Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Berne, le 20 juin 2025

Projet d'ordonnance sur l'e-ID

Rapport explicatif relatif à l'ouverture de la procédure de consultation

Condensé

L'ordonnance relative à la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (ordonnance sur l'e-ID, OeID) précise notamment les procédures et les compétences pour l'émission et l'utilisation de l'e-ID. En outre, elle définit l'infrastructure de confiance qui peut être utilisée aussi bien par les autorités que par les acteurs privés pour émettre et vérifier les preuves électroniques en toute sécurité. Le but de l'ordonnance est de créer une base claire et sûre pour l'utilisation de l'e-ID et d'autres preuves électroniques.

Contexte

Après le rejet de la loi fédérale sur les services d'identification électronique lors de la votation populaire du 7 mars 2021, le Conseil fédéral a chargé le Département fédéral de justice et police d'élaborer une preuve d'identité électronique sûre, en collaboration avec la Chancellerie fédérale et le Département fédéral des finances. Le 13 juin 2022, le Conseil national et le Conseil des États ont approuvé six motions demandant la mise en place d'une preuve d'identité électronique étatique. Le 22 novembre 2023, le Conseil fédéral a adopté le projet de loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (loi sur l'e-ID, LeID). L'objectif est d'introduire une e-ID gratuite et facultative permettant aux titulaires de prouver numériquement leur identité de manière simple et sûre. L'e-ID est émise par la Confédération et garantit une protection maximale des données personnelles notamment grâce à la limitation des données. Conformément au principe de l'autodétermination numérique, la demande d'émission et l'utilisation de l'e-ID sont facultatives. Les titulaires de l'e-ID peuvent en outre contrôler leurs données. En plus de l'e-ID, il est prévu de travailler avec d'autres preuves électroniques. La Confédération met à disposition l'infrastructure de confiance nécessaire, y compris un portefeuille électronique, une application de vérification des preuves ainsi qu'un registre de base et un registre de confiance. Cette infrastructure peut également être utilisée par des personnes privées qui souhaitent émettre et vérifier des preuves électroniques. Lors du vote final du 20 décembre 2024, la LeID a été adoptée par le Parlement à une nette majorité (Conseil national : 170 voix pour l'adoption du projet, 25 voix contre [1 abstention] ; Conseil des États : 43 voix pour l'adoption du projet, 1 voix contre [0 abstention]). Le référendum a formellement abouti le 7 mai. La LeID sera soumise à la votation populaire le 28 septembre 2025.

Si le peuple ne rejette pas la LeID, celle-ci pourra entrer en vigueur au milieu de l'année 2026 au plus tôt. D'ici là, les dispositions d'exécution de-

vront également avoir été adoptées par le Conseil fédéral. Cela n'est toutefois possible que si l'ouverture de la consultation n'est pas reportée après la votation.

Contenu du projet

La LeID doit permettre aux personnes domiciliées en Suisse et aux Suisses de l'étranger de disposer d'une preuve d'identité électronique afin de s'identifier numériquement de manière sûre, rapide et simple. Le projet d'ordonnance concrétise la mise en œuvre de la LeID et règle notamment l'infrastructure de confiance, l'e-ID et les aspects techniques et organisationnels des preuves électroniques qui y sont liées. L'infrastructure de confiance est destinée à toutes les preuves électroniques et comprend le registre de base dans lequel les identifiants sont inscrits, le registre de confiance pour la confirmation de ces identifiants, ainsi que les applications pour la conservation et la vérification des preuves électroniques. Le projet d'ordonnance règle l'enregistrement, l'utilisation et l'effacement d'informations relatives aux preuves électroniques par les personnes physiques et morales.

L'e-ID est demandée en ligne et émise par l'Office fédéral de la police (fedpol), qui en est responsable. La vérification de l'identité peut avoir lieu soit en ligne, soit sur place auprès d'un centre de saisie cantonal ou – pour les Suisses de l'étranger – auprès de la représentation consulaire de la Suisse compétente. La procédure de vérification de l'identité en ligne commence avec la prise d'une photo du document d'identité et d'un enregistrement vidéo du visage. Ces éléments sont vérifiés de manière automatisée. L'image faciale provenant des extraits vidéos est comparée avec la photographie enregistrée dans les systèmes d'information au sens de l'art. 17, al. 2, LeID (par exemple, le système d'information relatif aux documents d'identité). Lorsque le résultat est conforme, le requérant reçoit l'e-ID directement sur son appareil. Dans les cantons et dans les représentations consulaires qui effectuent une vérification de l'identité sur place, la procédure peut varier.

Des caractéristiques techniques importantes, telles que le format et les normes des preuves électroniques, sont publiées en tant que recommandations, mais peuvent être partiellement déclarées obligatoires.

Table des matières

Rapport explicatif

1. Principales caractéristiques du projet

Avec la LeID, les personnes domiciliées en Suisse et les Suisses de l'étranger doivent pouvoir disposer rapidement d'une preuve d'identité sous forme numérique et d'autres preuves électroniques de haute qualité et pouvoir les utiliser en toute sécurité. Le présent projet d'ordonnance concrétise la mise en œuvre de la LeID. Il règle notamment l'infrastructure de confiance et l'e-ID, ainsi que les aspects techniques et organisationnels relatifs à l'utilisation des preuves électroniques en général.

1.1 Infrastructure de confiance

Selon la LeID, les éléments de l'infrastructure de confiance ne sont pas uniquement destinés à l'e-ID, mais fondamentalement à toute preuve électronique compatible avec le système. L'infrastructure de confiance se décline en plusieurs éléments :

- un registre de base, dans lequel les émetteurs de preuves électroniques peuvent inscrire les informations requises, telles que leurs identifiants ;

- un registre de confiance, qui sert de système de confirmation des identifiants du registre de base ;

- une application pour la conservation et la présentation des preuves électroniques, ainsi qu'un système de copies de sécurité ; et

- une application pour la vérification des preuves électroniques.

Le projet d'ordonnance détaille de manière générale l'inscription et l'utilisation de l'infrastructure de confiance, ainsi que la suppression de données. Ces règles s'appliquent à toutes les personnes physiques et morales intéressées souhaitant émettre et utiliser des preuves électroniques.

1.2 Procédure de demande et procédure d'émission de l'e-ID

Le projet d'ordonnance concrétise en outre la procédure de demande, la vérification de l'identité, la procédure d'émission et la révocation de l'e-ID émise par la Confédération. L'e-ID est demandée en ligne et la vérification de l'identité peut être effectuée en ligne ou sur place, auprès d'un centre de saisie cantonal ou – pour les Suisses de l'étranger – auprès de la représentation consulaire compétente. L'émission de l'e-ID relève de la compétence de fedpol.

Dans un premier temps, l'application pour la conservation et la présentation des preuves électroniques de la Confédération (portefeuille électronique) est installée sur l'appareil du requérant, par exemple sur un téléphone portable. Dans un deuxième temps, le requérant prend une photo de son document d'identité officiel (carte d'identité, passeport, titre de séjour pour étrangers), et fait un enregistrement vidéo de son

visage. Les données sont envoyées au moyen de l'application pour la conservation et la présentation des preuves électroniques au service de contrôle de l'État qui les vérifie. En principe, cette vérification doit être automatisée. Si les données transmises concordent avec le registre national des documents d'identité, le requérant reçoit immédiatement l'e-ID sur son appareil. L'émission de l'e-ID peut se faire simultanément dans plusieurs applications sur un ou plusieurs appareils. Cette procédure ne devrait prendre que quelques minutes. Il faut toutefois s'attendre à des temps d'attente plus longs lors de l'introduction initiale de l'e-ID (système de file d'attente).

Si le requérant souhaite faire vérifier son identité sur place, la procédure de vérification de l'identité peut également avoir lieu auprès d'un centre de saisie cantonal ou – pour les Suisses de l'étranger – auprès de la représentation consulaire compétente. Comme la mise en œuvre de la procédure de vérification de l'identité sur place relève de la responsabilité des cantons, il faut s'attendre à des différences dans ce contexte.

1.3 Spécifications techniques

Les spécifications techniques sont précisées afin de garantir une utilisation sûre de l'e-ID. Le Département fédéral de justice et police (DFJP) détermine le format technique et les attributs pour la transmission des données, les exigences relatives à l'interface avec le système d'information pour l'émission et la révocation de l'e-ID ainsi que les normes et protocoles pour la communication des données lors de l'émission de l'e-ID.

Les spécifications techniques suivantes sont publiées en premier lieu sous forme de recommandations (art. 33 et 34) : d'une part le format des preuves électroniques, d'autre part les normes et protocoles applicables aux processus de communication des données lors de l'émission et de la présentation des preuves électroniques. Le DFJP peut prévoir que ces recommandations ou une partie de celles-ci soient déclarées de force obligatoire (art. 35).

2. Comparaison avec le droit européen

Au sein de l'Union européenne, des réformes sont en cours dans le domaine de l'identité numérique. Le Conseil fédéral estime que ces évolutions devraient être intégrées aux réflexions sur le plan national. Le 3 juillet 2021, la Commission européenne a adopté une proposition visant à modifier le règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance (règlement eIDAS) et à créer un cadre juridique pour une identité numérique européenne. Dans le cadre de ce nouveau règlement, il est prévu que les États membres mettent à la disposition des citoyens, dans un délai de 24 mois à compter de son entrée en vigueur, des portefeuilles électroniques leur permettant d'associer leur identité numérique nationale à des preuves comprenant d'autres caractéristiques sur la personne (par exemple, permis de conduire, diplômes, compte bancaire). Les portefeuilles peuvent être fournis par les autorités ou par des acteurs privés, à condition que ces derniers soient reconnus par les États membres.

Le 30 avril 2024, le Conseil européen a adopté la proposition de modification du règlement eIDAS. Le cadre défini par la Commission se fonde sur les principes de l'identité

autonome souveraine (Self-Sovereign Identity, SSI). Ce cadre est toutefois neutre sur le plan technologique lorsqu'il s'agit de mettre en œuvre ces principes. Entre le 12 août 2024 et le 9 septembre 2024[1], respectivement entre le 29 novembre 2024 et le 2 janvier 2025, la Commission a ouvert la consultation sur cinq projets concernant la mise en œuvre des modifications adoptées dans le règlement eIDAS. Les actes de mise en œuvre portent notamment sur des normes techniques, des procédures et des formats afin de garantir l'interopérabilité, la confiance et la sécurité juridique dans les États membres de l'UE. Ils règlent notamment la question des incidents de sécurité liés aux portefeuilles électroniques, l'utilisation transfrontalière des identités numériques, l'enregistrement et la tenue d'une liste d'émetteurs et de vérificateurs, ainsi que d'une liste de portefeuilles électroniques.

La Suisse adopte une approche moins réglementée que l'UE, ce qui laisse plus de place à l'innovation. Elle renonce à des procédures d'autorisation formelles et coûteuses, ainsi qu'à la tenue de listes. La Suisse n'est pas légalement tenue d'adopter le règlement eIDAS, ni les actes de mise en œuvre qui en découlent. Toutefois, compte tenu de sa forte interdépendance commerciale et sociale avec la plupart des pays membres de l'UE, elle a tout intérêt à concevoir un système de preuve d'identité électronique interopérable avec celui de l'UE. La LeID prévoit que le Conseil fédéral puisse conclure des traités internationaux pour faciliter l'utilisation et la reconnaissance juridique de l'e-ID à l'étranger et la reconnaissance des e-ID étrangères en Suisse (art. 32, LeID). Le projet d'ordonnance tient compte des développements en la matière au sein de l'UE et sont conçus de manière à rendre l'identification électronique compatible avec le droit européen.

3. Commentaire des dispositions

Préambule

Le projet d'ordonnance se fonde sur différentes dispositions de la LeID, mais les art. 2, al. 5, let. a, 3, al. 7, 4, 8, al. 2 et 3, 9, al. 2, 17, al. 1, 18, al. 5 et 6, 19, 20, 21, 28, al. 4, 30, 31, al. 5, 33 et 35, al. 2, LeID ne figurent pas séparément dans le préambule.

Chapitre 1 Objet

Art. 1

Globalement, l'ordonnance vise à garantir par des normes techniques et des règles de procédure l'exploitation sûre et le bon fonctionnement de l'infrastructure de confiance, ainsi que l'utilisation sûre de l'e-ID et des autres preuves électroniques. L'accent est

1 Adoption des règlements d'exécution de la Commission européenne le 4 décembre 2024 (2024/2977, 2024/2979, 2024/2980, 2024/2981, 2024/2982).

mis sur la sécurité afin d'empêcher toute utilisation abusive ou tout risque de manipulations, ainsi que d'instaurer et de maintenir la confiance dans le système.

Le projet d'ordonnance fixe les règles applicables à la mise à disposition et à l'exploitation des registres, de l'application pour la conservation et la présentation des preuves électroniques (portefeuille électronique)[2] et de l'application pour la vérification des preuves électroniques. L'ordonnance régit en outre l'ensemble du processus relatif à l'identité électronique (e-ID), qui comprend la demande d'émission, la vérification de l'identité du requérant, la procédure d'émission proprement dite ainsi que les conditions de révocation de l'e-ID. Enfin, l'ordonnance précise les modalités de conservation et d'effacement des données personnelles, notamment des données relatives à la procédure d'émission de l'e-ID et aux autres preuves électroniques.

Chapitre 2 Infrastructure de confiance

L'infrastructure de confiance et les autres services associés constituent une application spécialisée de l'Office fédéral de la justice (OFJ). L'OFJ agit en tant que mandant vis-à-vis de l'Office fédéral de l'informatique et de la télécommunication (OFIT) et assume la responsabilité globale.

Section 1 Portail pour le traitement des données des registres

Art. 2 But et exploitation du portail

Afin de permettre les inscriptions au registre de base et au registre de confiance, un portail numérique (portail) est mis à la disposition des émetteurs et des vérificateurs de preuves électroniques. Ce portail, à l'instar d'autres plateformes d'enregistrement, sert à demander les informations requises pour l'inscription au registre de base et au registre de confiance. L'OFJ est responsable du portail.

L'enregistrement s'effectue au moyen de l'ePortal mis à disposition par le Département fédéral des finances. Une application dédiée y est disponible, permettant aux émetteurs et aux vérificateurs d'effectuer l'ensemble des activités ainsi que de s'acquitter des émoluments. À moyen terme, le principe *Once-Only* devrait être mis en œuvre par l'intégration du système dans d'autres portails ou par l'interconnexion avec des ensembles de données préexistants.

