Avant-projet

Loi fédérale sur les moyens d'identification électronique reconnus

Loi e-ID

du …

L'Assemblée fédérale de la Confédération suisse,
vu les art. 95, al. 1, et 122, al. 1, de la Constitution[1],
vu le message du Conseil fédéral du …[2],
arrête:

Section 1 Dispositions générales

Art. 1 Objet et but

[1] La présente loi règle:

a. le contenu, l'établissement, l'utilisation, le blocage et la révocation des moyens d'identification électronique reconnus (e-ID);

b. la reconnaissance et la surveillance des fournisseurs d'identité et de leurs systèmes e-ID;

c. les droits et les devoirs des titulaires d'un e-ID;

d. les droits et les devoirs des exploitants d'un service utilisateur.

[2] Elle vise:

a. à promouvoir la sécurité des transactions électroniques entre les particuliers et avec les autorités, et

b. à garantir la normalisation et l'interopérabilité des e-ID.

Art. 2 Définitions

Au sens de la présente loi, on entend par:

RS .....
[1] RS **101**
[2] FF …

a. *moyen d'identification électronique*: élément électronique utilisé pour l'identification et l'authentification d'une personne physique;

b. *moyen d'identification électronique reconnu (e-ID):* moyen d'identification électronique délivré par un fournisseur d'identité conformément aux prescriptions de la présente loi;

c. *fournisseur d'identité (FI):* fournisseur de services d'identification reconnu au sens de la présente loi.

d. *identification:* processus consistant à utiliser des données d'identification personnelle représentant une personne de manière univoque;

e. *authentification*: processus consistant à vérifier une identité alléguée;

f. *données d'identification personnelle:* ensemble de données géré par l'État et permettant d'établir l'identité d'une personne;

g. *numéro d'enregistrement de l'e-ID:* numéro d'identification univoque attribué à une personne;

h. *système e-ID*: système électronique utilisé pour l'établissement, la gestion et l'utilisation d'un e-ID;

i. *exploitant d'un service utilisateur*: personne physique ou morale qui gère dans le cadre de son activité des services en ligne nécessitant d'établir de façon fiable l'identité et l'authenticité de la personne qui les utilise;

j. *service utilisateur*: application informatique qui exploite un système e-ID.

Section 2 Etablissement d'un e-ID

Art. 3 Conditions personnelles

[1] Les FI peuvent établir un e-ID pour les personnes ci-après:

a. les ressortissants suisses titulaires, au moment de l'établissement, d'un document d'identité suisse valable au sens de la loi fédérale du 22 juin 2001 sur les documents d'identité des ressortissants suisses[3];

b. les étrangers titulaires d'un titre de séjour valable au sens de la loi fédérale du 16 décembre 2005 sur les étrangers[4] au moment de l'établissement de l'e-ID;

[2] Le Conseil fédéral peut déterminer quels types de titres de séjour n'ont pas droit à l'e-ID. Il peut prévoir d'autres procédures d'identification et d'authentification électronique pour les personnes concernées.

[3] Le Conseil fédéral règle les conditions d'obtention, le processus d'établissement, le blocage et la révocation d'un e-ID.

3 RS **143.1**
4 RS **142.20**

Art. 4 Reconnaissance des FI

[1] Tout FI qui souhaite établir des e-ID doit obtenir une reconnaissance de l'organisme de reconnaissance (art. 21).

[2] Sont reconnus les FI qui:

a. ont leur siège social en Suisse;

b. disposent d'un numéro IDE au sens de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE)[5];

c. prouvent que les personnes responsables des systèmes e-ID ne présentent pas un danger pour la sécurité;

d. emploient du personnel possédant les connaissances, l'expérience et les qualifications nécessaires;

e. garantissent que les systèmes e-ID qu'ils gèrent satisfont aux conditions de sécurité prévues pour chaque niveau de garantie;

f. conservent et traitent les données des systèmes e-ID en Suisse conformément au droit suisse;

g. prouvent qu'ils ont une assurance suffisante pour couvrir la responsabilité visée à l'art. 24 ou présentent des sûretés financières équivalentes;

h. assurent le respect du droit applicable, notamment de la présente loi et de ses dispositions d'exécution.

