Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

Berne, le 22 février 2017

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID)

Rapport explicatif relatif à l'avant-projet

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. Les utilisateurs d'Internet bien formés, familiarisés avec la technologie, très connectés et constamment en ligne favorisent ce changement socio-économique. Afin que des transactions plus complexes puissent également être effectuées par la voie électronique, les prestataires (ci-après les « exploitants d'un service utilisateur ») 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. Un e-ID permet à un exploitant d'un service utilisateur de procéder en ligne à une identification et à une authentification 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 (FI) et qu'un e-ID soit remis 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 (par ex. pour le support technique, les systèmes de lecture, les logiciels) car ils n'offrent pas la flexibilité requise pour faire face à l'évolution rapide des besoins et de la technologie. En revanche, des offres d'identification électronique présentant différents niveaux de garantie se développent aujourd'hui dans le secteur privé (par ex. Apple-ID, Google-ID, Mobile-ID, OpenID, SuisseID, SwissPass, etc.). Il est difficile de dire quels e-ID utilisés à l'heure actuelle existeront encore à moyen et à long terme. C'est la raison pour laquelle le nouveau concept prévoit une répartition des tâches entre l'État et le secteur privé.

En sus des résultats de la consultation, on a tenu compte des récents développements qu'a connus l'Union européenne (UE) et vérifié que le concept était compatible avec le règlement

(UE) n° 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 (règlement eIDAS)[1].

Le 13 janvier 2016, le Conseil fédéral a pris acte du concept pour des systèmes d'e-ID, chargé le DFJP d'élaborer une loi et fixé le cadre de la législation.

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 met déjà, pour ce faire, à disposition des moyens d'identification conventionnels tels que le passeport suisse, la carte d'identité et le titre de séjour. Il sera également désormais possible de prouver l'identité d'une personne physique par la voie électronique. Des e-ID reconnus 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, tels que la signature électronique, peuvent être proposés par des FI, mais ils ne constituent pas un élément des e-ID.

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

1.2.2 Répartition des tâches entre l'État et les acteurs du marché

L'avant-projet (AP) prévoit une répartition des tâches entre l'État et les acteurs du marché. L'acceptation de l'e-ID passe par la mise en place d'un cadre légal et organisationnel fiable et dépend de la capacité de fonctionnement et du dynamisme du marché. Deux initiatives privées récentes attestent de la pertinence de la démarche adoptée. Deux grandes banques, Credit Suisse et UBS, travaillent avec Swisscom à un projet « passepartout pour Internet » ; les CFF et la Poste offrent une solution commune pour l'accès à travers leurs portails Web.

Les FI satisfaisant aux conditions requises seront habilités par la Confédération à délivrer des e-ID reconnus et à gérer des systèmes e-ID reconnus. Tous les systèmes e-ID reconnus doivent être interopérables afin que les titulaires puissent utiliser leur e-ID quel que soit le service utilisateur.

[1] Le lien vers ce règlement figure en annexe dans la liste des sources.

1.2.3 Fonction de l'e-ID

Grâce à un e-ID, les personnes physiques peuvent s'enregistrer de manière sûre et conviviale sur des portails en ligne (services utilisateurs) et s'y reconnecter ultérieurement. Lors de l'enregistrement, les données personnelles n'ont pas besoin d'être saisies manuellement ; elles sont transmises par voie électronique par le biais de l'e-ID une fois que le titulaire y a consenti. Lorsque ces personnes se reconnecteront ultérieurement à ces portails, elles s'identifieront ou s'authentifieront avec l'e-ID qu'elles auront enregistré précédemment et celui-ci sera reconnu, ce qui garantira une connexion fiable. L'e-ID constitue donc l'un des fondements de l'utilisation sécurisée des services en ligne.

On distingue trois niveaux de garantie, comme le prévoient d'ailleurs l'UE pour les e-ID de ses États membres et les États-Unis pour les services de confiance. La Confédération met, quant à elle, les données d'identification personnelle gérées par l'État (par ex. numéro d'enregistrement de l'e-ID, nom, prénom, etc.) à la disposition des FI via une interface électronique. La première transmission des données à un FI ou à un exploitant d'un service utilisateur requiert le consentement exprès de la personne concernée (cf. art. 6 et 17, al. 1, let. f, AP). L'e-ID pourra cependant être utilisé au quotidien sans qu'il y ait besoin de recourir à nouveau à l'infrastructure de la Confédération.

Le respect des processus et des normes techniques par les FI sera régulièrement contrôlé par un organisme de reconnaissance (art. 4, 11 et 12 AP), qui sera rattaché à l'administration fédérale (art. 21 AP) et qui sera habilité à délivrer et prolonger les reconnaissances en fonction du résultat de ces contrôles. Les détails de ces processus et normes seront réglés au niveau des ordonnances et éventuellement des directives, sur le modèle des règles existantes dans le domaine des signatures électroniques[2] et des plateformes de messagerie électronique. Il s'agit en effet de profiter des synergies en matière de certification. La procédure de reconnaissance des systèmes e-ID est similaire à celle des plateformes de communication sécurisée dans le domaine des procédures pénales et civiles et dans le domaine des poursuites pour dettes et faillite. Une liste des FI reconnus et de leurs systèmes e-ID reconnus sera publiée (art. 22 AP).

1.2.4 Établissement de l'e-ID

Un e-ID est généralement établi après que la personne concernée s'est adressée à un FI. L'enregistrement comprend une identification qui est effectuée, selon le niveau de garantie, à l'aide d'un moyen électronique ou lorsque le requérant se présente personnellement. L'enregistrement se déroule en plusieurs étapes (voir art. 6 et 17, al. 1, let. b, AP) :

1. Celui qui souhaite obtenir un e-ID demande à un FI de l'établir. Selon le niveau de garantie, le FI demandera à voir le requérant lors d'une présentation en personne ou d'un entretien virtuel équivalent, par exemple une identification par vidéo.
2. Le FI vérifie le document d'identité présenté (passeport, carte d'identité ou titre de séjour) et demande par voie électronique au Service d'identité électronique suisse (service d'identité) de lui confirmer les données figurant sur ce document.
3. Le service d'identité compare les données transmises par le FI avec les données d'identification personnelle contenues dans les registres de personnes tenus par la Confédération.
4. Le requérant consent à ce que le service d'identité attribue ses données d'identification

[2] Cf. loi du 19 décembre 2003 loi sur la signature électronique, SCSE, RS 943.03.

personnelle au numéro d'enregistrement de l'e-ID et à ce qu'il transmette ce numéro d'enregistrement et ces données au FI.
5. Le service d'identité transmet le numéro d'enregistrement de l'e-ID accompagné des données attestées au FI.
6. Le FI attribue au requérant un moyen d'authentification (support de l'e-ID) qui permettra à ce dernier de s'identifier sur Internet.
7. Le FI veille à l'attribution correcte du numéro d'enregistrement et du moyen d'authentification de l'e-ID puis active cet 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 sont définies au moyen de normes et de protocoles techniques.

1.2.5 Niveaux de garantie

Toutes les transactions ne requièrent pas le même niveau de garantie. Des exigences trop élevées en matière de sécurité peuvent être perçues comme gênantes en pratique, favoriser les actes de contournement 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 sont reconnus. Ces niveaux sont déterminés par 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 ici « niveaux de garantie » (cf. art. 5 AP). Chaque niveau de garantie offre un degré de fiabilité différent. Le niveau de garantie requis pour les différents types d'applications est 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 peut ainsi être différent de celui requis pour le vote électronique ou des applications de cybersanté.

La dénomination et les caractéristiques des niveaux de garantie proposés ont été reprises du règlement eIDAS et des dispositions d'exécution s'y rapportant[3]. On distingue ainsi trois niveaux de garantie – *faible*, *substantiel* et *élevé* – présentant un degré de fiabilité divers concernant les données attribuées. En principe, un e-ID d'un niveau de garantie substantiel ou élevé peut toujours être utilisé pour des services utilisateurs requérant un niveau de garantie inférieur.

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[4] 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. Ils doivent encore faire l'objet d'une réflexion plus approfondie.

Ce modèle permet, par exemple, d'enregistrer dans un premier temps à un niveau *faible* un

---

[3] Cf. liste des sources.

[4] 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)

e-ID qui conviendrait, sur le plan technique, pour un niveau de garantie *substantiel*, et de revoir, au besoin, ultérieurement ce niveau à la hausse à la suite d'un entretien personnel. Ce procédé permet de faciliter l'accès aux systèmes e-ID reconnus. Avec le niveau de garantie faible, l'accès aux e-ID reconnus demeure aisé, ce qui constitue un facteur de réussite important pour les fournisseurs de systèmes e-ID reconnus sur le marché. Par ailleurs, une personne peut posséder, si elle le désire, plusieurs e-ID de niveaux de garantie divers émis par différents FI.

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 ; cf. art. 7, al. 1, AP). 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 FI ou d'une identification par vidéo sur la base d'un document d'identité délivré par l'État. Dans le cas d'un niveau de garantie *substantiel*, d'autres données d'identification personnelles sont ajoutées (par ex. le sexe, le lieu de naissance, l'état civil ; cf. art. 7, al. 2, AP). 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).

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 FI 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. Toutes les données d'identification personnelle disponibles sont attribuées au numéro d'enregistrement de l'e-ID (cf. art. 7, al. 2, AP) et le moyen d'authentification de l'e-ID doit satisfaire à des conditions de sécurité technique très contraignantes.

