Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

18.049

Message relatif à la loi fédérale sur les services d'identification électronique

du 1er juin 2018

Monsieur le Président,
Madame la Présidente,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons, en vous proposant de l'approuver, le projet de loi fédérale sur les services d'identification électronique.

Dans le même temps, nous vous proposons de classer l'intervention parlementaire suivante:

2018 M 17.3083 Numérisation. Identification électronique pour réduire la bureaucratie dans tout le pays
(N 8.3.2017, Groupe LR; N 20.9.2017, E 28.02.2018)

Nous vous prions d'agréer, Monsieur le Président, Madame la Présidente, Mesdames, Messieurs, l'assurance de notre haute considération.

1er juin 2018

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Condensé

La numérisation de la société avance à grands pas. La possibilité de s'identifier simplement et sûrement sur Internet est un facteur de succès décisif des applications en ligne et de leur diffusion auprès du public. La loi fédérale sur les services d'identification électronique (LSIE) annexée au présent message a pour objet l'établissement de moyens d'identification électronique («e-ID») grâce auxquels tout un chacun pourra s'identifier dans le monde virtuel selon des données confirmées par l'État.

Le but de la LSIE est de promouvoir la sécurité des échanges électroniques entre les citoyens, les entreprises et les autorités publiques. Afin d'atteindre ce but, le projet de loi prévoit un partage des tâches entre le secteur public et le secteur privé. Dans ce cadre, l'État continuera d'assumer sa tâche centrale qui est la vérification et la confirmation officielles de l'identité d'une personne. Etant donné la dynamique de la révolution numérique, l'État ne saurait cependant développer et produire lui-même les supports technologiques requis pour une telle identification. Le secteur privé, plus proche des utilisateurs et des technologies du numérique nécessaires, est mieux placé pour assumer un tel rôle. L'exploitation des systèmes e-ID ainsi que l'émission des e-ID seront donc du ressort des prestataires privés (fournisseurs de services d'identité, en bref fournisseurs d'identité). L'État assumera néanmoins une charge importante à ce niveau, étant donné qu'il soumettra les fournisseurs et les systèmes qu'ils auront mis en place à une procédure de reconnaissance stricte et à des contrôles réguliers. Ainsi, les exigences concernant la sécurité et la protection des données seront vérifiées et constamment adaptées aux développements les plus récents. Une telle solution, réunissant les capacités et expérience du secteur public et du secteur privé, offre des conditions optimales pour la mise en place et l'utilisation des e-ID.

La LSIE ne règle pas exhaustivement l'identification sur Internet. Elle porte uniquement sur l'établissement et l'utilisation des e-ID reconnues. D'autres moyens d'identification électronique pourront être offerts et utilisés sur le marché, même s'ils ne répondent pas aux critères de confiance que confère la reconnaissance étatique.

Les personnes physiques détentrices d'une e-ID l'utiliseront pour s'enregistrer, simplement et de manière sûre, sur un site Internet public ou privé (service utilisateur) auquel elles pourront par la suite se connecter de nouveau. L'e-ID facilitera les démarches auprès des autorités, qui offrent de plus en plus souvent des guichets numériques. L'utilisation des services cyberadministratifs pourrait devenir entièrement informatique. Dans le domaine de la cybersanté, l'e-ID viendra s'ajouter dans un premier temps aux moyens d'identification prévus par la loi fédérale du 19 juin 2015 sur le dossier électronique du patient; elle pourrait à terme les remplacer.

Le projet ne détermine pas le support sur lequel l'e-ID sera implantée. Les moyens d'identification électronique actuels sont disponibles sur les téléphones portables (par ex. Mobile ID), ou sur des cartes ou des médias de stockage avec puce intégrée

(par ex. SuisseID), ou bien encore ils sont totalement dématérialisés et peuvent être utilisés sur Internet avec un nom d'utilisateur, un mot de passe et éventuellement un code de transaction à usage unique envoyé par téléphone portable (par ex. pour les transactions bancaires en ligne).

Trois niveaux de garantie sont prévus. Toutes les transactions ne demandent pas le même degré de sécurité, et tous les supports ne sont pas adaptés à tous les niveaux de garantie. Les fournisseurs d'identité devront donc pouvoir offrir des systèmes e-ID, selon les besoins, aux trois niveaux de garantie prévus, tels qu'ils sont définis par l'Union européenne et par le National Institute of Standards and Technology. Pour être reconnu par la Confédération, un système e-ID devra remplir au minimum les exigences du niveau de garantie «faible». Les niveaux de garantie «substantiel» et «élevé» devront satisfaire à des conditions supplémentaires.

La loi pose un cadre strict en matière de protection des données; la finalité et les conditions du traitement et de la communication des données dans le cadre de l'établissement et de l'utilisation de l'e-ID sont définies précisément par le projet de loi. Le fournisseur d'identité peut traiter les données d'identification pendant une période de temps déterminée et uniquement pour procéder aux identifications en vertu de la présente loi. En outre, il peut seulement communiquer aux exploitants d'un service utilisateur les données d'identification personnelle qui sont nécessaires à l'identification de la personne concernée – qui est la fonction de l'e-ID – et à la communication desquelles le titulaire de l'e-ID a consenti. Cette communication est requise pour assurer que le système e-ID remplit sa fonction: permettre une identification sûre et simple. Enfin, la présente loi prévoit une base légale pour le traitement et la communication des données par les organes fédéraux concernés.

Le projet tient compte des règles internationales, et en particulier du règlement nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Nul ne sait à ce jour si la Suisse s'associera à cet ensemble de règle par un accord bilatéral; néanmoins, la solution suisse en matière d'e-ID est conçue de sorte à pouvoir être notifiée à l'Union européenne.

Table des matières

Message

1 Grandes lignes du projet

1.1 Contexte

La diffusion d'Internet et la grande disponibilité d'appareils mobiles performants rendent la dématérialisation des transactions de plus en plus aisée. Afin que des transactions plus complexes puissent également être effectuées par la voie électronique, les prestataires (ci-après les «exploitants d'un service utilisateur*[1]») doivent avoir confiance dans l'identité et l'authenticité de leur interlocuteur. L'identification* sûre des personnes est fondamentale pour garantir la sécurité du droit, et ce même au-delà des frontières nationales. Pour répondre à ce besoin, des moyens d'identification électronique reconnus (également appelés «identité électronique e-ID» ou «e-ID»)* seront créés en Suisse pour les personnes physiques. Il existe déjà, pour les personnes morales, un moyen d'identification unique, le numéro d'identification des entreprises (IDE), qui peut être saisi à des fins d'identification dans des outils informatiques appropriés. Une e-ID permet à un exploitant d'un service utilisateur de procéder en ligne à une identification du titulaire de l'e-ID pour vérifier que celui-ci est une personne habilitée. Des e-ID fiables contribuent par conséquent à l'expansion des transactions en ligne.

Par décision du 19 décembre 2012, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'élaborer, en collaboration avec la Chancellerie fédérale (ChF), le Département fédéral de l'économie, de la formation et de la recherche (DEFR), le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) et le Département fédéral des finances (DFF), un concept et un projet de loi relatifs à des moyens d'identification électronique officiels qui puissent être proposés conjointement avec la carte d'identité. La première ébauche du concept, présentée dans la note de discussion du 28 février 2014, prévoyait que l'État soit le principal fournisseur d'identité et qu'une e-ID soit remise à tous les Suisses en même temps que la carte d'identité. Elle a fait l'objet d'une consultation auprès des offices et des acteurs du marché en 2014 et 2015.

Compte tenu des avis reçus et des expériences faites dans d'autres pays, le concept a été fondamentalement remanié. Le développement de solutions propres et l'établissement d'e-ID par l'État engendrent généralement, pour les pouvoirs publics, des coûts informatiques élevés non couverts car ils n'offrent pas la flexibilité requise pour faire face à l'évolution rapide des besoins et de la technologie, si bien que l'on a opté pour un partage des tâches entre la Confédération et le secteur privé. Des offres d'identification électronique présentant différents niveaux de garantie se développent déjà dans le secteur privé (par ex. Apple-ID, Google-ID, Mobile-ID, OpenID, SuisseID*, SwissID*, SwissPass, etc.). Il est difficile de dire quelles e-ID utilisées à l'heure actuelle existeront encore à moyen et à long terme à côté des e-ID reconnues.

[1] Les termes suivis d'un astérisque sont définis dans le glossaire qui figure à la fin du présent message.

On a également tenu compte des récents développements qu'a connus l'Union européenne (UE) et vérifié que le concept était compatible avec le règlement (UE) nº 910/2014 (règlement eIDAS)*[2].

Le 13 janvier 2016, le Conseil fédéral a pris acte du concept pour des systèmes d'e-ID remanié, chargé le DFJP d'élaborer un avant-projet de loi et fixé le cadre de la législation. La consultation relative à l'avant-projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) a duré du 22 février au 29 mai 2017. Le Conseil fédéral a pris acte des résultats de cette consultation le 15 novembre 2017 et chargé le DFJP d'élaborer un projet de loi.

1.2 Nouvelle réglementation proposée

1.2.1 Concept de l'e-ID

La sécurité juridique et la confiance sont des conditions essentielles pour le développement des transactions. Il est nécessaire de connaître clairement l'identité des parties prenantes. Dans le monde réel, la Confédération délivre des moyens d'identification conventionnels tels que le passeport suisse, la carte d'identité et le titre de séjour. Le passeport et la carte d'identité sont en outre des documents de voyage, avec lesquels il est possible d'entrer sur le territoire d'autres États en vertu de conventions internationales. Il sera également désormais possible de prouver l'identité d'une personne physique dans le cyberespace. Des e-ID reconnues par l'État permettront à leur titulaire de s'enregistrer de manière sécurisée auprès de services en ligne et de s'y reconnecter ultérieurement, toujours de manière sécurisée.

D'autres services de confiance allant au-delà de l'identification, tels que la signature électronique au sens de la loi du 18 mars 2016 sur la signature électronique (SCSE)[3], peuvent être proposés par des fournisseurs de services d'identification électronique (fournisseurs d'identité)*, mais ils ne constituent pas un élément des e-ID et ne sont pas régis par la LSIE. Le projet de loi ne règle pas non plus les modalités d'accès aux services en ligne (gestion des accès). Il ne s'agit pas là de l'identification de personnes mais de l'octroi d'un accès à un service à des personnes qui y ont de fait droit. Les fournisseurs d'identité sont libres de sécuriser ces accès en sus de l'identification et d'offrir une solution globale de gestion des identités et des accès (GIA; en anglais *Identity and Access Management*, *IAM*)*.

Le nouveau concept proposé s'appuie sur les travaux préparatoires réalisés par le DFJP (Fedpol) entre 2013 et 2015 et dans le cadre desquels des acteurs importants du marché ont également été consultés. Il prend en outre en considération les enseignements tirés de l'utilisation de solutions e-ID dans d'autres pays, les développements internationaux concernant la recherche de solutions e-ID pragmatiques ainsi

2 Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73.
Une liste des actes normatifs pertinents de l'UE est publiée sur le site de l'OFJ > État & Citoyen > Projets législatifs en cours > Identification électronique (e-ID).

3 RS **943.03**

que l'exigence de compatibilité avec les systèmes d'identification de l'UE fixée par le règlement eIDAS.

1.2.2 Combinaison des rôles de l'État et du secteur privé

Le projet de LSIE prévoit une combinaison des rôles entre État et secteur privé. La confiance créée par la reconnaissance et la surveillance étatiques sera associée au savoir-faire et au dynamisme du secteur privé. Ce procédé garantira que l'e-ID est bien acceptée par le public. Les fournisseurs d'identité satisfaisant aux conditions requises seront habilités par la Confédération à délivrer des e-ID et à gérer des systèmes e-ID*. Tous les systèmes e-ID devront être interopérables afin que les titulaires puissent utiliser leur e-ID quel que soit le service utilisateur*.

L'État ne se dessaisira pas de sa tâche de vérification et de confirmation officielle de l'identité d'une personne, au travers d'éléments tirés des systèmes d'information de la Confédération. Un service d'identité* créé à cet effet, établi au sein de Fedpol, lequel tient les registres officiels où sont consignées ces données, assumera cette fonction. Celui-ci vérifiera si les utilisateurs remplissent les critères d'admissibilité et sera responsable de l'établissement de l'identité des personnes lors de la première identification. De plus, le service d'identité attribuera le numéro d'enregistrement de l'e-ID* à la personne concernée, à qui il remettra les moyens d'accès.

Etant donné l'évolution technologique et la multitude de solutions techniques possibles, la Confédération ne saurait développer et produire elle-même les supports de ces éléments d'identité confirmés par l'État, supports qui seront, par exemple, les téléphones portables, les cartes bancaires ou les abonnements de transport public. Le secteur privé, plus proche des utilisateurs et des technologies du numérique nécessaires, est bien mieux placé pour le faire et pour innover. L'État assumera une autre fonction: il soumettra les fournisseurs et les systèmes qu'ils auront mis en place à une procédure de reconnaissance* stricte et à des contrôles réguliers. L'organisme de reconnaissance* sera rattaché à l'Unité de pilotage de la Confédération (UPIC).

Cette association fonctionnelle public-privé offre des conditions optimales pour une utilisation simple et conviviale des e-ID par l'administration, les particuliers et les entreprises, tout en assurant les moyens de s'adapter souplement aux évolutions technologiques, notamment en matière de sécurité.

1.2.3 Fonction de l'e-ID

Grâce à une e-ID, les personnes physiques pourront s'enregistrer de manière sûre et conviviale sur des portails en ligne (services utilisateurs) et s'y reconnecter ultérieurement. Lors de l'enregistrement auprès d'un service utilisateur, les données personnelles n'auront pas besoin d'être saisies manuellement; avec une e-ID reconnue, elles seront communiquées automatiquement une fois que le titulaire y aura consenti. Lorsque ces personnes se reconnecteront ultérieurement à ces portails, elles s'identifieront ou s'authentifieront avec l'e-ID qu'elles auront enregistrée précédemment et celle-ci sera reconnue, ce qui garantira une connexion fiable. L'e-ID

constitue donc l'un des fondements de l'utilisation simple et sécurisée des services en ligne; elle apportera à chacun plus de sécurité et de confort sur Internet.

L'e-ID facilitera le contact avec les autorités, qui offrent de plus en plus souvent des guichets virtuels aux administrés. Aujourd'hui, pour s'identifier auprès de leurs services, il faut le plus souvent utiliser des données d'accès reçues par courrier postal, par exemple un nom d'utilisateur et un mot de passe à usage unique, ou bien une liste avec une suite de chiffres à biffer. Pour clore la procédure, il faut en outre souvent renvoyer un formulaire papier. Ces démarches pourraient être évitées si l'identification avait lieu via une e-ID. L'utilisation des services en ligne des administrations publiques pourrait avoir lieu entièrement par voie électronique.

Dans le domaine de la cybersanté, l'e-ID viendra s'ajouter dans un premier temps aux moyens d'identification prévus par la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP)[4]; elle pourrait à terme les remplacer. L'accès du patient à son dossier serait possible avec une e-ID du niveau de garantie approprié, mais en tous les cas, il serait plus simple.

Quant aux prestataires du commerce en ligne, l'e-ID leur permettra d'avoir une plus grande certitude sur l'identité de leurs clients. Le contrôle de la solvabilité sera plus simple sans risque de confusions d'identité. Grâce à la possibilité de vérifier l'âge des utilisateurs, les enfants et les adolescents seront mieux protégés face aux contenus médiatiques inappropriés pour des mineurs, au cyberharcèlement et au manque de transparence dans le traitement des données personnelles. La création des e-ID et les développements techniques qui l'accompagnent pourraient permettre de mettre en œuvre de manière simple et sûre les normes visant la protection médiatique des mineurs. Il serait possible, par exemple, d'obliger les prestataires, de par la loi, à ne donner accès à des contenus potentiellement dangereux qu'à des utilisateurs dont l'âge est attesté par une e-ID[5].

Le projet ne détermine pas le support sur lequel l'e-ID sera implantée. Les moyens d'identification électronique* actuels sont disponibles sur les téléphones portables (par ex. Mobile ID), ou sur des cartes ou des médias de stockage avec puce intégrée (par ex. SuisseID), ou bien encore ils sont totalement dématérialisés et peuvent être utilisés sur Internet avec un nom d'utilisateur, un mot de passe et éventuellement un code de transaction à usage unique envoyé par téléphone portable (par ex. pour les transactions bancaires en ligne). Il est vraisemblable que l'offre d'e-ID comprendra plusieurs types de supports reflétant les préférences des utilisateurs.

4 RS **816.1**

5 Voir rapport du Conseil fédéral du 13 mai 2015 en réponse à la motion 10.3466 Bischofberger «Internet. Renforcer la protection des jeunes et la lutte contre la cybercriminalité», intitulé «Jeunes et médias. Aménagement de la protection des enfants et des jeunes face aux médias en Suisse», www.bsv.admin.ch/dam/bsv/fr/dokumente/kinder/berichte-vorstoesse/br-bericht-zukuenftige-ausgestaltung-kinder-und-jugendmedienschutz.pdf.download.pdf/rapport_du_conseilfederaljeunesetmedias.pdf.

1.2.4 Établissement de l'e-ID

Avant l'établissement d'une e-ID reconnue, Fedpol associera un numéro d'enregistrement de l'e-ID aux données d'identification personnelle* du requérant. Ce numéro sera unique pour chaque titulaire d'une e-ID. La procédure d'établissement de l'e-ID comprend une identification qui sera effectuée, selon le niveau de garantie, par voie électronique ou en personne, le requérant se présentant auprès du fournisseur d'identité. Elle se déroulera en plusieurs étapes (voir art. 6 LSIE):

1. Celui qui souhaite obtenir une e-ID s'adresse à un fournisseur d'identité, qui le dirige vers le site de Fedpol pour vérification initiale de l'identité alléguée. Fedpol contrôle les données d'identité du requérant au moyen d'un document d'identité valable (passeport, carte d'identité ou pièce de légitimation étrangère reconnue).
2. Fedpol demande au requérant des informations supplémentaires sur son identité (par ex. le nom de ses parents ou des documents d'identité supplémentaires), informations qu'il compare avec les données contenues dans les registres de personnes tenus par la Confédération. Si elles coïncident, Fedpol donne son accord à l'établissement de l'e-ID.
3. Le requérant donne à Fedpol son consentement à la communication au fournisseur d'identité de ses données d'identification personnelle, assorties d'un numéro d'enregistrement de l'e-ID[6].
4. Selon le niveau de garantie demandé, Fedpol communique le numéro d'enregistrement de l'e-ID accompagné des données attestées au fournisseur d'identité.
5. Le fournisseur d'identité attribue au requérant un moyen d'authentification comprenant un nom d'utilisateur avec lequel il peut s'identifier en ligne. Selon le niveau de garantie, le requérant peut être tenu de se présenter en personne ou par des moyens virtuels équivalents (par ex. une identification vidéo).
6. Le fournisseur d'identité veille, au moment de délivrer le moyen d'authentification, à l'attribution correcte du numéro d'enregistrement, puis il active l'e-ID afin que le titulaire puisse l'utiliser.

L'ensemble du processus ne devrait pas durer plus de quelques minutes. Les opérations techniques qui y sont liées seront définies dans des normes et des protocoles techniques.

La LSIE règle aussi ce qu'il adviendra des moyens d'identification électronique délivrés par des fournisseurs d'identité avant l'entrée en vigueur de la loi. Durant une période transitoire de deux ans, l'UPIC reconnaîtra comme e-ID de niveau de garantie faible, sur demande d'un fournisseur, les moyens d'identification électronique que ce dernier a établis avant l'entrée en vigueur de la présente loi. En outre, il reconnaîtra comme e-ID du niveau de garantie substantiel les moyens d'identification électronique qu'un fournisseur d'identité a établis avant l'entrée de la pré-

6 Sur les données d'identification personnelle, voir commentaire de l'art. 5.

sente loi. Dans ce dernier cas, l'identification devra avoir eu lieu dans le cadre d'une procédure qui est soumise par la loi à des règles et à une surveillance et qui garantit un niveau de sécurité comparable aux procédures prévues en vertu de la présente loi.

Les personnes possédant un certificat qualifié valable au sens de l'art. 2, let. h, SCSE pourront également demander à un fournisseur d'identité qu'il établisse à leur intention (sans nouvelle vérification d'identité) une e-ID d'un niveau de garantie substantiel.

Dans les trois cas, les conditions d'admissibilité visées à l'art. 3 devront être remplies, les titulaires devront avoir consenti à l'établissement de l'e-ID et les données d'identification personnelle (tels le numéro de carte d'identité ainsi que le nom, le prénom et la date de naissance) devront correspondre aux informations enregistrées dans le système d'information visé à l'art. 24.

Les modalités de la procédure d'établissement seront arrêtées par le Conseil fédéral par voie d'ordonnance.

1.2.5 Niveaux de garantie

Toutes les transactions ne requièrent pas le même degré de sécurité. Des exigences trop élevées en matière de sécurité peuvent être perçues comme gênantes en pratique, favoriser le contournement des règles et provoquer une augmentation des coûts, ce qui est problématique pour l'acceptation et la sécurité d'un système e-ID. C'est la raison pour laquelle des systèmes e-ID présentant trois niveaux de garantie et obéissant à des conditions différentes seront reconnus. Les niveaux de garantie seront déterminés par les données d'identification personnelle contenues dans l'e-ID, le processus d'établissement, la gestion du système et l'utilisation des e-ID ainsi que d'autres mesures de sécurité techniques ou organisationnelles.