[3] La reconnaissance doit être renouvelée après trois ans au plus tard.

[4] Le Conseil fédéral édicte des dispositions détaillées concernant les conditions de la reconnaissance, notamment :

a. les conditions techniques et les conditions de sécurité requises ainsi que leur contrôle;

b. la couverture d'assurance nécessaire ou les sûretés financières équivalentes;

c. les normes et les protocoles techniques applicables aux systèmes e-ID ainsi que leur contrôle régulier.

Art. 5 Niveau de garantie

[1] Les FI peuvent gérer des systèmes e-ID présentant des niveaux de garantie divers et superposables et établir sur cette base des e-ID qui offrent un degré de fiabilité:

a. faible: réduction du risque d'utilisation abusive ou d'altération de l'identité;

b. substantiel: réduction substantielle du risque d'utilisation abusive ou d'altération de l'identité;

5 RS **431.03**

c. élevé: prévention de l'utilisation abusive ou de l'altération de l'identité.

[2] Le niveau de garantie est déterminé:

a. par le processus d'établissement, en particulier pour l'identification et l'authentification du titulaire lors de l'enregistrement;

b. par la gestion du système, en particulier la mise à jour des données d'identification personnelle;

c. par l'utilisation des e-ID, en particulier lors de l'identification et de l'authentification du titulaire, et

d. par d'autres mesures de sécurité techniques ou organisationnelles, selon les possibilités techniques du moment.

[3] Un e-ID d'un niveau de garantie donné peut être utilisé pour un niveau de garantie inférieur.

[4] Le Conseil fédéral règle les différents niveaux de garantie et en particulier les exigences minimales d'identification et d'authentification.

Art. 6 Procédure d'établissement

[1] Celui qui souhaite obtenir un e-ID demande à un FI de l'établir.

[2] Le FI vérifie que les conditions personnelles sont remplies.

[3] Si la personne concernée y consent, il demande au Service d'identité électronique suisse (service d'identité) de lui transmettre les données d'identification personnelle au sens de l'art. 7, al. 1 et 2.

[4] Il attribue les données d'identification personnelle à l'e-ID et l'e-ID à la personne physique.

[5] Le service d'identité consigne la transmission des données.

Art. 7 Données d'identification personnelle

[1] Le service d'identité attribue à un e-ID les données d'identification personnelle suivantes:

a. le numéro d'enregistrement de l'e-ID;

b. le nom d'état civil;

c. les prénoms;

d. la date de naissance.

[2] Pour un niveau de garantie substantiel ou élevé, il peut attribuer en sus à l'e-ID les données d'identification personnelle suivantes:

a. le numéro AVS au sens de l'art. 50*c* de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[6];

6 RS **831.10**

b. le sexe;

c. le lieu de naissance;

d. l'état civil;

e. la nationalité, éventuellement le statut de séjour;

f. une photographie;

g. le numéro et le type du document d'identité ou du titre de séjour délivré par la Suisse;

h. une image de la signature.

[3] Il peut ajouter aux données d'identification personnelle d'autres informations, en particulier la date de la dernière mise à jour des données dans les systèmes d'information cités à l'art. 20.

[4] Le FI peut attribuer d'autres données à un e-ID.

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

[1] Le FI met à jour les données d'identification personnelle qu'il gère par requête automatique auprès du service d'identité en indiquant le numéro d'enregistrement de l'e-ID, au minimum:

a. une fois par an pour les e-ID d'un niveau de garantie faible;

b. une fois par trimestre pour les e-ID d'un niveau de garantie substantiel;

c. une fois par semaine pour les e-ID d'un niveau de garantie élevé.

[2] Il est de sa responsabilité qu'un e-ID qu'il a établi soit bloqué ou révoqué immédiatement si le numéro d'enregistrement de cet e-ID ne doit plus être utilisé.

[3] Le service d'identité perçoit un émolument des FI pour la mise à jour des données d'identification personnelle.

Art. 9 Utilisation systématique du numéro AVS pour l'échange de données

[1] Le service d'identité peut utiliser systématiquement le numéro AVS afin d'identifier les personnes lorsqu'il échange des données par voie électronique avec les registres de personnes cités à l'art. 20, al. 2.