L'utilisation de l'e-ID requiert au moins une authentification à deux facteurs, l'un des deux devant être biométrique (« facteur d'authentification inhérent » selon le règlement d'exécution eIDAS). Le fonctionnement s'apparente donc ici à celui d'un smartphone doté d'un système de reconnaissance digitale, faciale ou vocale. 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 loi e-ID. 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 Contribution de l'État aux systèmes e-ID

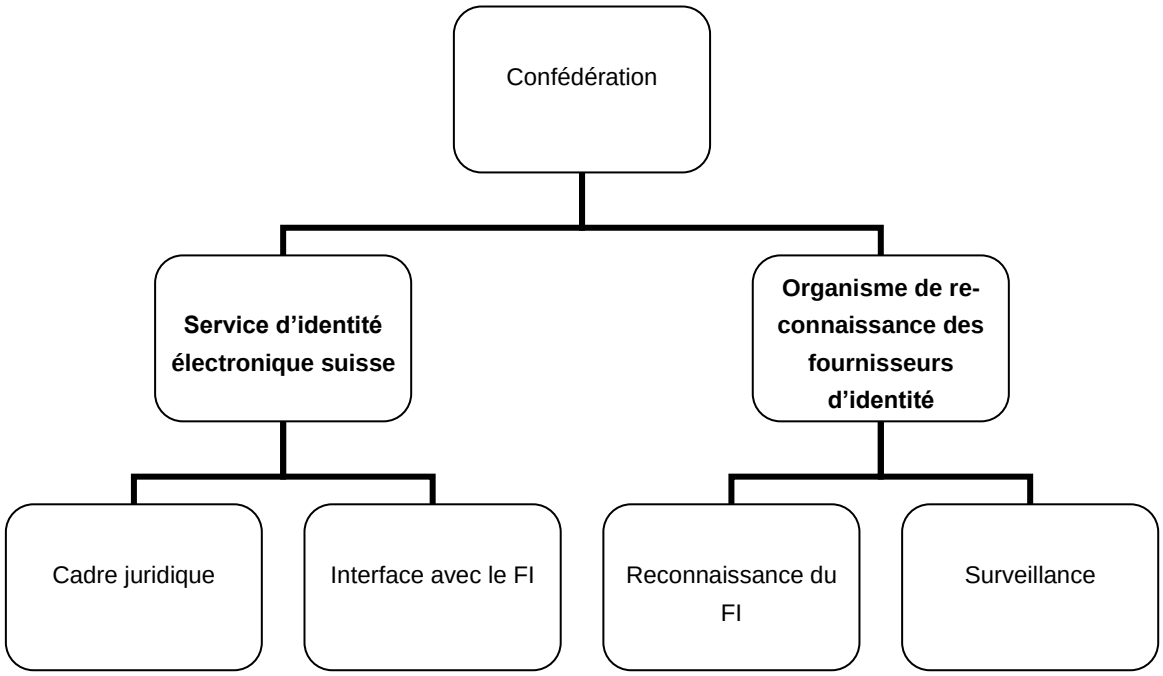
Vue d'ensemble

Un e-ID reconnu par l'État 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.

La Confédération garantit que les systèmes e-ID reconnus sont fiables et accomplit à cet effet quatre tâches dans le domaine des e-ID reconnus :

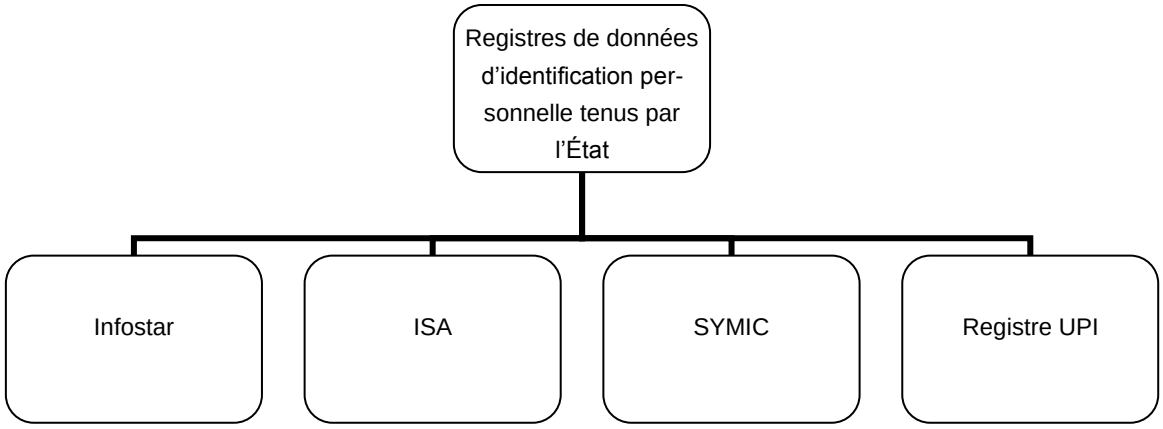
1. elle élabore et met à jour la réglementation en la matière, ce qui permet de garantir la transparence et la sécurité ;
2. elle définit les normes, les conditions de sécurité et les conditions d'interopérabilité à respecter pour pouvoir gérer un système e-ID ;
3. elle gère une interface électronique sur laquelle les FI reconnus peuvent obtenir des données d'identification personnelle gérées par l'État ;
4. elle reconnaît les FI et leurs systèmes e-ID et
5. elle surveille les FI et les systèmes e-ID reconnus.

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



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[5]). 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).

La loi du 23 juin 2006 sur l'harmonisation de registres (LHR, RS 431.02) définit le numéro AVS comme un identifiant personnel unique dans les registres concernés par le recensement de la population, à savoir les registres fédéraux de personnes ainsi que les registres cantonaux et communaux des habitants. La Confédération n'a pas accès à ces deux derniers registres et ne peut donc confirmer ni le lieu de domicile ni l'adresse par ce biais-là.



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)[6]. 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)[7]. Conformément à l'art. 50*e*, ce numéro ne peut être utilisé systématiquement que si une loi fédérale le prévoit et que le but de l'utilisation et les utilisateurs légitimés sont définis.

Selon la décision du Conseil fédéral concernant l'utilisation du numéro AVS, les institutions qui ne sont pas des autorités et qui sont chargées de l'accomplissement de tâches publiques

5 UPI est l'acronyme de « Unique Person Identification ».

6 RS **831.10**

7 RS **830.1**

peuvent être autorisées à utiliser le numéro AVS si une loi spéciale le prévoit. Ce numéro est souvent employé dans les relations entre le citoyen et l'administration. S'il n'était plus possible au FI 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. Les FI doivent donc être autorisés à utiliser le numéro AVS systématiquement (uniquement) dans ce but bien limité. Ils ne pourront le transmettre qu'aux exploitants d'un service utilisateur eux-mêmes habilités à utiliser systématiquement le numéro AVS (art. 9 AP).

L'utilisation systématique du numéro AVS sera par contre interdite 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 de lien entre la personne et son e-ID. Comme l'obtention d'un e-ID est laissée au bon vouloir de chacun et sera sans doute payante, et qu'elle est d'autre part réservée aux personnes détenant un document d'identité suisse ou un titre de séjour, le numéro d'enregistrement de l'e-ID ne se prêtera pas à une utilisation comme identifiant général.

Service d'identité électronique suisse (service d'identité)

Cadre légal

Le service d'identité s'occupe, en collaboration avec l'organisme de reconnaissance, des conditions juridiques, organisationnelles et techniques. Il définit 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 FI et des systèmes e-ID en fonction des progrès socio-économiques et techniques et des contraintes de sécurité du moment.

Les conditions-cadres définies par le Conseil fédéral requièrent l'élaboration d'un cadre légal permettant une reconnaissance ultérieure des e-ID suisses par l'UE et ses États membres. L'AP tient compte des exigences fixées par le règlement eIDAS et les décisions d'exécution s'y rapportant[8].

Interface

Le service d'identité met les données d'identification personnelle gérées par la Confédération à la disposition des FI reconnus via une interface électronique (art. 20 AP). L'établissement d'un numéro d'enregistrement de l'e-ID permet d'attribuer ces données de manière univoque et durable à une personne et à son e-ID, sans contestation possible. Cette interface n'est accessible qu'aux FI reconnus.

Le service d'identité est responsable de la gestion de l'interface servant à la transmission des données d'identification personnelle. Il est l'interlocuteur des FI reconnus et des autorités qui gèrent les registres étatiques raccordés au système.

Le service d'identité se procure les données d'identification personnelle dans divers registres (art. 20 AP). Le nom d'une personne est confirmé grâce à une comparaison des données avec Infostar tandis que, par exemple, le numéro des documents d'identité et les photographies proviennent d'ISA ou du SYMIC. Les données d'identification personnelle peuvent être assorties de métadonnées, telles que la source ou la date de saisie (art. 7, al. 3, AP).

---

[8] Cf. liste des sources.

Les FI sont tenus de mettre périodiquement à jour les données d'identification personnelle rattachées au numéro d'enregistrement d'un e-ID. Selon le niveau de garantie, ils doivent procéder à cette mise à jour tous les ans (niveau de garantie *faible*), tous les trimestres (niveau de garantie *substantiel*) ou toutes les semaines (niveau de garantie *élevé*) (cf. art. 8, al. 1, AP).

Organisme de reconnaissance des fournisseurs d'identité (organisme de reconnaissance)

Reconnaissance

Les FI (du secteur privé ou du secteur public) satisfaisant aux conditions requises peuvent faire reconnaître par l'organisme de reconnaissance leurs systèmes e-ID présentant l'un des trois niveaux de garantie prévus. Un FI peut 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 fixe, pour ce faire, des exigences juridiques, organisationnelles et techniques que les FI doivent satisfaire, l'organisme de reconnaissance devant s'assurer que celles-ci soient bien remplies.

L'organisme de reconnaissance publie une liste des FI 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 FI ou d'un système e-ID en particulier (art. 22 AP).

Surveillance

L'organisme de reconnaissance surveille les FI et les systèmes e-ID reconnus et prend des mesures en cas de non-respect des exigences fixées ou d'incidents remettant en cause la sécurité informatique. Pour ce faire, il demande aux FI de lui apporter, à une fréquence définie préalablement, les preuves de conformité requises et les vérifie. Il peut imposer des mesures et dans certains cas retirer la reconnaissance à un FI ou à un système e-ID (art. 12 AP).

1.3 Justification et évaluation des solutions proposées

1.3.1 Solution développée par le marché

Plusieurs e-ID sont déjà utilisés 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, qui se fient alors à cette identification.

Les services de cyberadministration proposés par l'État requièrent une identification claire et fiable du titulaire de l'e-ID, vérifiée par un processus standardisé. Plusieurs États ont créé leur propre e-ID, soit en reconnaissant des systèmes privés, soit dans un cadre entièrement étatique. Dans ce dernier cas, les solutions 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 faire face à l'évolution des technologies que très difficilement et au prix d'adaptations coûteuses ou en faisant l'objet de nouvelles mises au concours. Elles ne se développent souvent pas comme on le souhaiterait et sont parfois utilisées par obligation et uniquement une fois par an pour

effectuer la déclaration d'impôts. D'autres explications concernant le développement des e-ID créés par l'État figurent au point 1.5.

La solution proposée libère en grande partie l'État de la contrainte liée à ce dynamisme du marché et aux coûts élevés qui en résultent.

On trouve aujourd'hui sur le marché différents moyens d'identification électronique fiables, parfois proposés par des FI suisses et bénéficiant d'un accueil de plus en plus favorable (par ex. Mobile ID proposé par les opérateurs de téléphonie mobile ou SuisseID proposé par la Poste). Ces systèmes e-ID seront renforcés par la reconnaissance et utilisés pour les applications de cyberadministration. De surcroît, le fait d'instaurer des règles claires incitera d'autres FI potentiels à se lancer sur ce marché (par ex. les banques ou les éditeurs de cartes de crédit).

Les exigences posées aux systèmes e-ID suisses reconnus correspondent le plus possible aux conditions de notification des systèmes e-ID fixées par le règlement eIDAS.