La loi définit uniquement les catégories d'e-ID possibles, appelées «niveaux de garantie» (voir art. 4 LSIE). Chaque niveau de garantie offre un degré de fiabilité différent. Le niveau de garantie requis pour les différents types d'applications devra être déterminé dans les réglementations spéciales ou par les exploitants d'un service utilisateur du secteur privé. Le niveau de garantie choisi pour un portail de cyberéducation, par exemple, pourra ainsi être différent de celui requis pour le vote électronique ou des applications de cybersanté.

La désignation et les exigences de chaque niveau de garantie ont été reprises du règlement eIDAS et de ses dispositions d'exécution. Le projet distingue entre les niveaux *faible*, *substantiel* et *élevé*. Les e-ID d'un niveau de garantie *substantiel* ou *élevé* pourront être utilisées pour bénéficier de services utilisateurs pour lesquels seul un niveau *faible* est requis (compatibilité descendante).

La Confédération mettra les données d'identification personnelle contenues dans ses registres à la disposition des fournisseurs d'identité, par une interface électronique (numéro d'enregistrement de l'e-ID, nom d'état civil, prénoms et date de naissance pour le niveau de garantie *faible*, sexe, lieu de naissance et nationalité pour le niveau de garantie *substantiel* et enfin photographie pour le niveau de garantie *élevé*). La première communication des données à un fournisseur d'identité ou à un exploitant

d'un service utilisateur requerra le consentement exprès de la personne concernée (voir art. 6, al. 2, let. c, LSIE). Selon ce modèle, il sera par exemple possible d'enregistrer d'abord une e-ID du niveau *faible* et de la transformer par la suite, en cas de besoin, en e-ID de niveau *élevé*, en se présentant en personne (ou par des moyens virtuels équivalents). Le niveau de garantie *faible* permet d'avoir des e-ID d'un accès très facile, ce qui sera un facteur de succès essentiel sur le marché pour les fournisseurs de systèmes e-ID reconnus. De plus, rien n'interdit de posséder plusieurs e-ID de fournisseurs d'identité et de niveaux de garantie différents. Le numéro d'enregistrement de l'e-ID restera cependant toujours le même.

Les trois niveaux de garantie prévus pour les systèmes e-ID reconnus en Suisse satisfont aux mêmes exigences de sécurité que ceux définis par le règlement eIDAS de l'UE (art. 8 du règlement eIDAS et dispositions d'exécution s'y rapportant) et correspondent également aux niveaux de garantie définis par le NIST*[7] pour les applications de cyberadministration aux États-Unis. Ces niveaux de garantie constituent aujourd'hui une norme internationale. Pour atteindre leur but, ils se distingueront par des spécifications techniques, des normes et des procédures – y compris des contrôles techniques – qui leur seront propres, et qui feront l'objet d'ordonnances, de directives et de normes techniques. Le projet de loi assure ainsi la compatibilité avec l'Union européenne et les États-Unis.

Niveau de garantie *faible*

Dans le cas d'un niveau de garantie *faible*, l'e-ID a pour but de réduire le risque d'utilisation abusive ou d'altération de l'identité. Seules quelques données sont attribuées à l'e-ID (nom, prénoms, date de naissance et numéro d'enregistrement de l'e-ID; voir art. 5, al. 1, LSIE). L'enregistrement peut être effectué en ligne avec un document d'identité délivré par l'État. L'utilisation de l'e-ID requiert au moins une authentification* à un facteur. Le fonctionnement est donc similaire à celui d'un badge d'entrée ou des solutions de paiement sans contact proposées pour les petits montants.

Niveau de garantie *substantiel*

Le niveau de garantie *substantiel* renvoie à un moyen d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne. L'e-ID a pour but de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité. L'enregistrement est effectué lors d'un entretien personnel auprès du fournisseur d'identité, d'une identification par vidéo sur la base d'un document d'identité délivré par l'État ou de la comparaison avec la photographie apposée sur le document d'identité. Dans le cas d'un niveau de garantie *substantiel*, d'autres données d'identification personnelles sont ajoutées (le sexe, le lieu de naissance et la nationalité; voir art. 5, al. 2, LSIE). L'utilisation de l'e-ID requiert dans ce cas une authentification à deux facteurs. Le fonctionnement s'apparente ainsi à celui des solutions habituellement proposées dans le secteur bancaire (carte de compte, carte de crédit à code PIN, plateformes d'e-banking).

7 National Institute of Standards and Technology (Institut national des normes et de la technologie), United States Department of Commerce (Département du commerce des États-Unis).

Niveau de garantie *élevé*

Dans le cas d'un niveau de garantie *élevé*, l'e-ID a pour but de prévenir le risque d'utilisation abusive ou d'altération de l'identité. L'enregistrement est effectué lors d'un entretien personnel auprès du fournisseur d'identité ou d'une identification par vidéo sur la base d'un document d'identité délivré par l'État. Par ailleurs, l'authenticité de ce document et au moins une donnée biométrique (validité du document d'identité, photographie ou autre élément d'identification biométrique) sont vérifiées à l'aide d'une source officielle. Le moyen d'authentification de l'e-ID doit satisfaire à des conditions de sécurité technique très contraignantes. Il est délivré en mains propres.

L'utilisation de l'e-ID requiert au moins une authentification à deux facteurs, l'un des deux devant être biométrique. Le moyen d'authentification doit apporter une preuve directe de l'authenticité du titulaire à l'exploitant du service utilisateur. Le fonctionnement s'apparente donc ici à celui d'un smartphone doté d'un système de reconnaissance digitale, faciale ou vocale, intégré dans un secteur sécurisé et assorti d'un certificat personnel. L'authentification biométrique crée un lien encore plus étroit entre l'e-ID et son titulaire. En cas de perte du moyen d'authentification de l'e-ID, l'authentification biométrique protège le titulaire de l'exécution de transactions abusives à son nom. En ce qui concerne l'usurpation d'identité, les titulaires doivent être protégés des attaques informatiques, qu'elles visent le moyen d'authentification de l'e-ID lui-même ou le matériel informatique éventuellement nécessaire pour l'utilisation du moyen d'authentification mais qui n'est pas réglementé par la LSIE. Les transactions abusives effectuées grâce à l'usurpation d'identité doivent également être empêchées dans les cas où une attaque informatique aurait permis à un tiers de manipuler ce matériel informatique ou d'accéder aux informations qu'il contient. Afin de garantir cette protection, le moyen d'authentification de l'e-ID doit reposer sur des composants particulièrement fiables, adaptés à l'évolution de la technique.

1.2.6 Rôle de l'État concernant les systèmes e-ID

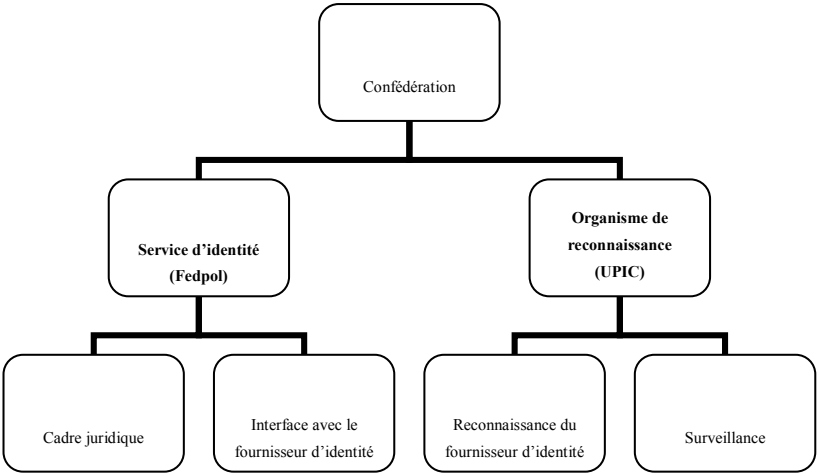
1.2.6.1 Vue d'ensemble

Une e-ID établie conformément à la présente loi confirme l'existence et l'identité d'une personne physique sur la base des données d'identification personnelle contenues dans des registres gérés et mis à jour par l'État. Ce dernier jouit en effet, et ce à tous ses échelons, d'une confiance particulière quant à l'exactitude des données relatives aux personnes. Cette confiance se fonde sur le fait que des identifications sont régulièrement effectuées par les services publics lors de l'établissement de documents d'identité et lors de la communication de modifications au registre étatique.

La Confédération garantit que les systèmes e-ID reconnus sont fiables et accomplit à cet effet un certain nombre de tâches dans le domaine des e-ID reconnues:

1. elle élabore et met à jour la réglementation en la matière, ce qui permet de garantir la transparence et la sécurité;

2. elle définit les normes, les conditions de sécurité et les conditions d'interopérabilité* à respecter pour pouvoir gérer un système e-ID;
3. elle gère une plateforme Internet sur laquelle les requérants peuvent se connecter pour une première vérification de leur identité;
4. elle vérifie l'identité des personnes et y associe le numéro d'enregistrement de l'e-ID;
5. elle gère une interface électronique sur laquelle les fournisseurs d'identité reconnus peuvent obtenir des données d'identification personnelle gérées par l'État;
6. elle reconnaît les fournisseurs d'identité et leurs systèmes e-ID;
7. elle surveille les fournisseurs d'identité et les systèmes e-ID reconnus;
8. elle peut, dans certaines circonstances, révoquer la reconnaissance d'un fournisseur d'identité.



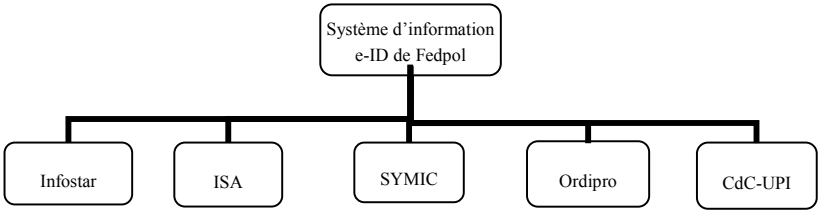
Ces tâches seront confiées à deux unités administratives au sein de la Confédération: Fedpol (service d'identité) et l'UPIC (organisme de reconnaissance).

1.2.6.2 Registres de données d'identification personnelle

Les autorités suisses, à leurs différents échelons, tiennent plusieurs registres contenant des données d'identification personnelle. À titre d'exemples, on peut citer les registres cantonaux et communaux des habitants, le registre informatisé de l'état civil (Infostar)* et le registre central de la Centrale de compensation de l'AVS

(CdC-UPI*[8]). L'UPI est la fonctionnalité du registre central des assurés de l'AVS qui a trait à l'identification de personnes, en relation avec l'attribution et la gestion du numéro AVS. En outre, le système d'information relatif aux documents d'identité (ISA)* contient des données d'identification personnelle des Suisses et Suissesses et sert de base pour l'établissement de documents d'identité (carte d'identité et passeport suisse). Les titres de séjour sont, quant à eux, établis à partir des données contenues dans le système d'information central sur la migration (SYMIC)*, les cartes de légitimation selon la législation sur l'État hôte à partir des données d'Ordipro*.

Les données tirées de ces registres seront rassemblées dans le système d'information de Fedpol prévu à l'art. 24:



1.2.6.3 Relation entre le numéro AVS et le numéro d'enregistrement de l'e-ID

Le numéro AVS est un identifiant personnel unique qui ne peut, selon la pratique actuelle, être utilisé que dans certains domaines si des bases légales formelles le prévoient. La possibilité d'utiliser systématiquement ce numéro comporte le risque d'une interconnexion des données personnelles enregistrées dans les différents systèmes. Aussi une telle utilisation n'est-elle permise qu'aux conditions énoncées aux art. 50*d* et 50*e* de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[9]. L'art. 50*a* LAVS désigne les organes auxquels des données, en particulier le numéro AVS, peuvent être communiquées en dérogation à l'art. 33 de la loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA)[10]. Conformément à l'art. 50*e* LAVS, ce numéro ne peut être utilisé systématiquement, en dehors du domaine des assurances sociales de la Confédération, que si une loi fédérale le prévoit et que le but de l'utilisation et les utilisateurs légitimés sont définis.

Le numéro AVS est souvent employé dans les relations entre le citoyen et l'administration. S'il n'était plus possible à Fedpol (service d'identité) de demander ou de faire confirmer ce numéro aux services administratifs, il faudrait utiliser d'autres moyens, plus coûteux. Cela compliquerait nettement le système que l'on essaie de mettre en place et réduirait son attrait. Fedpol doit donc être autorisé à utiliser le numéro AVS systématiquement (uniquement) pour identifier des per-

8 UPI est l'acronyme de «Unique Person Identification».
9 RS **831.10**
10 RS **830.1**

sonnes. Il ne pourra le communiquer, par un accès en ligne, qu'aux exploitants d'un service utilisateur eux-mêmes habilités à utiliser systématiquement le numéro AVS (art. 8, al. 2, LSIE), et toujours dans cette même finalité.

L'utilisation systématique du numéro AVS sera par contre interdite aux fournisseurs d'identité et aux autres particuliers. Il faut donc un autre numéro d'identification, indépendant du numéro AVS: ce sera le numéro d'enregistrement de l'e-ID, qui servira d'identifiant dans les relations avec les particuliers et notamment de lien entre la personne et son e-ID. Comme l'obtention d'une e-ID est laissée au bon vouloir de chacun, sans obligation que toutes les personnes habilitées en aient un, tous n'auront pas un numéro d'enregistrement de l'e-ID, qui ne se prêtera donc pas à une utilisation comme identifiant général.

1.2.6.4 Office fédéral de la police (service d'identité)

Cadre légal

Fedpol s'occupera, en collaboration avec l'UPIC, des conditions juridiques, organisationnelles et techniques. Il définira notamment les normes applicables aux interfaces pour que l'interopérabilité des systèmes e-ID soit garantie et adapte les exigences techniques et organisationnelles existant en matière de reconnaissance des fournisseurs d'identité et des systèmes e-ID en fonction des progrès techniques, de l'évolution des exigences en matière d'utilisation et des contraintes de sécurité du moment.

Page Web pour les requérants

Fedpol mettra en place une page Web sur laquelle les fournisseurs d'identité redirigeront les requérants pour qu'ils attestent de leur identité et donnent leur consentement à la communication des données d'identification personnelle auxdits fournisseurs d'identité.

Interface

Fedpol mettra les données d'identification personnelle gérées par la Confédération à la disposition des fournisseurs d'identité reconnus via une interface électronique (art. 23, al. 1, LSIE). L'établissement d'un numéro d'enregistrement de l'e-ID permettra d'attribuer ces données de manière univoque et durable à une personne et à son e-ID, sans contestation possible. Cette interface ne sera accessible qu'aux fournisseurs d'identité reconnus, lors de la première identification puis des mises à jour régulières des données d'identification personnelle.

Fedpol sera responsable de la gestion de l'interface servant à la communication des données d'identification personnelle. Il sera l'interlocuteur des fournisseurs d'identité reconnus et des autorités qui gèrent les registres étatiques raccordés au système.

Fedpol se procurera les données d'identification personnelle dans divers registres (art. 24, al. 3, LSIE). Le nom d'une personne sera confirmé grâce à une comparaison des données avec Infostar tandis que, par exemple, le numéro des documents d'identité et les photographies proviendront d'ISA ou du SYMIC. Dans la mesure où

il en a besoin pour accomplir les tâches que lui impose la LSIE, Fedpol pourra assortir les données d'identification personnelle de métadonnées concernant la mise à jour des données dans son système d'information (art. 5, al. 4, LSIE).

Les fournisseurs d'identité seront tenus de mettre périodiquement à jour les données d'identification personnelle rattachées au numéro d'enregistrement d'une e-ID. Selon le niveau de garantie, ils devront procéder à cette mise à jour au minimum tous les ans (niveau de garantie *faible*), tous les trimestres (niveau de garantie *substantiel*) ou toutes les semaines (niveau de garantie *élevé*) (voir art. 7 LSIE).

1.2.6.5 Unité de pilotage informatique de la Confédération (organisme de reconnaissance)

Reconnaissance

Les fournisseurs d'identité satisfaisant aux conditions requises pourront faire reconnaître par l'UPIC leurs systèmes e-ID présentant l'un des trois niveaux de garantie prévus. Un fournisseur d'identité pourra gérer plusieurs systèmes e-ID présentant des niveaux de garantie différents et les faire reconnaître tous ou uniquement certains d'entre eux. Le Conseil fédéral fixera, pour ce faire, des exigences juridiques, organisationnelles et techniques que les fournisseurs d'identité devront satisfaire, l'UPIC devant s'assurer que celles-ci sont bien remplies. En renouvelant périodiquement la reconnaissance, la Confédération contribuera à la sécurité durable des systèmes e-ID.

L'UPIC publiera une liste des fournisseurs d'identité et des systèmes e-ID reconnus, qui doit permettre aux exploitants d'un service utilisateur et aux personnes physiques de vérifier le statut d'un fournisseur d'identité ou d'un système e-ID en particulier (art. 25, al. 2, LSIE). Elle gèrera un système d'information servant à la reconnaissance des fournisseurs d'identité et à leur surveillance (art. 26 LSIE).

Surveillance

L'UPIC surveillera les fournisseurs d'identité et les systèmes e-ID reconnus et prendra des mesures en cas de non-respect des exigences fixées ou d'incidents remettant en cause la sécurité informatique. Pour ce faire, elle demandera aux fournisseurs d'identité de lui apporter, à une fréquence définie préalablement, les preuves de conformité requises et les vérifie. Elle pourra imposer des mesures au titre de sa mission de surveillance et dans certains cas retirer la reconnaissance à un fournisseur d'identité (art. 19 LSIE).

1.2.6.6 Fédération suisse d'identité (FSI)

La Fédération suisse d'identités (FSI) offre une solution technique pour simplifier l'accès aux services administratifs en ligne et la collaboration électronique entre les autorités. La FSI est un projet clé du plan stratégique de Cyberadministration suisse. Le Secrétariat d'État à l'économie (SECO) est responsable du projet.

La question de l'implication de la FSI dans les systèmes e-ID a été examinée. L'interopérabilité peut cependant aussi être assurée sans elle. Deux études indépendantes de l'École polytechnique fédérale de Zurich (EPFZ)[11] et d'IBM Research de Zurich[12] ont confirmé ce point de vue. L'intention du Conseil fédéral est de prévoir un mécanisme aussi simple que possible et de ne pas définir de rôles qui ne soient pas absolument nécessaires. La fonction de la FSI ne fait donc pas l'objet du projet de loi.

1.3 Justification et évaluation des solutions proposées

1.3.1 Solution public-privé

Plusieurs e-ID sont déjà utilisées à l'heure actuelle. Un profil e-ID est ainsi généralement établi lors de la configuration d'un appareil mobile connecté à Internet (par ex. AppleID, Google ID). Son titulaire peut, de cette manière, avoir facilement accès à d'autres services en ligne. Ces e-ID n'étant pas reconnues par l'État, elles ne contiennent pas de données d'identification personnelle fournies par l'État et ne suscitent pas même le degré de confiance que les e-ID établies conformément à la LSIE.

De nombreux services Internet requièrent une identification claire et fiable du titulaire de l'e-ID, vérifiée par un processus standardisé. C'est tout particulièrement vrai des services Internet du domaine de la cyberadministration. Plusieurs États ont de ce fait créé leur propre e-ID, soit en reconnaissant des systèmes privés, soit dans un cadre entièrement étatique. L'expérience a montré que dans ce dernier cas, les solutions techniques mises en place ne sont pas pour autant acceptées par le citoyen et s'accompagnent de coûts d'investissement mais aussi et surtout de coûts d'exploitation élevés pour les pouvoirs publics. Les solutions purement étatiques ne peuvent souvent faire face à l'évolution des technologies que très difficilement et au prix d'adaptations coûteuses. De plus, les procédures peuvent être assez lourdes en raison des exigences du droit des marchés publics et des adaptations des bases légales. Elles ne se développent donc souvent pas comme on le souhaiterait et sont parfois utilisées par obligation et uniquement une fois par an pour effectuer la déclaration fiscale. D'autres explications concernant le développement des e-ID créées par l'État figurent au ch. 1.5.

Selon la solution proposée, la Confédération met en place un cadre fiable, propre à garantir la sécurité, concrétisé par la procédure de reconnaissance et de surveillance. Elle ne doit par contre pas développer les modalités techniques des e-ID et investir dans leur réalisation. La mise en œuvre technique et la commercialisation des e-ID est l'affaire des acteurs privés.

11 Basin, D., Sasse, R., Interoperable, State-approved Electronic Identities, 26 janvier 2018, peut être consulté sur le site de l'OFJ: www.ofj.admin.ch > État & Citoyen > Projets législatifs en cours > Identification électronique (e-ID).

12 Camenisch, J., Dubovitskaya, M., Evaluation Report, Proof of Concept Interoperabilität E-ID, IBM Research, Zurich, 31 janvier 2018, peut être consulté sur le site de l'OFJ: www.ofj.admin.ch > État & Citoyen > Projets législatifs en cours > Identification électronique (e-ID).

On trouve aujourd'hui sur le marché différents moyens d'identification électronique fiables, parfois proposés par des fournisseurs d'identité suisses et bénéficiant d'un accueil de plus en plus favorable. La reconnaissance renforcera l'importance de ces systèmes e-ID – s'ils remplissent les conditions –, qui pourront être utilisés pour les applications de cyberadministration. De surcroît, la loi offre à de nouveaux acteurs la possibilité d'accéder à ce marché, dès lors qu'ils obtiennent la reconnaissance.

Les exigences posées aux systèmes e-ID au sens de la présente loi correspondent le plus possible aux conditions de notification des systèmes e-ID fixées par le règlement eIDAS.