[2] Le FI ne peut pas utiliser le numéro AVS pour identifier les personnes; il peut cependant l'avoir dans son système e-ID et le communiquer aux exploitants d'un service utilisateur qui sont habilités à l'utiliser systématiquement.

Art. 10 Traitement et transmission des données

[1] Les FI ne peuvent traiter les données d'identification personnelle transmises par le service d'identité que pour procéder aux identifications et aux authentifications au sens de la présente loi.

[2] Ils ne peuvent transmettre les données d'identification personnelle qu'aux exploitants d'un service utilisateur qui offrent le niveau de garantie requis et à condition que le titulaire de l'e-ID y consente.

[3] Ni les FI reconnus, ni les exploitants d'un service utilisateur ne peuvent communiquer à des tiers les données d'identification personnelle au sens de l'art. 7, al. 2, ou les profils d'utilisateur établis sur la base de ces données.

[4] Au demeurant, la législation sur la protection des données est applicable.

Art. 11 Expiration de la reconnaissance

[1] La reconnaissance devient caduque à l'ouverture de la faillite contre le FI. Les systèmes e-ID sont insaisissables et ne tombent pas dans la masse en faillite.

[2] Le FI annonce à l'organisme de reconnaissance la cessation programmée de son activité et indique la procédure prévue en ce qui concerne les e-ID qu'il a établis.

[3] Les systèmes e-ID d'un FI qui cesse son activité ou contre lequel une faillite a été ouverte peuvent être repris par un autre FI reconnu. Le produit de la reprise tombe dans la masse en faillite.

Art. 12 Mesures de surveillance et retrait de la reconnaissance

[1] L'organisme de reconnaissance prend les mesures nécessaires s'il constate qu'un FI enfreint certaines prescriptions, notamment si les conditions de la reconnaissance ne sont plus remplies.

[2] S'il apparaît que le manquement sera corrigé, l'organisme de reconnaissance fixe un délai approprié pour sa correction.

[3] L'organisme de reconnaissance peut retirer la reconnaissance:

a. si le FI a violé les dispositions de la présente loi;

b. si les conditions de la reconnaissance au sens de l'art. 4, al. 1, ne sont plus remplies;

c. si le FI ne respecte pas les exigences fixées par l'organisme de reconnaissance, ou

d. si la personne responsable des systèmes e-ID a été condamnée par un jugement entré en force pour des infractions relevant de la cybercriminalité.

Art. 13 Système e-ID subsidiaire de la Confédération

[1] Si aucun FI n'établit des e-ID d'un niveau de garantie substantiel ou élevé, le Conseil fédéral peut désigner une unité administrative qui gère un système e-ID répondant aux besoins des autorités et qui délivre des e-ID.

[2] Il peut en outre prévoir que ce système puisse être mis en place et géré en collaboration avec des partenaires privés.

Section 3 Titulaires d'un e-ID

Art. 14 Devoirs

[1] L'e-ID est personnel et ne peut être laissé à la disposition de tiers.

[2] Le titulaire d'un e-ID prend les mesures nécessaires et raisonnables au vu des circonstances pour empêcher l'utilisation abusive de l'e-ID.

[3] Le Conseil fédéral détermine les devoirs de diligence à respecter en ce qui concerne l'e-ID.

Section 4 Exploitants d'un service utilisateur

Art. 15 Accord avec un FI

[1] Quiconque souhaite gérer un service utilisateur doit conclure un accord avec un FI. L'accord fixe en particulier:

a. les niveaux de garantie applicables;

b. les processus techniques et organisationnels à respecter.

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

Lorsqu'une autorité, en exécution du droit fédéral, prévoit une identification électronique pour son service utilisateur, elle doit accepter tous les e-ID au sens de la présente loi du niveau de garantie requis.