1.3.2 Procédure de reconnaissance

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 cependant, 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 DFJP du 16 septembre 2014 sur la reconnaissance des plateformes de messagerie (RS 272.11). 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 est plus simple et a fait ses preuves. C'est la raison pour laquelle la procédure de reconnaissance des FI s'apparente à celle prévue pour les plateformes de messagerie : conformément à l'AP, l'organisme de reconnaissance est chargé de réceptionner et d'examiner les demandes de reconnaissance des FI 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 d'un département et soient mises à jour. Elles se rapprocheront des règles en vigueur pour les signatures électroniques et les plateformes de messagerie, de sorte qu'il soit possible pour les FI de profiter de synergies en matière de certification.

1.4 Harmonisation des tâches et du financement

1.4.1 Nouvelles tâches

La loi e-ID crée de nouvelles tâches pour l'administration fédérale. Sont créés, d'une part, le service d'identité, qui est chargé de mettre à disposition une interface pour la transmission des données d'identification personnelle, et d'autre part, l'organisme de reconnaissance, qui s'occupe des procédures de reconnaissance et de la surveillance des FI reconnus (cf. ch. 1.2.6). Ces deux services ne seront pas nécessairement rattachés à la même unité administrative au sein de la Confédération.

Le service d'identité effectuera les tâches suivantes :

a) gérer et maintenir les infrastructures informatiques qui lui sont nécessaires (interface avec les FI et rattachement des banques de données internes de l'administration comme ISA, Infostar, etc.),
b) apporter un soutien technique aux banques de données internes à l'administration concernées,
c) apporter un soutien technique aux FI reconnus,
d) développer et mettre à jour les exigences techniques et organisationnelles auxquelles les FI et les systèmes e-ID doivent satisfaire pour être reconnus,
e) acquérir les services proposés par les FI nécessaires à la Confédération et
f) se tenir informé sur les évolutions technologiques dans le domaine des e-ID ainsi que sur toute autre question liée à la sécurité informatique.

Selon l'art. 19 AP, le service d'identité est une unité administrative rattachée au DFJP (fedpol). Ce dernier est chargé d'élaborer la législation en matière de documents d'identité et a mis au point les concepts pour des systèmes d'e-ID. La plupart des banques de données utilisées pour attester les données d'identification personnelle sont gérées par le DFJP. Dans le cas où une correction de ces données serait éventuellement requise, une demande pourra être adressée au service de clearing UPI de la CdC.

L'organisme de reconnaissance :

a) reconnaît les FI,
b) contrôle que les FI et les systèmes e-ID continuent de satisfaire aux conditions de la reconnaissance et
c) tient et publie la liste des FI reconnus.

L'organisme de reconnaissance exercera, outre des fonctions de reconnaissance, des fonctions de contrôle comparables à celles assumées par l'organe de contrôle visé par le règlement eIDAS. D'autres fonctions de contrôle similaires sont exercées au sein de la Confédération par le DFF (UPIC). C'est la raison pour laquelle l'art. 21 AP prévoit le rattachement de l'organisme de reconnaissance au DFF (UPIC).

1.4.2 Financement

Prestations préalables de la Confédération

L'introduction d'e-ID reconnus requiert un investissement financier de 6,5 millions de francs de la part de la Confédération. Dans la mesure où elle constitue un objectif stratégique qui profite autant à l'administration publique au niveau fédéral, cantonal et communal qu'au secteur privé et à la population, on propose que les coûts soient financés par le DFJP, E-Government Suisse et les ressources centrales destinées au domaine informatique.

À ce jour, on table sur 1,5 million de francs de coûts d'exploitation informatique annuels et sur 0,7 million de francs pour les frais de personnel. Ces dépenses seront cependant compensées à moyen terme par les recettes provenant des émoluments. Le plan de financement de ces dépenses sera présenté avec le message après la consultation.

Financement par les émoluments
Plusieurs modèles de financement pour les prestations fournies par l'État aux FI ont été examinés. Si on a envisagé un modèle « prépayé », qui prévoyait que le FI 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 FI, celui-ci n'a pas été retenu. A également été rejeté un modèle prévoyant la vérification gratuite des données attestées après la première transmission de ces données, car un tel modèle aurait occasionné des déficits importants, ce qui aurait été inapproprié au regard des efforts d'économies demandés par les milieux politiques. 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 transmission des données d'identification personnelle lors de la procédure d'établissement est gratuite si l'obtention de l'e-ID est également gratuite pour le requérant. Un émolument modeste est cependant perçu pour toute autre transmission 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 reconnus, et notamment de ceux présentant un niveau de garantie *substantiel* ou *élevé*, de nouvelles recettes qui permettront de couvrir suffisamment les coûts pourront être générées.

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). 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.

1.5 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 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 na-

tionaux. Le concept pour les systèmes e-ID suisses reconnus tient compte de ces exigences de sorte que les e-ID suisses pourraient également être utilisés dans le contexte international.

La loi proposée crée, entre autres, un cadre pour les dispositions et les normes techniques qui réglementeront la reconnaissance des systèmes e-ID et des FI. Ce cadre est conçu de manière à ce que la reconnaissance mutuelle des systèmes e-ID entre la Suisse et l'UE ou certains de ses membres soit possible à l'avenir. Des accords bilatéraux seraient pour ce faire nécessaires.

1.5.2 Développements de ces 15 dernières années

Les États qui se sont intéressés à la question des e-ID se sont, dans un premier temps, interrogés sur la date à laquelle leur carte d'identité serait dotée d'un e-ID, les technologies qui seraient utilisées et les fonctions qui y seraient intégrées.

Se sont principalement posées les questions suivantes : quelle technologie à puce et quel système d'exploitation à puce utilisera-t-on ? La puce fonctionnera-t-elle par contact ou par hyperfréquences (NFC) ? Un aspect important sur les plans juridique et politique portait sur la question de savoir si l'e-ID s'appuierait sur un identifiant personnel existant et, le cas échéant, de quelle nature celui-ci serait. Sur le plan fonctionnel, il a fallu décider si la puce contiendrait également une clé de signature électronique et, par la suite, si la fonction de passeport électronique (ePasseport) basée sur une technologie sans contact normalisée par l'Organisation de l'aviation civile internationale (OACI) serait intégrée.

Forts de ces réflexions, la plupart des pays européens ont petit à petit introduit au cours des 15 dernières années un e-ID rattaché à la carte d'identité, qui est devenu 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'un 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, ce qui s'explique aussi peut-être par le fait que nombre d'entre eux 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 national, 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 pouvant être utilisés sur Internet.

Le premier système qui est apparu est celui des SmartCards dotées de puces à contact, qui était essentiellement basé 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 (2^{e} 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 l'Allemagne constitue le point d'orgue de la phase de 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.

En adoptant une stratégie globale, l'Allemagne a veillé à ce que les titres de séjour pour étrangers soient dotés de fonctions compatibles d'identification en ligne. Ces dernières années, la carte d'identité électronique allemande est, dans une certaine mesure, devenue une référence mondiale pour la création d'e-ID nationaux. En Allemagne, la moitié environ de la population possède désormais la carte d'identité électronique et 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. Par ailleurs, 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.

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 répandus, ceux-ci sont principalement installés 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.

Guidés par le projet américain de développement commun d'un « écosystème d'identité électronique »[9], 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 cybe-

[9] National Strategy for Trusted Identities in Cyberspace (stratégie nationale pour des identités de confiance dans le cyberespace) : écosystème d'identité électronique. Cf. liste des sources.

radministration. 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 acceptés par les services publics et peuvent être utilisés pour les applications de cyberadministration.

L'UE a fini par tenir compte de ces développements dans le règlement eIDAS susmentionné et accepte, pour la reconnaissance mutuelle, non seulement les e-ID créés 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 coûteuses. Au vu des expériences faites dans les pays voisins, une autre solution s'impose à la Suisse. Cette solution libère l'État de la contrainte liée à cette dynamique technologique et aux coûts élevés qui en résultent. Elle offre par ailleurs au secteur privé la place requise pour qu'il trouve des solutions flexibles et adaptées à ses besoins. Le rôle de l'État se limite donc au minimum requis pour garantir la fiabilité des transactions électroniques.

Voici ce qui ressort de la comparaison du concept relatif à la reconnaissance des moyens d'identification électronique proposé dans l'AP avec les développements, expériences et réflexions actuelles s'inscrivant dans le contexte international :

- La Suisse a tiré les enseignements des expériences faites au cours des 15 dernières années et innove avec son concept d'e-ID reconnu, qualifié d'exemplaire par plusieurs services.
- 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 un e-ID ne sert pour l'instant pas de document de voyage, il est utilisé 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'un e-ID est exigé 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 légale 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, l'e-ID suisse doit dès le départ être conçu de façon à pouvoir être notifié.

L'avant-projet vise, entre autres, à créer un cadre pour les dispositions et les normes techniques qui réglementeront la reconnaissance des systèmes e-ID et des FI. Ce cadre est conçu de façon à ce que la reconnaissance mutuelle des systèmes e-ID reconnus entre la Suisse et l'UE ou certains de ses membres soit possible à l'avenir.

1.6 Mise en œuvre

L'introduction des e-ID reconnus contribue à la mise en œuvre de la stratégie « Suisse numérique » et de l'objectif opérationnel n° 5 du plan stratégique de la stratégie suisse de cyberadministration (cf. chiffre 3).

Dans le cadre du mandat relatif au renouvellement du passeport suisse, le DFJP a élaboré des concepts et effectué des travaux préparatoires qui peuvent être réutilisés pour la mise en œuvre de l'e-ID. Plusieurs ordonnances qui seront élaborées par le Conseil fédéral et ce département ainsi que des directives viendront régler les détails techniques et organisationnels de la mise en œuvre. Leur élaboration démarrera dès que le projet de loi aura été examiné par les deux Chambres fédérales.

Il convient par ailleurs de désigner les unités administratives auxquelles seront rattachés le service d'identité et l'organisme de reconnaissance.

1.7 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 personnelles que les bénéficiaires de l'e-ID doivent remplir, la reconnaissance des FI, la procédure d'établissement et les niveaux de garantie. La troisième section établit les devoirs des titulaires d'un e-ID. Les sections suivantes définissent les devoirs des exploitants d'un service utilisateur et les devoirs des FI. Les sections 6 et 7, quant à elles, règlent l'organisation et les tâches du service d'identité et de l'organisme de reconnaissance. La compétence pour la réglementation des émoluments est définie dans la section 8. La section 9 fixe les règles de responsabilité. Enfin, la loi se termine avec la section 10 qui indique les dispositions transitoires. La modification d'autres actes est réglée en annexe.

1.8 Commentaire des dispositions

1.8.1 Préambule

La compétence de régler les moyens d'identification électronique reconnus (e-ID) résulte indirectement de la Constitution (Cst., RS 101). 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.

La présente loi fédérale règle certains aspects de droit civil relatifs aux relations contractuelles entre les fournisseurs d'identité, les titulaires et les exploitants d'un service utilisateur. Elle se fonde à cet égard sur l'art. 122, al. 1, Cst. qui établit la compétence de la Confédération en matière de droit civil.