1.3.2 Procédure de reconnaissance

Il existe plusieurs modèles de règlementation de la reconnaissance par la Confédération. Dans le domaine de la signature électronique, la procédure de reconnaissance incombe à un organisme privé. Cet organisme est, selon les règles de l'accréditation, habilité à reconnaître et à surveiller les fournisseurs de services de certification. L'accréditation est, quant à elle, décernée par un organisme d'accréditation désigné par le Conseil fédéral.

En ce qui concerne les plateformes de messagerie sécurisée, c'est une unité administrative du DFJP – l'Office fédéral de la justice (OFJ) – qui est chargée de recevoir et d'examiner les demandes de reconnaissance. Seul le respect des prescriptions techniques est vérifié en détail d'après les règles de l'accréditation. Les conditions et la procédure de reconnaissance des plateformes de messagerie sécurisée sont définies dans l'ordonnance du 16 septembre 2014 sur la reconnaissance des plateformes de messagerie[13]. Les exigences techniques et la liste exacte des normes les plus récentes à respecter font l'objet d'une annexe à cette ordonnance, qui est publiée sur le site Internet de l'OFJ. Ce procédé permet de garantir que les évolutions techniques que connaît le domaine des messageries sécurisées soient prises en compte le plus rapidement possible.

Ce procédé a fait ses preuves. C'est la raison pour laquelle la procédure de reconnaissance des fournisseurs d'identité s'apparente à celle prévue pour les plateformes de messagerie: conformément à la LSIE, l'organisme de reconnaissance (UPIC) est chargé de réceptionner et d'examiner les demandes de reconnaissance des fournisseurs d'identité et des systèmes e-ID et exerce, à ce titre, la même fonction que l'OFJ dans le domaine de la reconnaissance des plateformes de messagerie. Il est prévu que les exigences techniques et les normes à respecter fassent l'objet d'une nouvelle ordonnance départementale et soient mises à jour. Elles se rapprocheront des règles en vigueur pour les signatures électroniques, la cybersanté et les plateformes de messagerie, de sorte qu'il soit possible pour les fournisseurs d'identité de profiter de synergies en matière de certification.

La Confédération assumera sa fonction de surveillance notamment à travers la reconnaissance et son renouvellement périodique, lequel lui permettra de suivre les développements techniques dans le domaine de la sécurité. Elle imposera aux four-

13 RS **272.11**

nisseurs d'identité des exigences en matière de protection des données et vérifiera régulièrement qu'elles sont observées.

Le projet de loi prévoit des mesures qui permettraient d'assurer autant que possible la continuation du système e-ID. Dans le cas où un fournisseur d'identité n'obtiendrait pas le renouvellement de la reconnaissance pour établir des e-ID d'un niveau de garantie substantiel ou élevé ou ne demanderait pas le renouvellement, la loi prévoit que le système e-ID pourra être repris par un autre fournisseur d'identité ou – si aucun ne se présente – par la Confédération (sans contrepartie financière). Les titulaires d'une e-ID, les fournisseurs d'identité et les exploitants d'un service utilisateur doivent pouvoir se fier aux systèmes e-ID mis en place. La reprise du système e-ID par un autre fournisseur d'identité ou par la Confédération permettra de garantir la continuité des prestations.

1.3.3 Procédure de consultation et modifications apportées à l'avant-projet

L'avant-projet a été soumis pour consultation aux cantons, aux partis politiques représentés à l'Assemblée fédérale, aux associations faîtières des communes, des villes, des régions de montagne et de l'économie œuvrant au niveau national et à d'autres organisations intéressées.

Sur 65 destinataires consultés, 48 ont répondu. Dans l'ensemble, 88 participants ont donné leur avis, dont 26 cantons, 8 partis politiques et 54 organisations et autres participants. 40 participants ont écrit de manière spontanée. Il s'agit d'associations de l'économie, issues en particulier du domaine de l'informatique et des télécommunications et des services financiers, d'associations de la cyberadministration et de la cybersanté, et de particuliers.

Suite aux avis reçus, la liste des données d'identification personnelle a été considérablement raccourcie. Le numéro AVS, notamment, ne comptera plus au nombre des attributs de l'e-ID. Le numéro d'enregistrement de l'e-ID, généré de manière aléatoire, ne donnera aucun indice sur le numéro AVS. Le lien entre ces deux numéros ne sera fait qu'au sein du système d'information de Fedpol instauré par l'art. 24.

L'éventualité d'une e-ID pour les personnes morales est un thème récurrent des réponses reçues. Il existe manifestement un besoin d'identifier de manière sûre les personnes morales sur Internet. Cependant, elles n'ont pas l'exercice des droits civils mais agissent à travers leurs organes et plus précisément à travers les personnes physiques inscrites dans le registre du commerce comme habilitées à les représenter, si bien qu'il n'est pas nécessaire de créer une e-ID spécifique. S'il s'agit de savoir quelle entité juridique se trouve derrière tel site Internet, il existe d'autres possibilités, par exemple les certificats visés par la SCSE. Enfin, chaque entreprise en Suisse se voit maintenant attribuer un numéro d'identification des entreprises (IDE) univoque. L'objectif de l'IDE est notamment d'atténuer la charge administrative que représente l'identification des entreprises et d'accroître l'efficience de l'administration dans ce domaine. Il va au-delà de l'objectif d'identification simplifiée des personnes admissibles; une e-ID permet aux titulaires d'interagir dans le monde virtuel et de faire appel à une vaste gamme de services.

Suite aux demandes des participants à la consultation externe, la possibilité de mettre en place des intermédiaires d'identité, les *identity brokers*, a également été examinée. Deux études menées par l'EPFZ et IBM Research ont démontré toutefois que l'interopérabilité entre les systèmes e-ID peut être assurée par le biais de protocoles et ne nécessite pas l'intervention d'un tel intermédiaire. De ce fait, le projet de loi ne règle pas les activités des intermédiaires d'identité. Néanmoins, les fournisseurs d'identité pourront avoir recours aux prestations de tels intermédiaires, dans le cadre de leurs systèmes e-ID, qui devront être reconnus par l'organisme de reconnaissance.

1.4 Harmonisation des tâches et du financement

1.4.1 Identification sûre sur Internet

Il est à prévoir que divers services de la Confédération pourront faire bon usage de l'e-ID, en particulier lorsqu'ils doivent identifier de façon sûre les personnes physiques qui sont en contact direct avec l'administration fédérale. L'e-ID constitue une solution adaptée pour que des systèmes informatiques divers puissent procéder à l'identification et à l'authentification sûre des personnes, par exemple pour la commande en ligne d'extraits du casier judiciaire ou du registre des poursuites, ou pour la saisie de données dans les systèmes d'information des secteurs agricole et vétérinaire.

L'e-ID peut également être utilisée pour identifier et authentifier les employés de l'administration fédérale dans divers contextes. À ce titre, il constitue une étape importante dans la réalisation des projets IAM entrepris par la Confédération.

Les ressources nécessaires au projet et son financement sont détaillés aux ch. 1.4.3 et 3.1. Les dépenses supplémentaires se limiteront aux frais liés à l'adaptation des solutions informatiques et à l'acquisition des prestations auprès des fournisseurs d'identité. La simplification des processus permettra sans doute de réaliser des économies à cet égard.

1.4.2 Nouvelles tâches

La LSIE crée de nouvelles tâches pour l'administration fédérale. D'une part, Fedpol sera chargé de mettre en place un système d'information comprenant une interface pour la communication des données d'identification personnelle, et d'autre part, l'UPIC s'occupera des procédures de reconnaissance et de la surveillance des fournisseurs d'identité reconnus (voir ch. 1.2.6).

Fedpol accomplira les tâches suivantes:

a. vérifier l'identité des requérants,

b. gérer et maintenir les infrastructures informatiques qui lui sont nécessaires (page Web pour les requérants, interface avec les fournisseurs d'identité et

rattachement des banques de données internes de l'administration comme ISA, Infostar, etc.),

c. apporter un soutien technique aux banques de données internes à l'administration concernées,

d. apporter un soutien technique aux fournisseurs d'identité reconnus.

La règlementation dans le domaine des documents d'identité relève de sa compétence; c'est lui qui a développé les concepts relatifs à l'e-ID. La plupart des banques de données qui serviront de source lors de la vérification des données d'identification personnelle sont dans le champ d'activité du DFJP.

L'UPIC, pour sa part, sera chargée de:

a. reconnaître les fournisseurs d'identité,

b. surveiller les fournisseurs d'identité reconnus,

c. tenir et publier la liste des fournisseurs d'identité reconnus,

d. développer et mettre à jour les exigences techniques et organisationnelles auxquelles les fournisseurs d'identité doivent satisfaire pour être reconnus,

e. se tenir informée sur les évolutions technologiques dans le domaine des e-ID ainsi que sur toute autre question liée à la sécurité informatique.

L'UPIC exercera, outre des fonctions de reconnaissance, des fonctions de contrôle comparables à celles assumées par l'organe de contrôle visé par le règlement eIDAS. Elle assume déjà des fonctions de contrôle similaires au sein de la Confédération.

Les compétences du Préposé fédéral à la protection des données et à la transparence (PFPDT) prévues par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[14] sont réservées.

1.4.3 Financement

1.4.3.1 Prestations préalables de la Confédération

Le financement du projet est assuré jusqu'à hauteur de 6 920 000 francs par les fonds dont dispose le DFJP (y inclus la part prise sur les ressources centralisées destinées aux TIC et la participation de Cyberadministration suisse).

Vu les résultats de la consultation, il convient de créer un logiciel à part pour la recherche du numéro AVS, ce qui représente une dépense supplémentaire de 750 000 francs. Il en résultera des coûts supplémentaires de 230 000 francs. Le simulateur devra aussi être développé et entretenu. Les besoins supplémentaires pour des dépenses uniques, qui devront faire l'objet d'une demande de crédit pour la période de 2018 à 2020, se monteront à 980 000 francs. 100 000 francs proviendront de Cyberadministration suisse; la demande portera sur 880 000 francs, à prendre en compte sur les ressources centralisées destinées aux TIC.

14 RS **235.1**

Le recours à des tiers sera financé par le crédit d'engagement «Renouvellement du passeport et de la carte d'identité suisses» (V0224.00) de Fedpol, qui est de 19,6 millions de francs.

1.4.3.2 Financement par les émoluments

Plusieurs modèles de financement pour les prestations fournies par la Confédération aux fournisseurs d'identité ont été examinés. Si on a envisagé un modèle «prépayé», qui prévoyait que le fournisseur d'identité verse à l'État un émolument couvrant dans la mesure du possible les coûts, sans pour autant être sûr que la diffusion rapide de l'e-ID génère des recettes suffisantes pour ce fournisseur d'identité, celui-ci n'a pas été retenu. A également été rejeté un modèle prévoyant la vérification gratuite des données attestées après la première communication de ces données, car un tel modèle aurait occasionné des déficits importants pour la Confédération. Est donc proposé ici un modèle de «paiement à l'usage» financé par les émoluments.

D'après ce modèle, il faut édicter une ordonnance sur les émoluments. Afin d'accélérer la diffusion des e-ID, la première communication des données d'identification personnelle lors de la procédure d'établissement est gratuite si l'obtention et l'utilisation de l'e-ID sont également gratuites pour le requérant. Un émolument modeste est cependant perçu pour chaque autre communication de données d'identification personnelle. Cet émolument s'élèvera, conformément à une ordonnance que le Conseil fédéral doit élaborer, à une ou plusieurs dizaines de centimes. En fonction de la diffusion des e-ID au sens de la présente loi, et notamment de celles présentant un niveau de garantie *substantiel* ou *élevé*, de nouvelles recettes qui permettront de couvrir suffisamment les coûts pourront être générées.

1.4.3.3 Indemnisation par les exploitants d'un service utilisateur

Ce sont en premier lieu les exploitants d'un service utilisateur – qu'il s'agisse d'entreprises du secteur privé ou d'autorités – qui tirent un avantage de l'utilisation des e-ID par la simplification de leurs processus et la réduction de leurs coûts (par ex. moins de guichets, de papier et de changements de support ou de format de fichier, processus plus rapides, modèles de transactions novateurs, inutilité de développer leur propre mécanisme d'identification). Ils devraient par conséquent être prêts à voir l'utilisation des systèmes e-ID soumise à rémunération. C'est aux acteurs du marché qu'il revient de définir le mode de facturation des services qu'ils proposent.

1.4.4 Remarque concernant les marchés publics

Autorités en tant qu'exploitants d'un service utilisateur

Les autorités qui proposent un service utilisant les e-ID seront des exploitants d'un service utilisateur au sens de la LSIE et devront conclure un accord avec au moins un fournisseur d'identité pour utiliser un système e-ID.

Une application de cyberadministration pour laquelle les prestations en matière d'identification sont nécessaires servira à remplir une tâche d'intérêt public. Une autorité est un service soumis au droit des marchés publics; les prestations en matière d'identification sont des prestations informatiques soumises au droit des marchés publics. La LSIE crée un marché pour ces prestations qui sont fournies contre une rétribution.

Pour déterminer quelles prestations proposées par les fournisseurs d'identité acquérir, l'autorité devra donc effectuer une procédure d'adjudication conformément aux règles applicables aux marchés publics (loi fédérale du 16 décembre 1994 sur les marchés publics [LMP][15] ou droit cantonal), à moins que la Confédération n'instaure une unité administrative qui gère un système e-ID pour répondre aux besoins des autorités (art. 10 LSIE).

Reconnaissance des fournisseurs d'identité

La reconnaissance des fournisseurs d'identité n'est en revanche soumise à aucune procédure d'adjudication puisqu'il s'agit d'un acte relevant de la police économique. Les dispositions correspondantes se fondent sur l'art. 95, al. 1, de la Constitution ([Cst.[16]]; voir ch. 5.1).

L'octroi de la reconnaissance n'aura aucun effet de régulation économique: le nombre de reconnaissances octroyées n'est pas limité et les fournisseurs d'identité reconnus ne jouissent pas de droits exclusifs. Les fournisseurs d'identité non reconnus pourront toujours établir des moyens d'identification électronique, qui ne seront toutefois pas des e-ID au sens de la LSIE. La reconnaissance sera octroyée et renouvelée dès lors que les conditions seront remplies (art. 13, al. 2, LSIE) et que le fournisseur d'identité respectera les exigences techniques et organisationnelles.

1.5 Moyens d'identification électronique reconnus par l'État dans le contexte international et, plus particulièrement, européen

1.5.1 Remarque préliminaire

La Suisse n'est pas le seul pays à être confronté à l'introduction de moyens d'identification électronique. Ce sujet est à l'ordre du jour de nombreux États depuis plus de 15 ans. Au regard du caractère planétaire des services en ligne, il est important de développer, sur les plans conceptuel, technique et juridique, un moyen

15 RS **172.056.1**
16 RS **101**

d'identification électronique reconnu par l'État qui puisse être ultérieurement utilisé au-delà des frontières nationales, et notamment dans l'espace européen. Le règlement eIDAS et les normes techniques s'y rapportant définissent des conditions-cadres qui garantissent l'interopérabilité des différents systèmes nationaux. Le concept pour les systèmes e-ID suisses reconnus tient compte de ces exigences de sorte que les e-ID suisses pourraient également être utilisées dans le contexte international.

Le cadre proposé pour les dispositions et les normes techniques qui réglementeront la reconnaissance des systèmes e-ID et des fournisseurs d'identité est conçu de manière à ce que la reconnaissance mutuelle des systèmes e-ID entre la Suisse et l'UE (conformément au règlement eIDAS), ou bien entre la Suisse et certains États membres de l'UE ou des États tiers, soit possible à l'avenir. Des traités internationaux seraient pour ce faire nécessaires.

1.5.2 Développements de ces quinze dernières années

La plupart des États ont, dans un premier temps, pensé à développer une e-ID à partir de la conception des cartes d'identité. Les questions qui se sont posées concernaient principalement les modalités techniques. Par la suite, de nombreux pays européens ont introduit au cours des quinze dernières années une e-ID rattachée à la carte d'identité, qui est devenue un élément clé de leur système e-ID national. C'est la Finlande qui a ouvert la voie en créant en 1999 une carte d'identité dotée d'une e-ID. Ont suivi l'Estonie, la Belgique, l'Espagne et le Portugal. L'Allemagne a introduit une carte d'identité électronique en 2010. Ces dernières années, des pays du Proche-Orient et d'Asie, notamment, ont mis en circulation de nouvelles cartes d'identité nationales dotées d'une fonction e-ID, Ces projets s'expliquent souvent par le fait que nombre de ces États ne voulaient en aucun cas être en retard dans ce domaine. Les États-Unis et le Royaume-Uni n'ont, quant à eux, pas introduit d'e-ID nationale, ce qui confirme le scepticisme général qui existe dans ces pays concernant les cartes d'identité. Plusieurs États des États-Unis ont cependant introduit des permis de conduire électroniques.

Les premiers systèmes qui sont apparus étaient par exemple fondés sur des cartes dotées de puces à contact, qui était essentiellement basées sur la technologie des cartes de signature. À titre d'exemples, on peut citer les cartes e-ID finlandaises, estoniennes et belges, mais aussi la SuisseID.

Un autre système très répandu est né des efforts déployés par l'industrie européenne des puces pour définir un ensemble de normes ouvrant la possibilité de créer une carte d'identité européenne (ECC). Cette carte est dotée de la fonction ePasseport mise au point par l'OACI et d'une fonction associée permettant une identification en ligne. La Suède, Monaco, la Lettonie, la Finlande (2e génération) et les Pays-Bas disposent de cartes d'identité de ce type. La norme ECC n'a jamais cessé d'être modifiée. Certains éléments ont toutefois été repris, notamment dans les pays membres de l'UE, pour les documents pour étrangers (titres de séjour pour les membres de pays tiers), ce qui s'explique par le fait que l'UE peut légiférer dans ce

domaine (et non dans celui des cartes d'identité). Le titre de séjour biométrique pour étrangers délivré par la Suisse satisfait, lui aussi, aux exigences de cette norme.

L'introduction en 2010 de la carte d'identité électronique en Allemagne (ePA) est représentative de la direction prise pour le développement de l'e-ID. Cette carte contient, pour l'essentiel, les éléments mentionnés précédemment mais a fait l'objet de certaines améliorations, de nouvelles procédures techniquement complexes ayant notamment été mises au point pour renforcer la protection de la personnalité. Les prestataires de services (fournisseurs, exploitants d'un service utilisateur) doivent ainsi s'enregistrer auprès de l'État pour accéder à certains attributs et également s'authentifier lors de l'utilisation de la carte.

Ces dernières années, la carte d'identité électronique allemande est, dans une certaine mesure, devenue une référence mondiale pour la création d'e-ID nationales. En Allemagne, la moitié environ de la population possède désormais la carte d'identité électronique, mais seules 3 % de ces cartes sont dotées d'une fonction d'identification électronique active et utilisées de manière correspondante. On ne sait pas encore si la fonction e-ID sera un jour introduite à large échelle. Il s'avère en effet que cette carte bénéficie d'un accueil peu favorable auprès du secteur privé et des citoyens car, même si elle offre un degré de sécurité très élevé, elle est trop difficile à utiliser au quotidien et est très onéreuse. Cette solution exige que les citoyens se procurent et utilisent des éléments d'infrastructure spécifiques tels que des systèmes de lecture et des logiciels. L'État doit en outre effectuer des adaptations et des mises à jour constantes et en informer les utilisateurs, ce qui renchérit considérablement les coûts d'exploitation.

Le 22 août 2017, l'Allemagne a notifié à la Commission européenne la fonction d'identification en ligne de la carte d'identité et du titre de séjour, au plus haut niveau de garantie prévu par le règlement eIDAS. La notification a été publiée le 26 septembre 2017 au Journal officiel de l'Union européenne. Cinq autres pays sont en phase de préparation de la notification de leur service e-ID national: le Danemark, l'Espagne, la France, la Grande-Bretagne et l'Italie (pré-notification).

Les autres solutions e-ID exigeant que le citoyen dispose d'éléments d'infrastructure spécifiques se heurtent, elles aussi, à des problèmes d'acceptation. La solution classique consistant à lier l'e-ID à une carte n'a pas eu de véritable succès. Il s'est cependant avéré que les solutions flexibles permettant d'utiliser le smartphone comme support sont mieux acceptées. En Estonie, où les e-ID sont les plus répandues, celles-ci sont principalement installées sur des smartphones.

1.5.3 Solutions alternatives

Ces dernières années, les réflexions relatives aux mesures prises par l'État pour promouvoir les e-ID ont pris une nouvelle orientation. La principale raison en est que le cycle de production d'une carte d'identité nationale est très long en comparaison de la vitesse de développement dans le monde électronique et qu'une solution étatique ne tient pas suffisamment compte des besoins toujours plus diversifiés des utilisateurs.

Guidés par le projet américain de développement commun d'un «écosystème d'identité électronique»[17], de nombreux pays se sont mis à réfléchir plus en profondeur à la manière dont il faudrait concevoir l'architecture de l'écosystème e-ID national et international en associant tous les acteurs; la contribution que l'État pourrait y apporter fait également l'objet de réflexions. Ces pays sont parvenus à des conclusions divergentes. Aux États-Unis, l'État se contente d'organiser et de promouvoir l'écosystème e-ID; il ne met à disposition aucun service mais a une grosse influence sur le marché dans la mesure où il utilise les e-ID pour ses collaborateurs et qu'il gère des services utilisateurs dans le cadre des offres de cyberadministration. Le NIST a également élaboré des bases conceptuelles importantes en ce qui concerne la gestion fiable et interopérable des identités.