Art. 3 Données saisies lors de l'enregistrement

Al. 1

[2] Sous le nom protégé de "swiyu".

Afin de s'enregistrer sur le portail, les émetteurs et les vérificateurs de preuves électroniques doivent saisir les informations suivantes :

- s'il s'agit d'une personne physique, les nom(s) et prénom(s)
- s'il s'agit d'une personne morale ou d'une société de personnes :
    - la raison sociale, le siège de l'entreprise et le numéro d'identification de l'entreprise (IDE) au sens de la loi fédérale du 18 juin sur le numéro d'identification de l'entreprise[3] ;
    - l'adresse ;
    - l'adresse e-mail ;
    - le numéro de téléphone ;
    - les informations de paiement.

À moyen terme, il sera examiné si le registre UID peut être utilisé directement comme fournisseur de données. Pendant la procédure de consultation, il sera également évalué à partir de quand cette interface pourrait être réalisée. Par ailleurs, une comparaison avec le registre fédéral des bâtiments et des logements sera envisagée, afin que des informations telles que le siège d'une personne morale ou d'une société de personnes puissent également être reprises de manière automatisée.

Al. 2

L'adresse, le numéro de téléphone, l'adresse e-mail ou toute autre coordonnée ne sont pas saisis dans les registres, mais sont enregistrés auprès de l'OFIT. Ces données ne sont pas accessibles au public et servent uniquement à s'enregistrer sur le portail administratif et à gérer la relation commerciale et les données de base dans le système. La collecte des informations de paiement est nécessaire car des émoluments sont perçus auprès des émetteurs et des vérificateurs pour les données qu'ils inscrivent au registre de base et pour celles dont ils demandent l'inscription au registre de confiance (art. 38). Afin d'éviter les processus de contrôle fastidieux, les éventuelles radiations des registres et les procédures de recouvrement, seuls les moyens de paiement direct (par exemple par carte de crédit) seront prévus.

Section 2 Registre de base

Art. 4 Contenu

Après s'être enregistré sur le portail, un émetteur ou un vérificateur de preuves électroniques dispose d'un accès au registre de base. Il peut inscrire via une interface technique des données au registre de base visant à garantir l'authenticité et l'intégrité des

[3] RS **431.03**

preuves électroniques qu'il émet. Ces données comprennent des clés cryptographiques publiques et des données relatives à la révocation des preuves électroniques. En effet, l'émetteur obtient un accès sécurisé au registre de base afin de pouvoir gérer ses preuves électroniques révoquées. En plus de l'émetteur, le vérificateur des preuves électroniques peut également inscrire des données au registre de base. Lorsqu'il inscrit des données le concernant, l'émetteur ou le vérificateur reçoit un paramètre anonyme (identifiant), généré grâce à une interaction technique avec l'OFIT. L'émetteur ou le vérificateur est seul responsable de la gestion des données inscrites. Aucune information personnelle concernant l'émetteur ou le vérificateur ne peut être déduite de l'identifiant.

Les éléments du registre de base sont accessibles au public. La consultation des données publiques est possible sans enregistrement et sert à vérifier la validité cryptographique des preuves électroniques. Les données que l'émetteur ou le vérificateur a inscrites sont protégées contre des tiers, de sorte que seul l'émetteur ou le vérificateur concerné soit habilité à traiter les données et que l'authenticité des données soit à tout moment garantie.

Art. 5 Modification ou effacement de données par l'émetteur ou le vérificateur de preuves électroniques

L'émetteur et le vérificateur de preuves électroniques dispose librement des données qu'il a inscrites au registre de base. Il peut demander au moyen du portail que les données qu'ils ont inscrites soient effacées ou modifié du registre de base à tout moment. Dans ce cas, les identifiants attribués, les clés cryptographiques et les données relatives à la révocation des différentes preuves sont effacées. À noter que la validité des preuves émises ne peut plus être vérifiée, car les informations nécessaires à cet effet ne sont plus disponibles.

L'émetteur ou le vérificateur doit prouver qu'il est bien le propriétaire légitime de l'inscription, notamment par le biais de l'identifiant ou de la clé cryptographique privée requise. Cette étape de vérification peut être effectuée automatiquement. Si l'émetteur ou le vérificateur ne peut plus apporter cette preuve, notamment en raison de la perte de la clé cryptographique privée, une autre forme de preuve par la vraisemblance est requise. Il doit fournir par exemple les données recueillies et vérifiées lors de la procédure d'inscription au registre de confiance, ou toute autre donnée d'identification fiable s'il n'est pas inscrit au registre de confiance.

L'émetteur ou le vérificateur de preuves électroniques peut désactiver son inscription plutôt que de l'effacer afin que les preuves émises puissent encore être vérifiées. Par exemple, les preuves électroniques qui restent valables peuvent continuer à être vérifiées, même si l'organisation qui les a émises est désormais inactive. Si cette organisation souhaite disposer à nouveau d'un identifiant actif ultérieurement, elle devra procéder à un nouvel enregistrement et s'inscrire au registre de base.

Art. 6 Effacement de données non nécessaires

Al. 1 et 2

Si l'OFJ constate qu'un émetteur ou un vérificateur inscrit au registre de base des données qui ne sont pas nécessaires aux fins prévues à l'art. 2, al. 1, LeID, il charge l'OFIT d'effacer ces données, voire toute l'inscription. Avant que les données soient effacées, l'OFJ informe l'émetteur ou le vérificateur concerné lorsque cela est possible sans un effort disproportionné. Si les données inscrites au registre représentent une cybermenace ou si leur contenu est illicite, l'intégralité de l'inscription de l'émetteur ou du vérificateur concerné sera effacée sans information préalable.

Al. 3

Lors de la consultation du registre de base, des données peuvent être générées, notamment les adresses IP et d'autres données similaires conformément au protocole utilisé (art. 2, al. 5, let. a, LeID). Ces données générées ne peuvent être enregistrées qu'aux fins suivantes : pour garantir la sécurité de l'information et des services, pour assurer la maintenance de l'infrastructure ou pour contrôler le respect des règlements d'utilisation (art. 57l, let. b, ch. 1 à 3, de la loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[4]. L'enregistrement vise à garantir l'exploitation sûre et le fonctionnement de l'infrastructure de confiance en toute sécurité, ainsi que l'utilisation sûre de l'e-ID et des autres preuves électroniques. Pour atteindre cet objectif, les données peuvent être conservées pendant 90 jours au plus. Passé ce délai, elles doivent être détruites.

Art. 7 Conservation des données modifiées ou effacées

Si les données sont modifiées ou effacées, l'OFIT ou un autre service fédéral conserve les données antérieures pendant dix ans afin de garantir la traçabilité des données inscrites aux registres. La traçabilité des données inscrites est primordiale pour garantir l'intégrité, l'authenticité et la force probante des données. En cas de litige, il faut notamment pouvoir déterminer quelles données ont été publiées à quel moment. Par conséquent, la conservation des données après la modification d'une inscription au registre de base est déterminante pour la sécurité juridique. Le délai de dix ans correspond au délai de conservation général dans les transactions commerciales. Ces données ne sont toutefois pas accessibles au public.

La Confédération conserve ces données au-delà du délai de dix ans si cela est nécessaire pour une utilisation sûre des preuves électroniques. Dans ce cas, elle peut effacer certaines données ou l'intégralité de l'inscription au registre de base. Ce délai est nécessaire afin d'assurer la traçabilité des données et de pouvoir vérifier rétroactivement l'identification d'un émetteur ou d'un vérificateur qui n'est plus inscrit au registre de base ainsi que l'utilisation sûre et fiable des preuves électroniques.

[4] RS **172.010**

Section 3 Registre de confiance

Art. 8 Contenu

Al. 1

L'OFIT met à la disposition des utilisateurs un système accessible au public, qui contient des données utiles à la vérification de l'identité d'un émetteur ou d'un vérificateur et à l'utilisation sûre des preuves électroniques (registre de confiance). Les informations vérifiées par la Confédération concernant l'identité des acteurs connectés au système peuvent être consultées au moyen du registre de confiance. Par exemple, l'interdépendance entre l'identifiant et la clé publique est confirmée et communiquée à fedpol. L'application pour la conservation et la présentation des preuves électroniques affiche systématiquement les informations du registre de confiance lors d'une transaction (demande d'émission ou de vérification). Les participants connectés au système peuvent décider librement à tout moment s'ils souhaitent consulter le registre de confiance.

Lors de la consultation d'un identifiant confirmé au registre de confiance, l'identifiant inscrit au registre de base ainsi que le nom ou la raison sociale de l'émetteur ou du vérificateur sont affichés, accompagnés le cas échéant de l'indication qu'il s'agit d'une autorité ou d'un autre service qui accomplit des tâches publiques. Si l'émetteur ou le vérificateur inscrit au registre de confiance est une personne morale, les informations suivants seront également affichées : l'IDE et, le cas échéant, les informations éventuelles sur l'inscription dans d'autres registres, tels que le registre du commerce. Le registre de confiance contient en outre toute information éventuelle sur les preuves électroniques pouvant être émises ou vérifiées par des autorités ou des organismes chargés de missions publiques (article 13).

L'utilisation du registre de confiance n'est pas nécessaire pour la vérification cryptographique des preuves électroniques ou la création de canaux de communication techniquement sécurisés ; elle vise toutefois à renforcer la confiance qu'un acteur accorde à son interlocuteur, par exemple lorsqu'il n'existe aucune relation préalable entre eux, que l'un d'eux souhaite obtenir des informations supplémentaires ou que l'exactitude des informations transmises doit être confirmée. Pour toutes ces raisons, les informations concernant l'identité d'un acteur inscrit au registre de confiance sont toujours vérifiées par la Confédération.

Cette transparence permet à tous de savoir qui, par exemple, demande plus de données que nécessaire lors de la vérification d'une preuve électronique. Si un émetteur ou un vérificateur n'est pas inscrit au registre de confiance, cela signifie que la Confédération n'a pas vérifié son identité et que celle-ci n'est donc pas confirmée. Les données du registre de confiance sont accessibles au public. La consultation des données publiques est possible sans enregistrement.

Al. 2

Outre la vérification des identifiants, le registre de confiance fournit aux utilisateurs une mention en cas de soupçon d'utilisation abusive de l'infrastructure de confiance ou

d'une preuve électronique, ou lorsque les formats, normes et protocoles prévus à l'art. 35 ne sont pas respectés. Cette mention vise à favoriser une utilisation sûre des preuves électroniques. Les utilisateurs de de portefeuilles électroniques et d'applications pour la vérification des preuves électroniques y trouvent ainsi des repères pour une utilisation en toute sécurité.

L'objectif est de renforcer la confiance dans les échanges électroniques de données et de fournir aux utilisateurs du système des indicateurs efficaces pour une utilisation sécurisée. Outre la vérification de l'identité des émetteurs et des vérificateurs, les participants connectés au système doivent pouvoir se fier aux preuves électroniques présentées et vérifiées dans le cadre de leur utilisation quotidienne.

Art. 9 Demande d'inscription au registre de confiance

Al. 1

Pour déposer une demande d'inscription de ses données au registre de confiance, l'émetteur ou le vérificateur, qu'il soit une autorité ou un acteur privé, doit être inscrit au registre de base. Il doit fournir la preuve technique requise de son inscription au registre de base. La preuve à fournir est vérifiée via le portail dans le cadre d'une procédure automatisée.

Al. 2

Selon l'art. 3, al. 3, LeID, une autorité ou un autre service qui accomplit des tâches publiques peut demander que son identifiant soit confirmé. La demande comprend, en plus de la preuve technique au sens de l'al. 1, son IDE et le nom d'une personne de contact qui est responsable de l'identifiant.

Al. 3 et 4

Selon l'art. 3, al. 4, LeID, un émetteur ou un vérificateur privé (personne physique ou personne morale) peut demander que son identifiant soit confirmé par l'OFIT et inscrit au registre de confiance.

La demande d'une personne physique ou morale se distingue de celle d'une autorité ou d'un autre service qui accomplit des tâches publiques. Une personne physique doit posséder une e-ID et la présenter. La demande d'une personne morale doit être signée au moyen d'une signature électronique qualifiée par la ou les personnes habilitées à signer, au sens de la loi fédérale du 18 mars 2016 sur la signature électronique (SCSE)[5], et comprend, en plus de la preuve technique au sens de l'al. 1, (cumulativement) les informations suivantes :

[5] RS **943.03**

- l’IDE ;
- les coordonnées de la personne morale ;
- les coordonnées du responsable de l’identifiant ; et
- si la personne morale n’est pas inscrite au registre du commerce suisse, d’autres pièces justificatives, notamment une copie attestée conforme du contrat de société ou des statuts, un extrait attesté conforme actuel du registre du commerce étranger ou un document de même valeur.

Art. 10 Examen de la demande

Al. 1 et 2

L’OFJ examine l’exhaustivité de la demande et l’exactitude de son contenu. Une fois que la demande a été examinée et que l’identité du requérant a été vérifiée, ou qu’il a été établi que cette personne agit au nom de la personne morale ou de la société de personnes, le résultat de cette vérification est transmis à l’OFIT. L’OFIT confirme alors les données au sens de l’art. 8, al. 1, et inscrit cette confirmation au registre de confiance de manière visible.

Al. 3

Si l’OFJ constate, lors de l’examen de la demande, que celle-ci est incomplète ou incorrecte, il informe le requérant et l’invite à fournir les informations manquantes ou corriger les erreurs dans un délai de 30 jours. Cette disposition vise à rendre les procédures administratives efficaces et à garantir que le requérant dispose de suffisamment de temps pour remédier aux éventuelles insuffisances.

Si la demande n’est pas complétée ou rectifiée dans ce délai, la procédure d’examen sera interrompue. Cela signifie que la demande ne sera plus traitée et qu’aucune inscription au registre de confiance ne sera effectuée.

Art. 11 Mise à jour

Al. 1

Toute modification nécessite une nouvelle demande et doit être vérifiée par l’OFJ quant à son exhaustivité et à l’exactitude de son contenu. L’émetteur ou le vérificateur notifie au moyen du portail (art. 2) toute modification des données le concernant au sens de l’art. 8, al. 1, let. b à d. La notification porte notamment sur : le nom de la personne physique ou morale inscrite dans le registre de confiance ; les éventuelles informations relatives aux inscriptions de la personne morale dans d’autres registres, tels que le registre du commerce, le registre des entreprises (registre UID), ou l’identifiant d’entité juridique (LEI). La notification se concentre sur les données nécessaires à la confirmation de l’identifiant publiées dans le registre de confiance. Les modifications portant sur

d’autres données, recueillies lors de la demande d’inscription et non publiées dans le registre de confiance, ne doivent pas être signalées.