Section 5 Fournisseurs d'identité

Art. 17 Devoirs

[1] Le FI a les devoirs suivants:

a. il s'assure du fonctionnement correct et de la gestion sûre du système e-ID;

b. il attribue les données d'identification personnelle à l'e-ID et l'e-ID à la personne physique;

c. il organise le système e-ID de sorte que la validité de tous les e-ID qu'il a établis puisse être vérifiée en tout temps selon une procédure usuelle, de façon fiable et gratuite;

d. il respecte les conditions de sécurité mentionnées à l'art. 4, al. 1, let. e;

e. il effectue la mise à jour périodique des données d'identification personnelle auprès du service d'identité;

f. il requiert le consentement exprès du titulaire de l'e-ID pour la première transmission des données d'identification personnelle à des exploitants d'un système utilisateur;

g. il efface les données concernant l'utilisation d'un e-ID en particulier, après six mois.

[2] Il veille à mettre en place un service client qui permette de recevoir et de traiter les notifications de problèmes techniques ou de perte d'un e-ID. Il signale les erreurs dans les données d'identification personnelle au service d'identité.

[3] S'il y a lieu de craindre qu'un tiers ait accès à un e-ID ou que la perte ou un soupçon d'utilisation abusive d'un e-ID est notifié, le FI est tenu de bloquer immédiatement l'e-ID.

[4] Il s'assure que la personne qui a demandé le blocage a qualité pour le faire. Il informe immédiatement le titulaire de l'e-ID du blocage.

Art. 18 Interopérabilité

[1] Les FI reconnaissent mutuellement leurs systèmes e-ID et garantissent leur interopérabilité.

[2] Le Conseil fédéral définit les normes techniques et les interfaces.

Section 6 Service d'identité électronique suisse

Art. 19 Organisation

[1] Le Service d'identité électronique suisse (service d'identité) est rattaché au DFJP.

Art. 20 Tâches et devoirs

[1] Le service d'identité attribue les données d'identification personnelle au sens de l'art. 7, al. 1 et 2, au numéro d'enregistrement de l'e-ID correspondant et les transmet au FI.

[2] Il gère un système d'information pour la transmission des données d'identification personnelle aux FI. Le système d'information a accès aux registres de personnes suivants:

a. système d'information relatif aux documents d'identité (ISA);

b. système d'information central sur la migration (SYMIC);

c. registre informatisé de l'état civil (Infostar);

d. registre central de la Centrale de compensation de l'AVS (CdC-UPI).

[3] Les données contenues dans le système d'information doivent pouvoir être comparées avec celles qui figurent dans les registres de personnes cités à l'al. 2.

[4] Le service d'identité garantit que le FI puisse contrôler en tout temps la validité du numéro d'enregistrement de l'e-ID par une procédure usuelle, de façon fiable et gratuite.

[5] Le Conseil fédéral détermine les normes et les protocoles techniques applicables pour la transmission des données et règle la procédure pour les cas où différents registres de personnes transmettent des données contradictoires.

Section 7 Organisme de reconnaissance des FI

Art. 21 Compétence

[1] L'organisme de reconnaissance des FI (organisme de reconnaissance) est rattaché au DFF.

[2] Il assure la reconnaissance et la surveillance des FI et des systèmes e-ID.

Art. 22 Liste des FI

L'organisme de reconnaissance publie la liste des FI reconnus et de leurs systèmes e-ID.

Section 8 Émoluments

Art 23

[1] Le service d'identité et l'organisme de reconnaissance perçoivent des émoluments de la part des FI pour leurs décisions et leurs prestations.

[2] Le Conseil fédéral règle la perception des émoluments conformément à l'art. 46*a* LOGA. Pour fixer le montant des émoluments perçus lors de la transmission des données d'identification personnelle, il peut en particulier prendre en considération le fait qu'il s'agisse de la première transmission ou d'une mise à jour des données d'identification personnelle, ou que le FI établisse l'e-ID gratuitement pour le bénéficiaire.

Section 9 Responsabilité

Art. 24

[1] La responsabilité du titulaire de l'e-ID, de l'exploitant d'un service utilisateur et du FI est régie par le code des obligations[7].

[2] La responsabilité du service d'identité et de l'organisme de reconnaissance est régie par la loi du 14 mars 1958 sur la responsabilité[8].

Section 10 Dispositions finales

Art. 25 Modification d'autres actes

La modification d'autres actes est réglée en annexe.

[7] RS **220**
[8] RS **170.32**

Art. 26 Référendum et entrée en vigueur

[1] La présente loi est sujette au référendum.

[2] Le Conseil fédéral fixe la date de l'entrée en vigueur.