En Suède, en Norvège et au Danemark, les banques se sont imposées comme les principaux fournisseurs d'e-ID pour toutes les branches car elles proposent, depuis longtemps, ces produits pour leurs propres prestations. Des exigences minimales fixées par l'État garantissent la qualité et l'interopérabilité des systèmes. Ces e-ID sont acceptées par les services publics et peuvent être utilisées pour les applications de cyberadministration.

L'UE a fini par tenir compte de ces développements dans le règlement eIDAS et accepte, pour la reconnaissance mutuelle, non seulement les e-ID créées par l'État mais aussi les systèmes e-ID exploités par le secteur privé et reconnus par l'État.

1.5.4 Conséquences pour la Suisse

Les systèmes étatiques qui reposent sur un lien étroit entre l'e-ID et un document d'identité conventionnel, par exemple par le biais d'une puce placée sur la carte d'identité, ne peuvent faire face à l'évolution des technologies que très difficilement et au prix d'adaptations permanentes coûteuses. Au vu des expériences faites dans les pays voisins, une autre solution s'impose à la Suisse.

La solution proposée combine la confiance suscitée par l'État, au travers de la reconnaissance et de la surveillance, avec la maîtrise technologique et le dynamisme de l'initiative privée. Elle libère la Confédération de la contrainte liée aux décisions difficiles concernant les processus technologiques nouveaux et complexes et aux coûts élevés de développement et de mise en œuvre. Elle offre par ailleurs un espace pour des solutions novatrices, flexibles et adaptées aux besoins des acteurs impliqués. Le rôle de la Confédération se limite donc à poser les bases de la règlementation, en définissant les exigences à remplir en vue de la reconnaissance et au regard de la surveillance.

Voici ce qui ressort de la comparaison du concept de réglementation proposé dans le projet de LSIE avec les développements, expériences et réflexions actuelles s'inscrivant dans le contexte international:

17 National Strategy for Trusted Identities in Cyberspace (stratégie nationale pour des identités de confiance dans le cyberespace): écosystème d'identité électronique.

- La Suisse tient compte des expériences faites au cours des quinze dernières années et présente une conception de la reconnaissance des fournisseurs d'identité qualifiée d'exemplaire par plusieurs services.
- La conception suisse garantit l'existence de systèmes e-ID sûrs, obéissant à des exigences précises, et soumis à une procédure de reconnaissance et à la surveillance de l'État.
- Le concept suisse est, dans l'ensemble, conforme au règlement eIDAS de l'UE.
- Il tient compte des bases théoriques et techniques contemporaines concernant la gestion des identités dans l'écosystème numérique, comme celles que le NIST a élaborées.
- Il est très flexible et peut, par conséquent, tenir compte des évolutions technologiques et économiques cruciales.

1.5.5 Règlement eIDAS et exigence de compatibilité

S'il est important de pouvoir utiliser à l'échelle internationale les documents d'identité classiques comportant des données visibles comme documents de voyage et comme moyens d'identification à l'étranger, cela l'est encore plus pour les e-ID. Même si une e-ID ne sert pas de document de voyage, elle est utilisée pour s'identifier en ligne sur un Internet sans frontières. Pour l'UE, qui s'est engagée à créer un marché intérieur unique et sans obstacles, cette préoccupation revêt une importance particulière.

L'UE a adopté le règlement eIDAS le 23 juillet 2014. Outre des dispositions relatives à la réglementation et à la certification des fournisseurs de signature électronique et d'autres services de confiance, ce règlement contient de nouvelles règles concernant la notification et, partant, la reconnaissance mutuelle des systèmes nationaux d'identification électronique. Tous les États membres sont tenus, lorsqu'une e-ID est exigée pour accéder à un service en ligne fourni par un organisme du secteur public, de reconnaître tous les moyens d'identification électronique relevant d'un système notifié et qui ont été délivrés dans un autre État (art. 6 du règlement eIDAS). Cette obligation vaut également pour un État membre qui ne possède pas de système d'identification électronique notifié.

Quelles exigences un système e-ID suisse doit-il satisfaire pour être conforme aux dispositions du règlement eIDAS et pouvoir par la suite éventuellement être notifié? La Suisse n'a bien entendu aucune obligation juridique d'adopter le règlement de l'UE. Compte tenu de l'étroitesse des rapports commerciaux et sociaux qu'elle entretient avec la plupart des pays membres de l'UE, on part cependant du principe qu'elle a tout intérêt à être tôt ou tard intégrée dans le système européen pour l'interopérabilité des systèmes d'identification électronique. Même si, pour l'heure, on ne sait absolument pas si, quand et comment la Suisse sera intégrée dans ce système par un accord bilatéral, le système e-ID suisse doit dès le départ être conçu de façon à pouvoir être notifié.

Le projet vise, entre autres, à encadrer par des dispositions légales et des règles techniques la reconnaissance des systèmes e-ID et des fournisseurs d'identité, de façon à ce que la reconnaissance mutuelle des systèmes e-ID reconnus en Suisse et ceux notifiés selon le règlement eIDAS ou mis en place par certains membres de l'UE ou des États tiers soit possible à l'avenir.

1.6 Mise en œuvre

Le projet de loi règle de manière générale les principes et exigences applicables à l'établissement d'e-ID par des fournisseurs d'identité reconnus et à l'utilisation de ces e-ID. Afin de pouvoir être mises en œuvre, les dispositions proposées devront être précisées par voie d'ordonnance du Conseil fédéral et d'ordonnance départementale. Il est notamment prévu d'y régler les points suivants:

- les procédures qui permettent de vérifier les documents d'identité des ressortissants suisses ainsi que les documents de légitimation et l'identité des étrangers,
- les différents niveaux de garantie et en particulier les exigences minimales d'identification, en tenant compte de l'état actuel de la technique,
- les modalités de la procédure d'établissement,
- les modalités du blocage et de la révocation de l'E-ID,
- les devoirs de diligence des titulaires d'une e-ID,
- les conditions nécessaires pour obtenir la reconnaissance,
- les modalités de la communication des diverses informations prévues par la loi,
- les normes techniques de l'interopérabilité et les interfaces,
- la procédure de retrait de la reconnaissance,
- les normes et les protocoles techniques applicables à la communication des données et la procédure à suivre pour les cas où plusieurs registres de personnes transmettraient des données contradictoires,
- les mesures techniques et organisationnelles à prendre pour assurer la sécurité du traitement et de la communication des données d'identification personnelle,
- les modalités de la procédure d'établissement de l'e-ID selon les dispositions transitoires.

Le Conseil fédéral règlera également par voie d'ordonnance la perception des émoluments conformément à l'art. 46*a* de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[18].

Enfin, le projet de loi s'oriente vers les mesures techniques et organisationnelles applicables dans les domaines de la signature électronique et du dossier électronique

[18] RS **172.010**

du patient. Les dispositions d'exécution de la loi, que ce soit par voie d'ordonnance ou de directive, tiendront compte de ces standards.

1.7 Classement d'interventions parlementaires

L'identification électronique a fait l'objet d'une intervention parlementaire transmise au Conseil fédéral:

– Motion du groupe libéral-radical 17.3083 «Numérisation. Identification électronique pour réduire la bureaucratie dans tout le pays». Elle demande que la LSIE soit mise en œuvre de manière prioritaire, avec une attention particulière portée à l'interopérabilité et à la définition et au contrôle des normes de sécurité. Elle a été acceptée le 20 septembre 2017 par le Conseil national et le 28 février 2018 par le Conseil des États, conformément à la proposition du Conseil fédéral.

Le Conseil fédéral propose de classer cette motion dans le présent message.

2 Commentaire des dispositions

2.1 Structure

La première section de l'avant-projet de loi contient des dispositions générales et des définitions. La deuxième section définit l'établissement des e-ID, c'est-à-dire les conditions d'admissibilité que les requérants de l'e-ID doivent remplir, les niveaux de garantie, la procédure d'établissement, les données d'identification personnelle et leur mise à jour, l'utilisation systématique du numéro AVS pour l'échange de données, le traitement et la conservation des données, le système e-ID subsidiaire de la Confédération et, enfin, le blocage et la révocation de l'e-ID. La troisième section établit les obligations des titulaires d'une e-ID. La quatrième, les prescriptions applicables aux fournisseurs d'identité: leurs obligations, la procédure de reconnaissance, la communication des données, l'accessibilité des e-ID, l'interopérabilité des systèmes, les mesures de surveillance et le retrait de la reconnaissance. La cinquième section expose les exigences applicables aux exploitants d'un service utilisateur. Les sections 6 et 7, quant à elles, règlent l'organisation et les tâches du service d'identité (Fedpol) et de l'organisme de reconnaissance (l'UPIC). La compétence en matière de réglementation des émoluments est définie dans la section 8. La section 9 fixe les règles de responsabilité. Enfin, la section 10 comprend les dispositions finales, qui incluent le droit transitoire. La modification d'autres actes est réglée en annexe.

2.2 Préambule

La compétence de régler les moyens d'identification électronique (e-ID) résulte de la Constitution. L'art. 95, al. 1, Cst. en particulier autorise la Confédération à légiférer

sur l'exercice des activités économiques lucratives privées. Les fournisseurs d'identité reconnus sont chargés d'établir les e-ID. Afin de pouvoir prétendre à la reconnaissance, ces fournisseurs d'identité doivent remplir des conditions qui limitent leur activité économique lucrative privée.

En outre, l'art. 96, al. 1, Cst. donne à la Confédération la compétence de légiférer afin de lutter contre les conséquences sociales et économiques dommageables des cartels et des autres formes de limitation de concurrence. Or, le projet de loi consacre des mesures à prendre pour combattre les conséquences dommageables résultant de l'activité économique des fournisseurs d'identité occupant une place prépondérante sur le marché, y compris les abus qu'ils peuvent causer.

La loi se fonde par ailleurs sur l'art. 97, al. 1, Cst., qui donne à la Confédération la compétence de légiférer sur la protection des consommateurs. Le projet instaure un système de reconnaissance et de surveillance des fournisseurs d'identité propre à protéger les consommateurs.

La présente loi fédérale règle certains aspects de droit civil relatifs aux relations contractuelles entre les fournisseurs d'identité, les titulaires d'une e-ID et les exploitants d'un service utilisateur. Cependant, étant donné leur importance accessoire, le préambule ne cite pas l'art. 122, al. 1, Cst. qui établit la compétence de la Confédération en matière de droit civil.

2.3 Dispositions générales

Art. 1 Objet et but

Al. 1

La loi règle non seulement l'identification par l'État des titulaires d'une e-ID, mais aussi la reconnaissance et la surveillance des fournisseurs d'identité, les droits et les devoirs des titulaires d'une e-ID et des exploitants d'un service utilisateur, ainsi que le contenu, l'établissement, l'utilisation, le blocage et la révocation des e-ID.

Al. 2

La LSIE contribue à garantir la sécurité et la fiabilité des transactions électroniques (commerce électronique et cyberadministration). De plus, la protection des données devant être préservée, la let. b reprend le but fixé à l'art. 1 LPD. Les Suisses et les étrangers titulaires des documents d'identité nécessaires pourront prouver leur identité de façon fiable dans le monde électronique également. Tout comme avec un document d'identité dans le monde physique, les données d'identification personnelle comme le nom, les prénoms ou l'âge pourront être attestées sur Internet. Une e-ID sert principalement à effectuer des transactions de façon fiable, sur des applications de la cyberadministration ou du commerce électronique par exemple, sans que les partenaires de la transaction n'aient besoin de se rencontrer dans la vie réelle. Les e-ID remplissent une fonction importante en matière de numérisation de l'économie, de l'État et de la société.

Art. 2 Définitions

Let. a

Un fournisseur d'identité gère au moins un système e-ID. La distinction entre les fournisseurs d'identité et les systèmes e-ID est essentielle pour la reconnaissance. Pour un fournisseur d'identité, l'autorité compétente contrôle que les conditions fixées à l'art. 13, al. 2, LSIE sont remplies et que les processus liés à l'établissement des e-ID et à la gestion des systèmes sont respectés. En revanche, lors de la reconnaissance d'un système e-ID, elle accorde une importance particulière au respect des exigences techniques relatives à la sécurité. Un fournisseur d'identité reconnu peut gérer plusieurs systèmes e-ID de niveaux de garantie divers qui ne sont pas tous reconnus. La reconnaissance, son expiration et sa révocation sont réglées aux art. 14 et 19 LSIE.

Let. b

Un service utilisateur est une application informatique dont l'exploitant permet aux utilisateurs de s'identifier grâce à une e-ID, via un système e-ID. Il s'agit par exemple d'entreprises ou de services qui offrent en ligne des biens ou des prestations et qui utilisent un système d'identification pour les transactions.

2.4 E-ID: établissement, types, contenu, blocage et révocation

Art. 3 Conditions d'admissibilité

Remarque préliminaire

La formulation potestative de l'al. 1 garantit que les fournisseurs d'identité n'ont pas l'obligation d'établir une e-ID à l'intention de toute personne qui remplit les conditions nécessaires. L'art. 17 LSIE apporte une restriction à ce principe si le marché ne fonctionne pas, c'est-à-dire si le fournisseur d'identité abuse de sa position dominante sur le marché.

Le requérant devient un titulaire lorsqu'il obtient l'e-ID.

Mineurs

Les mineurs et les personnes dont la capacité d'exercer les droits civils a été partiellement ou complètement retirée pourront obtenir une e-ID. Ils devront disposer d'un document d'identité correspondant aux exigences de la loi. La personne habilitée à les représenter devra demander l'obtention d'une e-ID à leur nom; ils deviendront alors titulaires d'une e-ID. Ils devront cependant l'utiliser sous la surveillance de la personne habilitée à les représenter. Les modalités seront fixées au niveau de l'ordonnance.

Al. 1

Document d'identité comme preuve de l'identité

Pour demander une e-ID, il suffira au requérant d'avoir un document d'identité suisse valable (*let. a*) ou, s'il est étranger, une pièce de légitimation valable et reconnue au sens de l'art. 13, al. 1, de la loi du 16 décembre 2005 sur les étrangers (LEtr)[19] ou une carte de légitimation valable au sens de la législation sur l'État hôte (*let. b, ch. 1*). Les étrangers qui ne possèdent pas de papiers d'identité peuvent demander une e-ID si leur identité a pu être déterminée de façon fiable dans le cadre d'une procédure spéciale d'identification (*let. b, ch. 2*).

Prescriptions relatives aux étrangers

Afin que les étrangers puissent avoir accès aux services utilisateurs, services cyberadministratifs compris, sur la base d'une e-ID, il est prévu d'autoriser l'établissement d'une e-ID pour tous ceux qui ont un titre de séjour attestant une autorisation de séjour ou d'établissement (art. 41, al. 1, LEtr en relation avec l'art. 71, al. 1, de l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative [OASA][20], permis L, B, C), une carte de légitimation (art. 17, al. 1, de l'ordonnance du 7 décembre 2007 sur l'État hôte [OLEH][21] en relation avec l'art. 71*a*, al. 1, OASA) ou un permis de frontalier (art. 71*a* OASA, permis G).

Les personnes de nationalité étrangère titulaires d'un titre de séjour valable au sens de l'art. 41 LEtr pourront donc utiliser une e-ID ainsi que les applications de la cyberadministration. Comme, selon l'art. 89 LEtr, les étrangers doivent être munis d'une pièce de légitimation valable et reconnue au sens de l'art. 13, al. 1, LEtr, tel sera le cas des permis C, B, L et G. Les modalités seront réglées au niveau de l'ordonnance (voir commentaire de l'al. 2).

Les personnes titulaires des permis N, F, S et Ci ne seront pas systématiquement habilitées à obtenir une e-ID, car il n'est pas certain d'emblée que leur identité ait pu être vérifiée de façon fiable.

On renonce à garantir l'accès aux fonctions de l'e-ID aux autres étrangers, en particulier aux titulaires d'un permis N, F, ou S. Nombreux sont les demandeurs d'asile qui ne sont pas en mesure de présenter un document d'identité au cours de la procédure d'asile et qui ne peuvent donc pas être identifiés de façon fiable. Le DFJP (SEM) reçoit de nombreuses demandes de changement ou de rectification des données personnelles pour les personnes admises à titre provisoire, bien souvent sans que ces demandes soient attestées par des documents adaptés. À l'heure actuelle, aucun service électronique dans le domaine de l'asile ne nécessite que les titulaires d'un permis N, F ou S puissent y accéder directement. L'établissement d'e-ID pour ces personnes n'est pas un impératif.

19 RS **143.1**
20 RS **142.201**
21 RS **192.121**

Al. 2

La procédure de vérification des documents d'identité des ressortissants suisses et des documents de légitimation ainsi que de l'identité des étrangers sera réglée par voie d'ordonnance; il sera ainsi possible de s'adapter avec souplesse aux nouvelles technologies. Pour définir les processus d'identification, il est toutefois possible d'imiter les méthodes d'identification fiables utilisées dans le domaine bancaire. Par exemple, la législation sur le blanchiment d'argent détermine avec précision quelles méthodes d'identification des nouveaux clients sont autorisées. Dans ce cadre, une e-ID sera considérée en tant qu'un moyen d'identification ayant une valeur probante.

Toutes les dispositions relatives à la délégation des compétences législatives sont commentées au ch. 5.7.

Art. 4 Niveau de garantie

Al. 1

Toutes les transactions ne requièrent pas le même niveau de garantie. En général, plus le niveau de sécurité est élevé, plus l'obtention est fastidieuse et compliquée pour les utilisateurs et plus les coûts augmentent. Pour cette raison, la loi prévoit que les fournisseurs d'identité puissent proposer des systèmes e-ID de trois niveaux de garantie différents, comme définis par l'UE et le NIST. Les exploitants d'un service utilisateur peuvent déterminer eux-mêmes le niveau de garantie qu'ils souhaitent appliquer (voir art. 20 LSIE).

Pour bénéficier de la reconnaissance, un système e-ID doit offrir un niveau de garantie *faible* au moins. Les systèmes e-ID d'un niveau de garantie *substantiel* ou *élevé* doivent non seulement remplir les conditions minimales, mais aussi satisfaire à d'autres conditions. Cela signifie que les e-ID d'un niveau de garantie élevé remplissent les conditions des niveaux de garantie *faible* et *substantiel*, mais que le contraire n'est pas vrai (compatibilité descendante).

Les e-ID offrent un degré de fiabilité différent selon le niveau de garantie du système. Le niveau de garantie *faible* vise à réduire le risque d'utilisation abusive ou d'altération de l'identité; le niveau de garantie *substantiel* offre une protection élevée contre ce risque, et le niveau de garantie *élevé*, la protection la plus élevée possible.

Al. 2

Les niveaux de garantie se distinguent les uns des autres par les données d'identification personnelle communiquées, la procédure d'établissement, les exigences applicables à l'utilisation des e-ID et la gestion du système, notamment le rythme de la mise à jour des données, Ces conditions sont inscrites dans la loi de la manière la plus neutre possible sur le plan technologique, et seront détaillées par voie d'ordonnance ou de directive; les conditions relatives aux différents types de support d'une e-ID sont également précisées.

Al. 3

Une e-ID d'un niveau de garantie supérieur peut également être utilisée pour un service utilisateur qui requiert un niveau de garantie moins élevé. Les titulaires d'une e-ID peuvent utiliser celui-ci pour tous les services utilisateurs, à condition que l'e-ID soit d'un niveau de garantie égal ou supérieur à celui exigé par l'exploitant du service utilisateur.

Al. 4

Le Conseil fédéral fixera les exigences par rapport aux différents niveaux de garantie, en tenant compte de l'état actuel de la technique. Il règlera en particulier les exigences minimales en matière d'identification.

Art. 5 Données d'identification personnelle

Al. 1, 2 et 3

Le type et la quantité de données d'identification personnelle attribuées à une e-ID dépendent de son niveau de garantie. Alors qu'on requiert des données d'identification de base (numéro d'enregistrement de l'e-ID, le nom d'état civil, les prénoms et la date de naissance) pour une e-ID de niveau de garantie faible, des données supplémentaires (le sexe, le lieu de naissance et la nationalité) seront exigées pour l'établissement d'une e-ID de niveau de garantie substantiel ou élevé. De plus, une photographie sera également requise pour le niveau de garantie élevé.

La communication des données d'identification personnelle au sens de l'al. 2 est soumise à des conditions techniques et organisationnelles plus strictes pour la procédure d'enregistrement, l'identification et le système e-ID.

Al. 4

Dans la mesure où il en a besoin pour accomplir les tâches que lui confie la LSIE, Fedpol pourra ajouter aux données d'identification personnelle des informations complémentaires concernant la mise à jour des données dans son système d'information.

Les fournisseurs d'identité privés offrant des prestations supplémentaires peuvent traiter des données qui ne sont pas prévues par la présente loi, comme l'adresse de livraison ou les indications de paiement, pour autant qu'ils obtiennent à cette fin le consentement du titulaire de l'e-ID. Par contre, un fournisseur d'identité public (au sens de l'art. 10) peut uniquement procéder à un tel traitement de donnée si cette compétence est prévue par la loi.

Art. 6 Procédure d'établissement

Remarque préliminaire

Le requérant et Fedpol lancent la procédure d'établissement. Suivant le niveau de garantie, le requérant doit se présenter en personne ou s'identifier d'une manière équivalente. Le Conseil fédéral règle la procédure d'établissement selon les niveaux

de garantie; la délégation de cette compétence est mentionnée à plusieurs reprises dans le projet, en particulier aux art. 3, al. 2, 4, al. 4, et 6, al. 5.