Si un émetteur ou un vérificateur inscrit au registre de confiance peut fournir la preuve technique qu’il possède l’identifiant initialement confirmé, des identifiants supplémentaires peuvent être ajoutés à l’identifiant déjà confirmé sans nouvelle vérification. Dans ce cas, aucun frais supplémentaire n’est facturé.

Al. 2 à 6

Lorsque l’inscription au registre de confiance a été modifiée pour la dernière fois il y a plus de cinq ans, l’OFJ vérifie auprès de l’émetteur ou du vérificateur si les données le concernant sont encore actuelles. Cette prise de renseignement ne constitue pas une sommation de fournir les données actuelles pour un nouvel examen (al. 3). Toutefois, selon le résultat obtenu, cela peut mener à l’ouverture d’une procédure de sommation.

Une procédure de sommation est engagée lorsqu’il y a une raison de supposer que l’inscription n’est plus actuelle et que l’émetteur ou le vérificateur n’a pas signalé les modifications conformément à l’al. 1. L’OFJ demande alors à l’émetteur ou au vérificateur de rectifier les données dans un délai de 30 jours. La sommation doit être effectuée par écrit, cette sommation écrite étant en principe envoyée par voie électronique. Elle doit être brièvement motivée et les actions nécessaires doivent être énumérées. L’émetteur ou le vérificateur doit pouvoir comprendre ce qui est exigé de lui et la raison de la sommation.

L’OFJ examine les données et les pièces justificatives reçues et communique à l’OFIT le résultat. Si les exigences requises sont satisfaites sont remplies, l’OFIT inscrit la mise à jour au registre de confiance.

Les délais de conservation des données antérieures sont régis par l’art. 7, al. 1. Ces données ne sont pas accessibles au public.

Art. 12 Effacement sur demande de l’émetteur ou du vérificateur

Al. 1

Un émetteur ou un vérificateur peut à tout moment demander que son inscription au registre de confiance soit effacée. Si cette demande ne concerne que l’inscription au registre de confiance, l’émetteur ou le vérificateur conserve son identifiant inscrit au registre de base. Cependant, en cas d’utilisation de preuves électroniques le concernant, l’identité de l’émetteur ou du vérificateur ne peut plus être confirmée par l’OFIT. Le titulaire de la preuve électronique ne peut plus vérifier si l’identité indiquée est effectivement correcte. Au lieu de demander l’effacement de l’inscription, l’émetteur ou le vérificateur peut donc aussi exiger qu’il soit précisé dans le registre de confiance qu’un certain identifiant lui était attribué, ou que son identifiant était confirmé jusqu’à sa désactivation. Cette information sera accessible au public.

Comme pour la demande d'effacement d'une inscription au registre de base, l'émetteur ou le vérificateur inscrit au registre de confiance doit prouver qu'il est bien le propriétaire légitime de l'inscription, notamment au moyen de l'identifiant ou de la clé cryptographique privée requise (art. 5, al. 3). En outre, l'OFJ vérifie que l'autorité, l'organisation ou la personne qui fait la demande dispose de la preuve d'identité requise.

Al. 2

Lorsqu'un émetteur ou un vérificateur a été sommé par l'OFJ de lui transmettre les documents visant à actualiser les données du registre de confiance, conformément à l'art. 11, al. 3, et qu'il n'y donne pas suite dans le délai fixé, l'OFJ demande à l'OFIT d'effacer l'identifiant du registre de confiance.

Al. 3

Le délai de conservation des données relatives à l'identifiant confirmé qui ont été effacées est régi par l'art. 7, al. 1. Ce délai s'applique également à toute modification des informations du registre de confiance (mutations vérifiées des inscriptions au registre). Un délai de conservation de dix ans s'applique ; il peut être prolongé par la Confédération si une utilisation sûre des preuves électroniques l'exige.

Art. 13 Inscription d'autres données par une autorité

Outre l'identifiant confirmé et la mention relative à un soupçon d'utilisation abusive de l'infrastructure de confiance ou d'une preuve électronique au sens de l'art. 18, le registre de confiance met également à la disposition des utilisateurs les informations fournies par une autorité ou un autre service qui accomplit des tâches publiques. Il s'agit notamment des données permettant de déterminer quelle autorité ou quel service est habilité à émettre et à vérifier un type particulier de preuve électronique. L'autorité ou le service qui fournit ces informations est responsable de leur exactitude.

Les autorités et autres services qui accomplissent des tâches publiques doivent être inscrits au registre de base et au registre de confiance afin de pouvoir eux-mêmes inscrire des données supplémentaires dans le registre de confiance. Sur demande à l'OFJ, un accès dédié au système leur est accordé. Cela leur permet de publier de manière autonome des informations sur les types de justificatifs dont ils sont responsables. Cela comprend, par exemple, des schémas techniques définissant les champs de données constituant un justificatif. Il est également possible d'indiquer quels acteurs, sur la base de leurs identifiants, sont considérés comme émetteurs et vérificateurs légitimes. Il faut inscrire au moins l'identifiant ou les identifiants de l'autorité ou des autorités concernées ainsi que la désignation du justificatif électronique correspondant.

Section 4 Applications numériques

Art. 14 Exigences relatives à l'application de conservation et de présentation des preuves électroniques

Al. 1

L'OFIT met à disposition une application pour la conservation et la présentation des preuves électroniques (portefeuille électronique). Il doit veiller à ce que l'application soit accessible aux personnes handicapées (art. 28, al. 2, LeID). Pour garantir le bon fonctionnement de l'application, l'appareil utilisé (par exemple un smartphone) doit répondre à certaines exigences. Celles-ci se fondent sur les normes actuelles et largement admises en matière de développement d'applications mobiles. Cela signifie que le système d'exploitation installé sur l'appareil doit être largement répandu, toujours pris en charge par le fournisseur du système concerné et continuer à recevoir des mises à jour de sécurité.

Al. 2

Lorsqu'un émetteur n'est pas inscrit au registre de base ou au registre de confiance (let. a) ou lorsqu'un vérificateur n'est pas inscrit au registre de base ou au registre de confiance et n'utilise pas l'application fournie par la Confédération pour vérifier les preuves électroniques (let. b), un utilisateur peut ne pas savoir à qui il a affaire. Le fait qu'un émetteur ou un vérificateur ne soit pas inscrit représente un risque accru pour la protection des données, car l'identité des acteurs concernés ne peut être établie avec certitude. Sans transparence, il est difficile d'évaluer si les acteurs sont dignes de confiance. En outre, aucune information de sécurité ne peut être enregistrée, ce qui peut potentiellement conduire à des abus, à un accès non autorisé à des données personnelles ou à d'autres failles de sécurité.

L'application indique donc à l'utilisateur, avant un éventuel transfert de données, si un émetteur ou un vérificateur n'est pas inscrit au registre de base ou au registre de confiance. Il s'agit d'une mesure technique et organisationnelle appropriée pour assurer la protection et la sécurité des données (art. 33, let. e, LeID). En revanche, ceci n'est pas nécessaire lorsque le vérificateur utilise l'application de la Confédération pour la vérification des preuves électroniques, car l'utilisateur est informé que le vérificateur utilise l'application officielle visée à l'art. 9 LeID. Dans ce cas, la communication des données en toute sécurité est assurée, car l'application a été conçue de manière conforme aux exigences de la protection des données dès le départ.

Art. 15 Système pour les copies de sécurité

Lors de la perte de l'appareil ou en cas d'achat d'un nouvel appareil, il est courant de restaurer les applications installées et les données stockées à partir d'une sauvegarde. Ainsi, les fonctionnalités de l'ancien système peuvent être rapidement remises à disposition en cas de changement d'appareil. Une possibilité comparable est offerte aux titulaires du portefeuille électronique de la Confédération. Les preuves électroniques ne sont plus réutilisables si, comme c'est le cas pour l'e-ID, un lien avec l'appareil du titulaire est nécessaire au moyen d'un processeur cryptographique. En conséquence,

ces preuves électroniques devront faire l'objet d'une nouvelle demande auprès de l'émetteur.

Al. 1

La fonction de base de l'application pour la conservation et la présentation de preuves électroniques est de permettre au titulaire de générer et de crypter une copie de sécurité du contenu du portefeuille électronique (en particulier des preuves électroniques). Le titulaire peut décider lui-même où il souhaite conserver cette copie de sécurité. Après un changement d'appareil (smartphone, ordinateur, etc.), les preuves électroniques qui y sont conservées pourront être restaurées manuellement.

La transmission et la restauration de ces copies de sécurité sont largement influencées par les fonctions mises à disposition par le système d'exploitation de l'appareil. En outre, le titulaire doit se souvenir d'un mot de passe (par exemple, le cryptage Wordlist), qui est nécessaire pour décrypter les copies de sécurité créées. En cas de perte ou d'oubli de ce mot de passe, il est impossible de récupérer les données. Les mots de passe ne sont pas connus de la Confédération.

Al. 2

L'OFIT met à disposition un système dans lequel le titulaire peut déposer les copies de sécurité des preuves électroniques conservées dans l'application sur son appareil (art. 8, al. 2, LeID). Le système est conçu de manière à empêcher l'accès par des tiers. L'utilisation du système pour les copies de sécurité est facultative et est réservée aux utilisateurs du portefeuille électronique étatique. Seuls les titulaires peuvent accéder au contenu de leurs copies de sauvegarde. En cas d'inactivité prolongée, si les copies de sécurité ne sont pas mises à jour ou téléchargées, les fichiers sont effacés après trois ans.

À noter que les preuves électroniques ne sont plus réutilisables après la restauration des données à partir d'une sauvegarde si, comme c'est le cas pour l'e-ID, un lien avec l'appareil du titulaire est nécessaire au moyen d'un processeur cryptographique (art. 18, al. 2, LeID). Dans ce cas, la preuve du lien avec le titulaire est liée à l'appareil initialement utilisé lors de l'émission. En cas de perte ou de changement de l'appareil en question, il faut déposer une nouvelle demande d'émission pour pouvoir utiliser les preuves électroniques correspondantes.

Art. 16 Vérification d'autres preuves électroniques au moyen de l'application visée à l'art. 9 LeID

Al. 1 et 2

Cette disposition concrétise la norme de délégation prévue à l'art. 9, al. 2, LeID pour la vérification des autres preuves électroniques au moyen de l'application de la Confédération. Au-delà de la vérification de l'e-ID prévue à l'al. 1, l'application doit également servir à vérifier la validité d'autres preuves électroniques, le but étant d'encourager l'utilisation de l'infrastructure de confiance et la diffusion des preuves électroniques.

L’utilisation de l’application de la Confédération pour la vérification des preuves électroniques est facultative. Tous les vérificateurs peuvent décider librement s’ils souhaitent utiliser l’application de la Confédération ou une autre application comparable.

Les autorités, les services qui accomplissent des tâches publiques et les émetteurs privés peuvent demander à l’OFJ que l’application de la Confédération puisse également vérifier leurs preuves électroniques. Pour ce faire, les preuves en question doivent satisfaire aux exigences techniques (formats, normes et protocoles) et l’émetteur doit être inscrit au registre de confiance.

Al. 3

La vérification d’une preuve électronique d’un émetteur privé au moyen de l’application de la Confédération peut être autorisée si, en plus des exigences de l’al. 2, aucun motif d’intérêt public ne s’y oppose, par exemple pour des raisons de sécurité ou de protection des données. En outre, il est nécessaire que la preuve soit largement diffusée et généralement reconnue.

L’application de la Confédération est destinée en premier lieu à vérifier l’e-ID. Étendre la vérification à d’autres preuves électroniques exige des ressources supplémentaires sur le plan de la technique et de l’organisation. Pour assurer que l’extension à d’autres preuves électroniques soit dans l’intérêt général et que les coûts restent proportionnés, la vérification se limitera aux preuves électroniques jugées d’importance supérieure pour la collectivité.

Al. 4

Si un émetteur souhaite que l’application de la Confédération puisse vérifier sa preuve électronique, il pourra adresser une demande correspondante à l’OFJ. L’adaptation de l’application pour la vérification des preuves électroniques est une prestation gratuite. Si la preuve électronique de l’émetteur remplit toutes les exigences fixées, l’OFJ décidera qu’elle pourra être vérifiée au moyen de l’application de la Confédération et en informera l’OFIT, qui prendra les mesures nécessaires.

Section 5 Utilisation inappropriée de l’infrastructure de confiance ou d’une preuve électronique

Art. 17 Procédure de contrôle

Al. 1 et 2

Si l’OFJ apprend que l’infrastructure de confiance ou une preuve électronique a été utilisée de manière inappropriée, par exemple par le titulaire d’une preuve électronique, par un émetteur ou par un vérificateur, il mène une procédure de contrôle. Le contrôle vise à protéger l’intégrité du système au sein duquel les preuves électroniques sont

utilisées. Les personnes connectées au système ont la possibilité de signaler des problèmes à l'OFJ, ce qui permet de détecter et de réparer rapidement d'éventuelles failles de sécurité et de limiter le plus possible les risques en matière de sécurité et de protection des données. Le projet d'ordonnance précise ce qu'on entend par utilisation inappropriée.

a. L'émetteur ou le vérificateur doit recourir à des données officielles, faute de quoi il ne remplit pas une condition essentielle garantissant une utilisation sûre de la preuve électronique. S'il n'utilise pas les données officielles, si l'identité inscrite au registre de confiance ne correspond pas à son identité réelle ou s'il prétend être quelqu'un d'autre au cours de transactions commerciales, il y a utilisation inappropriée. S'agissant du dernier exemple cité, il suffit que l'émetteur ou le vérificateur soit inscrit au registre de base.