1.8.2 Section 1 Dispositions générales

Art. 1 Objet et but

Al. 1

La loi régit non seulement la reconnaissance des fournisseurs d'identité mais également les droits et les devoirs des titulaires d'un e-ID et des exploitants d'un service utilisateur, ainsi que le contenu, l'établissement, la révocation et l'utilisation des moyens d'identification électronique reconnus (e-ID).

Al. 2, let. a et b

Les e-ID contribuent à garantir la sécurité et la fiabilité des transactions électroniques (commerce électronique et cyberadministration). 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. Un 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 contribuent à assurer à temps le passage réussi de la Suisse à une société de l'information développée.

Art. 2 Définitions

Dans la mesure du possible, les termes choisis correspondent à la terminologie de la SCSE et du règlement eIDAS.

Lettres a et b

Dans la loi, « e-ID » désigne toujours un moyen d'identification électronique reconnu. L'e-ID reconnu n'est cependant pas le seul moyen d'identification électronique qui existe. Comme mentionné dans la 1re partie du présent rapport explicatif, plusieurs offres d'identification électronique de niveaux de garantie différents sont déjà disponibles sur le marché.

Le terme d'« e-ID » provient du concept pour des moyens d'identification électronique reconnus par l'État (délivrance d'un e-ID conjointement avec la carte d'identité, cf. ch. 1.1). Si la loi e-ID, contrairement au concept, ne prévoit pas de rattacher le moyen d'identification électronique à un document d'identité, c'est-à-dire à une carte d'identité suisse ou à un titre de séjour, le terme d'« e-ID », ou d'« eID » au niveau international, s'est répandu. De plus, l'intitulé « e-ID » résulte d'une logique simple : lors d'une transaction électronique, l'e-ID sert à prou-

ver l'identité de son titulaire, tout comme un document d'identité habituel qui comporte une photographie et qui nécessite une présentation en personne du requérant.

Le terme « e-ID » tel qu'utilisé ci-après ne désigne que les moyens d'identification électronique qui sont établis par un FI conformément aux dispositions de la loi e-ID.

Let. c
Le terme de « fournisseur d'identité » est utilisé au niveau national et international.

Let. d et e
L'identification s'effectue lors de l'enregistrement auprès d'un FI (obtention d'un e-ID) ou d'un service utilisateur (application informatique). Il s'agit d'enregistrer via un processus soumis à un contrôle les données d'identification personnelle et les facteurs d'authentification qui représentent l'identité d'une personne.

L'authentification s'effectue lors des connexions suivantes au service utilisateur. Il s'agit de vérifier via un processus soumis à un contrôle et avec les facteurs d'authentification de l'e-ID que l'identité enregistrée et l'identité alléguée d'une personne correspondent.

Let. f
Les données d'identification personnelle sont les attributs d'identité enregistrés par l'État, comme le nom ou la date de naissance. Cet ensemble de données géré par l'État contient également un numéro d'enregistrement de l'e-ID auquel sont rattachées toutes les données d'identification personnelle relatives à une même personne.

Let. g
La loi e-ID introduit un numéro d'identification unique et étatique pour les personnes physiques (numéro d'enregistrement de l'e-ID). De façon analogue au numéro d'identification des entreprises (IDE)[10], un numéro d'enregistrement de l'e-ID doit être attribué à toute personne qui obtient un e-ID. Puisqu'il est possible et autorisé de disposer de plusieurs e-ID, sur des supports différents par exemple, le numéro d'enregistrement de l'e-ID permet d'attribuer les données d'identification personnelle à une seule et même personne de façon cohérente. Le numéro d'enregistrement de l'e-ID garantit également que les données issues de registres de personnes différents soient attribuées durablement à une personne en particulier ; l'exactitude des données d'identification personnelle utilisées avec un e-ID est ainsi assurée.

Let. h
Un FI gère au moins un système e-ID. La distinction entre les FI et les systèmes e-ID est essentielle au cours de la reconnaissance. Pour un FI, l'autorité compétente contrôle que les conditions fixées à l'art. 4 AP 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 FI reconnu peut gérer plusieurs systèmes e-ID de niveaux de garantie divers qui ne sont pas tous reconnus. La reconnaissance est réglée aux art. 4 ss AP.

[10] Cf. art. 3, al. 1, let. c, de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE, RS 431.03)

Let. i et j
En ce qui concerne les exploitants d'un service utilisateur, une distinction est également faite entre la personne physique ou morale qui gère l'application technique et l'application technique elle-même. La communication s'effectue soit entre des personnes, c'est-à-dire le FI et l'exploitant d'un service utilisateur (*relying party*), soit entre les applications informatiques, c'est-à-dire le système e-ID et le service utilisateur (*relying party application*).

La Confédération, les cantons et les communes, ainsi que les unités administratives ou les autorités qui leur sont rattachées sont également des personnes morales habilitées à gérer un service utilisateur.

1.8.3 Section 2 Établissement d'un e-ID

Art. 3 Conditions personnelles

Remarque préliminaire
Les FI n'ont pas l'obligation de conclure un contrat avec une personne dès lors que celle-ci remplit les conditions nécessaires. La formulation potestative de l'al. 1 garantit que les FI ne puissent pas être contraints d'établir un e-ID.

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

Al. 1
Document d'identité comme preuve d'identité
Pour pouvoir obtenir un e-ID reconnu par l'État, le requérant doit établir son identité à l'aide d'un document d'identité suisse valable (let. a) ou d'un titre de séjour suisse valable (let. b).

Mineurs
Les mineurs et les personnes dont la capacité d'exercer les droits civils a été partiellement ou complètement retirée peuvent obtenir un e-ID. Ils doivent disposer d'un document d'identité correspondant. La personne habilitée à les représenter demande l'obtention d'un e-ID à leur nom ; ils deviennent alors titulaires d'un e-ID. Ils doivent cependant l'utiliser sous la surveillance de la personne habilitée à les représenter.

Étrangers
Les personnes de nationalité étrangère titulaires d'un titre de séjour valable au sens de l'art. 41 de la loi fédérale du 16 décembre 2005 sur les étrangers (LEtr, RS 142.20) doivent également pouvoir utiliser un e-ID ainsi que les applications de la cyberadministration.

Al. 2
Le titre de séjour indique le type d'autorisation octroyée (en ce qui concerne l'établissement, le séjour ou l'exercice d'une activité lucrative par exemple). Il doit être accompagné d'une photographie de l'étranger, de la signature de celui-ci et de toutes les informations relatives à son statut. Le DFJP (SEM) détermine le type (biométrique ou non) et le contenu du titre de séjour.

Peuvent obtenir un e-ID sans démarches supplémentaires les étrangers qui reçoivent les titres de séjour suisses suivants en vertu de 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, RS 142.201) :

1. permis C pour les étrangers établis en Suisse ;
2. permis B pour les étrangers qui séjournent en Suisse ;

3. permis L pour les étrangers qui exercent une activité lucrative de courte durée ou qui séjournent en Suisse temporairement.

Ces titres de séjour peuvent être établis sous forme biométrique ou non biométrique selon le pays de provenance, aujourd'hui sous forme papier, à partir de 2019 sous forme de carte en polycarbonate. Les exigences de l'accord d'association à Schengen sont prises en compte pour les ressortissants de pays tiers. Les titulaires de ces permis sont autorisés à séjourner en Suisse conformément à l'art. 41, al. 1, LEtr.

En outre, les titres de séjour suivants sont établis en vertu de l'art. 71*a*, al. 1, OASA, avec ou sans limitation du séjour :

1. permis G pour les frontaliers ;
2. permis N pour les demandeurs d'asile ;
3. permis F pour les étrangers admis à titre provisoire (art. 83 et 85 LEtr) et pour les réfugiés admis à titre provisoire (art. 59 LAsi) ;
4. permis S pour les personnes à protéger ;
5. permis Ci pour les partenaires exerçant une activité lucrative ou les enfants des personnes membres de représentations étrangères ou d'organisations intergouvernementales.
6. De plus, la personne bénéficiaire de privilèges, d'immunités et de facilités reçoit une carte de légitimation délivrée par le DFAE en vertu de l'art. 71*a*, al. 2, OASA. Cette carte n'est pas biométrique.

Les personnes titulaires de ces titres de séjour ne sont pas systématiquement habilitées à obtenir un e-ID. Le Conseil fédéral détermine les types de titres de séjour dont les étrangers doivent disposer pour pouvoir obtenir un e-ID (al. 2).

Afin que le plus grand nombre d'étrangers possible puisse avoir accès aux applications de la cyberadministration avec un e-ID, il est prévu que tous les étrangers titulaires d'un titre de séjour qui autorise le séjour (art. 41, al. 1, LEtr, en relation avec l'art. 71, al. 1, OASA ; permis L, B et C) et tous les frontaliers (art. 71*a* OASA, permis G) puissent obtenir un e-ID. En règle générale, les cantons sont responsables des contacts avec les étrangers ; des applications de la cyberadministration seront vraisemblablement mises en place dans ce domaine. Le Conseil fédéral peut prévoir d'autres procédures pour l'identification électronique.

On renonce à garantir l'accès aux fonctions de l'e-ID aux autres étrangers, en particulier les étrangers 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.

Al. 3
Le domaine des e-ID est sujet à une évolution technique rapide. Pour définir les processus d'identification, il est toutefois possible d'imiter les méthodes d'identification fiables utilisées dans le domaine bancaire : l'Autorité fédérale de surveillance des marchés financiers (FINMA) détermine avec précision quelles méthodes d'identification des nouveaux clients sont

autorisées. Afin de permettre l'adaptation du cadre légal aux nouvelles technologies, le Conseil fédéral règlera par voie d'ordonnance les conditions d'obtention, la procédure d'établissement, le blocage et la révocation d'un e-ID.

Toutes les dispositions relatives à la délégation des compétences législatives sont commentées au chiffre 4.4.

Art. 4 Reconnaissance des FI

Remarque préliminaire

La reconnaissance des fournisseurs d'identité comprend le contrôle et la reconnaissance de leurs systèmes e-ID. En revanche, les conditions techniques que les services utilisateurs doivent respecter ne sont 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)[11].

Al. 1 et 2

Un FI souhaitant établir des e-ID reconnus doit respecter diverses exigences techniques et organisationnelles. L'organisme de reconnaissance des fournisseurs d'identité (organisme de reconnaissance) contrôle régulièrement que c'est le cas. Les conditions à respecter garantissent que les FI et les données qu'ils ont enregistrées peuvent être soumis à un contrôle suffisant.

Let. a et b

Le siège des FI doit se trouver en Suisse. Tout service privé ou public est habilité à gérer un système e-ID, pour autant qu'il dispose d'un numéro IDE, condition de la reconnaissance. Il est ainsi indirectement établi que les personnes physiques ou morales qui ne sont pas inscrites au registre du commerce ne peuvent pas bénéficier de la reconnaissance, ni gérer des systèmes e-ID reconnus.