Al. 1

Il n'y a pas d'obligation d'obtenir une e-ID. Si quelqu'un veut en avoir une, il devra contacter un fournisseur d'identité. La demande doit émaner du futur titulaire de l'e-ID (requérant). Le fournisseur d'identité ne sera cependant pas autorisé à établir l'e-ID lui-même, même si la personne concernée est l'un de ses clients.

Bien que devant avoir recours à un fournisseur d'identité, le requérant sera amené à s'identifier directement auprès de Fedpol. Il est prévu, par exemple, que, lors du processus d'identification, il soit transféré du site Internet du fournisseur d'identité sur le site Internet de Fedpol afin de fournir les informations requises. Ainsi, le requérant pourra déposer sa demande d'identification directement au travers du système d'information de Fedpol.

Al. 2

Fedpol contrôle que le requérant remplit les conditions définies à l'art. 3. Si tel est le cas, il procède à son identification au moyen des informations requise pour le niveau de sécurité concerné. Ces informations sont issues des registres fédéraux selon l'art. 24, al. 3. Lorsque la personne concernée a été identifiée conformément au niveau de garantie demandé et y consent, Fedpol communique au fournisseur d'identité les données d'identification personnelle visées à l'art. 5.

Al. 3

Fedpol journalise les communications de données effectuées dans le cadre de la procédure d'établissement. Cette journalisation permet de garantir la traçabilité des opérations et peut servir de preuve en cas d'un différend entre les parties concernées. Elle est en outre une conséquence du devoir d'information qui incombe à Fedpol à l'encontre des titulaires de l'e-ID.

Al. 4

Le fournisseur d'identité associe les données d'identification personnelle à l'e-ID et garantit que celle-ci est attribuée à la personne physique correspondante (rattachement). Pour Mobile-ID par exemple, l'e-ID est attribuée à une carte SIM qui sert aussi de support pour l'abonnement du requérant et qui est insérée dans l'appareil. Les exigences relatives à l'attribution dépendent du niveau de garantie. Le fournisseur d'identité doit notamment contrôler le ou les facteurs d'authentification nécessaires pour l'utilisation de l'e-ID. Il vérifie par exemple que le requérant possède un appareil personnel, qu'il connaît la réponse à une question secrète ou que les données biométriques lui correspondent.

Al. 5

Le Conseil fédéral précisera les modalités de la procédure d'établissement dans une ordonnance, où il fixera notamment le déroulement de la procédure et les données d'identification personnelle supplémentaires, connues uniquement du requérant, qui seront utilisées pour l'identifier avec certitude.

Art. 7 Mise à jour des données d'identification personnelle

Certains attributs d'identité peuvent être modifiés, notamment le nom. Le projet prend en compte cette réalité avec l'obligation de mettre à jour les données de façon régulière.

La fiabilité de l'e-ID est renforcée par une mise à jour régulière des données d'identification personnelle avec les systèmes d'information étatiques. La périodicité maximale de ces mises à jour est définie pour chaque niveau de garantie. Les fournisseurs d'identité sont responsables de la demande de mise à jour, qui se fait par une requête automatique à Fedpol, fondée sur le numéro d'enregistrement de l'e-ID. Ils payent un émolument pour cette prestation.

Art. 8 Utilisation systématique du numéro AVS pour l'échange de données

Remarque préliminaire

Le numéro AVS au sens de la LAVS ne doit pas être révélé à large échelle et sans surveillance, puisque des personnes ou des groupes de personnes pourraient alors en faire une utilisation systématique sans y être habilités. L'art. 8 du projet établit la base légale et les principes de traitement associés à l'utilisation systématique du numéro AVS pour les e-ID par Fedpol.

Al. 1

Fedpol sera habilité à utiliser systématiquement le numéro AVS pour identifier une personne lors des échanges de données électroniques avec les registres de personnes visés à l'art. 24, al. 3, LSIE. Ce numéro servira d'identifiant univoque lors de l'interrogation d'autres banques de données qui l'utilisent également de façon systématique. Il est indispensable pour comparer ou communiquer automatiquement les données issues de banques de données différentes; seul ce numéro permet de garantir que les personnes sont identifiées de manière univoque dans les différents registres, même après un changement de nom. Il est possible de changer d'identité légalement en faisant modifier son nom; de nouveaux documents d'identité qui ne permettent pas de déduire l'ancienne identité sont alors établis. Le numéro AVS permet toutefois d'attribuer les données à une seule et même personne.

Al. 2

Fedpol ne pourra rendre le numéro AVS accessible en ligne aux exploitants de service utilisateur que si ceux-ci sont eux-mêmes habilités à utiliser systématiquement ce numéro en vertu des dispositions de la LAVS. La possibilité de communiquer cet attribut d'identité à des tiers non habilités à l'utiliser systématiquement doit être techniquement exclue.

Puisque le numéro AVS ne peut pas servir de numéro d'enregistrement de l'e-ID, il sera nécessaire de développer une nouvelle application, par laquelle les organismes habilités à utiliser systématiquement le numéro AVS pourront établir la correspondance entre ces deux identifiants.

Art. 9 Traitement et conservation des données

Remarque préliminaire

Le traitement, la conservation et la communication des données sont l'activité proprement dite des fournisseurs d'identité. L'identification et l'authentification sont des services proposés aux exploitants d'un service utilisateur et aux titulaires d'une e-ID. Les fournisseurs d'identité ayant un rôle d'intermédiaire, il est d'autant plus important de réglementer la protection des données. La LPD et ses ordonnances d'exécution s'appliqueront à toutes les parties impliquées. L'article précise le but et définit les conditions spécifiques du traitement et de la conservation des données par les fournisseurs d'identité. Il précise notamment les exigences de la LPD par rapport au traitement des données et il les renforce en ce qui concerne les mesures de sécurité à prendre.

Al. 1 et 2

Les dispositions des al. 1 et 2 correspondent au cadre fixé par la législation sur la protection des données. Le titulaire peut choisir quelles données d'identification personnelle sont communiquées à l'exploitant du service utilisateur lorsqu'il se sert de l'e-ID. Seules les données d'identification personnelle qui correspondent au niveau de garantie exigé par le service utilisateur peuvent être communiquées. Ces données ne peuvent être traitées et conservées par le fournisseur d'identité que jusqu'à la révocation de l'e-ID. En outre, elles ne peuvent être utilisées que pour l'identification au sens de la LSIE. Pour les e-ID d'un niveau de garantie substantiel, le fournisseur d'identité peut utiliser la photographie du titulaire de l'e-ID (enregistrée dans le système d'information visé à l'art. 24) uniquement dans le cadre de la procédure d'établissement.

Al. 3

Cet alinéa va au-delà des dispositions de la LPD en exigeant que les fournisseurs d'identité aient recours à des mesures de sécurité spécifiques. Il garantit que les données d'identification personnelle, les données concernant l'utilisation et les autres données sont traitées et conservées de manière sûre. Ces trois catégories de données seront conservées séparément tant du point de vue physique qu'organisationnel. Cette séparation est faite en fonction du type de données et du but de leur traitement. Elle représente une mesure de sécurité supplémentaire propre à empêcher les personnes non autorisées d'avoir accès à toutes les données concernant le titulaire d'une e-ID. Cette mesure vise notamment à limiter les conséquences néfastes d'un accès non autorisé au système.

Art. 10 Système e-ID subsidiaire de la Confédération

Le projet part de l'hypothèse du bon fonctionnement du marché. Si toutefois aucun fournisseur d'identité du secteur privé ne souhaitait faire reconnaître un système e-ID d'un niveau de garantie *substantiel* ou *élevé*, la Confédération se réserve la possibilité de gérer son propre système e-ID à ces niveaux de garantie. Dans ce cas, l'unité administrative chargée de gérer un système e-ID sera soumise au même traitement que les fournisseurs d'identité concernant l'application de la présente loi:

les dispositions applicables aux fournisseurs d'identité s'appliqueront également à elle.

Le Conseil fédéral ne pourra cependant charger une unité administrative de cette tâche que si elle est autorisée à fournir des prestations commerciales à des tiers par l'art. 41*a* de la loi du 7 octobre 2005 sur les finances (LFC)[22]. Les unités qui entrent en ligne de compte sont le Centre de services informatiques du DFJP, l'Office fédéral des constructions et de la logistique et l'Office fédéral de l'informatique et de la télécommunication (voir art. 41*a*, al. 1, LFC).

Art. 11 Blocage et révocation

Al. 1 à 4

En vertu de l'art. 23, al. 2, LSIE, Fedpol veillera à ce qu'il soit possible de vérifier en tout temps, au moyen d'une procédure usuelle, la validité du numéro d'enregistrement de l'e-ID. Actuellement, il est prévu qu'il tienne une liste électronique que les fournisseurs d'identité devront périodiquement consulter. Ils devront bloquer ou révoquer immédiatement toute e-ID dont le numéro d'enregistrement serait invalide. La consultation régulière de la liste de Fedpol est de nature à accroître la confiance dans les e-ID établies conformément à la LSIE, et elle sera donc gratuite. Les fournisseurs d'identité devront à leur tour mettre en place une fonction gratuite de consultation, limitée aux e-ID qu'ils auront établies eux-mêmes (art. 15, al. 1, let. c, LSIE).

La distinction entre le blocage d'une e-ID et le blocage et la révocation d'un numéro d'enregistrement de l'e-ID est la suivante: si le titulaire signale par exemple qu'il a perdu le support de son e-ID et que des tiers risquent d'accéder à cette dernière, l'e-ID est à invalider provisoirement. Le statut de son numéro d'enregistrement ne change cependant pas, car il est lié à l'identité officielle de la personne concernée, valable indépendamment du moyen d'identification. Pour éviter les abus, le fournisseur d'identité devra vérifier la provenance de l'information avant de bloquer l'e-ID (*al. 1*).

L'e-ID pourra être réactivée et utilisée à nouveau dès que le motif du blocage aura disparu. Par contre, toutes les e-ID attachées à un numéro d'enregistrement devront être révoquées si ce numéro lui-même ne doit plus être utilisé, par exemple parce que son titulaire est décédé (*al. 3*). Une e-ID révoquée ne pourra plus être réactivée, contrairement à une e-ID provisoirement bloquée. Le fournisseur d'identité informera aussitôt le titulaire de l'e-ID du blocage de celle-ci.

Al. 5

Le Conseil fédéral arrêtera les modalités du blocage et de la révocation. Il définira en particulier les cas de révocation de l'e-ID.

22 RS **611.0**

2.5 Titulaires d'une e-ID

Art. 12

Al. 1 et 2

Les obligations des titulaires d'une e-ID établies dans la LSIE correspondent à peu près aux devoirs de diligence qui doivent habituellement être respectés lors de l'utilisation d'une carte de crédit ou d'une carte bancaire. Il est par exemple nécessaire et raisonnablement exigible de ne pas révéler le code PIN éventuel et de ne pas le conserver au même endroit que le support de l'e-ID. Il est également raisonnablement exigible d'activer les fonctions de restriction d'accès à l'appareil mobile qui sert de support de l'e-ID, par exemple la reconnaissance des empreintes digitales ou le code PIN, ou d'installer un logiciel antivirus sur ce support.

Malgré toutes les précautions possibles, personne n'est totalement à l'abri d'un vol d'identité. Des sanctions pénales adéquates pour punir un tel comportement devraient être mises en place. Le projet de loi du 15 septembre 2017 sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales[23] complète le code pénal[24] par un art. 179^{decies}, une disposition punissant l'usurpation d'identité d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire. Afin d'éviter des redondances, le projet de loi ne contient pas de dispositions sanctionnant le même comportement.

Al. 3

Dans le cadre de la responsabilité délictuelle (extracontractuelle), l'art. 12 du projet représente une norme de protection au sens du droit de la responsabilité. Le Conseil fédéral peut fixer par voie d'ordonnance quels devoirs de diligence supplémentaires doivent être respectés par le titulaire de l'e-ID. Lorsque les devoirs de diligence sont définis de façon claire, le titulaire a la possibilité de se libérer de la responsabilité délictuelle. L'ordonnance établira par exemple que toute erreur dans les données d'identification personnelle doit être immédiatement signalée au fournisseur d'identité, comme tout soupçon d'utilisation abusive ou toute perte de l'e-ID.

2.6 Fournisseurs d'identité

Art. 13 Reconnaissance

Remarque préliminaire

Les fournisseurs d'identité seront soumis à un examen approfondi dans le cadre de la procédure de reconnaissance, comprenant un contrôle des inscriptions au casier judiciaire et des finances du fournisseur et un audit et visant à s'assurer qu'il accomplira sa fonction comme il se doit. La reconnaissance des fournisseurs d'identité comprendra le contrôle et la reconnaissance de leurs systèmes e-ID. En revanche, les

23 FF **2017** 6803
24 RS **311.0**

conditions techniques que les services utilisateurs doivent respecter ne seront réglées qu'indirectement par le biais des conditions et des exigences établies pour les systèmes e-ID. En ce qui concerne la sécurité et la fiabilité, ces exigences correspondent à celles formulées par le NIST dans le *Cybersecurity-Framework* (cadre pour la sécurité sur Internet)[25].

Al. 1

Un fournisseur d'identité souhaitant établir des e-ID au sens de la LSIE devra respecter diverses exigences techniques et organisationnelles. L'UPIC contrôlera régulièrement que c'est le cas. Les conditions à respecter garantissent que les fournisseurs d'identité et les données qu'ils ont enregistrées peuvent être soumis à un contrôle suffisant.

Let. a

Les personnes physiques ou morales qui ne sont pas inscrites au registre du commerce ne pourront pas bénéficier de la reconnaissance. Comme les autorités peuvent aussi s'y faire inscrire[26], il leur sera possible en principe de gérer des systèmes e-ID reconnus.

Let. b et c

Les personnes qui contrôlent les documents d'identité présentés lors de la procédure d'établissement et qui pourraient avoir une influence sur la communication des données lors de la gestion du système sont soumises à une exigence organisationnelle. Elles devront disposer d'une formation suffisante, posséder les connaissances, l'expérience et les qualifications nécessaires et ne pas représenter un danger pour la sécurité.

Une personne condamnée par un jugement entré en force pour certaines infractions ou une personne endettée et donc susceptible de faire l'objet de chantages pourrait par exemple représenter un danger pour la sécurité. Des extraits du casier judiciaire et du registre des poursuites permettront de vérifier ces points-là.

Let. d

Le respect des normes de sécurité en vigueur et la certification des processus permettront de prouver que les systèmes e-ID sont fiables et sûrs.

Let. e

Le fournisseur d'identité devra garantir que les données seront traitées et conservées exclusivement en Suisse. Il y a lieu d'empêcher que des tiers non autorisés établis à l'étranger puissent avoir accès aux données. La notion de traitement des données englobe toutes les opérations effectuées sur les données indépendamment des moyens et procédés utilisés, en particulier la collecte, la conservation, l'archivage et la destruction. Cette disposition s'applique à toutes les données que le fournisseur

25 National Institue of Standards and Technology (NIST), U.S. Department of Commerce, Cybersecurity Framework; le texte peut être consulté sur le site du NIST: www.nist.gov.

26 Voir l'art. 2, let. a, ch. 13, de l'ordonnance du 17 octobre 2007 sur le registre du commerce (RS **221.411**), avec une référence à l'art. 2, let. d, de la loi du 3 octobre 2003 sur la fusion (RS **221.301**).

d'identité traite dans le cadre des prestations prévues par la LSIE, y compris les données temporaires, celles provenant d'enregistrements intermédiaires et les données secondaires.

Let. f

Le fournisseur d'identité aura l'obligation de s'assurer contre les risques en matière de responsabilité civile. La responsabilité sera régie par le code des obligations (CO)[27] (voir art. 28 LSIE).

Let. g

Il va de soi que seuls les fournisseurs d'identité qui respectent le droit applicable pourront être reconnus. Ce sont non seulement la LSIE et ses dispositions d'exécution qui devront être observées, mais également d'autres actes tels que la LPD.

Al. 3

Les évolutions techniques de ces prochaines années dans le domaine de l'identification et de l'authentification électroniques sont imprévisibles, si bien que la reconnaissance devra être renouvelée à intervalles réguliers. Le Conseil fédéral définira par voie d'ordonnance la forme et le contenu des contrôles à effectuer. Il pourrait par exemple soumettre les fournisseurs d'identité à l'obligation de présenter un rapport de sécurité annuel à l'UPIC.

Al. 4

La réglementation de la procédure et des détails techniques est déléguée aux autorités chargées d'édicter les ordonnances.

Les conditions de la reconnaissance seront précisées par voie d'ordonnance ou de directive, en particulier les règles techniques et les règles de sécurité, les normes et les protocoles techniques applicables aux systèmes e-ID et la couverture d'assurance requise. L'UPIC contrôlera régulièrement l'application de ces règles, qui sera un prérequis de la reconnaissance des systèmes e-ID.

Art. 14 Expiration de la reconnaissance

Al. 1

Pour pouvoir gérer un système e-ID, un fournisseur d'identité doit disposer de ressources suffisantes. Au moment de l'ouverture d'une faillite, cette capacité économique disparaît et la reconnaissance expirera en vertu de la loi. Les systèmes e-ID seront insaisissables et ne rentreront pas dans la masse en faillite. Les données attestées par le biais d'un système e-ID ne seront pas négociables et n'auront donc pas de valeur commerciale. La reconnaissance expirera également si le fournisseur d'identité cesse son activité.

Al. 2 et 3

Ces dispositions visent à préserver les réseaux e-ID déjà constitués. Puisque le produit éventuel de la reprise d'un système e-ID tombe dans la masse en faillite, un

27 RS **220**

système e-ID dans son ensemble prend une valeur commerciale, même si les données prises individuellement ne sont pas négociables.

Al. 4

En cas d'expiration de la reconnaissance, la volonté du titulaire de l'e-ID doit être respectée. Si celui-ci ne consent pas à la reprise de ses données par un autre fournisseur d'identité ou par la Confédération, ces données ne seront pas transférées, mais elles seront détruites.

Al. 5

Il importe de permettre que les réseaux e-ID mis en place puissent continuer de fonctionner si aucun fournisseur d'identité ne peut reprendre les systèmes e-ID de celui dont la reconnaissance expire, tant dans l'intérêt de l'utilisateur que des partenaires économiques qui y ont placé leur confiance. Dans une telle situation, l'UPIC ordonnera soit que la Confédération reprenne les systèmes e-ID sans contrepartie financière, soit que les données qu'ils contiennent soient détruites.

Art. 15 Obligations

Al. 1

Let. a

Le fournisseur d'identité gèrera au moins un système e-ID. Il pourra en proposer plusieurs, de niveaux de garantie différents, et les faire reconnaître par l'État, mais n'y sera pas contraint. Les conditions techniques et organisationnelles de la reconnaissance, réglées par voie d'ordonnance ou de directive, incluent la sécurité des processus associés à la gestion du système.

Let. b

Lors de l'établissement d'une e-ID, le fournisseur d'identité sera responsable de l'attribution correcte des données d'identification personnelle à cette e-ID ainsi que du rattachement et de la remise corrects de l'e-ID à une personne physique. Pour ce faire, il suivra trois étapes qui pourront varier selon le niveau de garantie:

1. Avec le numéro d'enregistrement de l'e-ID, le fournisseur d'identité attribue de manière univoque les données d'identification personnelle communiquées par Fedpol (art. 5 LSIE) à l'e-ID et au moyen d'authentification qui permet d'établir l'identité du titulaire. Au moins pour le niveau de garantie élevé, le moyen d'authentification est généralement directement intégré au support (par ex. à la puce d'une carte ou à la carte SIM d'un téléphone portable).
2. Il garantit que l'e-ID est bien attribuée à la personne physique identifiée (par exemple que les données déjà présentes sur la puce de la carte correspondent à la même personne, ou que l'abonnement de téléphone est au même nom).
3. Il veille à ce que l'e-ID soit remise à cette personne, par exemple par l'envoi d'une lettre recommandée, ou lorsqu'elle se présente en personne, ou bien encore au cours d'un contact virtuel sûr pendant lequel le moyen d'authentification est rattaché à la bonne personne.

Let. c

Le domaine de la communication sécurisée des données est sujet à des évolutions techniques rapides. L'avant-projet prévoit que la validité de tous les e-ID puisse être vérifiée selon une procédure usuelle, par analogie avec la formulation employée dans la SCSE. Fedpol pourrait par exemple tenir et publier une liste des numéros d'enregistrement d'e-ID qui ne peuvent donner droit, temporairement ou durablement, à l'obtention ou à l'utilisation d'une e-ID, comme en cas de déclaration d'absence, de décès d'une personne ou d'expiration d'un titre de séjour pour un étranger. Le fournisseur d'identité consulterait régulièrement la liste des numéros d'enregistrement des e-ID bloqués ou révoqués et déterminerait si les numéros d'enregistrement des e-ID qu'il a établies sont concernés en suivant la procédure usuelle qu'il a fixée.

Let. d

Le fournisseur d'identité sera tenu de se renseigner sur les nouvelles conditions de sécurité et de contrôler que les systèmes qu'il gère les respectent.

Let. e

La mise à jour des données d'identification personnelle améliorera la sécurité. La périodicité de cette mise à jour dépendra du niveau de garantie; elle est fixée à l'art. 7, al. 1.

Let. f et g

Afin de s'assurer du bon fonctionnement du système e-ID, le fournisseur d'identité aura l'obligation de communiquer aux autorités concernées certaines informations dont il aura pu prendre connaissance. Ainsi, il devra signaler à Fedpol les erreurs dans les données d'identification personnelle et communiquer à l'UPIC les incidents concernant la sécurité d'un système e-ID ou de l'utilisation de l'e-ID qui lui ont été signalés ou qu'il a lui-même découverts.