   L'identité officielle des personnes physiques, tout comme le contenu de l'e-ID selon l'art. 15, al. 3, LeID, peut inclure des mentions supplémentaires, notamment le nom d'alliance, le nom reçu dans un ordre religieux, le nom d'artiste ou le nom de partenariat, ainsi que la mention de signes particuliers. Dans certaines situations, ces informations peuvent s'avérer utiles, voire nécessaires, lors des transactions commerciales. Si ces mentions figurent sur la carte d'identité, sur un autre document d'identité ou sur la carte de légitimation du titulaire et qu'elles ont été utilisées dans la procédure de demande visée à l'article 9, elles peuvent faire partie de l'identité. Des informations supplémentaires peuvent également être mentionnées dans le cas des personnes morales, dont l'identité est souvent assimilée à un produit de marque ou à un service spécifique.

b. La preuve électronique ne doit pas présenter de contenu illicite ni servir à des fins illicites.

c. Si une preuve électronique contient des données personnelles particulièrement sensibles, telles que des données relatives à la santé ou des informations sur les convictions religieuses, le titulaire de cette preuve doit en être informé par écrit. Cette information doit préciser que les données contenues sont particulièrement sensibles et qu'elles sont donc soumises à une protection renforcée. De cette manière, on s'assure que la personne concernée est consciente du caractère sensible de ses données et qu'elle peut, le cas échéant, donner son consentement au traitement en question. La notification écrite a donc pour but d'informer le titulaire de l'importance et de la protection de ces données avant qu'un traitement déterminé n'ait lieu. Le portefeuille électronique de la Confédération prendra en charge un format de données permettant aux émetteurs de marquer les informations sensibles directement dans l'application. Lors de la demande de données de ce type de champ, les utilisateurs sont explicitement avertis avant la transmission.

d. Pour garantir l'utilisation sûre des preuves électroniques, les principes fondamentaux de la protection des données doivent être respectés lors de la vérification. Cela signifie notamment que les données personnelles ne doivent pas être

collectées de manière disproportionnée. Les données ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée. Cela signifie qu'il est interdit de traiter ultérieurement les données de manière incompatible avec les finalités déterminées au préalable. Les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. Cette procédure protège la vie privée des personnes concernées et garantit que le traitement de leurs données est conforme à la législation sur la protection des données.

Al. 3 et 4

Pour mener la procédure de contrôle, l'OFJ peut prendre diverses mesures. Il peut par exemple vérifier les données saisies sur le portail visé à l'art. 2, ainsi que les données inscrites au registre de base et au registre de confiance. En outre, il peut par exemple recevoir lors de l'annonce des informations techniques sur les données transmises ou les demander ultérieurement afin de s'assurer qu'elles ont été traitées correctement et dans le respect des exigences de sécurité. L'OFJ peut également enquêter sur l'origine de la preuve électronique afin de détecter d'éventuelles failles de sécurité ou des irrégularités. Il peut par ailleurs prendre directement contact avec le titulaire concerné, l'émetteur ou le vérificateur de la preuve électronique. Il peut demander des informations complémentaires sur la transaction en question afin de clarifier les faits.

L'OFJ ne peut vérifier les cas d'utilisation inappropriée que si un identifiant unique est utilisé. En cas de soupçon de violation grave des prescriptions de protection des données, il informe le Préposé fédéral à la protection des données et à la transparence ou l'autorité cantonale compétente.

Art. 18 Mention relative à l'utilisation inappropriée

Si l'OFJ constate à la suite du contrôle prévu à l'art. 17, al. 3, que l'infrastructure de confiance ou qu'une preuve électronique a été utilisée de façon inappropriée, il communique le résultat à l'OFIT. L'OFIT inscrit le résultat de manière visible dans le registre de confiance ; la mention sera visible pendant six mois au plus. L'OFJ informe l'émetteur ou le vérificateur lorsque cela est possible sans un effort disproportionné. La mention sert à assurer la transparence et à instaurer la confiance, afin que les utilisateurs puissent décider en connaissance de cause s'ils souhaitent utiliser la preuve électronique en question. Cela permet de renforcer la sécurité globale du système de preuves électroniques et de garantir l'exactitude des informations du registre de confiance. La mention sera effacée du registre de confiance au plus tard à l'expiration du délai mentionné à l'al. 3.

Le délai fixé initialement peut être prolongé. L'OFJ contrôle à l'expiration du délai imparti, ou en cas de nouvelles annonces reçues entre temps, si les problèmes liés à la sécurité subsistent. Le cas échéant, l'inscription de la mention relative à l'utilisation inappropriée restera visible pendant une période supplémentaire afin de garantir une utilisation sûre des preuves électroniques. La prolongation du délai dans les cas clairs permet aux utilisateurs d'avoir accès à des informations actuelles concernant la sécurité d'une preuve électronique et de prendre des décisions en connaissance de cause

sans qu'une annonce soit nécessaire. Cette transparence contribue au respect des exigences légales nécessaires au maintien de la confiance dans l'utilisation des preuves électroniques.

L'utilisation inappropriée subsiste de manière manifeste notamment lorsqu'un émetteur ou un vérificateur se fait passer pour quelqu'un d'autre, lorsque les preuves électroniques émises ont un contenu illicite ou poursuivent des fins illicites, ou encore lorsqu'un émetteur ou un vérificateur a été identifié comme un programme automatisé (BOT). En cas de prolongation pour des motifs clairs, l'OFJ peut prévoir que la mention sera publiée pour une durée indéterminée.

Art. 19 Effacement de la mention

L'OFIT efface la mention du registre de confiance à l'expiration du délai fixé. Les données relatives à la mention et les informations collectées par l'OFJ lors de la procédure de contrôle sont conservées pendant dix ans par la Confédération ; elles ne sont pas généralement accessibles au public. La Confédération peut conserver les données effacées plus longtemps si l'utilisation sûre de l'infrastructure de confiance ou des preuves électroniques le requiert.

Chapitre 3: e-ID

Section 1 Demande

Art. 20 Conditions générales

Al. 1

Quiconque souhaitant obtenir une e-ID doit utiliser un appareil répondant aux exigences requises afin qu'un lien entre l'e-ID et son titulaire puisse être établi (art. 18, al. 2, LeID). Le requérant doit installer sur son appareil une application visée à l'art. 18, al. 1, LeID ou une autre application au sens de l'art. 18, al. 4 ou 5, LeID, dans laquelle sera émise l'e-ID. Le propriétaire de l'appareil peut conserver dans l'application sa propre e-ID, mais aussi celle d'une personne tierce, par exemple la personne mineure ou sous curatelle dont il est le représentant légal.

L'art. 18, al. 4, LeID, élargit les possibilités de garantir un lien avec le titulaire par d'autres solutions. La disposition est volontairement formulée de manière technologiquement neutre afin que différentes solutions puissent être envisagées. Une garantie automatisée et une preuve technique sont en principe nécessaires. Cette preuve technique permet notamment de démontrer que les deux clés cryptographiques utilisées pour établir le lien avec le titulaire proviennent bien d'un processeur cryptographique dédié.

Al. 2 et 3

La demande doit émaner du futur titulaire de l'e-ID. Si la personne intéressée est mineure ou sous curatelle de portée générale, elle doit produire l'autorisation de son représentant légal. Ce dernier peut donner son accord directement dans le processus en ligne avec sa propre e-ID, à condition qu'il en possède une. Si tel n'est pas le cas, il doit remettre l'autorisation signée à la personne mineure ou sous curatelle, ou l'accompagner lorsque celle-ci va faire vérifier son identité auprès d'un auprès d'un centre de saisie cantonal ou d'une représentation consulaire de la Suisse à l'étranger. En cas d'autorité parentale conjointe, l'autorisation d'un des parents suffit.

Art. 21 Exigences relatives à la photographie

La vérification de l'identité sur la base d'une vérification faciale automatisée peut être effectuée uniquement si la photographie du requérant enregistrée dans les systèmes d'information visés à l'art. 17, al. 2, LeID est de qualité suffisante. Elle doit notamment être conforme aux standards de la Convention du 7 décembre 1944 sur l'aviation civile internationale (OACI)[6]. Enfin, elle doit pouvoir être consultée de manière électronique.

Art. 22 Dépôt de la demande

Le requérant doit déposer la demande dans l'application pour la conservation et la présentation des preuves électroniques au sens de l'art. 8 LeID (portefeuille électronique de la Confédération).

Art. 23 Vérification de l'identité au moyen de l'application visée à l'art. 8 LeID

Al. 1

Si son identité a déjà été vérifiée sur place au moins une fois, le requérant peut faire vérifier son identité au moyen de l'application pour la conservation et la présentation des preuves électroniques. En d'autres termes, la vérification de l'identité doit avoir eu lieu sur place soit lors d'une première émission de l'e-ID, soit dans le cadre de l'établissement du document visé à l'art. 14, let. a, LeID (carte d'identité, passeport, titre de séjour ou carte de légitimation).

Si le requérant possède une carte de légitimation valable au sens de l'art. 17, al. 1, de l'ordonnance du 7 décembre 2007 sur l'État hôte (OLEH)[7] en relation avec l'art. 71a, al. 1, de l'ordonnance relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA)[8], la vérification de l'identité sur place se déroule auprès d'un auprès d'un centre de saisie désigné par le Département fédéral des affaires étrangères (DFAE).

---

6 RS **0.748.0**

7 RS **192.121**

8 RS **142.201**

Al. 2

Pour faire vérifier son identité en ligne, le requérant scanne la zone de lecture optique (MRZ) ou le CHIP de son document d'identité officiel (carte d'identité, passeport ou titre de séjour), puis il filme son visage (*Liveness-Check*). Ensuite, il transmet le résultat du scan et/ou de la lecture du CHIP, ainsi que son image faciale (sous la forme d'extraits vidéo) directement au moyen de l'application à fedpol, qui examinera la demande.

Al. 3

Pour vérifier les données biométriques transmises par le requérant, fedpol utilise un module du système d'information pour l'émission et la révocation de l'e-ID visé à l'art. 26, al. 1, LeID. Ce système permet de comparer de manière automatisée les informations transmises, notamment l'image faciale, avec celles figurant dans les systèmes d'information auxquels fedpol a accès en vertu de l'art. 26, al. 3, LeID. fedpol peut intervenir dans le processus de comparaison d'images faciales à des fins de contrôle qualité.

Art. 24 Vérification de l'identité sur place

Le requérant souhaitant faire vérifier son identité en personne et non au moyen de l'application pour la conservation et la présentation des preuves électroniques, doit prendre rendez-vous à cet effet. Des frais peuvent être perçus pour les prestations effectuées sur place.

Le service cantonal compétent ou la représentation consulaire compétente vérifie l'identité du requérant sur la base du document d'identité présenté par le requérant, de son visage et des informations provenant des systèmes d'information visés à l'art. 17, al. 2, LeID. La comparaison du visage peut être effectuée automatiquement. La station d'acquisition des données biométriques peut être utilisée à cet effet. Dans ce cas, le requérant doit être informé que son identité est vérifiée au moyen de la station d'acquisition. Ce dispositif offre une aide à la décision qui consiste en une évaluation, mais la décision finale est du ressort de l'agent spécialisé. Lors de la vérification de l'identité sur place, aucune donnée n'est enregistrée dans le système, ni conservée. Le résultat de la vérification de l'identité est transmis sous forme électronique à fedpol, au moyen du système d'information pour l'émission et la révocation de l'e-ID.

Toute personne souhaitant obtenir une e-ID peut soumettre la demande en combinaison avec une demande pour une carte d'identité ou un passeport visé à l'art. 14, let. a, ch. 1, LeID. En cas de demande d'émission combinée, la vérification de l'identité du requérant est effectuée dans le cadre de l'émission du ou des documents d'identité visés à l'art. 14, let. a, ch. 1, LeID. Le fait de pouvoir demander une e-ID en même temps qu'un passeport et/ou une carte d'identité est un service supplémentaire proposé. Étant donné que la vérification de l'identité vient d'être effectuée, aucune vérification d'identité supplémentaire n'est prévue pour valider l'émission de l'e-ID en cas de demande d'émission combinée. Une fois la procédure de vérification de l'identité terminée, l'émission de l'e-ID peut être validée avant la réception du document d'identité.

Les Suisses de l'étranger selon la loi fédérale du 26 septembre 2014 sur les Suisses de l'étranger[9] peuvent également faire vérifier leur identité auprès de la représentation consulaire compétente.

Art. 25 Décision automatisée

Lors de l'installation de l'application, le requérant est informé du traitement automatisé de ses données personnelles, conformément à l'art. 21 de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[10]. Pour poursuivre la procédure, le requérant doit expressément consentir à ce que la décision soit prise de manière automatisée. Sur demande auprès du service d'assistance technique de fedpol ou à des fins de contrôle qualité, la décision individuelle automatisée peut être revue par un agent chargé de la vérification de l'identité.

L'art. 21 al. 1 LPD prévoit que le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (décision individuelle automatisée). L'art. 21 al. 2 LPD ajoute que si la personne concernée le demande, le responsable du traitement lui donne la possibilité de faire valoir son point de vue.

Art. 26 Demande de l'e-ID depuis l'étranger

Si l'application au sens de l'art. 8, al. 1, LeID ou l'application au sens de l'art. 18, al. 4 ou 5, LeID ne peut pas être installée à l'étranger, notamment en raison d'un blocage géographique, il n'est pas possible de demander l'e-ID.

Section 2: Émission et révocation

L'e-ID est émise exclusivement par fedpol pour les personnes physiques au travers de l'infrastructure de confiance, sous la forme d'une preuve d'identité électronique. L'e-ID permet de prouver son identité dans le monde virtuel, ce qui est nécessaire pour certaines démarches en ligne, par exemple pour demander un extrait du casier judiciaire ou pour obtenir, auprès d'un fournisseur certifié, une signature électronique, avec laquelle il est possible de signer valablement. Elle est comparable à la carte d'identité ou au passeport dans le monde physique. Cependant, l'e-ID ne remplace pas ces deux documents. Tous les citoyens doivent pouvoir décider librement s'ils souhaitent utiliser une e-ID, une carte d'identité ou un passeport lorsqu'ils présentent une preuve d'identité en Suisse.

[9] RS **195.1**

[10] RS **235.1**

Dans la plupart des cas, fedpol pourra exécuter les tâches requises pour l'émission de l'e-ID de manière automatisée. En cas de doute de la part de fedpol ou d'incertitude du système automatique, fedpol pourra intervenir et revoir les données générées lors de la vérification faciale. fedpol décide quand la décision automatisée doit être revue par une autorité de contrôle.

Art. 27 Émission

Al. 1

Pour une même demande, il est possible d'obtenir l'e-ID dans plusieurs applications, sur un ou plusieurs appareils (avec un maximum de dix portefeuilles électroniques). L'émission simultanée a pour but de prévenir toute utilisation abusive de l'e-ID.