Let. c et d

Les personnes qui contrôlent les documents d'identité présentés lors de la procédure d'établissement et qui pourraient avoir une influence sur la transmission des données lors de la gestion du système sont soumises à une exigence organisationnelle. Elles doivent 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 (cf. les explications relatives à l'art. 12, al. 2, let. d) 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 permettent de vérifier ces points-là.

Let. e

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

[11] cf. lien dans la liste des sources

Let. f
Le FI doit 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 FI traite dans le cadre des prestations prévues par la loi e-ID, y compris les données temporaires, celles provenant d'enregistrements intermédiaires et les données secondaires.

Let. g
Le FI a l'obligation de s'assurer contre les risques en matière de responsabilité civile. La responsabilité est régie par le code des obligations (cf. section 9, art. 24 AP).

Al. 3
Les évolutions techniques de ces prochaines années dans le domaine de l'identification et de l'authentification électroniques ne peuvent guère être prévues. La reconnaissance doit être renouvelée à intervalles réguliers. Le FI rédige un rapport de sécurité annuel qui inclut tous les systèmes e-ID reconnus qu'il gère et le transmet à l'organisme de reconnaissance. Le Conseil fédéral définit la forme et le contenu du rapport de sécurité.

Al. 4
La réglementation de la procédure et des détails techniques est déléguée aux autorités chargées d'édicter les ordonnances.

Sont en particulier réglés par voie d'ordonnance ou de directive les normes et les protocoles techniques applicables aux systèmes e-ID. L'organisme de reconnaissance contrôle régulièrement l'application de ces normes et protocoles. Cette procédure établit la reconnaissance des systèmes e-ID.

Art. 5 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, l'avant-projet prévoit que les FI puissent s'adapter aux besoins du marché et 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 (cf. art. 15 AP).

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.

Les e-ID offrent un degré de fiabilité différent selon le niveau de garantie du système. Les niveaux de garantie *faible* et *substantiel* réduisent le risque d'utilisation abusive ; le niveau de garantie *élevé* vise à empêcher l'utilisation abusive ou l'altération de l'identité.

Al. 2
Les niveaux de garantie sont définis plus en détail par voie d'ordonnance. Ils dépendent de la procédure d'établissement, de la gestion du système, de l'utilisation des e-ID et d'autres mesures de sécurité techniques et organisationnelles. 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'un e-ID sont également précisées.

Al. 3
Un e-ID d'un niveau de garantie supérieur peut également être utilisé pour un service utilisateur qui requiert un niveau de garantie moins élevé. Les titulaires d'un 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.

Art. 6 Procédure d'établissement
Remarque préliminaire
Le requérant, le FI et le service d'identité participent à 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 l'avant-projet, en particulier aux art. 3, al. 3, et 5, al. 4.

Al. 1
Le FI ne peut pas décider de lui-même d'établir un e-ID, même si la personne concernée est l'un de ses clients. Une personne qui souhaite obtenir un e-ID doit en faire la demande ; le FI n'a pas l'obligation de satisfaire à cette demande.

Al. 2 et 3
Le FI contrôle que le requérant remplit les conditions personnelles définies à l'art. 3 et demande au service d'identité de lui transmettre les données d'identification personnelle par voie électronique. Si le FI ne souhaite établir des e-ID que pour certaines personnes (clients), il vérifie également qu'il existe une relation de clientèle avec le requérant. Celui-ci doit expressément consentir à ce que ses données d'identification personnelle soient transmises. Le service d'identité doit s'assurer par des mesures techniques et organisationnelles que les données d'identification personnelle ne puissent pas être obtenues de manière abusive. Les FI ne devraient par exemple pas pouvoir obtenir les données d'identification personnelle en donnant uniquement le numéro du document d'identité ou sans le consentement exprès du titulaire. Le consentement doit être donné lors d'un contact direct entre le service d'identité et le requérant.

Al. 4
Le FI attribue les données d'identification personnelle à l'e-ID et garantit que celui-ci est attribué à la personne physique correspondante (rattachement). Pour Mobile-ID par exemple, l'e-ID est attribué 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 FI 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
La demande de transmission des données d'identification personnelle est déposée par voie électronique auprès du service d'information du service d'identité. Le système d'information du service d'identité consigne la demande.

Art. 7 Données d'identification personnelle

Al. 1 et 2
La transmission 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'authentification et le système e-ID.

Certaines données d'identification personnelle mentionnées sont des données biométriques (photographie, image de la signature). Seules les données gérées par les systèmes d'information de la Confédération (cf. art. 20 AP) peuvent être attestées ; leur liste est donc fixe. Le titulaire de l'e-ID peut déterminer quelles données d'identification personnelle sont transmises par le FI à l'exploitant d'un service utilisateur pour une utilisation précise de l'e-ID (cf. art. 17, al. 1, let. f, AP). La dénomination des données d'identification personnelle se base autant que possible sur la terminologie de la loi sur l'harmonisation des registres.

Al. 3
Afin d'aider les FI à gérer les e-ID, le service d'identité peut ajouter des informations complémentaires aux données d'identification personnelle, comme le nom du système d'information qui les a fournies et la date de leur dernière mise à jour par ce système d'information.

Al. 4
Le FI peut attribuer d'autres données à un e-ID (plus précisément au numéro d'enregistrement de l'e-ID), par exemple une adresse, un numéro de téléphone ou un numéro de client. Il serait également envisageable qu'une banque ayant fonction de FI associe une carte de crédit ou une carte bancaire à un e-ID.

Art. 8 Mise à jour des données d'identification personnelle

Al. 1
Certains attributs d'identité peuvent être modifiés. L'exécution de la modification du code civil relative au droit du nom (CC, RS 210, en particulier art. 29 ss et art. 160) a montré que les cas de changement de nom sont de plus en plus nombreux ; les changements d'état civil et de sexe sont également plus fréquents qu'au siècle précédent. On 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 FI sont responsables de la demande de mise à jour et payent un émolument pour celle-ci.

Al. 2
Le service d'identité permet aux FI de contrôler systématiquement la validité des numéros d'enregistrement des e-ID par une procédure usuelle (cf. art. 20, al. 4, AP). À l'heure actuelle, la procédure usuelle consiste à tenir une liste électronique. Les FI doivent se renseigner de manière périodique sur le statut des numéros d'enregistrement des e-ID qu'ils ont

établis. Ils sont tenus de bloquer ou de révoquer immédiatement les e-ID rattachés à un numéro d'enregistrement non valable. Cette demande accroît la fiabilité des e-ID reconnus et n'est donc pas soumise à un émolument. Les FI sont également tenus d'aménager la possibilité pour le titulaire de contrôler gratuitement la validité des e-ID qu'ils ont établis (art. 17, al. 1, let. c, AP).

Suivant le résultat de la demande, l'e-ID doit être bloqué ou révoqué. Il est nécessaire de distinguer le blocage ou la révocation d'un e-ID du blocage ou de la révocation du numéro d'enregistrement de l'e-ID. S'il est par exemple notifié que le support et donc l'e-ID qui y est rattaché ont été perdus et que des tiers pourraient y avoir accès, cette e-ID spécifique est temporairement invalide ; le numéro d'enregistrement n'est pas concerné puisqu'il est rattaché à l'identité officielle d'une personne et donc valide indépendamment du statut de l'e-ID. L'e-ID peut être réactivé et utilisé lorsque la cause du blocage disparaît. Par contre, la révocation de tous les e-ID rattachés à un numéro d'enregistrement est effectuée lorsque ce numéro d'enregistrement ne peut plus être utilisé de façon durable, par exemple en cas de décès du titulaire. Contrairement à un numéro d'enregistrement bloqué, un numéro d'enregistrement révoqué ne peut pas être réactivé.

La mise à jour des données d'identification personnelle est soumise à un émolument qui fera l'objet d'une ordonnance du Conseil fédéral. Cet émolument couvrira tous les frais et son montant sera fixé à quelques dizaines de centimes par mise à jour pour un e-ID.

Art. 9 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. 9 de l'AP établit la base légale et les principes de traitement associés à l'utilisation systématique du numéro AVS pour les e-ID.

Al. 1

Le service d'identité utilise le numéro AVS pour identifier une personne lors de l'établissement de l'e-ID et de la mise à jour des données (art. 8 AP). Il sert d'identifiant univoque lors de l'interrogation d'autres banques de données qui l'utilisent également de façon systématique. Le numéro AVS est indispensable pour comparer ou transmettre 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. Suite aux révisions du droit du nom de ces dernières années, il est plus facile de changer d'identité ; 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

Les FI sont habilités à enregistrer le numéro AVS dans leurs systèmes. Le numéro AVS n'est transmis qu'aux exploitants d'un service utilisateur qui sont habilités à l'utiliser et aux services qui sont habilités à l'utiliser de façon systématique d'après la LAVS. La possibilité de transmettre cet attribut d'identité à des tiers non habilités à l'utiliser systématiquement doit être techniquement exclue. Il doit être caviardé dans le rapport relatif à la transmission des données. Le numéro d'identification univoque pour les FI est alors le numéro d'enregistrement de l'e-ID.

Art. 10 Traitement et transmission des données

Remarque préliminaire

Le traitement et la transmission des données sont l'activité proprement dite des FI. L'identification et l'authentification sont des services proposés aux exploitants d'un service utilisateur et aux titulaires d'un e-ID. Les FI ayant un rôle d'intermédiaire, il est d'autant plus important de réglementer la protection des données.

Al. 1 et 2

Les dispositions des al. 1 et 2 ne vont pas au-delà du cadre légal fixé par la législation sur la protection des données. Le titulaire peut choisir quelles données d'identification personnelle sont transmises au service utilisateur lors de l'utilisation de l'e-ID. Seules les données d'identification personnelle qui correspondent au niveau de garantie exigé par le service utilisateur peuvent être transmises.

Al. 3

Les FI et les exploitants d'un service utilisateur ne sont pas en droit de transmettre ni vendre les données d'identification personnelle attestées par l'État et correspondant à un niveau de garantie *substantiel* ou *élevé*. Le modèle économique adopté par les FI ou les exploitants d'un service utilisateur ne peut pas se fonder sur la vente de données ou de profils d'utilisateurs attestés par l'État et donc particulièrement fiables. Ces données ne pourront pas non plus être transmises gratuitement, par exemple, à des fins commerciales, à une autre entreprise du groupe. Cette interdiction du commerce ne concerne pas les données supplémentaires attribuées à l'e-ID en vertu de l'art. 7, al. 4, AP.

Al. 4

La législation sur la protection des données comprend la loi fédérale du 19 juin 1992 sur la protection des données (LPD, RS 235.1) ainsi que les actes normatifs subordonnés. En particulier, les FI et les exploitants d'un service utilisateur sont soumis aux art. 16 à 25bis LPD ainsi qu'à la surveillance conformément à l'art. 27 LPD.