Let. h

Chaque fois qu'une e-ID est utilisée et que des données d'identification personnelle doivent être communiquées, le fournisseur d'identité doit obtenir le consentement du titulaire. Celui-ci doit expressément déterminer quelles données d'identification personnelle peuvent être communiquées à l'exploitant d'un service utilisateur à chaque utilisation de l'e-ID.

Let. i

La LSIE va au-delà de l'art. 8 LPD concernant le droit d'accès à ses propres données; elle oblige le fournisseur d'identité à communiquer sur demande toutes les données qu'il traite et qui concernent le requérant. Pour des raisons de transparence et de confiance, les titulaires de l'e-ID auront accès en ligne à leurs données d'identification personnelle et aux données relatives à l'utilisation qu'ils font de l'e-ID. La let. i prévoit donc une obligation, pour le fournisseur d'identité, d'accorder un accès à ces données, pour autant qu'il n'ait pas déjà détruit les données journalisées conformément à la let. j.

Let. j

Les données que le fournisseur d'identité a enregistrées relatives à l'utilisation d'une e-ID devront être détruites après six mois. Un délai identique est prévu par exemple dans le domaine de la surveillance des télécommunications (voir art. 26, al. 5, de la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication[28]). Les données journalisées peuvent être utiles pour la communication des informations visées à la let. i et pour la reconstitution des transactions en cas de litige.

Les données d'enregistrement, les données de transaction et les autres données que le service utilisateur a consignées sont réservées.

Let. k

Le PFPDT pourra prendre position sur les modèles des accords que les fournisseurs d'identité entendent conclure avec les exploitants de services utilisateurs. Ces modèles devront lui être soumis pour examen.

Let. l

La reconnaissance devant être renouvelée tous les trois ans au plus tard, le fournisseur d'identité est tenu d'annoncer toutes les modifications qu'il entend apporter à son système e-ID et tous changements planifiés dans le cadre de ces activités. Ainsi, les modifications intervenues durant cette période devront être approuvées séparément par l'UPIC. En effet, il se pourrait qu'au courant de cette période, une reconnaissance ne puisse plus être maintenue lorsque, suite à ces changements, les conditions de reconnaissance visées à l'art. 13, al. 2, ne sont plus remplies.

Al. 2

Le fournisseur d'identité s'assurera qu'un problème d'utilisation de l'e-ID ou que la perte du support puissent être signalés. Les acteurs du marché détermineront si cette notification doit s'effectuer par téléphone, par courriel ou par d'autres canaux de communication.

Al. 3

Enfin, le Conseil fédéral édictera des prescriptions détaillées sur les diverses procédures d'annonce et de communication prévues par la présente loi. Il s'agit de la communication de la cessation programmée de l'activité du fournisseur d'identité, des erreurs dans les données d'identification personnelle, des incidents concernant la sécurité d'un système e-ID ou de l'utilisation de l'e-ID et des modèles d'accords avec les services utilisateurs.

28 RS **780.1**

Art. 16 Communication des données

Al. 1

Les fournisseurs d'identité pourront communiquer aux exploitants d'un service utilisateur certaines données d'identification personnelle visées à l'art. 5 seulement si elles sont nécessaires pour l'identification de la personne concernée et qu'elles correspondent au niveau de garantie requis. En outre, le titulaire de l'e-ID devra avoir consenti à leur communication.

Cette communication est requise pour assurer que le système e-ID remplit sa fonction et pour garantir le niveau de confort, de flexibilité et de simplicité attendu par les utilisateurs. Le principe de proportionnalité est respecté lors de cette communication, car l'atteinte à la vie privée prévue n'excède pas ce qui est nécessaire pour atteindre l'objectif poursuivi. Les données personnelles communiquées ne sont en outre pas des données sensibles au sens de l'art. 3, let. c, LPD.

Al. 2

Il sera interdit tant au fournisseur d'identité qu'à l'exploitant d'un service utilisateur de communiquer les données d'identification personnelle gérées par l'État au sens de l'art. 5 en dehors de l'utilisation de l'e-ID, et notamment d'en faire le commerce. Le modèle commercial des fournisseurs d'identité et des exploitants de services utilisateurs ne doit pas se fonder sur la vente de données ou de profils établis sur la base de l'utilisation de l'e-ID, confirmés par l'État et donc particulièrement susceptibles de révéler la personnalité du titulaire. Ces données ne devront pas non plus être communiquées gratuitement, par exemple entre entreprises d'un même groupe.

Art. 17 Accessibilité des e-ID

Cet article vise à protéger les personnes éligibles à l'obtention d'une e-ID ainsi que les titulaires d'une e-ID des effets dommageables qui pourraient se produire si un ou deux fournisseurs d'identité occupent une position prépondérante sur le marché. Une telle situation pourrait survenir notamment si un fournisseur d'identité décidait de ne pas émettre d'e-ID ou de ne pas offrir cette e-ID à une section de la population aux mêmes conditions qu'à la plus vaste part de la population.

En outre, l'al. 1 requiert que des indices concrets et répétitifs démontrent que le ou les fournisseurs d'identité concernés n'ont pas assuré un tel accès à toutes les personnes admissibles, ou pas aux mêmes conditions. Il ne précise pas toutefois qui devrait rendre vraisemblable qu'une telle situation s'est produite. Ainsi, les personnes admissibles, les titulaires d'une e-ID, d'autres fournisseurs d'identité, des exploitants d'un service utilisateur ou des associations de protection des consommateurs pourraient faire valoir une telle inégalité de traitement. L'UPIC ou le fournisseur d'identité devront alors intervenir aussitôt que les conditions de l'al. 1 seront remplies.

Les critères à prendre en compte lors de l'évaluation d'un cas ont été concrétisés autant que possible afin de faciliter l'interprétation et l'application de l'article. Ainsi, la marge d'appréciation de l'UPIC et du fournisseur d'identité est limitée et permettra de rendre des décisions en la matière plus efficacement.

Art. 18 Interopérabilité

L'interopérabilité des systèmes e-ID est une condition importante pour la diffusion des e-ID. Les fournisseurs d'identité devront reconnaître mutuellement leurs systèmes e-ID grâce à des normes techniques et des interfaces définies par voie d'ordonnance ou de directive.

Les titulaires pourront utiliser leur e-ID auprès de tous les services utilisateurs, pour autant qu'elle soit adaptée au moins au niveau de garantie exigé, et ceci indépendamment de si l'exploitant de ce service utilisateur a conclu un accord avec le fournisseur d'identité qui a établi l'e-ID. Pour atteindre cet objectif, les fournisseurs d'identité doivent fédérer leurs services d'identification, de façon analogue au réseau des cartes de crédit ou à l'itinérance dans le domaine de la téléphonie mobile, par l'élaboration de normes et de règles d'interopérabilité que tous les fournisseurs d'identité devront respecter.

Voir en outre les explications données au ch. 1.2.6.6.

Art. 19 Mesures de surveillance et retrait de la reconnaissance

Al. 1

L'UPIC interviendra si elle constate, au cours d'un contrôle ou par le biais d'une notification, qu'un fournisseur d'identité enfreint la LSIE ou qu'il ne remplit plus les conditions de la reconnaissance (art. 13, al. 2, LSIE). Sont en particulier considérées comme mesures nécessaires les exigences techniques, par exemple le respect des normes les plus récentes, et les mesures organisationnelles, comme les exigences relatives à la formation des collaborateurs. L'UPIC fixera un délai au terme duquel l'état conforme au droit doit être rétabli.

Al. 2

Si le fournisseur d'identité ne rétablit pas l'état conforme au droit, l'UPIC pourra lui retirer la reconnaissance. Le retrait devra dans tous les cas obéir au principe de proportionnalité.

Al. 3

Le Conseil fédéral réglera par voie d'ordonnance la procédure de retrait de la reconnaissance.

2.7 Exploitants d'un service utilisateur

Art. 20 Accord avec un fournisseur d'identité

Tout exploitant d'un service utilisateur sera lié par contrat à un fournisseur d'identité au moins. Au minimum, ce contrat définira le niveau de garantie ainsi que les processus techniques et organisationnels applicables.

Art. 21 Utilisation du numéro d'enregistrement de l'e-ID

Cette disposition autorise l'identification de personnes par les exploitants d'un service utilisateur à l'aide du numéro d'enregistrement de l'e-ID. Ce seront vraisemblablement dans la plupart des cas des acteurs privés. Toutefois, il se pourrait également que des autorités proposent un service utilisateur au sens de la loi. Elles pourront notamment offrir une application cyberadministrative faisant appel à un service d'identification afin de remplir une tâche d'intérêt public. Une base légale est requise afin de donner, dans ce cas de figure, la compétence à ces autorités d'utiliser le numéro d'enregistrement de l'e-ID dans leurs systèmes à des fins d'identification.

Art. 22 Obligation d'accepter les e-ID

Les exploitants de services utilisateurs, mais aussi les autorités et les organismes accomplissant des tâches publiques qui doivent recourir à l'identification électronique en exécution du droit fédéral, seront tenus d'accepter toute e-ID du niveau de garantie requis. Les autorités des cantons et des communes sont incluses parmi les destinataires de cette norme. Le recours à des moyens d'identification électronique déjà utilisés aujourd'hui n'est pas exclu.

Cette disposition reflète l'importance des e-ID au sens de la présente loi et de leur accueil par la population, mises en évidence par la stratégie Suisse numérique et la stratégie de cyberadministration du Conseil fédéral (voir ch. 3). Il s'agit notamment de soutenir les investissements de la Confédération destinés à la mise en œuvre des e-ID et de contribuer à la diffusion de celles-ci dans la cyberadministration, ce qui profitera non seulement à la Confédération, aux cantons et aux communes, qui pourront ainsi faire des économies, mais aussi à la population suisse.

2.8 Rôle de l'Office fédéral de la police

Art. 23 Tâches et obligations

Al. 1

Fedpol associe les données d'identification personnelle au numéro d'enregistrement de l'e-ID et les communique aux fournisseurs d'identité. Le nombre de données communiquées varie selon le niveau de garantie (voir art. 6 LSIE).

Al. 2

Fedpol fera en sorte que la validité des numéros d'enregistrement de l'e-ID puisse être vérifiée en tout temps dans une procédure usuelle. Actuellement, il est prévu qu'il tienne une liste électronique que les fournisseurs d'identité devront régulièrement consulter. Ils seront tenus de bloquer ou de révoquer immédiatement les e-ID liées à un numéro d'enregistrement invalide. La consultation par les fournisseurs d'identité de la liste de Fedpol accroîtra la confiance dans les e-ID établies par les fournisseurs d'identité concernés et sera donc gratuite. Les fournisseurs d'identité

devront de leur côté mettre en place une fonction de consultation gratuite de la liste des e-ID qu'ils auront eux-mêmes émises (art. 15, al. 1, let. c, LSIE).

Voir les explications relatives à l'art. 11, al. 1 à 4.

Al. 3

Les différents systèmes d'information sont alimentés par différentes sources. Infostar contient les données saisies dans toute la Suisse par les offices de l'état civil cantonaux. ISA reprend les données d'Infostar et des registres de contrôle des habitants, pour autant que ceux-ci soient gérés sur la base des actes d'origine ou du registre des familles. Le SYMIC est géré par le SEM et contient des données personnelles relevant du domaine des étrangers et de l'asile et relatives aux étrangers qui sont autorisés à séjourner en Suisse en vertu d'accords internationaux.

Si une personne enregistrée dans le SYMIC annonce un fait d'état civil (mariage, divorce, naissance, etc.), la saisie des modifications peut donner lieu à des translittérations divergentes. Dans ce cas, le Conseil fédéral règle la procédure à suivre. En ce qui concerne le numéro AVS, la CdC-UPI effectue déjà aujourd'hui des vérifications lorsque des données d'identification personnelle sont contradictoires; les vérifications portant sur les e-ID pourraient également lui être confiées.

Art. 24 Système d'information

Al. 1 et 2

Fedpol exploitera un système d'information qui traitera des données personnelles visées à l'art. 5, le numéro AVS et les données journalisées relatives à la procédure d'établissement.

Le but du traitement des données est réglé de manière exhaustive à l'al. 2. Le système d'information permettra de recevoir les demandes et les déclarations de consentement des requérants, d'assurer l'exécution automatisée des tâches de Fedpol dans le cadre de l'établissement des e-ID, de mettre à jour les données d'identification personnelle et de vérifier la validité des numéros d'enregistrement des e-ID.

Al. 3

Le système d'information aura des interfaces avec les registres de personnes suivants, gérés au niveau fédéral; le but sera d'obtenir et de mettre en concordance les données d'identification personnelle:

- le système d'information relatif aux documents d'identité (ISA) visé à l'art. 11 de la loi du 22 juin 2001 sur les documents d'identité (LDI)[29] et à l'art. 10 de l'ordonnance du 20 septembre 2002 sur les documents d'identité (OLDI)[30];
- le système d'information central sur la migration (SYMIC) visé aux art. 101 ss LEtr et dans l'ordonnance SYMIC du 12 avril 2006[31];

29 RS **143.1**
30 RS **143.11**
31 RS **142.513**

- le registre informatisé de l'état civil (Infostar) visé à l'art. 39 du code civil (CC)[32] et à l'art. 6*a* de l'ordonnance du 28 avril 2004 sur l'état civil (OEC)[33];
- le système d'information Ordipro du DFAE visé à l'art. 5 de la loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères[34] et à l'art. 2 de l'ordonnance Ordipro du 7 juin 2004[35];
- le registre central de la centrale de compensation de l'AVS (CdC-UPI) visé à l'art. 71 LAVS.

Le fournisseur d'identité sera tenu de collaborer avec Fedpol. Son système devra donc être relié au système d'information de Fedpol, afin que les données d'identification personnelle puissent être communiquées. Fedpol donnera ainsi accès à son système d'information au fournisseur d'identité, au moyen d'une interface, afin que ce dernier puisse enregistrer les données d'identification personnelle des titulaires de l'e-ID et les communiquer aux exploitants d'un service utilisateur. De son côté, le fournisseur d'identité exploitera donc son propre système d'information où il enregistrera les données personnelles d'identification qu'il obtiendra de Fedpol et les données concernant l'utilisation des e-ID par leur titulaires. En vertu de l'art. 15, al. 1, let. i, il doit donner accès en ligne à ces types de données aux titulaires de l'e-ID. En aucun cas le fournisseur d'identité n'aura accès aux registres des personnes au sens de l'art. 24, al. 3. En outre, le fournisseur d'identité sera tenu d'obtenir le consentement exprès du titulaire de l'e-ID pour la première communication des données d'identification à des exploitants d'un système utilisateur (art. 15, al. 1, let. h). Enfin, les art. 9 et 16 prévoient des exigences supplémentaires concernant le traitement, la conservation et la communication des données par le fournisseur d'identité.

2.9 Rôle de l'Unité de pilotage informatique de la Confédération

Art. 25 Compétences

Al. 1

La procédure de reconnaissance des fournisseurs d'identité, menée par l'UPIC, s'inspire de la procédure de reconnaissance prévue pour les plateformes de messagerie (voir ch. 1.3.2).

Al. 2

L'organisme de reconnaissance publiera et mettra à jour une liste de tous les fournisseurs d'identité et de tous les systèmes e-ID reconnus avec le niveau de garantie

32 RS **210**
33 RS **211.112.2**
34 RS **235.2**
35 RS **235.21**

correspondant. La disposition reprend la réglementation concernant la liste des plateformes reconnues.

Art. 26 Système d'information

Afin d'accomplir les tâches prévues par la loi, l'UPIC gèrera son propre système d'information, qui contiendra les données, les informations et les preuves soumises par les fournisseurs d'identité dans le cadre de la procédure de reconnaissance, les informations concernant la cessation programmée de l'activité du fournisseur d'identité (art. 14, al. 2), les communications concernant les incidents de sécurité d'un système e-ID et l'utilisation de l'e-ID (art. 15, al. 1, let. g), les communications concernant les modèles des accords avec les services utilisateurs (art. 15, al. 1, let. l) ainsi que les informations relatives aux mesures de surveillance. Ce système d'information sera tenu à des fins de reconnaissance et de surveillance des fournisseurs d'identité.

2.10 Émoluments

Art. 27

Tant l'UPIC que Fedpol percevront des émoluments auprès des fournisseurs d'identité pour leurs décisions et leurs autres prestations. Les demandes concernant la validité des numéros d'enregistrement des e-ID en seront exonérées. Plusieurs possibilités sont envisageables pour fixer le montant de ces émoluments. Le Conseil fédéral décidera de la solution à adopter au vu des circonstances concrètes de l'exécution de la loi. Il devra en particulier déterminer si les frais administratifs, notamment du service d'identité, devront être couverts intégralement dans les premières années. Demander des émoluments réduits aux fournisseurs d'identité qui établissent les e-ID gratuitement pour les particuliers pourrait encourager la diffusion rapide des e-ID et ainsi améliorer à moyen ou à long terme l'efficience des transactions électroniques effectuées entre des acteurs privés ou avec les autorités.

2.11 Responsabilité

Art. 28

Remarque préliminaire

La responsabilité pour les dommages qui peuvent être causés lors de l'utilisation de l'e-ID est soumise aux règles de responsabilité usuelles du code des obligations ou de la loi du 14 mars 1958 sur la responsabilité (LRCF)[36].

Les dispositions de la LSIE relatives à la responsabilité ont une valeur déclaratoire et visent à clarifier quelles règles de responsabilité sont applicables, par exemple en ce

36 RS **170.32**

qui concerne la notion de dommage, la possibilité de se libérer de la responsabilité ou la responsabilité des auxiliaires. On renonce à définir des normes de responsabilité plus détaillées.

En particulier, la responsabilité envers des tiers des titulaires d'une clé de signature, définie à l'art. 59*a* CO, n'est pas étendue aux titulaires d'une e-ID. L'e-ID seule ne permet pas de conclure des actes juridiques; la LSIE ne concerne que l'identification sûre des participants au cours de transactions électroniques.

À l'heure actuelle, on renonce également à introduire une responsabilité causale du fournisseur d'identité analogue à celle définie à l'art. 17 SCSE. Il en résulte que les règles de prescription du CO sont applicables. Lorsque des accords bilatéraux devront être conclus afin de permettre la notification des e-ID suisses reconnues à l'UE, les modifications nécessaires de la LSIE devront être effectuées, en prêtant une attention particulière aux règles de responsabilité en vigueur entre les États.

Al. 1

La responsabilité du titulaire de l'e-ID, de l'exploitant d'un service utilisateur et du fournisseur d'identité, soit la responsabilité des acteurs privés, est régie par le CO. Déterminer s'il s'agit d'une responsabilité contractuelle ou extracontractuelle (art. 41 ss CO) dépend du cas d'espèce.

Al. 2

Fedpol et l'UPIC sont des unités administratives de la Confédération et sont soumis à ce titre à la LRCF.

2.12 Dispositions finales

Art. 29 Dispositions transitoires

Le but de ces dispositions est de faciliter la reconnaissance des moyens d'identification établis avant l'entrée en vigueur de la LSIE. Dans la plupart des cas, les titulaires d'un tel moyen d'identification électronique ont déjà fait l'objet d'une procédure d'établissement rigoureuse auprès d'un fournisseur d'identité ou d'un autre organe similaire.

Durant une période transitoire de deux ans, l'UPIC reconnaîtra donc comme e-ID d'un niveau de garantie faible, sur demande d'un fournisseur d'identité, les moyens d'identification électronique que ce dernier a établis. En outre, elle reconnaîtra comme e-ID d'un niveau de garantie substantiel les moyens d'identification électronique qu'un fournisseur d'identité a établis si l'identification a eu lieu dans le cadre d'une procédure qui est soumise par la loi à des règles et à une surveillance et qui garantit un niveau de sécurité comparable aux procédures prévues en vertu de la LSIE. Les personnes possédant un certificat qualifié valable au sens de l'art. 2, let. h, SCSE pourront également demander à un fournisseur d'identité qu'il établisse à leur intention (sans nouvelle vérification d'identité) une e-ID d'un niveau de garantie substantiel. Dans les trois cas, les exigences visées à l'al. 1, let a, devront être remplies: le titulaire devra remplir les conditions d'admissibilité visées à l'art. 3, il devra

avoir consenti à l'établissement de l'e-ID, et les données d'identification personnelle (tels le numéro de carte d'identité ainsi que le nom, le prénom et la date de naissance) devront correspondre aux informations enregistrées dans le système d'information visé à l'art. 24.

Les modalités de la procédure d'établissement seront réglées par le Conseil fédéral par voie d'ordonnance. Il y définira notamment les exigences par rapport à cette procédure, les différentes étapes à suivre et les compétences de l'organe chargé de la reconnaissance.

Il devra tout particulièrement déterminer comment le numéro d'enregistrement de l'e-ID sera associé par le fournisseur d'identité au moyen d'identification électronique établi avant l'entrée en vigueur de la LSIE.

Art. 30 Modification d'autres actes

Le projet propose la modification d'autres actes. Ces adaptations visent principalement à permettre à Fedpol d'accéder aux systèmes d'information ISA, Infostar, et SYMIC. Le système d'information de la CdC-UPI ne doit pas être accessible en ligne.

Art. 31 Référendum et entrée en vigueur

Comme toute loi fédérale, la LSIE est sujette au référendum et le Conseil fédéral est chargé de fixer la date de son entrée en vigueur.