Al. 2

Les données relatives à la procédure d'émission de l'e-ID sont enregistrées dans le système d'information pour l'émission et la révocation de l'e-ID :

a. les scores de la procédure automatisée de vérification de l'identité au moyen de l'application visée à l'art. 8 LeID ;

b. le numéro d'identification de l'agent chargé de la vérification de l'identité et les décisions qu'il a rendues ;

c. le nom, le prénom et le numéro de l'e-ID du représentant légal ;

d. les informations relatives au lien entre l'e-ID et son titulaire ;

e. les numéros de version du système d'information pour l'émission et la révocation de l'e-ID ou des modules inhérents à ce système ;

f. la date de début et de fin de la procédure d'émission ;

g. la caractéristique technique de l'e-ID (par ex. code résultant du hachage cryptographique ou valeur hash).

Ces données, y compris les données biométriques visées à l'art. 17, al. 3, LeID, qui sont nécessaires à des fins d'enquête concernant l'obtention frauduleuse ou l'utilisation abusive d'une e-ID et conservées uniquement à cet effet, sont détruites 5 ans après la date d'expiration de l'e-ID, selon l'art. 27, al. 1, let. b, LeID.

Al. 3

L'ordonnance du département précise le format technique et les attributs pour la transmission des données, les exigences relatives à l'interface avec le système d'information pour l'émission et la révocation de l'e-ID ainsi que les normes et protocoles pour

la communication des données lors de l'émission de l'e-ID. Actuellement, ces exigences sont encore en cours d'élaboration et sont documentées sur GitHub.

Art. 28 Durée de validité

Al. 1 et 2

La validité de l'e-ID est déterminée par la date d'émission : l'e-ID est valable à partir du moment où fedpol l'a émise. Lorsque plusieurs e-ID ont été émises pour la même demande, la date d'émission de la première e-ID émise fait foi.

Lorsque la personne demande l'e-ID en même temps qu'un des documents visés à l'art. 14, let. a, LeID, la durée de validité de l'e-ID est calculée à partir de la date d'émission de l'e-ID et non de l'émission du ou des documents en question.

L'e-ID est au plus valable aussi longtemps que le document qui a été utilisé lors de la procédure d'émission.

Al. 3

Pour des raisons de sécurité de l'information, le DFJP peut fixer une durée de validité inférieure. La durée de validité de l'e-ID ne doit pas dépasser celle du document utilisé lors de la procédure d'émission.

Art. 29 Demande de révocation

Al. 1

Sur demande du titulaire ou, s'agissant d'une personne mineure ou sous curatelle de portée générale, de son représentant légal, fedpol peut révoquer l'e-ID. Une personne mineure ou sous curatelle de portée générale peut demander la révocation de sa propre e-ID sans l'autorisation de son représentant légal.

Al. 2 et 3

Pour toute demande de révocation auprès de fedpol, le titulaire de l'e-ID ou le représentant légal d'une personne mineure ou sous curatelle de portée générale doit prouver son identité à l'aide d'un document d'identité valable ou, s'il est (encore) en possession de l'e-ID, à l'aide de celle-ci.

Lorsqu'il demande la révocation de l'e-ID d'une personne mineure ou sous curatelle de portée générale, le représentant légal doit en plus prouver l'identité de la personne mineure ou sous curatelle de portée générale et qu'il est bien le représentant légal.

Absatz 4

En cas de perte de l'appareil, le titulaire ou son représentant légal peut déclarer la perte à la police ou à la représentation consulaire compétente. L'autorité compétente transmet la déclaration de perte à fedpol, qui procède immédiatement à la révocation de l'e-ID.

Art. 30 Procédure en cas de soupçon d'obtention frauduleuse ou d'utilisation abusive ou de sécurité compromise

S'il existe un soupçon d'obtention frauduleuse ou d'utilisation abusive de l'e-ID ou que la sécurité de l'e-ID est compromise, fedpol peut mener une procédure d'examen. Dans ce cadre, fedpol peut notamment vérifier une nouvelle fois l'identité du titulaire concerné, analyser les données biométriques collectées lors de la procédure d'émission, entendre le titulaire, la personne concernée ou des tiers.

fedpol peut révoquer d'office une e-ID. La révocation est automatique et journalisée. Elle est mentionnée au registre de base. En consultant la liste de révocation, le vérificateur constatera que l'e-ID en question n'est plus valide.

Art. 31 Exploitation du système d'information pour l'émission et la révocation de l'e-ID

Al. 1 et 2

fedpol procède quotidiennement à la consultation automatisée des systèmes d'information visés à l'art. 26, al. 3, LeID. Le DFJP règle les interfaces et les modalités de fonctionnement du système d'information pour l'émission et la révocation de l'e-ID.

Chapitre 4 : Accessibilité des applications aux personnes handicapées

Art. 32

L'OFIT est tenu de veiller à ce que l'application pour la présentation et la conservation des preuves électroniques et l'application pour la vérification des preuves électroniques soient également accessibles aux personnes handicapées. fedpol doit également prendre les mesures nécessaires pour garantir l'accès aux applications utilisées lors de la procédure d'émission ou de révocation de l'e-ID. Les interfaces utilisateur pour la saisie des données, mais aussi certaines parties de la procédure d'émission en font notamment partie. L'OFIT et fedpol doivent en particulier tenir compte de l'accès des applications aux personnes handicapées lors de mises à jour importantes des systèmes, appelées *Releases*. Les mesures prises contribuent à promouvoir l'inclusion numérique et à garantir l'accès aux services importants à toute personne.

Chapitre 5 : Format des preuves électroniques et normes et protocoles applicables aux processus de communication des données

Art. 33 Publication des formats, normes et protocoles

Al. 1

Cette disposition vise à créer une base solide, favorisant l'interopérabilité, pour l'utilisation sûre des preuves électroniques et leur vérification fiable.

Dans ce contexte, les preuves électroniques peuvent être, par exemple, des documents numériques, des certificats ou d'autres formes de preuves transmises dans un format électronique infalsifiable. Afin que ces preuves électroniques soient conformes au droit et suffisamment claires quelle que soit la situation dans laquelle elles sont utilisées – communication avec les autorités, transmission de certificats ou vérification d'une preuve électronique – il faut définir sur le plan technologique des conditions-cadre uniformisées, comprenant notamment des formats, tels que les formats de documents ou les formats de données structurées, ainsi que des normes et protocoles qui assurent une communication des données en toute sécurité. Les normes et protocoles contiennent principalement les recommandations techniques et organisationnelles visant à garantir l'intégrité et l'authenticité des preuves électroniques, ainsi que l'interopérabilité entre les acteurs connectés au système.

L'OFJ est chargé de créer et de maintenir un cadre favorable à l'interopérabilité en vue de l'utilisation sûre des preuves électroniques dans l'infrastructure de confiance.

Al. 2

L'OFJ publie les formats et les normes et protocoles sur le site Internet de la Confédération. Il peut également renvoyer à des sites Internet qu'il gère, tel GitHub. La publication se fait sous la forme de recommandations (bonnes pratiques). Les bonnes pratiques contiennent des explications détaillées sur la manière dont les preuves électroniques doivent être créées, vérifiées et utilisées de manière sûre et efficace. Leur publication permet à tous les acteurs de se référer aux mêmes normes, sans pour autant limiter leur potentiel de développement et d'innovation. Les bonnes pratiques contribuent à la sûreté et à l'interopérabilité du système pour l'utilisation et la vérification des preuves électroniques, tout en renforçant la confiance dans une infrastructure numérique conviviale et facilement accessible.

Art. 34 Développement des recommandations

Al. 1 et 2

La publication des recommandations visées à l'art. 33 (bonnes pratiques) implique que l'OFJ adapte en permanence les formats et les normes au dernier état de la technique et aux exigences légales. Les acteurs privés profitent également des dernières innovations sur les plans technologiques et juridiques et peuvent ainsi tenir leurs systèmes à jour.

Pour le développement des bonnes pratiques, l'OFJ peut faire appel à des experts internes et externes, à des institutions spécialisées et à des organisations de normalisation.

Al. 3

Les modifications apportées aux bonnes pratiques doivent également être publiées. L'art. 33, al. 2, s'applique par analogie à leur publication.

Art. 35 Formats, normes et protocoles obligatoires

Al. 1

Le DFJP peut déclarer obligatoire, dans une ordonnance du département, l'intégralité ou une partie des formats pour les preuves électroniques et des normes et protocoles applicables aux processus de communication des données. L'obligation vise les participants à l'infrastructure de confiance, en particulier les émetteurs et les vérificateurs de preuves électroniques ainsi que les fournisseurs d'applications au sens de l'art. 18, al. 4 et 5, LeID. L'instauration de l'obligation s'imposera notamment lorsque les formats et les normes appliqués ne garantissent pas l'interopérabilité requise entre les différents systèmes et les différents acteurs. Si l'interopérabilité fait défaut, les données ne peuvent pas être échangées de manière efficace et sans erreur entre les services concernés. Les formats, normes et protocoles obligatoires valent dans tous les cas pour l'application de la Confédération pour la conservation et la présentation des moyens de preuves électroniques au sens de l'art. 8, al. 1, LeID.

Par ailleurs, des formats, normes et protocoles obligatoires sont nécessaires pour remplacer des versions obsolètes par de nouvelles versions plus sûres et plus efficaces. En outre, l'obligation peut contribuer à faire avancer un éventuel processus de normalisation et à accélérer la mise en œuvre des progrès techniques. Sans règlementation contraignante, l'utilisation d'un trop grand nombre de solutions différentes risque d'aboutir à des fragmentations et à des pertes d'efficacité.

Al. 2

Avant de déclarer un format, une norme ou un protocole obligatoire, le DFJP consulte tous les acteurs et les groupes d'intérêt pertinents, afin de s'assurer que les règles proposées sont applicables en pratique et acceptées par les parties concernées. L'objectif est d'obtenir des informations sur la praticabilité des changements envisagés et d'identifier rapidement les défis éventuels.

Ces consultations sont également un moyen de promouvoir conjointement et de manière consolidée le processus de normalisation et d'harmonisation au sein de l'écosystème suisse. L'implication des parties intéressées garantit une large acceptation et une mise en œuvre aussi fluide que possible. En outre, elle favorise une utilisation consolidée et uniforme des normes.

Al. 3

Les formats et les normes et protocoles obligatoires entrent en vigueur au plus tôt trois mois après avoir été déclarés comme tels par le DFJP. Ce délai permet aux parties concernées de se préparer. Durant cette période, elles peuvent adapter leurs systèmes et leurs processus afin de se conformer aux exigences.

Selon l'ampleur et la complexité des modifications, le DFJP peut toutefois prévoir un délai plus long si la déclaration de force obligatoire requiert une intervention importante dans l'infrastructure ou les systèmes existants. Par exemple, pour une adaptation et implémentation complètes, il faudrait prévoir une période de transition de plusieurs mois, voire de plusieurs années. Il est important de laisser suffisamment de temps aux acteurs pour mettre à jour leurs systèmes et assurer une certaine compatibilité en permanence, en particulier lors de l'introduction de nouvelles technologies ou de formats plus sûrs. Cette flexibilité permet de mener à bien le processus de mise à jour sans perturbations ni retards inutiles.

En cas d'urgence, lorsqu'il existe un risque immédiat pour la fonctionnalité des preuves électroniques ou de l'infrastructure de confiance, l'OFIT peut procéder immédiatement aux ajustements nécessaires. La loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI)[11] en constitue le fondement. De telles mesures d'urgence sont particulièrement pertinentes en cas de menaces, dangers, vulnérabilités et failles de sécurité susceptibles de compromettre l'intégrité ou la confidentialité des données. Dans ce type de situations, il faut pouvoir agir vite pour éviter des dommages plus importants ou des failles de sécurité. Il n'est alors pas nécessaire de déclarer certains formats, normes et protocoles obligatoires.

Art. 36 Mention relative au non-respect des formats, normes et protocoles

Une mention n'est pas seulement inscrite au registre de confiance en cas de soupçon d'utilisation inappropriée de l'infrastructure de confiance ou des preuves électroniques, mais aussi lorsque l'OFJ apprend que les émetteurs ou vérificateurs n'ont pas respecté les formats, normes et protocoles obligatoires. Dans ce cas, l'OFJ peut mener une procédure de contrôle portant sur la conformité technique ou juridique. En cas de non-conformité, l'art. 18 s'applique par analogie pour l'inscription d'une mention au registre de confiance, et l'art. 19 pour son effacement. Il en va de même des fournisseurs d'applications au sens de l'art. 18, al. 4 et 5, LeID.

Chapitre 6 : Émoluments

Art. 37 Émoluments relatifs aux registres

Dès l'entrée en vigueur de la LeID, il sera possible, sur les plans technique et opérationnel, de proposer rapidement aux habitants de la Suisse et aux Suisses de l'étranger

[11] RS **128**

un moyen d'identification numérique (e-ID) et d'autres preuves numériques de haute qualité (par ex. extrait du casier judiciaire, permis de conduire électronique ou autres preuves dans le domaine de la santé ou des droits politiques).

Les frais totaux de l'infrastructure de confiance sont estimés à 20,8 millions de francs par an, dont près de la moitié est générée par l'exploitation de l'infrastructure de confiance. Les frais d'exploitation comprennent les frais d'inscription au registre de base, les frais liés à la vérification des demandes d'inscription et d'actualisation des données dans le registre de confiance ainsi que les autres frais d'exploitation de l'infrastructure de confiance. Étant donné que les frais liés à l'utilisation reposeront sur des hypothèses, le montant des émoluments devra faire l'objet d'examens réguliers une fois que le système sera entré dans la phase d'exploitation.

Les émoluments dépendent des coûts annuels de l'infrastructure de confiance, qui sont formés des dépenses de l'unité e-ID de l'OFJ et de l'OFIT, à savoir des coûts de personnel directs de l'unité, des frais généraux, des coûts des postes de travail, des frais de matériel et d'exploitation de l'OFIT, des frais de licence et des amortissements.

Coûts annuels de l'infrastructure de confiance qui entrent dans le calcul des émoluments :	
Coûts de personnel directs	CHF 3,96 millions
Frais généraux (art. 4, al. 2, let. c, OGEmol [20%])	CHF 0,79 million
Coûts des postes de travail (art. 4, al. 2, let. b OGEmol) pour 22 postes de travail ; montant selon le tableau de l'AFF pour l'année 2025	CHF 0,31 million
Frais de matériel et d'exploitation OFIT	CHF 3,0 millions
Frais de licence	CHF 0,1 million
Amortissements comptables sur les installations (infrastructure de confiance)	CHF 2,67 millions
Total	**CHF 10,83 millions**

Les autres coûts, d'un montant de 9,93 millions de francs, ne seront pas pris en compte dans le calcul des émoluments, car l'exploitation de l'infrastructure de confiance répond aussi à un intérêt public. La Confédération a en effet un intérêt à développer et à exploiter un système informatique ou de communication moderne pour l'économie et la population.