Annexe

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Loi du 22 juin 2001 sur les documents d'identité[9]

Art. 1, al. 3, 2e phrase

3 … Ces personnes peuvent être de nationalité étrangère.

Art. 11, al. 1, let. k, et 3

1 L'Office fédéral de la police exploite un système d'information. Ce système contient les données personnelles qui figurent sur le document d'identité et celles qui y sont enregistrées ainsi que:

k. le numéro AVS au sens de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[10];

3 Le traitement des données sert également à établir et à mettre à jour les moyens d'identification électronique conformément à la loi e-ID du …[11].

Art. 12, al. 2, let. g et h

2 Pour accomplir les tâches qui leur incombent de par la loi, les autorités et organes suivants sont habilités à consulter en ligne les données du système d'information:

g. la Direction consulaire du Département fédéral des affaires étrangères;

h le Service d'identité électronique suisse (service d'identité) d'après l'art. 19 de la loi e-ID du ….[12].

Art. 14 Interdiction de tenir des fichiers parallèles

La tenue de fichiers parallèles est interdite à l'exception de la conservation provisoire, par l'autorité d'établissement, des formules de demande, et par le service d'identité, des données qui lui sont transmises.

9 RS **143.1**
10 RS **831.10**
11 RS …
12 RS ….

2. Code civil[13]

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

[4] Les autorités suivantes peuvent accéder en ligne aux données nécessaires à la vérification de l'identité d'une personne:

5. le Service d'identité électronique suisse d'après l'art. 19 de la loi e-ID du ….[14].

3. Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[15]

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

[1] Dans la mesure où aucun intérêt privé prépondérant ne s'y oppose, les organes chargés d'appliquer la présente loi ou d'en contrôler ou surveiller l'application peuvent communiquer des données, en dérogation à l'art. 33 LPGA:

b^quater^ au Service d'identité électronique suisse (service d'identité) d'après l'art. 19 de la loi e-ID du ….[16];

4. Loi fédérale du 18 mars 2016 sur la signature électronique[17]

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

[1bis] Toute personne dont l'identité est attestée par un e-ID au sens de la loi e-ID du … [18] n'a pas l'obligation de se présenter en personne.