2.13 Modification d'autres actes

Remarque préliminaire

On estime à ce stade que les conditions d'identification et d'authentification pour les applications de la cyberadministration doivent, dans la mesure où elles sont nécessaires, être réglées par voie d'ordonnance ou de directive. Plusieurs ordonnances et directives devront être modifiées en vue de la mise en œuvre de la LSIE, par exemple l'ordonnance du 6 juin 2014 concernant les systèmes d'information du service vétérinaire public (OSIVét)[37] ou l'ordonnance du 23 octobre 2013 sur les systèmes d'information dans le domaine de l'agriculture (OSIAgr)[38].

37 RS **916.408**
38 RS **919.117.71**

1. Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA)[39]

Art. 9, al. 1, let. c, et 2, let. c, ch. 3 (nouveau)

L'art. 9, al. 1, énumère les autorités auxquelles le SEM peut donner accès en ligne aux données relevant du domaine des étrangers qu'il a traitées ou fait traiter dans le système d'information régi par la LDEA. La let. c précise les buts pour lesquels un tel accès pourrait être donné aux autorités fédérales compétentes dans les domaines de la police. La LSIE ajoute à cette liste un nouveau but, notamment l'identification des personnes ainsi que l'attribution et la mise à jour des données d'identification personnelle selon la LSIE.

L'art. 9, al. 2, énumère les autorités auxquelles le SEM peut donner accès en ligne aux données relevant du domaine de l'asile qu'il a traitées ou fait traiter dans le système d'information régi par la LDEA. La let. c énumère les buts dans lesquels un tel accès pourrait être donné aux autorités fédérales compétentes dans le domaine de la police. Le projet ajoute un nouveau but à cette liste, notamment l'accomplissement de leurs tâches selon la LSIE.

2. Loi du 22 juin 2001 sur les documents d'identité (LDI)[40]

Art. 1, al. 3, 2e phrase

Les passeports diplomatiques et les passeports de service peuvent être établis uniquement pour des ressortissants suisses. Certains pays d'accueil ou certaines tâches effectuées dans l'intérêt et sur mandat de la Confédération nécessitent parfois, pour des raisons de sécurité, d'établir de tels passeports diplomatiques ou des passeports de service pour des personnes de nationalité étrangère, afin d'éviter des problèmes pour les ressortissants étrangers qui accompagnent les diplomates suisses ou d'autres employés d'une représentation suisse. Disposer d'un passeport diplomatique ou d'un passeport de service est parfois indispensable au moment de s'annoncer dans le pays d'accueil ou d'obtenir un visa. De plus, les diplomates sont de plus en plus nombreux à avoir des conjoints ou des partenaires de nationalité étrangère. Il s'agit également de simplifier l'exercice des fonctions pour les collaborateurs étrangers. Dans les régions en crise ou en guerre qui présentent un danger pour la vie ou l'intégrité corporelle, il est fréquent qu'aucun ressortissant suisse ne soit intéressé par le poste et le DFAE doit dès lors engager des spécialistes de nationalité étrangère. Ces personnes n'obtiennent pas la nationalité suisse; le passeport mentionne leur nationalité sur la page des données personnelles et le lieu d'origine est remplacé par «***».

Art. 11, al. 1, let. k, et 2

Le numéro AVS et le numéro d'enregistrement de l'e-ID doivent venir compléter les données renseignées sur une personne dans ISA afin que les données issues de

39 RS **142.51**
40 RS **143.1**

divers registres fédéraux et nécessaires à l'utilisation d'une e-ID soient attribuées à une personne de façon univoque.

Art. 12, al. 2, let. g

En plus de Fedpol (let. a inchangée), le DFAE (Direction consulaire) doit pouvoir consulter ISA afin d'obtenir les données nécessaires à l'établissement d'une e-ID, en particulier celles qui ne sont pas disponibles sur Infostar, comme le numéro du document d'identité, la photographie et l'image de la signature. Lors de l'établissement de l'e-ID, les données sont attribuées correctement à une personne grâce au numéro AVS ou au numéro d'enregistrement de l'e-ID.

Art. 14 Interdiction de tenir des fichiers parallèles

Avec l'introduction des e-ID reconnues, les données d'ISA seront également disponibles dans les systèmes d'information des fournisseurs d'identité reconnus et du service d'identité. Ceux-ci doivent être exemptés de l'interdiction de tenir des fichiers parallèles.

3. Code civil[41]

Art. 43a, al. 4, ch. 5

L'art. 43*a* CC règle l'accès en ligne aux registres informatisés visant à gérer l'état civil. Fedpol est ajouté à la liste des services qui ont accès à Infostar.

4. Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[42]

*Art. 50a, al. 1, let. b^quater^*

L'art. 50*a* LAVS détermine les services qui sont autorisés à recevoir des données, en particulier le numéro AVS, en dérogation à l'art. 33 LPGA. Fedpol sera mentionné dans la liste de ces services. Lui et les fournisseurs d'identité pourront utiliser systématiquement le numéro AVS aux conditions fixées à l'art. 8, al. 1, LSIE.

5. Loi du 18 mars 2016 sur la signature électronique[43]

*Art. 9, al. 1^bis^*

Toute personne qui demande la délivrance d'une signature électronique doit se présenter en personne. Elle n'est pas soumise à cette obligation si elle peut prouver son identité avec une e-ID d'un niveau de garantie substantiel.

41 RS **210**
42 RS **831.10**
43 RS **943.03**

3 Conséquences

3.1 Conséquences sur les finances et l'état du personnel

Vu l'importance stratégique du projet concernant l'identification électronique, nous ferons une distinction entre les conséquences, en matière de finances et de personnel, de la phase de réalisation et de la phase d'exploitation. La phase de réalisation comprend aussi l'avant-projet, qui a duré jusque fin 2017.

3.1.1 Réalisation

3.1.1.1 Avant-projet (jusqu'à 2017)

Durant la phase de l'avant-projet (jusque fin 2017), diverses variantes théoriques d'une e-ID reconnue par l'État ont été analysées, et un avant-projet de loi a été élaboré. Un simulateur (logiciel de démonstration de l'identification électronique) a en outre été développé. Le but du simulateur est d'une part de présenter le projet, d'autre part de permettre de tester et de mettre au point les spécifications techniques requises, en vue de l'élaboration de l'ordonnance et des autres dispositions d'exécution. Le coût de cette phase préliminaire se monte à 390 000 francs, dont 290 000 francs ont été apportés par le DFJP et 100 000 par Cyberadministration suisse.

3.1.1.2 Organisation

Il est prévu de mettre en place entre 2018 et 2020 un service d'identité au sein de Fedpol et un organisme de reconnaissance au sein de l'UPIC. Les dépenses afférentes comprennent le recrutement de personnel et la création de processus et d'interfaces. Le service d'identité sera chargé d'une part d'assurer l'infrastructure technique et l'assistance informatique (assistance technique et ligne d'aide aux utilisateurs), d'autre part d'adapter le cas échéant les règles concernant les conditions de la reconnaissance. L'organisme de reconnaissance mettra la LSIE en œuvre dans le domaine de la reconnaissance des fournisseurs d'identité, mènera les contrôles requis et surveillera la conformité aux règles.

Dépenses en jours-personnes	2018	2019	2020	Total
Mise en place du service d'identité	–	150	75	225
Mise en place de l'organisme de reconnaissance	–	50	25	75
Total	–	200	100	300
Coûts (en francs)	–	160 000	80 000	**240 000**

Base de calcul: 220 jours par personne et par an

Avec un taux de 800 francs par jour-personne, le total des dépenses pour la phase de réalisation du service d'identité et de l'organisme de reconnaissance est de **240 000 francs**.

3.1.1.3 Systèmes

Le travail du service d'identité sera automatisé dans toute la mesure du possible. Il faudra pour cela une application informatique dotée d'interfaces avec les registres de personnes fédéraux (ISA, SYMIC, Infostar et CdC-UPI) et avec les fournisseurs d'identité, à qui les données d'identité gérées par l'État seront communiquées via cette interface. L'application comprendra également une page Web de la Confédération, sur laquelle les personnes qui désirent obtenir une e-ID confirmeront leur identité et donneront leur consentement. Enfin, il sera possible, par une interface accessible au public, de vérifier gratuitement dans l'application si le numéro d'enregistrement d'une e-ID est valable et si un fournisseur d'identité est reconnu par l'État.

Comme le numéro AVS ne peut pas être utilisé directement comme numéro d'enregistrement de l'e-ID, il faut développer une autre application, qui permettra aux organismes habilités à utiliser systématiquement le numéro AVS de rechercher quel numéro AVS correspond à tel numéro d'enregistrement de l'e-ID.

Outre ces logiciels, les dépenses prévues comprennent notamment le recours à des experts externes pour traiter les questions pointues telles que celle de la sécurité informatique.

Le coût de la phase de réalisation des systèmes informatiques (2018 à 2020), le coût total du projet et son financement sont exposés au ch. 3.1.1.4.

3.1.1.4 Coût total et financement de la phase de réalisation

	Avant-projet			Réalisation	Total
Dépenses en francs	2015–2017	2018	2019	2020	
Dépenses de personnel (gestion du projet comprise)	200 000	240 000	320 000	250 000	1 010 000
Développement du système (simulateur)	180 000	110 000	100 000	50 000	440 000
Développement du système (application/système d'information)	–	260 000	2 580 000	1 950 000	4 790 000
Développement du système (interface nº AVS)	–	50 000	400 000	300 000	750 000
Autres dépenses (experts en sécurité informatique)	10 000	150 000	240 000	270 000	670 000

	Avant-projet			Réalisation	Total
Dépenses en francs	2015–2017	2018	2019	2020	
Mise en place des services (service d'identité et organisme de reconnaissance)	–	–	160 000	80 000	240 000
Total des dépenses	**390 000**	**810 000**	**3 800 000**	**2 900 000**	**7 900 000**
./. Ressources centralisées destinées aux TIC	–	700 000	800 000	–	1 500 000
./. Cyberadministration suisse	100 000	450 000	900 000	–	1 450 000
./. Ressources propres DFJP	290 000	–	1 660 000	1 920 000	3 970 000
./. Réserve à affectation spéciale		–340 000	340 000	–	–
Besoins supplémentaires pour des dépenses uniques liées au projet	–	–	**100 000**	**880 000**	**980 000**
./. Ressources centralisées destinées aux TIC	–	–	–	880 000	880 000
./. Cyberadministration suisse	–	–	100 000	–	100 000

Le financement de ces dépenses est assuré jusqu'à hauteur de 6 920 000 francs par les fonds dont dispose le DFJP (y inclus la part prise sur les ressources centralisées destinées aux TIC et la participation de Cyberadministration suisse).

Vu les résultats de la consultation, il convient de créer un logiciel à part pour la recherche du numéro AVS, ce qui représente une dépense supplémentaire de 750 000 francs. Il en résultera des coûts supplémentaires de 230 000 francs. Le simulateur devra aussi être développé et entretenu. Les besoins supplémentaires pour des dépenses uniques, qui devront faire l'objet d'une demande de crédit pour la période de 2018 à 2020, se monteront à 980 000 francs. 100 000 francs proviendront de Cyberadministration suisse; la demande portera sur 880 000 francs, à prendre en compte sur les ressources centralisées destinées aux TIC.

Le recours à des tiers sera financé par le crédit d'engagement «Renouvellement du passeport et de la carte d'identité suisses» (V0224.00) de Fedpol, qui est de 19,6 millions de francs.

3.1.2 Exploitation (à partir de 2020)

Selon les prévisions, la création de 8 postes sera nécessaire pour constituer le service d'identité et l'organisme de reconnaissance à partir de 2020.

Les coûts d'exploitation informatique sont budgétés actuellement à 15 % des investissements nécessaires, soit environ un million de francs, à partir de l'année 2020. La phase d'exploitation se recoupera en partie avec la phase de réalisation cette année-là. D'autres ressources seront nécessaires pour la communication, le recours à des consultants externes et les imprévus.

Les dépenses d'exploitation nécessaires pour mettre la loi en œuvre atteindront au maximum 2,4 millions de francs (1,4 million pour au plus 8 postes et 1 million pour les dépenses de biens et services). Les ressources nécessaires seront de nouveau évaluées, avec plus de précision, au moment de l'élaboration des ordonnances d'exécution et une fois connu le résultat des délibérations parlementaires. Le Conseil fédéral présentera une demande de crédit lorsqu'il fixera la date de l'entrée en vigueur de la LSIE. À ce moment-là, on se sera aussi enquis auprès de fournisseurs d'identité potentiels du volume probable de la demande d'e-ID.

3.1.3 Compte de résultats à long terme

Dans sa décision du 22 février 2017 portant sur l'ouverture d'une procédure de consultation sur la loi sur les moyens d'identification électronique reconnus, le Conseil fédéral a chargé le DFJP de lui proposer, en même temps qu'un message, un plan de financement, en principe sans incidence budgétaire, pour l'exploitation du service d'identité et de l'organisme de reconnaissance, postes nécessaires compris. Le scénario exposé ici part d'hypothèses conservatrices et table sur une progression arithmétique, à partir de zéro, du nombre d'e-ID.

Les coûts sont conformes aux indications qui précèdent. Pour ce qui est des recettes, le calcul se base sur deux hypothèses.

Premièrement, des émoluments sont perçus par l'organisme de reconnaissance pour la reconnaissance des fournisseurs d'identité et de leurs systèmes e-ID. Leur montant dépend du niveau de garantie considéré. La reconnaissance doit être renouvelée tous les trois ans. On suppose que le total des émoluments de reconnaissance se montera en moyenne à 50 000 francs par an, ce qui équivaut à autant de recettes.

Deuxièmement, des émoluments sont perçus par le service d'identité. Les recettes ainsi engendrées dépendent fortement du succès des e-ID. Les émoluments perçus pour la consultation de données d'identification personnelle par les fournisseurs d'identité se monteront environ à 26 centimes (niveau de garantie faible, 1 fois par an; substantiel, 1 fois par trimestre; élevé, 1 fois par semaine). Si 24 % des e-ID sont d'un niveau de garantie faible, 75 % d'un niveau de garantie substantiel et 1 % d'un niveau de garantie élevé, cela revient à un franc environ par e-ID et par an. Le scénario postule également que la première communication des données est gratuite, car les fournisseurs d'identité octroient gratuitement leurs e-ID.

En résumé, on obtient les résultats suivants:

Dépenses	2020	2021	2022	2023	2024	2025	2026
Frais de personnel	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000	1 400 000
Coûts d'exploitation informatique	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000	1 000 000
Total des dépenses	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000	2 400 000

Dépenses	2020	2021	2022	2023	2024	2025	2026
Recettes							
Nombre d'e-ID	–	400 000	800 000	1 200 000	1 600 000	2 000 000	2 400 000
Émoluments de reconnaissance	50 000	50 000	50 000	50 000	50 000	50 000	50 000
Émoluments de communication de données	–	400 000	800 000	1 200 000	1 600 000	2 000 000	2 400 000
Total des recettes	50 000	450 000	850 000	1 250 000	1 650 000	2 050 000	2 450 000
Résultat	–2 350 000	–1 950 000	–1 550 000	–1 150 000	–750 000	–350 000	50 000

Le projet, en soi, devrait passer dans les chiffres noirs au bout de six ans. Le seuil de rentabilité pourrait être atteint plus vite si la diffusion des e-ID était plus rapide, par exemple parce qu'un fournisseur d'identité ayant une grosse clientèle obtient la reconnaissance.

La neutralité des coûts de ce projet ne saurait cependant être considérée de manière isolée. La numérisation des échanges administratifs au niveau de la Confédération, des cantons et des communes, notamment, apportera des gains financiers et des économies. Ces avantages, non quantifiables à l'heure actuelle, doivent être pris en compte lorsqu'il s'agit de se faire une idée d'ensemble du rapport coût-utilité des e-ID. Il ne sera possible d'en faire un bilan fiable que quelques années après l'instauration des e-ID, une fois pris en considération tout leur écosystème. C'est à ce moment seulement que l'on saura combien d'exploitants de services utilisateurs renoncent à avoir leur propre système de gestion de l'identité, entreprise généralement coûteuse, pour recourir à l'e-ID.

3.2 Conséquences pour les cantons et les communes, ainsi que pour les villes, les agglomérations et les régions de montagne

Les cantons et les communes utilisent de nombreux logiciels de cyberadministration. Les processus d'identification et d'authentification permettant d'accéder à ces systèmes seront considérablement simplifiés par la mise en place des e-ID. Dans le canton de Berne par exemple, il est possible de saisir sa déclaration fiscale électroniquement, mais uniquement après avoir entré un mot de passe reçu par la poste et en envoyant un formulaire signé à la main. Ces envois ne seraient plus nécessaires si la personne imposable disposait d'une e-ID.

L'identification simple et sûre favorise l'utilisation des services de la cyberadministration proposés par les villes et les communes. Si les processus sont adaptés, les démarches administratives pourront être simplifiées. Les particuliers peuvent entrer en contact avec les autorités cantonales et communales indépendamment du lieu, depuis un appareil connecté à Internet.

Il est difficile de chiffrer le coût de l'adaptation éventuelle des logiciels de cyberadministration offerts par les cantons, les villes et les communes pour permettre l'identification par e-ID. Il sera plus ou moins grand selon le type de logiciel. Il est néanmoins prévu que les collectivités publiques agissant en tant qu'exploitants d'un service utilisateur prendront à leur charge les coûts d'utilisation des données d'identification communiquées par le fournisseur d'identité. Ces coûts pourront toutefois être couverts par les économies que les communes, les villes et les cantons feront grâce à la mise en place d'un processus d'identification par e-ID.

3.3 Conséquences économiques

La réglementation et la sécurité des échanges sur Internet améliorent l'attrait et la compétitivité de la place économique suisse. Le Conseil fédéral a pour objectif d'apporter les contributions nécessaires au passage réussi de la Suisse à une société de l'information. Dans ce but, il a pris de nombreuses mesures visant principalement à adapter le cadre légal (la SCSE par exemple, ou la création de numéros d'identification unique pour les personnes et les entreprises ainsi que des registres correspondants) ou à mettre en place des infrastructures.

L'introduction de moyens d'identification électronique reconnus et largement disponibles est un élément clé pour la mise en place d'un vaste écosystème e-ID qui garantit la fiabilité et la sécurité des transactions électroniques. Les transactions complexes avec l'État ou entre des partenaires privés peuvent être effectuées électroniquement et donc de manière plus efficace. De plus, ce projet ouvre de nouveaux secteurs d'activité importants.

3.4 Conséquences sociales

L'identification sûre du partenaire lors des échanges électroniques complique ou empêche l'utilisation abusive et favorise la confiance sur Internet.

L'abus sur Internet se fonde souvent sur l'impossibilité d'identifier son interlocuteur de façon sûre. Il n'est pas possible de différencier les expéditeurs de spams des expéditeurs fiables ni de les placer devant leurs responsabilités. Dans les cas d'hameçonnage, les expéditeurs de courriels se font passer pour quelqu'un qu'ils ne sont pas, par exemple pour la banque du destinataire, et peuvent causer des dommages importants. Les moyens d'identification électronique reconnus contribuent à protéger l'identité de leurs titulaires dans une société mondialisée et fortement interconnectée. Usurper l'identité d'une personne et en faire une utilisation potentiellement extrêmement dangereuse devient bien plus difficile. Grâce à l'introduction du numéro d'enregistrement de l'e-ID, la nécessité d'indiquer le nom, le prénom et la date de naissance pourrait n'avoir plus lieu d'être. Le numéro d'enregistrement de l'e-ID est un pseudonyme univoque qui ne permet pas à des tiers de déduire d'autres données personnelles. La sphère privée est mieux protégée puisque le nom, que tout un chacun peut aisément associer à une personne en particulier, ne doit plus être communiqué.

3.5 Conséquences environnementales

Ce projet n'a pas de conséquences directes sur l'environnement. Passer de transactions physiques à des transactions électroniques permettrait d'économiser des ressources et aurait par conséquent des répercussions positives sur l'environnement. Par exemple, l'encombrement des infrastructures de transport qui résulte de la nécessité de se présenter en personne pourrait être évité.

3.6 Autres conséquences

Le Conseil fédéral ne prévoit pas de conséquences négatives, ou uniquement des effets négligeables, sur l'économie et les entreprises. Il renonce à effectuer une analyse d'impact de la réglementation détaillée et formelle.

4 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

L'avant-projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) a été annoncé dans le message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[44] et dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[45].

Le présent projet permet en particulier de mettre en œuvre des objectifs fixés par diverses stratégies du Conseil fédéral, stratégies également citées dans les lignes directrices du programme de la législature 2015 à 2019. Le Conseil fédéral a ainsi mis à jour la stratégie Suisse numérique en avril 2016 et a défini les champs d'action dans lesquels le potentiel novateur des TIC peut déployer au maximum ses effets. Les moyens d'identification électronique sûrs sont une condition préalable à la mise en œuvre de plusieurs de ces champs d'action et font partie de l'objectif principal Transparence et sécurité. Grâce aux moyens d'identification électronique reconnus, les personnes vivant en Suisse peuvent se mouvoir dans le monde virtuel aussi sûrement que dans le monde réel et sont pleinement en mesure d'exercer leur libre choix en matière d'information.

La création d'une identité électronique valable en Suisse et à l'étranger est un des objectifs opérationnels fixés par la stratégie suisse de cyberadministration dans le plan stratégique 2016–2019. Afin de favoriser l'innovation et de promouvoir l'attrait de la Suisse, celle-ci devrait disposer d'un programme fiable de mise en œuvre d'une identité durable dans l'«espace virtuel» et ouvrir ainsi des perspectives à long terme pour l'économie et la société numérique.