Al. 1

La part des coûts du registre de base par rapport à ceux de l'infrastructure de confiance pris en compte dans le calcul des émoluments est estimée à un tiers, soit des coûts de 3,61 millions de francs. D'autres utilisations de l'infrastructure sont également envisagées –notamment en lien avec le permis de conduire électronique (mDL), dans le domaine de la santé ou encore dans le contexte des droits politiques –, qui concernent

les autorités tant fédérales que cantonales. Les autorités sont donc les premières à bénéficier de l'infrastructure de confiance ainsi que de l'utilisation des preuves électroniques telles que l'e-ID. Vu ces circonstances, on peut partir du principe que près de 60 % des coûts totaux du registre de base, soit 2,17 millions de francs, seront générés par l'utilisations du système par les autorités. Bien que la LeID prévoie que les autorités ne paient pas d'émoluments, la part des coûts induits par leur utilisation de l'infrastructure de confiance doit être prise en compte dans le calcul de l'émolument dans son ensemble. Ainsi les coûts restants (40 %, soit 1,44 million de francs) sont imputables à l'utilisation de l'infrastructure de confiance par les acteurs du secteur privé. Pour cette utilisation, le montant de l'émolument est calculé à partir des frais d'exploitation restants et du nombre d'inscriptions prévu.

Le calcul des émoluments couvrira, dans la mesure du possible, une période de planification assez longue, en intégrant de possibles développements futurs. Dans ce contexte de prévisions à long terme, on estime que les inscriptions annuelles au registre de base représenteront en moyenne 20 % des nouvelles inscriptions dans les registres du commerce cantonaux[12]. Ces projections reposent sur une estimation prudente du nombre d'inscriptions, qui tient compte à la fois de la grandeur du groupe-cible et du caractère facultatif de l'enregistrement. Seules les nouvelles inscriptions sont prises en compte, étant donné que les émetteurs et vérificateurs gèrent eux-mêmes leurs données dans le registre de base, c'est-à-dire qu'ils procèdent eux-mêmes aux modifications et adaptations. L'utilisation du registre de base n'est toutefois pas réservée aux entreprises qui sont déjà inscrites au registre du commerce, mais aussi aux autres entreprises et aux particuliers. Malgré ce groupe-cible élargi, l'utilisation effective du registre est estimée de façon prudente. Les 20 % sont donc une estimation basse de la participation effective.

Il résulte des coûts totaux restants de 1,44 millions de francs, mis en relation avec nombre d'inscriptions au registre de base estimé, un émolument de 150 francs par inscription

Al. 2

Selon l'art. 31 LeID, un émolument est perçu pour les données dont les émetteurs et les vérificateurs demandent l'inscription au registre de confiance. Contrairement à l'inscription au registre de base, l'inscription au registre de confiance de l'identifiant d'un émetteur ou d'un vérificateur privé requiert un examen de la demande d'inscription conformément à l'art. 10 ou un examen de la mise à jour des données du registre de confiance conformément à l'art. 11, al. 4. Un émolument a été calculé sur une base forfaitaire en fonction de la charge de travail attendue. Il s'élève à 350 francs par examen.

[12] La moyenne des nouvelles inscriptions se fonde sur les tableaux comparatifs des rapports annuels cantonaux, mis à disposition par l'Office fédéral du registre du commerce conformément à l'art. 5a de l'ordonnance sur le registre du commerce (voir Statistiques du registre du commerce).

Art. 38 Émoluments pour la vérification de l'identité sur place

Al. 1

Les cantons fixent le montant des émoluments pour la vérification de l'identité effectuée sur place dans le cadre de la procédure d'émission de l'e-ID. Conformément à l'ordonnance, ils peuvent percevoir les émoluments suivants :

a. en cas d'émission de la seule e-ID, le montant de l'émolument s'élève à 29 francs au plus ;

b. en cas d'émission combinée avec une carte d'identité et/ou un passeport, le montant de l'émolument s'élève à 15 francs au plus, en sus des émoluments dus pour l'émission de la carte d'identité ou du passeport.

Cette réglementation assure une structure claire des émoluments perçus en fonction de la variante choisie pour l'émission de l'e-ID et empêche que les cantons demandent pour l'e-ID un montant dépassant les frais de l'examen d'identité effectué sur place.

Al. 2

Selon l'art. 14, al. 3, de l'ordonnance du 7 octobre 2015 sur les émoluments du Département fédéral des affaires étrangères[13], les représentations consulaires peuvent percevoir un émolument de 28 francs au plus pour la vérification de l'identité sur place.

Chapitre 7 : Dispositions finales

Art. 39 Modification d'autres actes

Le projet propose la modification d'autres actes. Ces adaptations visent notamment à favoriser l'utilisation de l'e-ID à la fois dans le monde virtuel et dans le monde réel. L'e-ID doit toujours être acceptée comme preuve d'identité, en particulier par les autorités, indépendamment du fait que l'identification soit effectuée en ligne ou sur place. L'e-ID ne remplace pas les documents d'identité physiques, mais doit pouvoir être présentée à leur place. Grâce à l'application pour la vérification des preuves électroniques, les autorités peuvent par exemple vérifier facilement une e-ID lors d'un contact direct avec une personne. Elles devront accepter l'e-ID (art. 24 LeID), même si cela se fait dans le cadre d'un processus qui ne requiert pas de copie d'un document d'identité.

Art. 40 Entrée en vigueur

[13] RS **191.11**

L'art. 35, al. 2, let. b, LeID prévoit une mise à disposition échelonnée du système visé à l'art. 15 P-OeID, permettant au titulaire de stocker les copies de sécurité de ses preuves électroniques. Le système pour les copies de sécurité sera mis en place dans un délai de deux ans à compter de l'entrée en vigueur de l'ordonnance. L'adaptation éventuelle de l'application pour la vérification des preuves électroniques conformément à l'art. 16 et la vérification de l'identité sur place visée à l'art. 24 P-OeID devront également être réalisées dans un délai de deux ans à compter de l'entrée en vigueur de l'ordonnance.

4. Commentaires relatifs à l'annexe 1 (modification d'autres actes législatifs)

Avec l'introduction de la loi et de l'ordonnance sur l'e-ID, le titulaire d'une e-ID pourra s'identifier en présentant la preuve d'identité électronique émise par la Confédération, ou – comme jusqu'à présent – au moyen d'un document d'identité. Afin de tenir compte notamment de la possibilité de présenter l'e-ID, diverses ordonnances du Conseil fédéral doivent être modifiées.

À noter que certaines ordonnances du Département fédéral de justice et police devront également être modifiées au niveau de l'Office concerné, comme l'ordonnance de la CFMJ sur le blanchiment d'argent, OBA-CFMJ.

4.1 Ordonnance du 12 avril 2006 sur le système d'information central sur la migration[14]

Art. 9, let. B, ch. 9

Tous les citoyens étrangers vivant en Suisse sont enregistrés dans le Système central d'information des migrations (SYMIC) avec des données personnelles uniformes. Toutes les fonctions et activités, de l'entrée en Suisse au départ en passant par le séjour, sont traitées via SYMIC. Plus de 30 000 collaborateurs des offices des migrations de la Confédération, des cantons et de certaines communes ainsi que de divers offices du travail travaillent avec cette application.

4.2 Ordonnance du 20 septembre 2002 sur les documents d'identité[15]

28, let. l

L'objectif du traitement des données visé à l'article 28 doit être ajouté dans une nouvelle lettre l. Le système ISA sert notamment à vérifier l'identité lors de l'émission d'une e-ID conformément à l'art. 16, LeID.

[14] RS **142.513**

[15] RS **143.11**

Le système ISA recueille toutes les données pertinentes pour l'établissement de passeports et de cartes d'identité suisses dans le système ISA. Le cercle des utilisateurs au sein des autorités fédérales, des centres de saisie cantonaux et des représentations consulaires compte plusieurs centaines de personnes.

Annexe 1 (Art. 30, al. 1)

Les autorisations des autorités concernées pour accéder à ISA et l'étendue des droits d'accès sont précisées à l'annexe 1. Le Domaine Service national d'identité (fedpol SID) reçoit les mêmes autorisations que le service de police compétent de la Confédération (fedpol Pol, art. 12, al. 2, let. d et f, et art. 12, al. 3, LDI) pour traiter ou consulter les données enregistrées dans ISA, à l'exception de la signature, des empreintes digitales et de l'état des documents d'identité. fedpol SID recevra en outre les données suivantes : inscriptions relatives à l'interdiction d'émettre des documents, déclaration de perte/révocation.

4.3 Ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[16]

Art. 11, al. 5

Jusqu'à présent, seule l'adresse postale privée des particuliers et des représentants d'organisations pouvait être traitée dans les systèmes IAM, selon l'art. 9, let. b, OIAM. Désormais, il est également possible de traiter dans les systèmes IAM, les services d'annuaire et la base centralisée des identités (art. 13, OIAM) l'adresse postale privée des personnes visées à l'art. 8, OIAM, mais pas des personnes visées à l'art. 9, let. a, OIAM, d'où les services assortis de deux astérisques dans l'annexe. Les données des personnes visées à l'article 8 assorties de deux astérisques ne peuvent être traitées et communiquées qu'aux systèmes d'information de l'administration fédérale centrale. Le respect de cette restriction doit être garanti par les systèmes IAM correspondants. La liste des données personnelles visée à l'art. 15, al. 2, OIAM, comprend dès lors l'adresse postale privée lorsque celle-ci peut être communiquée à un système d'information en aval. Par exemple, la communication de l'adresse postale privée à un exploitant externe selon l'art. 17 OIAM n'est pas autorisée.

Cette limitation du traitement des données des personnes visées à l'art. 8, OIAM concerne uniquement les services assortis de deux astérisques. Elle ne s'applique pas à l'adresse postale privée des personnes visées à l'art. 9, let. b, OIAM. En effet, il est déjà possible de traiter l'adresse postale privée, voire de la communiquer à des exploitants externes.

Art. 19, al. 1

[16] RS **172.010.59**

L’e-ID peut être utilisée comme preuve d’identité électronique, mais pas comme autorisation d’accès. L’e-ID permet de prouver sa propre identité.

Art. 19, al. 3

Lors de la présentation de l’e-ID, le contenu de l’e-ID est transmis au vérificateur sous forme du paquet de données visé à l’art. 7, al. 1, LeID.

Annexe, let. g

Les données supplémentaires contenues dans l’e-ID selon l’art. 15, al. 2, LeID (notamment numéro de l’e-ID, émetteur et date d’émission) doivent également pouvoir être traitées par un système IAM. Ces informations doivent également pouvoir être stockées dans les mémoires d’audit correspondantes pour les scénarios de recherche.

Le traitement des données contenues dans l’e-ID est autorisé car ces données figurent déjà dans les autres lettres de l’annexe.

4.4 Ordonnance du 19 octobre 2022 sur le casier judiciaire[17]

Art. 52 Absatz 2

L’art. 52, al. 2 et 3, OCJ définit les exigences relatives à la preuve de l’identité visées à l’art. 54, al. 3, LCJ. Conformément à l’art. 52, al. 2, OCJ, seuls les documents d’identité officiels suivants sont reconnus : passeport, carte d’identité et permis de séjour pour étrangers. Dans le cadre de la procédure de commande en ligne, la preuve d’identité électronique (e-ID) au sens de la loi du 20 décembre 2024 sur l’e-ID est également acceptée.

4.5 Ordonnance du 27 octobre 1976 réglant l’admission à la circulation routière[18]

Art. 11, al. 3 et 4

Utilisation de l’e-ID pour les demandes de permis de conduire
La liste des preuves d’identité figurant à l’art. 11, al. 3, OAC, doit être complétée par l’e-ID. L’utilisation de l’e-ID permet de poursuivre la numérisation des demandes de permis d’élève conducteur, de permis de conduire ou d’autorisations de transport professionnel de personnes, pour autant que les cantons souhaitent y recourir et mettre en œuvre les mesures correspondantes. Comme l’identité est déjà vérifiée lors de l’émission d’une e-ID conformément à la LeID (en ligne par fedpol [art. 17, al. 1, let. a, LeID] ou en personne auprès de services ou d’autorités désignés à cet effet [art. 17, al. 1, let. b, LeID]), il n’est pas nécessaire de se présenter en personne dans ce cas.

[17] RS **331**

[18] RS **741.51**

Afin que les autorités puissent également traiter les demandes reçues par voie électronique, la personne chargée de leur réception doit pouvoir confirmer l'identité sous une forme électronique appropriée. Il est donc proposé de compléter l'art. 11, al. 4, OAC et l'annexe 4 OAC.

4.6 Ordonnance du 30 novembre 2018 sur le système d'information relatif à l'admission à la circulation[19]

Annexes 1 et 2

Adresse e-mail et numéros de téléphone
La gestion de l'adresse e-mail ainsi que des numéros de téléphone (tant les numéros de téléphone mobile et que les numéros de téléphone fixe) constitue un élément essentiel de la communication numérique entre les autorités et les citoyens. Elle contribue à faciliter l'administration des deux côtés. Ces données sont nécessaires pour le processus de délivrance du permis d'élève conducteur électronique (ePEC) et seront également requises à l'avenir pour d'autres preuves et documents électroniques.

Selon l'art. 14 de l'ordonnance sur l'admission à la circulation (OAC)[20], les autorités d'immatriculation transmettent les données personnelles des demandeurs au sous-système SIAC-Personnes. Ainsi, la «Demande de délivrance d'un permis d'élève conducteur, d'un permis de conduire ou d'une autorisation pour le transport professionnel de personnes» selon l'annexe 4 OAC doit être complétée avec l'adresse e-mail et le numéro de téléphone mobile.

Afin que ces attributs puissent être gérés dans le système d'information relatif à l'admission à la circulation (SIAC), le terme générique «numéros de téléphone» ainsi que «adresse e-mail» doivent être intégrés à l'ordonnance sur le système d'information relatif à l'admission à la circulation (OSIAC)[21] comme suit : à l'annexe 1, ch. 22, et à l'annexe 2, ch. 112, 212, 222, 223 et 232.

Numéro AVS
Le numéro AVS est un identifiant unique d'une personne résidant en Suisse (ou enregistrée auprès d'une assurance sociale ou en activité professionnelle). Il s'avère donc utile pour optimiser les processus administratifs. Depuis la révision de la loi sur l'AVS, de nombreuses autorités cantonales utilisent déjà ce numéro comme identifiant unique. Cela répond au principe de protection des données relatif à l'exactitude des données et réduit les charges administratives, allégeant ainsi le travail des autorités d'exécution. Les coûts liés à la rectification des erreurs d'identification de noms et les inconvénients pour les personnes concernées peuvent ainsi être largement évités.