Art. 11 Expiration de la reconnaissance

Al. 1

Pour pouvoir gérer un système e-ID, un FI doit disposer de ressources suffisantes. Au moment de l'ouverture d'une faillite, cette capacité économique disparaît et la reconnaissance expire en vertu de la loi. Les systèmes e-ID sont insaisissables et ne rentrent pas dans la masse en faillite. Les données attestées par le biais d'un système e-ID ne sont pas négociables et n'ont donc pas de valeur commerciale.

Al. 2 et 3

Les systèmes e-ID sont interopérables (art. 18 AP) et forment les nœuds des réseaux qui relient les services utilisateurs entre eux. L'al. 3 vise 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 système e-ID dans son ensemble prend une valeur commerciale, même si les données prises individuellement ne sont pas négociables.

Art. 12 Mesures de surveillance et retrait de la reconnaissance

Al. 1 et 2

L'organisme de reconnaissance intervient lorsqu'il constate, au cours d'un contrôle ou par le biais d'une notification, qu'un FI enfreint les prescriptions de la loi e-ID ou qu'il ne remplit plus les conditions de la reconnaissance (art. 4 AP). 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'organisme de reconnaissance fixe un délai au terme duquel le manquement doit être corrigé. Si ce n'est pas le cas, il peut retirer la reconnaissance.

Al. 3

Let. a à c

Le retrait de la reconnaissance est une sanction administrative. Elle est prononcée si le FI enfreint les dispositions de la loi e-ID ou si les conditions de la reconnaissance ou les exigences formulées lors de la procédure de reconnaissance ne sont pas remplies dans les délais. La disposition potestative garantit que cette sanction, qui a des conséquences graves, ne soit prononcée que si le principe de proportionnalité est respecté.

Let. d

Les infractions en lien avec la criminalité sur Internet qui peuvent mener à une usurpation d'identité doivent faire l'objet d'une attention particulière. L'usurpation d'identité désigne l'usage abusif de données personnelles (de l'identité) d'une tierce personne. Elle vise souvent, soit à nuire à la réputation d'une personne, soit à se procurer un avantage patrimonial indu. Lorsque l'auteur cherche, par ce moyen, à se procurer ou à procurer à un tiers un enrichissement illégitime, il peut se rendre punissable d'escroquerie ou de tentative d'escroquerie (art. 146 du code pénal, CP, RS 311.0) et s'exposer ainsi à une peine privative de liberté pouvant aller jusqu'à cinq ans. Dans le cadre du « phishing » ou hameçonnage (usurpation d'identité à des fins d'enrichissement indu), l'usurpation d'identité peut tomber sous le coup de l'art. 143bis CP (accès indu à un système informatique), si l'auteur s'introduit sans droit dans le système informatique d'un tiers, ou du piratage, puni par l'art. 143 CP (soustraction de données), s'il accède à des données qui ne lui sont pas destinées. Selon l'intention de l'auteur et les circonstances du cas d'espèce, d'autres infractions peuvent entrer en ligne de compte, notamment la détérioration de données, l'atteinte astucieuse aux intérêts pécuniaires d'autrui, la menace ou la contrainte (art. 144bis, 151, 180 ou 181 CP). L'usurpation d'identité peut aussi être sanctionnée par les art. 173 ss CP, si elle sert de moyen pour commettre une infraction contre l'honneur ou une infraction contre le domaine secret ou le domaine privé. Enfin, dans les rares cas où elle ne se rattache pas à l'un de ces cas de figure, l'auteur peut encore, selon le canton, s'exposer à une amende pour troubles causés à une personne ou trouble de l'ordre public.

Art. 13 Système e-ID subsidiaire de la Confédération

L'avant-projet présuppose que des acteurs du secteur privé demanderont la reconnaissance. Si aucun FI du secteur privé ne souhaite 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, en particulier pour identifier et authentifier les personnes qui utilisent des applications de la cyberadministration ou qui entrent en contact avec l'administration. L'al. 2 établit également la possibilité de mettre en place et de gérer un système e-ID étatique, éventuellement en collaboration avec des partenaires privés.

1.8.4 Section 3 Titulaires d'un e-ID

Art. 14 Devoirs

Al. 1 et 2

De nos jours, les moyens électroniques ne sont plus une nouveauté. Les devoirs des titulaires d'un e-ID établis dans la loi e-ID ne vont pas au-delà des 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.

Al. 3

Dans le cadre de la responsabilité délictuelle (extracontractuelle), l'art. 14 de l'avant-projet établit 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 FI, comme tout soupçon d'utilisation abusive ou toute perte de l'e-ID.

1.8.5 Section 4 Exploitants d'un service utilisateur

Art. 15 Accord avec un FI

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

Art. 16 Autorités en tant qu'exploitants d'un service utilisateur

Les autorités en tant qu'exploitants d'un service utilisateur ne peuvent exiger une authentification électronique pour l'utilisation de leur application que si cette authentification est nécessaire dans le cas concret. Si elle est effectivement nécessaire, les autorités cantonales et communales qui exécutent le droit fédéral doivent accepter tous les e-ID reconnus du niveau de garantie correspondant. Le recours à des moyens d'identification électronique déjà utilisés aujourd'hui n'est pas exclu.

Cette disposition reflète l'importance des e-ID reconnus pour l'État, mise en évidence par la stratégie Suisse numérique et la stratégie de cyberadministration du Conseil fédéral (cf. ch. 3). Les autorités en tant qu'exploitants d'un service utilisateur soutiendront ainsi les investissements de la Confédération destinés à la mise en œuvre des e-ID et participeront à la diffusion des e-ID 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.

1.8.6 Section 5 Fournisseurs d'identité

Art. 17 Devoirs

Al. 1

Let. a

Le FI gère au moins un système e-ID. Il peut en proposer plusieurs, de niveaux de garantie différents, et les faire reconnaître par l'État, mais n'y est pas contraint. Les conditions tech-

niques 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'un e-ID, le FI est responsable de l'attribution correcte des données d'identification personnelle à cet e-ID ainsi que du rattachement et de la remise corrects de l'e-ID à une personne physique. Pour ce faire, il suit trois étapes qui peuvent varier selon le niveau de garantie.

1. Avec le numéro d'enregistrement de l'e-ID, le FI attribue de manière univoque les données d'identification personnelle transmises par le service d'identité (art. 7 AP) 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 exemple à la puce d'une carte ou à la carte SIM d'un téléphone portable).
2. Il garantit que l'e-ID est bien attribué 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 remis à cette personne, par exemple lorsqu'elle se présente en personne, au cours d'un contact virtuel sûr pendant lequel le moyen d'authentification est rattaché à la bonne personne, ou par l'envoi d'une lettre recommandée.

Let. c
Le domaine de la transmission 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 révision de la SCSE. Actuellement, la procédure usuelle consiste à tenir une liste électronique. Le service d'identité pourrait par exemple tenir et publier une liste des numéros d'enregistrement d'e-ID qui ne peuvent prétendre, temporairement ou durablement, à l'obtention ou à l'utilisation d'un 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 FI consulte régulièrement la liste des numéros d'enregistrement des e-ID bloqués ou révoqués et détermine si les numéros d'enregistrement des e-ID qu'il a établis sont concernés en suivant la procédure usuelle qu'il a fixée.

Let. d
Le FI est 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 améliore la sécurité. La périodicité de cette mise à jour dépend du niveau de garantie ; elle est fixée à l'art. 8, al. 1.

Let. f
Lorsqu'un e-ID est utilisé et que des données d'identification personnelle doivent être transmises (au moment de l'enregistrement auprès d'un service utilisateur par exemple), le FI doit obtenir le consentement du titulaire.

Un exemple : la titulaire d'un e-ID souhaiterait jouer au casino en ligne. Elle doit prouver qu'elle a dépassé dix-huit ans. Ce casino a conclu un accord avec un FI. La titulaire dispose d'un e-ID installé sur son smartphone ; elle en informe le casino. Le casino prend contact avec le FI par Internet. Celui-ci envoie un message à la titulaire et lui demande si elle accepte de transmettre son nom, son prénom et sa date de naissance à ce casino. Elle donne

son consentement et le FI transmet les données en question au casino. Le casino dispose d'une preuve attestée par l'État de l'âge de la titulaire et peut donc l'autoriser à jouer en ligne si aucune autre raison ne l'exclut. Lors de ses prochaines visites sur le site Internet, la titulaire devra simplement se connecter avec son e-ID.

Let. g
Les données que le FI a enregistrées relatives à l'utilisation d'un e-ID doivent être effacées après six mois. Les données d'enregistrement, les données de transaction et les autres données que le service utilisateur a consignées sont réservées.

Al. 2, 3, et 4
Le FI s'assure 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.

Les exploitants d'un service utilisateur ou le FI peuvent constater avant le titulaire que l'e-ID est utilisé de façon abusive, s'il est utilisé dans un lieu inhabituel par exemple. Il est également possible qu'un tiers tente de bloquer un e-ID de façon abusive. Avant de bloquer un e-ID, le FI doit s'assurer que la personne qui demande le blocage est habilitée à le faire.

Art. 18 Interopérabilité
L'interopérabilité des systèmes e-ID est une condition importante pour la diffusion des e-ID. Les FI doivent reconnaître mutuellement leurs systèmes e-ID grâce à des normes techniques et des interfaces définies par voie d'ordonnance ou de directive.

Les titulaires peuvent utiliser leur e-ID auprès de tous les services utilisateurs, pour autant qu'il soit adapté au moins au niveau de garantie exigé, et ceci indépendamment de si l'exploitant de ce service utilisateur a conclu un accord avec le FI qui a établi l'e-ID. Pour atteindre cet objectif, les FI 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, soit par l'élaboration de normes et de règles d'interopérabilité que tous les FI doivent respecter, soit par la mise en place d'une plateforme à laquelle tous les FI doivent être liés. Cette deuxième possibilité nécessiterait de mettre sur pied une organisation qui pourrait éventuellement être instaurée par la Confédération et les cantons dans le cadre de la Fédération suisse d'identités. La solution la plus adaptée et la plus avantageuse sur le plan économique sera adoptée en temps voulu, après consultation des acteurs de l'économie et de l'administration.

1.8.7 Section 6 Service d'identité électronique suisse

Art. 19 Organisation
Le Service d'identité électronique suisse (service d'identité) est rattaché au DFJP. Le Conseil fédéral règle son organisation.
Voir les explications au chiffre 1.4.1.

Art. 20 Tâches et devoirs
Al. 1
Le service d'identité attribue les données d'identification personnelle au numéro d'enregistrement de l'e-ID et transmet ce numéro aux FI. Le nombre de données transmises varie selon le niveau de garantie (cf. art. 7 AP).