44 FF **2016** 981 1048 1100
45 FF **2016** 4999 5001

5 Aspects juridiques

5.1 Constitutionnalité

La compétence de régler les e-ID découle de la Constitution. L'établissement des e-ID est délégué aux fournisseurs d'identité. Afin d'obtenir la reconnaissance étatique, ceux-ci doivent remplir plusieurs conditions qui limitent leur activité. L'art. 95, al. 1, Cst., autorise le Conseil fédéral à légiférer sur l'exercice des activités économiques lucratives privées.

En outre, le ou les fournisseurs d'identité occupant une position prépondérante sur le marché doivent également s'assurer qu'ils offrent les e-ID aux personnes éligibles aux mêmes conditions qu'à la plus vaste part de la population. Le projet vise ainsi à lutter contre les conséquences dommageables de l'activité économique de certains fournisseurs d'identité importants, notamment de ceux qui dominent le marché. En effet, il soumet leur offre d'e-ID à des conditions et encadre leur activité. Le projet se fonde donc sur l'art. 96, al. 1, Cst., qui donne à la Confédération la compétence de légiférer afin de lutter contre les conséquences sociales et économiques dommageables des cartels et des autres formes de limitation de la concurrence.

La présente loi contient des dispositions qui permettent d'assurer un meilleur accès à une e-ID aux personnes admissibles. Il prévoit également un système de reconnaissance, de surveillance et de sanctions pour les fournisseurs d'identité. De cette façon, le projet vise à renforcer la protection des consommateurs. Il se fonde ainsi sur l'art. 97, al. 1, Cst., qui donne à la Confédération la compétence de prendre des mesures destinées à protéger les consommateurs et les consommatrices. Le projet de loi règle également des points de droit civil, dans la mesure où il touche les relations contractuelles entre les fournisseurs d'identité, les titulaires d'une e-ID et les exploitants de services utilisateurs. Comme cet aspect est relativement accessoire, il est inutile de mentionner dans le préambule l'art. 122, al. 1, Cst., qui donne à la Confédération la compétence de légiférer en matière de droit civil.

5.2 Compatibilité avec les obligations internationales

L'avant-projet est compatible avec les obligations internationales en vigueur. Lors de son élaboration, le Conseil fédéral s'est efforcé de ne pas exclure la possibilité de la notification au sens du règlement eIDAS. Si cela est souhaité ultérieurement, les e-ID reconnues en Suisse pourront obtenir la reconnaissance européenne. À cet effet, la conclusion de traités internationaux sera nécessaire.

5.3 Forme de l'acte à adopter

Au vu de l'objet, du contenu et de la portée du projet , il est indispensable, selon l'art. 164, al. 1, Cst., d'édicter les dispositions relatives aux services d'identification électronique sous la forme d'une loi fédérale.

5.4 Frein aux dépenses

Comme le projet entraîne des dépenses périodiques de plus de 2 millions de francs, il doit être adopté à la majorité des membres de chaque conseil, conformément à l'art. 159, al. 3, let. b, Cst.

5.5 Respect du principe de la subsidiarité et du principe de l'équivalence fiscale

L'opportunité d'instaurer les e-ID est un point incontesté. Ni le partage des tâches prévu, ni leur exécution ne violent le principe de la subsidiarité ni celui de l'équivalence fiscale. Les conséquences financières du projet pour la Confédération et les cantons sont inférieures à 10 millions de francs. Le projet est donc conforme aux principes cités.

5.6 Conformité à la loi sur les subventions

La LSIE ne prévoit pas d'aides financières ni d'indemnités. Sa mise en œuvre relèvera du libre marché. Des modèles d'affaires sont disponibles. Nous renonçons donc à de plus amples explications.

5.7 Délégation de compétences législatives

Procédures de vérification de l'identité et des documents d'identité

Le Conseil fédéral déterminera par voie d'ordonnance les procédures qui permettent de vérifier les documents d'identité des ressortissants suisses ainsi que les documents de légitimation et l'identité des étrangers. Le but de ces procédures est de permettre d'évaluer au cas par cas la situation spécifique des personnes concernées. En effet, il ne s'agit pas de donner la compétence au Conseil fédéral d'exclure des catégories de personnes, mais plutôt de mettre en place des procédures qui permettent de vérifier objectivement, dans le cas d'espèce, si la personne concernée peut être identifiée de manière fiable et si elle remplit les exigences pour obtenir une e-ID. La délégation de compétence se trouve à l'art. 3, al. 2, LSIE.

Prescriptions techniques et organisationnelles

Afin de s'adapter le plus rapidement possible aux avancées technologiques, les conditions relatives aux processus (reconnaissance des fournisseurs d'identité et niveaux de garantie), aux exigences techniques et aux normes seront fixées par voie d'ordonnance ou de directive.

L'art. 4, al. 4, prévoit que le Conseil fédéral réglemente les différents niveaux de garantie en tenant compte de l'état actuel de la technique. Il réglementera en particulier les exigences minimales d'identification pour chaque niveau de garantie.

L'art. 6, al. 5, donne au Conseil fédéral la compétence d'édicter des dispositions détaillées sur le déroulement de la procédure d'établissement d'une e-ID ainsi que sur les données d'identification personnelles à utiliser lors de l'identification. De par sa nature complexe et détaillée, la matière à régler dans ce cas de figure relève davantage d'une ordonnance que d'une loi. De plus, le Conseil fédéral édictera par voie d'ordonnance des dispositions détaillées sur la procédure d'établissement d'une e-ID pour les personnes possédant des moyens d'identification valides et conformes au droit fédéral selon l'art. 29. Les dispositions techniques visant à assurer l'interopérabilité des systèmes e-ID devront pouvoir être adaptées rapidement et relèvent du niveau de l'ordonnance (art. 18, al. 2, LSIE).

En vertu de l'art. 13, al. 4, LSIE, le Conseil fédéral fixe les conditions de la reconnaissance, en particulier celles ayant trait aux conditions techniques et aux conditions de sécurité que les fournisseurs d'identité doivent remplir, à leur contrôle, à la couverture d'assurance nécessaire (ou aux sûretés financières équivalentes), aux normes et protocoles techniques applicables aux systèmes e-ID et au contrôle régulier de ces systèmes. Les normes nationales et internationales à respecter lors de l'utilisation seront mises à jour et publiées à intervalle rapproché. Le Conseil fédéral est plus à même de réagir rapidement que le Parlement.

Le destinataire de l'ordonnance qui fixera les normes et protocoles techniques applicables à la communication des données d'identification est Fedpol. Le Conseil fédéral règlera la marche à suivre au cas où plusieurs registres de personnes livrent des données différentes (art. 23, al. 3, LSIE).

Enfin, le Conseil fédéral réglera les mesures techniques et organisationnelles à prendre pour assurer la sécurité du traitement et de la communication des données d'identification personnelle en se fondant sur l'art. 24, al. 4. Ces mesures devront pouvoir être adaptées rapidement aux développements techniques. Il est plus opportun de les régler par voie d'ordonnance.

Système e-ID subsidiaire de la Confédération

Si aucun fournisseur d'identité n'établit d'e-ID d'un niveau de garantie substantiel ou élevé, le Conseil fédéral pourra charger une unité administrative de gérer un système e-ID du niveau de garantie considéré (art. 10, al. 1).

Règles de protection des titulaires relevant du droit de la responsabilité civile

Le Conseil fédéral peut définir par voie d'ordonnance les devoirs de diligence du titulaire de l'e-ID (art. 12, al. 3, LSIE) ainsi que le blocage et la révocation de cette dernière (art. 11, al. 5, LSIE). Ces devoirs de diligence peuvent devoir être adaptés relativement rapidement en fonction de l'évolution de la technique. Il est donc raisonnable de prévoir une réglementation par voie d'ordonnance.

Perception d'émoluments

Voir les explications relatives à l'art. 27.

5.8 Protection des données

5.8.1 Remarques générales

La protection des données est un des buts de la LSIE, dans son champ d'application. L'art. 1, al. 2, let. b, reprend d'ailleurs le but fixé à l'art. 1 LPD. Les dispositions du droit de la protection des données (LPD et ordonnances associées) s'appliquent à toutes les parties impliquées. Les fournisseurs d'identité et les exploitants de services utilisateurs sont soumis aux dispositions applicables aux personnes privées, Fedpol et l'UPIC aux dispositions applicables aux organes fédéraux. Par souci de transparence, la loi reprend et précise certaines exigences de la LPD. Dans quelques cas, elle vise à aller au-delà de ces exigences et à les renforcer.

Le projet règle expressément l'obligation d'obtenir le consentement du titulaire de l'e-ID. Il limite le traitement des données d'identification personnelle attestées par l'État; les fournisseurs d'identité ne pourront y avoir recours que pour procéder aux identifications prévues par la LSIE (art. 9, al. 1, LSIE).

En outre, la communication des données d'identification personnelle, des données générées par l'utilisation de l'e-ID et des profils basés sur ces dernières est interdite (art. 16, al. 2, LSIE).

5.8.2 Consentement à la communication

Les conditions de la protection des données doivent être respectées et les mesures de sécurité nécessaires doivent être prises pour toute utilisation des données d'identification personnelle. Les titulaires d'e-ID devront consentir explicitement à la communication des données d'identification personnelle. Lors de l'établissement de l'e-ID, ils autoriseront les fournisseurs d'identité à se procurer ces données auprès de Fedpol (art. 6, al. 2, let. c, LSIE); chaque fois qu'ils utiliseront leur e-ID auprès d'un exploitant d'un service utilisateur, le fournisseur d'identité demandera à nouveau leur consentement avant de communiquer les données à l'exploitant (art. 16, al. 1, let. c, LSIE).

5.8.3 Séparation des données d'identification personnelle et des données générées par l'utilisation de l'e-ID

En prévoyant des mesures de sécurité spécifiques, la présente loi va au-delà des exigences de la LPD en ce qui concerne l'obligation de garantir la sécurité des données. L'art. 9, al. 3, exige que le fournisseur d'identité conserve les données d'identification personnelle visées à l'art 5, les données concernant l'utilisation de l'e-ID et les autres données séparément les unes des autres. La séparation physique et organisationnelle, en fonction du type de données et du but de leur traitement, représente une mesure de sécurité supplémentaire propre à empêcher les personnes non autorisées d'avoir accès à toutes les données concernant le titulaire d'une e-ID. Elle vise notamment à limiter les conséquences néfastes d'un accès non autorisé au

système. En effet, elle permet de s'assurer que leur sécurité respective puisse être garantie même si la sécurité de l'une d'entre elle est compromise.

5.8.4 Accès aux données d'identification personnelle et aux données générées par l'utilisation de l'e-ID

La présente loi vise à renforcer le principe de reconnaissance de la finalité du traitement des données personnelles visé à l'art. 4, al. 4, LPD ainsi que le droit d'accès aux données personnelles prévu à l'art. 8 LPD. Selon l'art 15, al. 1, let. i, LSIE, le fournisseur d'identité accorde au titulaire de l'e-ID un accès en ligne aux données générées par l'utilisation de l'e-ID et à ses données d'identification personnelle visées à l'art. 5. Par la même occasion, cette mesure vise donc à améliorer la transparence du système e-ID et à augmenter la confiance des utilisateurs dans les procédures d'établissement de l'e-ID.

5.8.5 Finalité et restrictions

La finalité et les conditions du traitement, de la conservation et de la communication des données sont définies strictement par le projet de loi. L'art. 9, al. 1, prévoit notamment que le fournisseur d'identité peut traiter les données d'identification personnelle communiquées par Fedpol uniquement le temps que l'e-ID n'a pas été révoquée et uniquement pour procéder aux identifications en vertu de la présente loi. En outre, l'art. 16, al. 1, prévoit que le fournisseur d'identité peut communiquer aux exploitants d'un service utilisateur uniquement les données d'identification personnelle qui offrent le niveau de garanti requis, qui sont nécessaires pour l'identification de la personne concernée et à la communication desquelles le titulaire de l'e-ID a consenti. Par ailleurs, des règles spécifiques s'appliquent aux photographies enregistrées dans le système d'information de Fedpol. Pour les e-ID d'un niveau de garantie élevé, ces photographies ne peuvent être utilisées que dans le cadre de la procédure d'établissement. En outre, seules les e-ID d'un niveau de garantie élevé peuvent contenir ces photographies.

La communication de données prévue par le projet de loi est requise pour assurer le fonctionnement du système e-ID ainsi que pour garantir le niveau de confort, de flexibilité et de simplicité attendu par les utilisateurs. Le principe de proportionnalité est respecté lors de cette communication, car l'atteinte à la vie privée prévue n'excède pas ce qui est nécessaire pour atteindre l'objectif poursuivi. En outre, les données personnelles communiquées ne sont pas des données sensibles au sens de l'art. 3, let. c, LPD.

En vertu des art. 17, al. 1, et 19, al. 1, LPD, un organe fédéral n'est en droit de traiter et de communiquer des données personnelles que s'il existe une base légale. En application des art. 3, let. i, et 4, al. 3 et 4, LPD, il y a lieu de définir la finalité du système envisagé de manière précise et reconnaissable pour les personnes concernées. Ainsi, la présente loi prévoit des règles précises permettant à Fedpol de gérer un système d'information pour l'identification des requérants. L'art. 24 définit la

nature, le contenu et la finalité de ce système. L'art. 24, al. 1, énumère les types de données qui y sont enregistrées: les données journalisées relatives à la procédure d'établissement de l'e-ID visées à l'art. 6, al. 5, les données d'identification personnelle visées à l'art. 5, leur origine et les informations concernant leur mise à jour et les numéros AVS. L'al. 2 du même article précise les buts poursuivis. Le système sert à la réception des demandes et des déclarations de consentement des personnes concernées, à l'exécution automatisée des tâches de Fedpol dans le cadre de l'établissement des e-ID, à la mise à jour des données d'identification personnelle prévue à l'art. 7 et à la vérification de la validité du numéro d'enregistrement de l'e-ID prévue à l'art. 23, al. 2.

5.8.6 Interdiction du commerce des données

La vente des données traitées, conservées et communiquées dans le cadre de la LSIE est strictement limitée. Selon l'art. 16, al. 3, le fournisseur d'identité ne peut communiquer à un tiers ni les données d'identification personnelle visées à l'art. 5, ni les données générées par l'utilisation de l'e-ID ni des profils basés sur ces données. Cette interdiction s'applique indépendamment du niveau de garantie prévu par l'e-ID. De ce fait, les données régies par la LSIE ne peuvent pas être vendues à un tiers.

L'interdiction du commerce des données affaiblit la valeur économique des données d'identification personnelle attestées par l'État. Ces données seront insaisissables et ne tomberont pas dans la masse en faillite (art. 14, al. 1, LSIE). Afin d'assurer la continuité d'un système e-ID reconnu et des e-ID qui y sont associés, un fournisseur d'identité en difficulté financière pourra vendre l'ensemble de son système e-ID à un autre fournisseur d'identité. Le montant de la vente tombera dans la masse en faillite (art. 14, al. 3, LSIE).

Glossaire

Terme	Définition
authentification d = Authentifizierung i = autentificazione	Processus consistant à vérifier une identité alléguée lors de l'utilisation de l'e-ID. Dans ce cadre, le titulaire prouve au fournisseur d'identité son identité. Il doit tout d'abord s'identifier en entrant dans le système son nom d'utilisateur. Celui-ci doit être ensuite authentifié: le système envoie au titulaire un mot de passe permettant de vérifier s'il s'agit bien de la bonne personne.
données d'identification personnelle d = Personen-identifizierungsdaten i = dati d'identificazione personale	Ensemble de données géré par l'État dans Infostar, ISA, SYMIC et Ordipro, permettant d'établir l'identité d'une personne.
exploitant d'un service utilisateur d = Betreiberin von E-ID-verwendenden Diensten i = gestori di servizi che utilizzano l'eID	Personne physique ou morale qui gère dans le cadre de son activité des services en ligne nécessitant d'établir de façon fiable l'identité et l'authenticité de la personne qui les utilise. Le terme anglais est: *relying party*.
fournisseur d'identité d = Identity Provider (IdP) i = fornitori di servizi d'identificazione elettronica *(identity provider; IdP)*	Fournisseur de services d'identification reconnu au sens de la LSIE.
identification d = Identifizierung i = identificazione	Processus d'établissement de l'identité d'une personne à l'aide de données d'identification personnelle la représentant de manière univoque.
gestion des identités et des accès (GIA) d = Identity and Access Management (IAM) i = Identity and Access Management (IAM)	L'ensemble des processus et applications mis en œuvre par un organisme pour la gestion des identités et de l'administration des droits d'accès à ses applications, systèmes et ressources. Le terme anglais est: *Identity and Access Management (IAM).*

Terme	Définition
interopérabilité d = Interoperabilität i = interoperabilità	Capacité à opérer ensemble au niveau des systèmes, des techniques et de l'organisation. À cette fin, des règles techniques communes doivent être appliquées. Les systèmes de téléphonie mobile fonctionnent par exemple de façon interopérable.
moyen d'identification électronique d = elektronische Identifizierungseinheit i = mezzo d'identificazione elettronica	Élément électronique utilisé pour l'identification et l'authentification d'une personne physique.
moyen d'identification électronique reconnu (e-ID) d = anerkannte elektronische Identifizierungseinheit (E-ID) i = mezzo d'identificazione elettronica riconosciuto	Moyen d'identification électronique délivré par un fournisseur d'identité conformément aux prescriptions de la présente loi. Le support d'une e-ID peut être par exemple un smartphone ou une carte à puce).
numéro d'enregistrement de l'e-ID d = E-ID-Registrierungsnummer i = numero di registrazione eID	Numéro d'identification univoque attribué à une personne.
National Institute of Standards and Technology (NIST)	Agence des États-Unis, appartenant à l'administration technologique du département du Commerce, responsable en matière de processus de normalisation.
organisme de reconnaissance d = Anerkennungsstelle i = servizio di riconoscimento	L'Unité de pilotage informatique de la Confédération (UPIC) est l'organisme de reconnaissance prévu par la LSIE. Elle est responsable en particulier de la réception et de l'examen des demandes de reconnaissance des fournisseurs d'identité.

Terme	Définition
Ordipro	Système d'information du Département fédéral des affaires étrangères. Ordipro sert en particulier au traitement administratif des questions liées à l'accréditation et à l'administration des différentes catégories de cartes de légitimation pour les personnes bénéficiaires visées à l'art. 2, al. 2, de la loi du 22 juin 2007 sur l'Etat hôte (RS *192.12*).
procédure de reconnaissance d = Anerkennungsverfahren i = procedura di riconoscimento	Dans le cadre de cette procédure, les fournisseurs d'identité et leurs systèmes e-ID sont reconnus lorsqu'ils remplissent les conditions professionnelles, techniques et organisationnelles et les exigences de sécurité. La reconnaissance est contrôlée et renouvelée à intervalles réguliers.
registre de l'état civil (Infostar) d = Personenstandregister (Infostar) i = registro informatizzato dello stato civile (Infostar)	Registre informatisé dans lequel tous les événements d'état civil sont consignés. Tous les offices de l'état civil suisses y sont raccordés.
règlement eIDAS d = eIDAS-Verordnung i = regolamento eIDAS	Règlement de l'Union européenne sur l'identification électronique et les services de confiance pour les transactions électroniques (electronic IDentification, Authentication and trust Services). Il vise à assurer l'interopérabilité des systèmes d'identification et à faciliter l'identification dans la fourniture transfrontalière de services au niveau européen.
service d'identité d = Identitätsstelle i = servizio delle identità	L'Office fédéral de la police (Fedpol) est le service d'identité prévu par la LSIE. Il a en particulier la responsabilité de vérifier les informations fournies par les requérants lors de l'identification.
service utilisateur d = E-ID-verwendender Dienst i = servizi che utilizzano l'eID	Application informatique qui exploite un système e-ID pour l'identification et l'authentification.

Terme	Définition
SuisseID	Moyen d'identification électronique mis en œuvre par le Secrétariat d'Etat à l'économie (SECO) disponible sous forme de carte à puce ou de clé USB. La SuisseID permet de recourir à des services électroniques qui présupposent une identification sûre de l'utilisateur et de munir un document d'une signature électronique présentant la même valeur juridique que la signature manuscrite.
SwissID	Moyen d'identification électronique de SwissSign. Le développement de la SwissID a profité de l'expérience acquise avec la SuisseID. Le nouveau service sera développé progressivement et remplacera la SuisseID sur le moyen terme.
système d'information central sur la migration (SYMIC) d = Zentrales Migrationsinformationssystem (ZEMIS) i = sistema d'informazione centrale sulla migrazione (SIMIC)	Système d'information du Secrétariat d'État aux migrations (SEM). SYMIC contient des données personnelles relevant des domaines des étrangers et de l'asile.
système e-ID d = E-ID-System i = sistema di eID	Système électronique utilisé pour l'établissement, la gestion et l'utilisation d'une e-ID.
système d'information relatif aux documents d'identité (ISA) d = Informationssystem Ausweisschriften (ISA) i = servizio d'informazione per documenti d'identità (ISA)	Système d'information dans lequel sont enregistrées les données saisies lors de l'établissement d'un document d'identité pour les ressortissants suisses.
Unique Person Identification (CdC-UPI) d = (ZAS-UPI) i = (UCC-UPI)	Fonctionnalité permettant d'identifier des personnes physiques et de gérer l'identifiant NAVS13 (numéro AVS) dans le registre central des assurés des assurances sociales fédérales.