L'OSIAC doit donc être complétée par le numéro AVS à l'annexe 1, ch. 21, et à l'annexe 2, ch. 111 et 211.

---

19 RS **741.58**

20 RS **741.51**

21 RS **741.58**

Numéros d'identification commerciale (IDE, numéro REE, numéro de partenaire commercial)
Par souci d'exhaustivité, les identifiants uniques des personnes morales, qui doivent être ajoutés dans le cadre des modifications liées à l'introduction de l'e-ID sont regroupés sous le terme générique de «numéros d'identification professionnelle».

- Le numéro d'identification des entreprises (IDE) et le numéro du registre des entreprises et établissements (numéro REE) représentent pour les personnes morales l'équivalent du numéro AVS et servent donc d'identifiants uniques. L'Office fédéral de la douane et de la sécurité des frontières (OFDF) prévoit d'utiliser l'IDE et les numéros REE dans le cadre de la facturation de la redevance sur le trafic des poids lourds liée aux prestations (RPLP)[22], et de les extraire à cette fin du système IAC pour une exécution efficace[23]. Comme pour le numéro AVS, l'utilisation de l'IDE et du numéro REE permet d'optimiser davantage la qualité des données.
- Le numéro de partenaire commercial est la clé permettant d'identifier de manière univoque les partenaires commerciaux lors de la facturation et de simplifier la gestion des données de base.

Le terme générique «numéros d'identification professionnelle» doit donc être inscrit dans l'OSIAC comme suit : à l'annexe 1, ch. 21, et à l'annexe 2, ch. 212, 221, 222, 231, 232 et 241.

Langue de correspondance
Le terme «langue» étant trop imprécis, il convient de le préciser par «langue de correspondance» dans l'OSIAC, annexe 1, ch. 22.

4.7 Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication[24]

Art. 20a, al. 1, phrase introductive, et let. d, al. 2, let. a, phrase introductive, et ch. 3, al. 4 et 5

La vérification de l'identité de la personne physique est impérative pour les services de communication mobile. La procédure de ladite vérification d'identité n'est pas règlementée. Il est possible de procéder à l'identification en présence de la personne physique, par vidéo ou en ligne. Pour cette dernière possibilité les normes de sécurité et de qualité définies dans la circulaire de la FINMA 2016/7 « Identification par vidéo et en ligne » doivent être respectées. Afin de garantir une identification sûre, la preuve

[22] RS **641.81**

[23] Dans le cadre de l'art. 89d, let. f de la loi sur la circulation routière (LCR, RS **741.01**).

[24] RS **780.11**

d'identité doit être valable le jour de sa saisie, c'est-à-dire celui où la preuve en question est présentée au fournisseur ou au revendeur, respectivement est utilisé en ligne.[25]

L'art. 20*a* OSCPT est modifié pour tenir compte de la preuve d'identité électronique émise par la Confédération pour les personnes physiques (e-ID) qui sera introduit par la nouvelle LeID[26].

À l'al. 1, l'énumération des documents est donc complétée par l'e-ID (*let. d*).

L'e-ID consiste en un paquet de données servant de preuve d'identité électronique (art. 7, LeID). Ainsi, le terme plus général de « preuve de l'identité » (*Identitätsnachweis*) est préféré et remplace donc le terme « document » dans la phrase introductive.

A *l'al. 2,* l'unique modification consiste dans le remplacement de « preuve de l'identité » au lieu de « document », plus adéquat pour tenir compte de l'e-ID.

L'*al. 3* reste inchangé.

L'*al. 4 première phrase* reste inchangée. Le terme « document » peut continuer à être utilisé, car il vise les documents cités à l'al. 1 let. a à c et non pas l'e-ID.

Une *seconde phrase* est rajoutée afin de tenir compte des informations spécifiques à récolter en cas d'usage d'une e-ID. Seules les données selon l'al. 2 ainsi que la photographie sont récoltées, à la place d'une copie du document d'identité physique. En effet, l'e-ID inclut des informations que le passeport, la carte d'identité ou le titre de séjour ne contiennent pas, principalement le numéro AVS (art. 15 al. 1 let. i, LeID). Il serait disproportionné et contraire à l'art. 6 LPD de demander à celui qui choisit de s'identifier avec une e-ID de livrer cette information, alors qu'il n'aurait pas eu à le faire s'il avait choisi de s'identifier avec un document d'identité physique.

De plus, les données requises pour la vérification de l'authenticité et de l'intégrité, telle que la signature électronique (art. 5 al. 2, LeID), doivent également être saisies. En effet, un fournisseur ou un revendeur n'a pas l'obligation d'examiner minutieusement une pièce d'identité pour s'assurer de son authenticité, mais est tenu de n'accepter le document présenté que si son authenticité est plausible[27]. Ainsi, seulement un contrôle sommaire doit exister. Pour l'e-ID, l'absence de tout contrôle permettrait de faire inscrire des données erronées ou de présenter une photographie d'une autre personne auprès d'un fournisseur ou d'un revendeur peu scrupuleux, et ce, de manière aisée. En outre, la production de ces données de vérification sera vraisemblablement rapide,

---

25 Voir le rapport explicatif du 15.11.2023 relatif à la révision partielle d'ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (**LSCPT**), ad art. 20*a*, p. 20 ss.

26 Loi fédérale du 20 décembre 2024 sur l'identité électronique et d'autres moyens de preuves électroniques (**Loi sur l'e-ID**, **LeID** ; **FF 2023 2842**).

27 Voir le rapport explicatif précité, ad art. 20a, p. 20.

de sorte que sa récolte et sa transmission ne devraient pas prendre davantage de temps que pour un document physique.

L'*al. 5* contient la règle de la seconde phrase de l'ancien al. 4 avec les adaptations dues à l'e-ID. Afin d'assurer une meilleure lecture, un nouvel alinéa 5 a été créé. S'agissant des données récoltées, le renvoi aux alinéas concernés a donc été complété avec l'al. 4. Le délai pour la transmission des données du revendeur au fournisseurs de services de télécommunication demeure inchangé (trois jours).

4.8 Ordonnance du 29 août 2012 sur la poste[28]

Art. 35e Abs. 2 Bst. c und Abs. 3

Les utilisateurs du système de distribution hybride, à savoir les expéditeurs ainsi que les destinataires, doivent s'identifier et s'authentifier auprès de la Poste (al. 1). Pour l'identification des personnes, l'e-ID peut être utilisée conformément à la let. c. Il est ainsi précisé que, dans le cadre du service universel, l'e-ID sert de preuve d'identification électronique. Grâce à l'e-ID, il n'est plus nécessaire que la Commission fédérale de la poste détermine les preuves d'identification électronique pouvant être utilisées pour identifier les utilisateurs (al. 3).

.9 Ordonnance du 9 mars 2007 sur les services de télécommunication[29]

Art. 41 Abs. 5 Bst. b

La loi sur l'e-ID crée la base pour l'émission de preuves d'identité électroniques permettant à chaque individu de s'identifier numériquement leur identité dans l'espace numérique grâce aux données confirmées par l'État. Elle établit ainsi le fondement de l'e-ID, grâce à laquelle les personnes peuvent prouver leur identité. Dans le cadre du contrôle de l'âge en lien avec le blocage obligatoire de l'accès aux services à valeur ajoutée lorsqu'il s'agit de personnes mineures, il est désormais également possible d'utiliser son e-ID pour prouver son identité.

4.10 Ordonnance du 6 octobre 1997 sur les ressources d'adressage dans le domaine des télécommunications[30]

Art. 4 Abs. 1ter und Art. 4 Abs. 1ter Bst. a

[28] RS **783.01**

[29] RS **784.101.1**

[30] RS **784.104**

La loi sur l'e-ID crée la base pour l'émission de preuves d'identité électroniques permettant à chaque individu de s'identifier numériquement leur identité dans l'espace numérique grâce aux données confirmées par l'État. Elle établit ainsi le fondement de l'e-ID, grâce à laquelle les personnes peuvent prouver leur identité. Lors de l'attribution des éléments d'adressage, le requérant peut désormais également utiliser son e-ID pour prouver son identité.

4.11 Ordonnance du 5 novembre 2014 sur les domaines Internet[31]

Art. 24 Abs. 3 Bst. a

La loi sur l'e-ID crée la base pour l'émission de preuves d'identité électroniques permettant à chaque individu de s'identifier numériquement leur identité dans l'espace numérique grâce aux données confirmées par l'État. Elle établit ainsi le fondement de l'e-ID, grâce à laquelle les personnes peuvent prouver leur identité. Lors de l'attribution de noms de domaine, il est désormais également possible d'utiliser son e-ID pour prouver son identité et faire vérifier les conditions d'attribution.

4.12 Ordonnance du 4 décembre 2000 sur la procréation médicalement assistée[32]

Art. 21 Abs. 2

Le requérant peut en principe attester de son identité, soit par l'envoi d'une copie d'un document d'identité (passeport, carte d'identité ou document d'identité équivalent), soit en utilisant son e-ID au sens de la LeID. La possibilité de soumettre une copie du document d'identité en ligne a déjà fait ses preuves lors de la commande d'extraits du casier judiciaire. Avec l'introduction de l'e-ID, une variante numérique supplémentaire de la preuve d'identité est proposée, sans qu'il soit nécessaire de soumettre une copie.

4.13 Ordonnance du 22 mars 2017 sur le dossier électronique du patient[33]

Le fournisseur d'un moyen d'identification requis pour accéder au dossier électronique du patient (DEP) doit vérifier l'identité de la personne qui en fait la demande. À l'avenir, l'e-ID devrait également permettre d'apporter la preuve de l'identité.

Avec l'adoption de la loi sur l'e-ID (LeID), la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP)[34] est modifiée comme suit : seuls les fournisseurs privés de moyens d'identification devront être certifiés par un organisme reconnu (art. 11,

[31] RS **784.104.2**
[32] RS **810.112.2**
[33] RS **816.11**
[34] RS **816.1**

let. c, LDEP). Les cantons, en tant que fournisseurs de moyens d'identification[35], ne sont pas soumis à cette obligation de certification. Toutefois, les moyens d'identification délivrés par les cantons doivent répondre aux mêmes exigences que ceux émis par des fournisseurs privés. Les cantons sont responsables du respect de ces exigences.

Au même titre que ceux des fournisseurs privés, les moyens d'identification délivrés par les cantons doivent pouvoir permettre aux professionnels de la santé ainsi qu'aux patients de s'authentifier auprès du système du DEP. Le système exploité par la Chancellerie fédérale (AGOV) pour l'authentification des personnes physiques avec l'e-ID devra désormais également pouvoir être utilisé à cette fin.

Art. 9, al. 2, let. e

Les moyens permettant aux professionnels de la santé de s'authentifier pour accéder au dossier électronique du patient (DEP) sont élargis aux moyens d'identification délivrés par les cantons. L'authentification par AGOV est également autorisée.

Art. 16, al. 1, let. a–c

Les moyens permettant aux patients de confirmer leur consentement à la création d'un DEP sont élargis aux moyens d'identification délivrés par les cantons (let. b). La confirmation du consentement via AGOV est également autorisée (let. c).

Art. 17, al. 1, let. c

Les moyens permettant aux patients de s'authentifier pour accéder au dossier électronique du patient (DEP) sont élargis aux moyens d'identification délivrés par les cantons. L'authentification via AGOV est également autorisée.

Art. 24, al. 1

La personne qui demande un moyen d'identification pour accéder au dossier électronique du patient (DEP) peut désormais également s'identifier auprès du fournisseur de moyens d'identification avec son eID.

Art. 27a Moyen d'identification émis par les cantons

Comme seuls les fournisseurs privés de moyens d'identification doivent être certifiés (art. 11, let. c LDEP), il faut définir qui assume la responsabilité de garantir que seuls des moyens d'identification sûrs sont utilisés pour l'authentification lors de l'accès au dossier électronique du patient (DEP). L'al. 1 attribue cette responsabilité aux cantons, en tant que fournisseurs de ces moyens. Les cantons doivent s'assurer que les moyens d'identification qu'ils délivrent répondent aux exigences des art. 23 à 27 de l'ordonnance sur le dossier électronique du patient (ODEP) ainsi qu'aux précisions des al. 2

[35] Les cantons de Genève et de Vaud proposent désormais des moyens d'identification pour accéder au DEP.

et 3 de l'art. 31. Ces précisions figurent en annexe 8 de l'ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient (ODEP-DFI)[36].

Les cantons communiquent les moyens d'identification qu'ils délivrent à l'Office fédéral de la santé publique (OFSP) (al. 2). Selon l'al. 3, cet office veille à la publication de ces moyens d'identification – de manière analogue à la publication des certificats des fournisseurs privés de moyens d'identification selon l'art. 33, al. 2.

La clause de protection relative aux moyens d'identification délivrés par des fournisseurs certifiés (art. 37, al. 1, let. b) s'applique également aux moyens d'identification délivrés par les cantons (al. 4). L'OFSP peut exiger des cantons les documents nécessaires à l'évaluation des circonstances.

Art. 28, al. 2

Seuls les fournisseurs privés de moyens d'identification doivent être certifiés. L'accréditation concerne donc uniquement les services qui certifient ces fournisseurs privés de moyens d'identification. L'al. 2 est précisé en ce sens.

Art. 31, titre et al. 1

Seuls les émetteurs privés de moyens d'identification doivent être certifiés. Les cantons sont responsables des moyens d'identification qu'ils émettent. Le titre et l'al. 1 sont précisés en ce sens.

Art. 32, al. 3

L'organisme de certification délivre le certificat uniquement aux émetteurs privés de moyens d'identification, pour autant que les exigences applicables soient remplies. Les émetteurs cantonaux de moyens d'identification ne sont pas certifiés et ne reçoivent donc pas de certificat. L'al. 3 est précisé en ce sens.

Art. 36, al. 1

Seuls les émetteurs privés de moyens d'identification sont tenus de notifier au service de certification les adaptations techniques ou organisationnelles essentielles. Cette obligation ne s'applique pas aux émetteurs cantonaux de moyens d'identification, la responsabilité des moyens d'identification cantonaux incombant aux cantons. L'al. 1 est précisé en ce sens.