Al. 2 et 3
Le service d'identité gère un système d'information qui dispose d'un accès aux registres de personnes administrés au niveau fédéral et procède à une comparaison entre les données contenues dans son système et les données contenues dans ces registres. Au moment de l'élaboration de la loi, il s'agit :

a. du système d'information relatif aux documents d'identité (ISA) selon l'art. 11 de la loi du 22 juin 2001 sur les documents d'identité (LDI, RS 143.1) et l'art. 10 de l'ordonnance du 20 septembre 2002 sur les documents d'identité (OLDI, RS 143.11) ;
b. du système d'information central sur la migration (SYMIC) selon les art. 101 ss de la loi fédérale du 16 décembre 2005 sur les étrangers (LEtr, RS 142.20) et l'ordonnance SYMIC du 12 avril 2006 (RS 142.513) ;
c. du registre informatisé de l'état civil (Infostar) selon l'art. 39 du code civil (CC, RS 210) et l'art. 6*a* de l'ordonnance du 28 avril 2004 sur l'état civil (OEC, RS 211.112.2) ;
d. du registre central de la centrale de compensation de l'AVS (CdC-UPI) selon l'art. 71 LAVS (RS 831.10).

Al. 4
Voir les explications relatives à l'art. 8, al. 2.

Al. 5
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.

1.8.8 Section 7 Organisme de reconnaissance des FI

Art. 21 Compétence

L'organisme de reconnaissance des fournisseurs d'identité (organisme de reconnaissance) sera rattaché au DFF. La procédure de reconnaissance des FI s'inspire de la procédure de reconnaissance prévue pour les plateformes de messagerie (cf. ch. 1.3.2). Une unité administrative est responsable de la procédure de reconnaissance ; or, selon le règlement eIDAS, cette fonction doit être prise en charge par l'organe de contrôle national. Comme le DFF-UPIC assume déjà d'autres fonctions que le règlement eIDAS attribue aux organes de contrôles nationaux, on propose qu'il se charge également de diriger l'organisme de reconnaissance. À cet égard, voir également le chiffre 1.4.1.

Art. 22 Liste des FI

L'organisme de reconnaissance publie et met à jour une liste de tous les FI et de tous les systèmes e-ID reconnus avec le niveau de garantie correspondant. Cette disposition reprend la réglementation concernant la liste des plateformes reconnues.

1.8.9 Section 8 Émoluments

Art. 23

Plusieurs possibilités sont envisageables pour fixer le montant des émoluments perçus par le service d'identité et par l'organisme de reconnaissance. 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 FI qui établissent les e-ID gratuitement pour les citoyens 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.

On part du principe que les moyens d'identification électronique reconnus seront disponibles sur un support qui a lui-même une fonction, que ce soit une carte bancaire, un smartphone, ou le support d'un moyen de signature (SuisseID par exemple). Il est également envisageable de rattacher l'e-ID à la carte d'accès de tous les collaborateurs d'une entreprise, dans une clinique par exemple. L'entreprise pourrait ainsi déléguer l'identification de ses collaborateurs à un FI reconnu et utiliser les systèmes e-ID de celui-ci pour l'authentification à son système informatique. C'est aux acteurs du marché qu'il revient de décider si les coûts d'utilisation générés ultérieurement seront facturés et, le cas échéant, comment ils le seront. Le concept propose un modèle de « paiement à l'usage » sans pour autant exclure la mise en œuvre d'autres modèles.

1.8.10 Section 9 Responsabilité

Art. 24

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 (CO, RS 220) ou de la loi du 14 mars 1958 sur la responsabilité (LRCF, RS 170.32).

Les dispositions relatives à la responsabilité de la loi e-ID ont une valeur déclaratoire et visent à clarifier quelles règles de responsabilité sont applicables, par exemple en ce 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'un e-ID. L'e-ID seul ne permet pas de conclure des actes juridiques ; la loi e-ID 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 FI analogue à celle définie à l'art. 17 de la nouvelle 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 reconnus à l'UE, les modifications nécessaires de la loi e-ID 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 FI, 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
Le service d'identité et l'organisme de reconnaissance sont des unités administratives de la Confédération et sont soumises à ce titre à la LRCF.

1.8.11 Section 10 Dispositions finales

Art. 25 Modification d'autres actes
On propose de modifier d'autres actes en annexe de l'avant-projet. Ces modifications visent principalement à permettre au service d'identité d'accéder aux systèmes d'information ISA, Infostar, et SYMIC. Le système d'information de la CdC-UPI ne doit pas obligatoirement être accessible en ligne.

Art. 26 Référendum et entrée en vigueur
Comme toute loi fédérale, la loi e-ID est sujette au référendum et le Conseil fédéral est chargé de fixer sa date d'entrée en vigueur.

1.8.12 Annexe Modification d'autres actes
Remarque préliminaire
Identification et authentification auprès des services utilisateurs de la Confédération
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.

Par exemple, les droits d'accès des services du secteur agricole au système d'information pour le service vétérinaire public sont définis dans l'ordonnance du 6 juin 2014 concernant les systèmes d'information du service vétérinaire public (OSIVét, RS 916.408). Pour le système d'information Agate, les informations concernant les droits d'accès sont détaillées en annexe de l'ordonnance du 23 octobre 2013 sur les systèmes d'information dans le domaine de l'agriculture (OSIAgr, RS 919.117.71). La connexion au portail Internet lui-même se fait avec une SuisseID ou un certificat AdminPKI ; elle est exigée pour certaines applications.

StartBiz, une prestation en ligne que le SECO met à la disposition des PME, peut être utilisée avec une SuisseID après l'enregistrement. Il est également possible d'avoir recours à une SuisseID pour commander en ligne un extrait du casier judiciaire auprès de l'OFJ.

E-ID en tant que document d'identification
Un e-ID au sens de la loi e-ID sert de pièce justificative pour identifier une personne. Les institutions financières et les maisons de jeux qui sont soumises à la loi du 10 octobre 1997 sur le blanchiment d'argent (RS 955.0) et qui doivent procéder à une identification électronique sûre peuvent utiliser l'e-ID comme pièce justificative au sens de l'art. 3 de la loi sur le blanchiment d'argent. L'ordonnance de la FINMA sur le blanchiment d'argent, qui définit plus précisément le concept de pièce justificative, peut éventuellement être adaptée pour permettre que les e-ID soient utilisés par les institutions financières et les maisons de jeu au cours des transactions électroniques.

1. Loi du 22 juin 2001 sur les documents d'identité (LDI ; RS 143.1)

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, lettre k
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 divers registres fédéraux et nécessaires à l'utilisation d'un e-ID soient attribuées à une personne de façon univoque. Si le numéro AVS (let. k) peut être utilisé comme un identifiant personnel univoque au sein de l'administration fédérale, l'ajout du numéro d'enregistrement de l'e-ID ne sera pas nécessaire.

Art. 12, al. 2, lettres g et h
Le service d'identité doit pouvoir consulter ISA afin d'obtenir les données nécessaires à l'établissement d'un 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 reconnus, les données d'ISA seront également disponibles dans les systèmes d'information des FI reconnus et du service d'identité. Ceux-ci doivent être exemptés de l'interdiction de tenir des fichiers parallèles.

2. Code civil (CC, RS 210)

Art. 43*a*, al. 4, ch. 5
L'art. 43*a* du CC règle l'accès en ligne aux registres informatisés visant à gérer l'état civil. Le service d'identité est ajouté à la liste des services qui ont accès à Infostar.

3. Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS, RS 831.10)

Art. 50*a*, 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 de la loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA, RS 830.1). Le service d'identité est mentionné dans la liste de ces services. Le service d'identité et les FI peuvent utiliser systématiquement le numéro AVS aux conditions fixées à l'art. 9 AP.

4. Loi fédérale du 18 mars 2016 sur la signature électronique (SCSE, RS 943.03)

Art. 9, al. 1bis
Toute personne qui demande la délivrance d'une signature électronique doit se présenter en personne. Cette obligation disparaît si elle peut prouver son identité avec un e-ID.

2 Conséquences

2.1 Conséquences pour la Confédération

2.1.1 Identification sûre sur Internet

On prévoit que les autorités fédérales pourront faire bon usage de l'e-ID, en particulier lorsqu'elles 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 utilisé 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 au chiffre 1.4.2. Les dépenses supplémentaires se limiteront aux frais liés à l'adaptation des solutions informatiques et à l'acquisition des prestations auprès des FI. La simplification des processus permettra sans doute de réaliser des économies à cet égard.

Au vu du succès mitigé des diverses solutions adoptées à l'étranger, il est possible que la solution proposée ne s'impose pas sur le marché malgré toutes les analyses effectuées et les retours positifs reçus. Plusieurs raisons peuvent être à l'origine de cette situation. Le concept proposé tient compte des expériences faites à l'étranger et tente d'en tirer les bonnes conclusions. En définitive, c'est cependant les utilisateurs et le marché qui décideront du succès de la solution choisie.

2.1.2 Remarque concernant les marchés publics

Autorités en tant qu'exploitants d'un service utilisateur

Les autorités qui proposent un service utilisateur sont des exploitants d'un service utilisateur au sens de la loi e-ID et doivent conclure un accord avec au moins un FI pour utiliser un système e-ID.

Une application de la cyberadministration qui sert à remplir une tâche d'intérêt public doit faire appel à un service d'identification. Une autorité est un service soumis au droit des marchés publics ; les services d'identification sont des prestations informatiques également soumises au droit des marchés publics. La loi e-ID crée un marché pour ces prestations qui sont fournies contre une rétribution issue des recettes fiscales.

Pour déterminer quelles prestations proposées par les FI acquérir, il faut donc effectuer une procédure d'adjudication conformément aux règles applicables aux marchés publics (loi fédérale du 16 décembre 1994 sur les marchés publics, LMP, RS 172.056.1, 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. 13 AP).

Fournisseurs d'identité
La reconnaissance des FI n'est en revanche soumise à aucune procédure d'adjudication puisqu'il s'agit d'une mesure destinée à protéger le consommateur. Cette disposition de la loi e-ID se base sur l'art. 95, al. 1, de la Constitution (cf. ch. 4.1).
L'octroi de la reconnaissance ne relève pas d'une politique économique : le nombre de reconnaissances octroyées n'est pas limité et les FI reconnus ne jouissent pas de droits exclusifs. Les FI non reconnus peuvent établir des moyens d'identification électronique ; ceux-ci ne sont cependant pas des e-ID au sens de la loi e-ID. La reconnaissance est octroyée et renouvelée si les conditions de la reconnaissance (art. 4 AP) sont remplies et que les exigences techniques et organisationnelles sont respectées.

2.2 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 d'impôt 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'un 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.

2.3 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.

2.4 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 (*phishing*), 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 n'a 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.

2.5 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.

2.6 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.

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

L'avant-projet relatif à une 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[12] et dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[13].

Il 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[14] 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 le cinquième objectif opérationnel fixé par la stratégie suisse de cyberadministration[15] 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.

