comments to the target vision of an E-ID by the Expert Group 'Blockchain Technology in Interorganisational Collaboration' of Data Innovation Alliance

Where do you see the particular benefit of an e-ID, and which use cases are most important to you?

To be able to create added value with the possibilities of digitalization, we need ecosystems, in which seamless and secure processes can be implemented. That requires digital proofs (verifiable credentials) to be issued, exchanged and verified securely and tamperproof across organizational and national borders.

Proof of identity of persons, organizations and, increasingly, of things (IoT) are only the basis.

On top of that qualifications and authorizations of all kinds (e.g. education and health certificates, certificates of origin, employee and membership cards) issued, exchanged and verified digitally will enable seamless processes beyond company or country borders.

In such an ecosystem, the E-ID is only one digital proof among many. However, the level of ambition determines the exploitation potential of the digital transformation and thus quite directly the performance and competitiveness of Switzerland in an increasingly digital world.

Keeping Switzerland internationally competitive and promoting (digital) innovation can therefore only be achieved with ambition level 3. It would also be perfectly in line with the European ambitions of the EUiD.

In your view, what are the three most important requirements for a governmental e-ID as a digital identity card?

1 The state E-ID is issued exclusively by a state agency. In perspective this might be done in the same process in which a citizen receives a passport/ID or a foreigner receives a residence permit.

2. The E-ID can easily be used abroad (at least in the EU) in digital and analogue processes.

3. The E-ID is issued and used in an evolving ecosystem as one of many digitally verifiable credentials. Other such proofs can be health (e.g. vaccination certificate) or education certificates, identity and membership cards, driving and vehicle licenses or many other confirmations in digitally verifiable form.

What benefits do you see in a national infrastructure that enables the state and private parties to issue and verify digital proofs (e.g. e-ID, digital driving license, employee identity cards, training certificates)?

An infrastructure (a trust network) that enables private individuals and companies as well as government to issue and verify digital proofs is the essential basis for exploiting the potential of Switzerland's digitalization in the first place and at the same time meeting today's data protection requirements.

This infrastructure makes it possible for digital evidence to be used securely across organizations and borders. Therefore, such an infrastructure cannot be designed as isolated national solution but must at least be thought of in an European perspective and follow global standards. Thereby ensuring high interoperability between different possible implementations.

Blockchain-based networks can be of help in establishing such a trust network. Without digitally verifiable credentials however no blockchain applications can realistically be scaled to productive levels. This is a key requirement for Switzerland to defend its leading-edge position as a “Crypto Nation” in this highly competitive and innovative environment.

In the name of the Expert Group ‘Blockchain Technology in Interorganisational Collaboration’

Michael Lustenberger, Research Associate ZHAW

Co-Leader of the Expert Group