[36] RS **816.111**

4.14 Ordonnance du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques[37]

Art. 5, al. 1bis

Les prestataires de services de certification doivent établir l'identité exacte des personnes qui demandent la délivrance d'un certificat réglementé (art. 9, al. 1 de la loi fédérale sur la signature électronique [SCSE, RS 943.03]). Le requérant doit en principe se présenter en personne auprès d'un prestataire de services de certification reconnu (art. 5, al. 1 de l'ordonnance du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques). L'obligation de se présenter en personne est levée lorsque l'identité est prouvée par une e-ID. Ce nouvel alinéa clarifie une fois de plus la situation concernant l'identification par e-ID.

Art. 6, al. 1

L'obligation pour une personne qui demande un certificat réglementé pour une entité IDE qui n'est pas une personne physique de présenter un passeport, une carte d'identité suisse ou un document d'identité reconnu pour l'entrée en Suisse est clarifiée en ce sens qu'une e-ID émise conformément à la loi sur l'e-ID peut également être utilisée.

4.15 Ordonnance du 11 novembre 2015 sur la lutte contre le blanchiment d'argent et le financement du terrorisme[38]

Art. 17, al. 3, let. b et 3bis

L'art. 17, al. 3 de l'ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme (OBA) précise, pour les négociants au sens de l'art. 2, al. 1, let. b OBA, la procédure selon laquelle ils doivent procéder à l'identification de la partie contractante conformément aux dispositions relatives à la lutte contre le blanchiment d'argent.

En pratique, seuls les documents d'identité valides sont acceptés pour l'identification de la partie contractante. Ceci est contrôlé par la révision interne et externe. La lettre b doit donc être complétée en fin de texte par « … et est valide », afin que la pratique en vigueur soit reflétée et que le texte de l'ordonnance concorde avec la nouvelle let. b de l'al. 3bis.

Dans un souci de clarté, il est prévu de préciser, par le nouvel al. 3bis de l'art. 17 OBA, que la vérification de l'identité du cocontractant peut également être effectuée au

[37] RS **943.032**

[38] RS **955.01**

moyen de l'e-ID émise conformément à la loi fédérale sur la preuve d'identité électronique et autres preuves électroniques.

Indépendamment de cela, les possibilités d'utilisation de l'e-ID pour vérification de l'identité du cocontractant par les intermédiaires financiers (art. 2, al. 1, let. a OBA) découlent des prescriptions de l'Autorité fédérale de surveillance des marchés financiers FINMA. L'utilisation de l'e-ID pour la vérification de l'identité du cocontractant des négociants en métaux précieux et leurs sociétés affiliées, qui exercent professionnellement le commerce des métaux précieux (art. 42bis de la loi fédérale du 20 juin 1933 sur le contrôle des métaux précieux, LCMP) et sont également considérés comme intermédiaires financiers (art. 2, al. 2, let. g LBA), résulte de l'ordonnance sur les intermédiaires financiers (OBA-OFDF) (voir l'art. 17, al. 1, let. d LBA et l'art. 42ter, al. 4, LCMP).

Indépendamment de l'art. 17, al. 3bis OBA, l'utilisation de l'e-ID est également possible pour vérifier l'identité des clients dont le titulaire d'une autorisation de fusion ou d'une autorisation d'achat reçoit des matières de fusion (article 168a, al. 2 ou art. 172e, al. 1, OCMP ainsi que les directives et instructions encore à publier).

5. Conséquences

5.1 Conséquences pour la Confédération

Le présent projet d'ordonnance n'a pas de conséquences sur les ressources financières ou humaines au-delà des besoins déjà définis dans le cadre du programme e-ID pour la mise à disposition, l'exploitation et l'utilisation de l'infrastructure de confiance, l'émission de l'e-ID et les projets pilotes e-ID menés de 2023 à 2028.

5.2 Conséquences pour les cantons et les communes

Outre la demande d'émission de l'e-ID et son émission en ligne, il sera également possible de demander l'émission d'une e-ID sur place, auprès d'un service cantonal compétent. Les personnes intéressées pourront ainsi se rendre dans un bureau pour le contrôle de l'identité nécessaire à l'émission de l'e-ID, par exemple pour éviter l'enregistrement de données biométriques supplémentaires ou pour demander des documents d'identité physiques en combinaison avec la demande d'émission de l'e-ID.

Sur la base d'expériences internationales et d'estimations, on part du principe que qu'environ 1 % de l'ensemble des utilisateurs potentiels de l'e-ID préféreront se rendre sur place pour faire vérifier leur identité en vue de l'obtention d'une e-ID. Pour la variante combinée, on estime que seulement 5 % des personnes qui vont renouveler leur carte d'identité ou leur passeport décideront de se procurer l'e-ID en même temps ; cela représente environ 40'000 cas par an dans les bureaux des passeports. Pour des raisons de procédure, seules les personnes demandant une carte d'identité suisse ou un passeport suisse pourront recourir à cette possibilité.

5.3 Conséquences économiques

La transformation numérique de la Suisse progresse. De plus en plus d'opérations peuvent être effectuées en ligne. Il est de moins en moins nécessaire de se présenter en personne. On s'attend de plus en plus à ce que diverses opérations puissent être effectuées par voie électronique, de préférence sur un smartphone. La LeID et ses dispositions d'exécution posent les fondements pour l'utilisation de preuves électroniques dans le commerce virtuel. Elles créent les conditions nécessaires au fonctionnement d'un écosystème numérique permettant l'émission, l'utilisation et la présentation en toute sécurité des diverses preuves électroniques. Ces conditions-cadre comprennent un ensemble de normes et de standards, de processus, de concepts et de composants d'infrastructure destinés à instaurer la confiance dans les processus numériques, à garantir leur conformité et à assurer leur utilisation par un large public. Avec l'e-ID, les autorités et les entreprises pourront utiliser les mêmes formats pour une multitude de services en ligne. Pour les utilisateurs de ces services, le nombre des différentes identifications requises sera réduit. Cela contribue également à la minimisation des données et à la protection de la vie privée. La définition des normes et la réduction des entraves à l'utilisation des services en ligne créent d'importantes opportunités d'innovation pour les entreprises et les services publics.

5.4 Conséquences sociales

Dans une société interconnectée, les preuves d'identité électroniques reconnues contribuent à protéger l'identité des titulaires. L'usurpation d'identité, qui peut entraîner des conséquences néfastes, deviendra ainsi plus difficile. Dans les applications de la Confédération pour la conservation et la présentation des preuves électroniques et pour la vérification des preuves électroniques, les utilisateurs auront la possibilité de vérifier l'identité des émetteurs et des vérificateurs de preuves électroniques. Les applications seront aussi conviviales que possible afin que l'utilisation des preuves électroniques soit facilement accessible à tous.

L'approche de l'identité autonome souveraine vise à promouvoir la résilience et la souveraineté numérique et à garantir la gestion décentralisée des données pour chaque utilisateur. Les données sont communiquées directement entre les parties impliquées dans une transaction, sans passer par une instance centrale.

6. Aspects juridiques

6.1 Sécurité de l'information

L'utilisation abusive d'informations et la perturbation de l'infrastructure de confiance et du système d'information pour l'émission et la révocation de l'e-ID peuvent porter gravement atteinte aux intérêts essentiels de la Suisse et aux droits des personnes, ainsi

que compromettre la tâche légale consistant à garantir le bon fonctionnement de l'infrastructure de confiance et du système d'information. La LSI[39] et l'ordonnance correspondante (OSI)[40] constituent la base légale permettant de garantir au mieux la sécurité de l'information.

L'OFJ et l'OFIT, en ce qui concerne l'infrastructure de confiance, et fedpol, en ce qui concerne le système d'information pour l'émission et la révocation de l'e-ID, sont tenus de veiller à ce que les violations de la sécurité de l'information soient rapidement identifiées, à ce que leurs causes soient élucidées et à ce que leurs éventuelles conséquences soient minimisées. À cette fin, les autorités concernées prennent les mesures nécessaires pour identifier les incidents ou les failles de sécurité (par exemple en analysant régulièrement les *log files*). En cas d'incident ou de faille de sécurité, l'OFIT prend les mesures d'urgence nécessaires concernant l'infrastructure de confiance et fedpol prend les mesures d'urgence nécessaires concernant le système d'information afin de minimiser les éventuelles répercussions sur la sécurité de l'information. Dans le contexte de l'infrastructure de confiance et de l'e-ID, on parle d'incidents ou de failles de sécurité notamment lorsque la confidentialité, l'intégrité ou la disponibilité des preuves électroniques ou de l'infrastructure de confiance ou du système d'information sont menacées ou compromises, lorsqu'il existe un risque de perturbations graves du fonctionnement ou que de telles perturbations se sont produites, ou lorsqu'il existe des vulnérabilités ou des erreurs dans le système qui représentent une cybermenace importante.

Il n'est pas nécessaire que l'OeID contienne des règles détaillées sur la gestion des risques en matière de sécurité de l'information étant donné que la LSI et l'OSI constituent déjà la base légale pour traiter ces risques. De manière analogue à ce qui est prévu dans la LPD, on renvoie ici au système juridique en vigueur : les dispositions existantes dans les lois pertinentes sont suffisantes pour garantir une gestion sûre des risques en matière de sécurité de l'information.

6.2 Protection des données

Les règles de la législation sur la protection des données (LPD et ordonnances correspondantes) s'appliquent à tous. Les personnes physiques, les émetteurs et les vérificateurs du secteur privé sont soumis aux dispositions de la LPD applicables aux particuliers. La Confédération (fedpol et autres autorités) ainsi que les émetteurs et les vérificateurs du secteur public sont soumis aux dispositions applicables aux organes fédéraux. Afin d'éviter des répétitions et de faciliter la compréhension, l'ordonnance ne renvoie pas aux articles pertinents de la LPD. La LeID précise déjà comment la protection des données s'applique dans le cadre de la mise en œuvre de la législation sur l'e-ID. Les dispositions d'exécution précisent le cadre créé par la LeID pour le traitement, la conservation et l'effacement des données.

[39] RS **128**

[40] RS **128.1**

L’OFIT met à la disposition du public un registre de base, qui permet aux vérificateurs de contrôler si les preuves électroniques ont été modifiées ultérieurement et qu’elles proviennent bien de l’émetteur inscrit au registre de base. Le registre de base contient les clés cryptographiques permettant de vérifier l’authenticité et l’intégrité des preuves électroniques, les identifiants des émetteurs et des vérificateurs, ainsi que les données concernant la révocation des preuves électroniques. Les données concernant la révocation ne doivent pas permettre de tirer des conclusions sur l’identité du titulaire ni sur le contenu des preuves électroniques.

Pour l’inscription au registre de base, l’utilisateur doit fournir des informations le concernant, mais sur une base volontaire. Les modifications apportées au registre de base sont enregistrées quotidiennement et conservées pendant dix ans. Lors de la consultation du registre de base, certaines données telles que les adresses IP sont collectées et peuvent être conservées pour des raisons de sécurité et de maintenance de l’infrastructure pendant 90 jours au plus. L’enregistrement de données lors de la présentation et de la vérification des preuves électroniques est soumis au consentement du titulaire ; ce consentement peut être révoqué en tout temps. Toutes les autres données sont supprimées 90 jours après leur saisie.

L’OFIT met à la disposition du public un registre de confiance. Il contient des informations qui ont été vérifiées sur l’identité des émetteurs et des vérificateurs afin de garantir une utilisation sûre des preuves électroniques. L’inscription au registre de confiance ne se fait que sur demande et avec le consentement explicite de la personne concernée. Le registre peut contenir d’autres informations qui ont été vérifiées, comme des informations du registre du commerce ou des attestations. Des données personnelles supplémentaires, telles que les coordonnées des personnes autorisées à signer, sont collectées au cours du processus de vérification, mais ne sont pas accessibles au public.

L’OFIT met également à la disposition des utilisateurs une application permettant de vérifier les justificatifs électroniques. Celle-ci permet de vérifier aisément la validité cryptographique d’une preuve électronique, en particulier de l’e-ID. En sa qualité de conceptrice de l’application, la Confédération n’a pas accès au contenu des preuves électroniques ni aux informations concernant leur utilisation. Dans l’application, les utilisateurs peuvent conserver diverses preuves électroniques et enregistrer des données personnelles de manière décentralisée. Les copies de sécurité stockées sur le système géré par la Confédération restent également illisibles grâce au cryptage qui est effectué du côté de l’utilisateur. Pour garantir l’authenticité du portefeuille électronique, des identifiants techniques sont utilisés, qui sont principalement traités par les émetteurs de l’e-ID.

Le portefeuille électronique permet aux utilisateurs de déposer sous une forme cryptée, dans un système de copies de sécurité, des données provenant des preuves électroniques. Lors de la consultation, la personne doit s’authentifier de manière univoque. Même si ces données sont cryptées et ne sont pas accessibles à la Confédération, leur enregistrement constitue un traitement de données personnelles, voire de données sensibles. Le traitement a pour seule finalité de fournir un service de protection des preuves électroniques contre la perte.

L’e-ID contient des données personnelles telles que le nom officiel, le prénom, la date de naissance, le sexe, le lieu d’origine, le lieu de naissance, la nationalité, l’image faciale et le numéro AVS. Elle peut contenir des informations supplémentaires relatives au document qui a été utilisé lors de la procédure d’émission. Les données relatives à la procédure d’émission, à la révocation et à la représentation légale des mineurs ou des personnes sous tutelle sont également enregistrées dans le système d’information pour l’émission et la révocation de l’e-ID. Il faut réaliser une courte vidéo de son visage pour prouver son identité. Cet enregistrement vidéo ne pourra être utilisée qu’à des fins d’enquête en cas de soupçon d’usurpation d’identité.

Le système d’information pour l’émission et la révocation de l’e-ID enregistre les données pertinentes pendant 20 ans, les données relatives à la procédure d’émission – y compris les données biométriques – pendant cinq ans et toutes les autres données pendant 90 jours. L’enregistrement s’effectue de manière décentralisée, sur le smartphone du titulaire. fedpol, en tant qu’émetteur de l’e-ID, n’est pas informé de l’utilisation de l’e-ID. Le titulaire décide lui-même des données qu’il transmet lors de la présentation. Les vérificateurs sont légalement tenus de protéger les données personnelles.

Le traitement des données personnelles prévu en lien avec le système pour les copies de sécurité, l’émission de l’e-ID et l’infrastructure de confiance peut toucher aux droits fondamentaux des personnes concernées. Une analyse d’impact relative à la protection des données sera réalisée pour évaluer le risque pour les droits fondamentaux.