4 Aspects juridiques

4.1 Constitutionnalité

La compétence de régler les e-ID découle indirectement de la Constitution (Cst., RS 101). 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.

Dans la mesure où certaines dispositions du projet concernent les rapports contractuels entre les fournisseurs d'identité et les utilisateurs, le législateur règle des aspects de droit civil. Il se fonde à cet égard sur l'art. 122, al. 1, Cst., qui dispose que la législation en matière de droit civil relève de la compétence de la Confédération.

---

[12] FF **2016** 981, 1048 et 1100

[13] FF **2016** 4999, 5001

[14] Stratégie Suisse numérique : cf. le lien dans la liste des sources

[15] Stratégie suisse de cyberadministration : cf. le lien dans la liste des sources

4.2 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 reconnus en Suisse pourront obtenir la reconnaissance européenne. À cet effet, la conclusion d'un accord bilatéral avec l'UE ou avec chaque État membre sera nécessaire.

4.3 Forme de l'acte à adopter

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

4.4 Délégation de compétences législatives

Obtention d'un e-ID pour les étrangers
Le Conseil fédéral peut édicter une ordonnance pour que les étrangers qui ne peuvent pas être identifiés de façon fiable sur la base d'un document d'identité étranger et qui ne reçoivent pas d'autorisation de séjour ne soient pas habilités à obtenir un e-ID. S'il est nécessaire que l'étranger ait accès à des services utilisateurs, dans le domaine de l'asile en particulier, le Conseil fédéral peut prévoir d'autres procédures d'identification et d'authentification, par exemple l'envoi d'un code d'accès par courrier. La compétence pour ce faire lui est donnée à l'art. 3, al. 2, AP.

Prescriptions techniques et organisationnelles
Afin de s'adapter le plus rapidement possible aux avancées technologiques, les conditions relatives aux processus, aux exigences techniques et aux normes seront fixées par voie d'ordonnance ou de directive.

L'art. 3, al. 3, AP, octroie au Conseil fédéral la compétence de régler l'obtention, la procédure d'établissement, le blocage et la révocation d'un e-ID.

En vertu de l'art. 4, al. 4, AP, le Conseil fédéral fixe les conditions de la reconnaissance, en particulier celles ayant trait aux conditions techniques et aux conditions de sécurité que les FI doivent remplir, à la couverture d'assurance nécessaire et aux normes et protocoles techniques applicables aux systèmes e-ID. 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.

Les exigences minimales auxquelles les procédures d'identification et d'authentification doivent satisfaire pour un certain niveau de garantie peuvent être édictées par voie d'ordonnance, en vertu de l'art. 5, al. 4, AP. Définir ces exigences demande également une certaine flexibilité puisqu'elles doivent rester en adéquation avec les possibilités techniques du moment.

Les normes techniques qui visent à garantir l'interopérabilité des systèmes e-ID doivent également être rapidement adaptées aux évolutions techniques et sont donc fixées par voie d'ordonnance (art. 18, al. 2, AP).

Le destinataire de l'ordonnance qui fixera les normes et protocoles techniques applicables à la transmission des données d'identification est le service d'identité. Le Conseil fédéral règlera la marche à suivre au cas où plusieurs registres de personnes livrent des données différentes (art. 20, al. 5, AP).

Système e-ID subsidiaire de la Confédération
Si aucun FI n'établit d'e-ID adapté pour l'identification et l'authentification aux services utilisateurs gérés par les autorités, le Conseil fédéral peut désigner une unité administrative qui gère un tel système e-ID. Cette unité administrative peut éventuellement mettre en place et gérer le système e-ID en collaboration avec des acteurs privés (art. 13 AP).

Règles de protection des titulaires relevant du droit de la responsabilité civile
Le Conseil fédéral peut définir les devoirs de diligence du titulaire de l'e-ID par voie d'ordonnance en vertu de l'art. 14, al. 3, AP. Ces devoirs de diligence peuvent changer 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. 33.

4.5 Conformité à la législation sur la protection des données

4.5.1 Droit de la protection des données suffisant

Les dispositions du droit de la protection des données (loi fédérale du 19 juin 1992 sur la protection des données, RS 235.1, et les ordonnances associées) suffisent à garantir la protection des données dans le domaine des e-ID. Toutefois, une disposition explicite relative à l'obligation d'obtenir le consentement du titulaire de l'e-ID a été ajoutée au projet. Le traitement des données d'identification personnelle attestées par l'État est limité et les FI ne peuvent y avoir recours que pour procéder aux identifications et aux authentifications (art. 10, al. 1, AP).

En outre, la transmission de certaines données d'identification personnelle et des profils d'utilisateur établis sur la base de ces données est limitée (art. 10, al. 3, AP).

4.5.2 Consentement pour la transmission

Il est crucial que les conditions de la protection des données soient respectées et que les mesures de sécurité nécessaires soient prises pour toute utilisation des données d'identification personnelle. Les titulaires de l'e-ID consentent explicitement à la transmission de certaines données d'identification personnelle. Lors de l'établissement d'un e-ID, ils autorisent les FI à demander les données au service d'identité (art. 6, al. 3, AP) ; lorsqu'ils utilisent leur e-ID auprès d'un exploitant d'un service utilisateur, le FI demande à nouveau leur consentement avant de transmettre les données à cet exploitant (art. 17, al. 1, let. f, AP).

4.5.3 Limitation du commerce des données

Le Conseil fédéral apporte une attention particulière au commerce des données. L'art. 10, al. 3, AP, interdit la communication à des tiers des données attestées par l'État et des profils d'utilisateur établis sur la base de ces données. Les données transmises pour un niveau de garantie faible et celles ajoutées pour un niveau de garantie substantiel et élevé ne sont cependant pas soumises aux mêmes restrictions. Les données de base tel que le numéro d'enregistrement de l'e-ID, le nom et la date de naissance, ainsi que les données attribuées par le FI lui-même (l'adresse ou le numéro de client par exemple) ne sont pas concernées par l'interdiction de vente. Par contre, les profils d'utilisateur établis sur la base d'autres données attestées, comme le sexe ou l'état civil, ne peuvent pas faire l'objet d'un commerce.

La limitation du commerce des données implique une diminution de la valeur économique des données d'identification personnelle attestées par l'État. Ces données sont déclarées insaisissables et ne tombent pas dans la masse en faillite (art. 11, al. 1, AP). Afin d'assurer la continuité d'un système e-ID reconnu et des e-ID qui y sont associés, un FI en difficulté financière peut vendre l'ensemble de son système e-ID à un autre FI. Le montant de la vente tombe dans la masse en faillite (art. 11, al. 3, AP).

5 Autres documents

- Moyens d'identification électronique (e-ID) reconnus par l'État, Concept 2016
- Liste des sources
- Tableau d'équivalence des termes

5.1 Liste des sources citées dans le rapport explicatif relatif à l'avant-projet de la loi e-ID

Page	Document	Liens (consultés le 17 décembre 2016)
3	Règlement eIDAS	Règlement (UE) n° 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 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910
5 9	Règlements et décisions d'exécution se rapportant au règlement eIDAS	Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, paragraphe 7, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 53 du 25.2.2015, p. 14 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015D0296
		Décision d'exécution (UE) 2015/1505 de la Commission du 8 septembre 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 235 du 9.9.2015, p. 26 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015D1505
		Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen

		et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 235 du 9.9.2015, p. 37 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015D1506
		Décision d'exécution (UE) 2015/1984 de la Commission du 3 novembre 2015 définissant les circonstances, les formats et les procédures pour les notifications visés à l'article 9, paragraphe 5, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 289 du 5.11.2015, p. 18 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015D1984
		Décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 109 du 26.4.2016, p. 40 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016D0650
		Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 235 du 9.9.2015, p. 1–6, rectifié dans JO L 28 du 4.2.2016, p. 18-18 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015R1501

		Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur JO L 235 du 9.9.2015, p. 7 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015R1502
		Règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés JO L 128 du 23.5.2015, p. 13 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32015R0806
		Règlement (UE) 2015/1017 du Parlement européen et du Conseil du 25 juin 2015 sur le Fonds européen pour les investissements stratégiques, la plateforme européenne de conseil en investissement et le portail européen de projets d'investissements et modifiant les règlements (UE) no 1291/2013 et (UE) no 1316/2013 — le Fonds européen pour les investissements stratégiques JO L 348 du 20.12.2013, p. 129, modifié par le règlement (UE) 2015/1017, JO L 169 du 1.7.2015, p. 1 http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32015R1017
15	Stratégie NSTIC des États-Unis	National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem https://www.nist.gov/itl/tig
21	Conditions de sécurité NIST	Cybersecurity-Framework https://www.nist.gov/cyberframework
39	Stratégies du Conseil fédéral	Stratégie Suisse numérique https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-

		numerique-et-internet/strategie-suisse-numerique/strategie.html
		Stratégie suisse de cyberadministration https://www.egovernment.ch/fr/umsetzung/e-government-strategie/

5.2 Tableau d'équivalence des termes

Concept e-ID	Loi e-ID	eIDAS en français	Terme anglais
Organisme de reconnaissance des fournisseurs d'identité (ORFI)	Organisme de reconnaissance des FI (organisme de reconnaissance)	-	Accreditation Authority
Requérant	-	Demandeur	Applicant
Authentification	Authentification	Authentification	Authentication
Identifiant personnel unique (IPU)	Numéro d'enregistrement de l'e-ID	Identifiant unique	Unique Personal Identification Number
Moyen d'identification électronique reconnu par l'État (e-ID)	Moyen d'identification électronique reconnu (e-ID)	Moyens d'identification électronique	Credential
Système d'identification électronique (système e-ID)	Système e-ID	Schéma d'identification électronique	Identity System
Identification électronique	Identification électronique	Identification électronique	Identification
Fournisseur de services d'identité reconnu par l'État (Identity Provider, IdP), éditeur, émetteur	Fournisseur d'identité (FI)	Emetteur	Identity Provider (IdP), Credential Service Provider (CSP)
Détenteur	Titulaire	Personne physique	Claimant/Subscriber
Interopérabilité	Interopérabilité	Interopérabilité	Interoperability
Services en ligne	Services en ligne	Services en ligne	Online Services
Données d'identification personnelle	Données d'identification personnelle	Données d'identification personnelle	IdentityAttribute
Enregistrement	Enregistrement	Enregistrement	Registration
Service d'identité électronique suisse (SIE)	Service d'identité électronique suisse (service d'identité)	Source faisant autorité	Steering Group and Attribute Authority, Root Attribute Authority
Partie utilisatrice (PU)	Exploitant d'un service utilisateur	Partie utilisatrice	Relying Party (RP)
Service de confiance	Service utilisateur	-	Relying Service
Niveau de sécurité	Niveau de garantie	Niveau de garantie	Level of Assurance / Assurance Level

-