[13] RS **210**
[14] RS …
[15] RS **831.10**
[16] RS ….
[17] RS **943.03**
[18] RS …

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

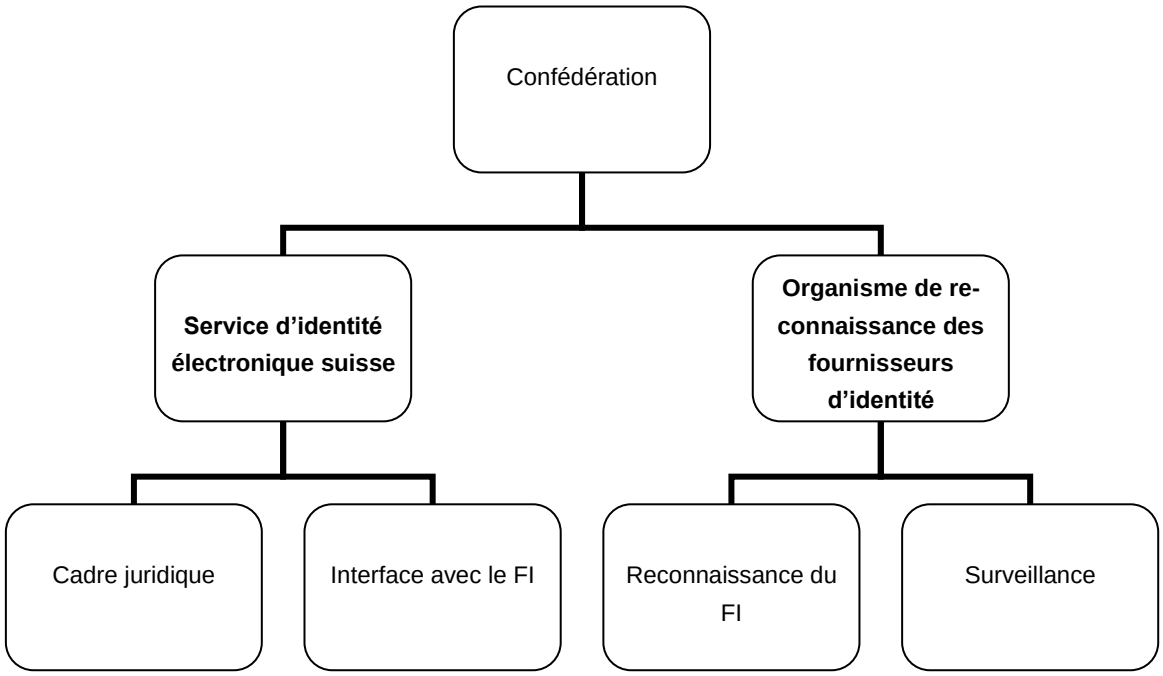
Vue d'ensemble

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 :

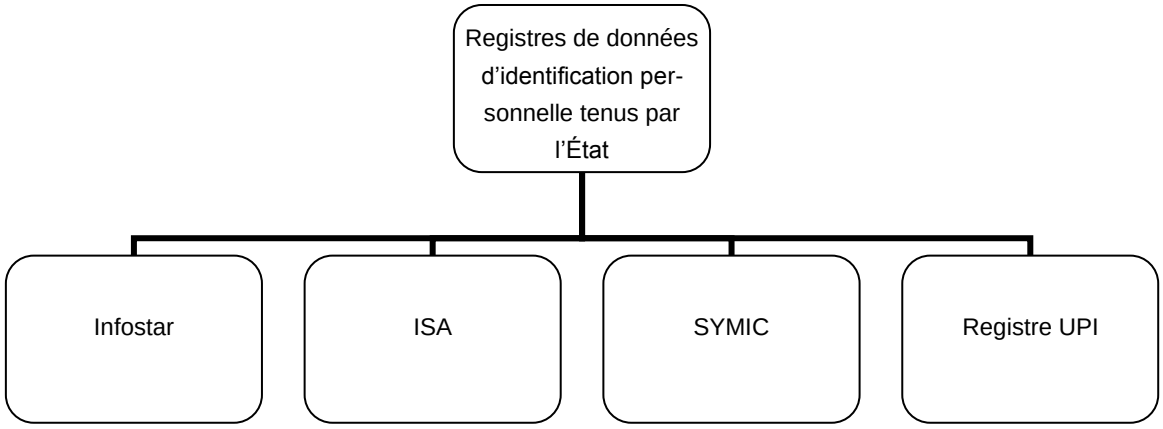
1. elle élabore et met à jour la réglementation en la matière, ce qui permet de garantir la transparence et la sécurité ;
2. elle définit les normes, les conditions de sécurité et les conditions d'interopérabilité à respecter pour pouvoir gérer un système e-ID ;
3. elle gère une interface électronique 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 eI-DAS	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 eI-DAS	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

-

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol
Domaine Développement des documents d'identité

Moyens d'identification électronique (e-ID) reconnus par l'Etat

Concept 2016

Version du 02.02.2017

Hermes

Un e-ID sert à prouver
son identité dans un environnement numérique.

Remarques liminaires

La popularisation d'Internet et la disponibilité importante d'appareils mobiles performants permettent un transfert de plus en plus facile des processus commerciaux vers le numérique. Selon les indications de l'Office fédéral de la statistique (Bundesamt für Statistik, Informationsgesellschaft, 2016), 88% de la population en moyenne a utilisé Internet en 2015: 56% pour des achats en ligne, 49% pour l'e-banking, 48% pour des prestations liées à un voyage, 48% pour remplir en ligne un formulaire officiel et 35% pour des activités politiques. Pour prendre contact avec les autorités, 79% des internautes ont passé par Internet. En une décennie (chiffres 2014), les dépenses en e-commerce des ménages ont passé à plus de sept milliards de francs.

La sécurité du droit et la confiance sont des conditions essentielles pour réaliser des affaires. Il s'agit notamment de connaître de manière adéquate l'identité des parties concernées. Dans le monde réel, la Confédération met actuellement à disposition des moyens d'identification conventionnels, à savoir le passeport suisse, la carte d'identité et le livret pour étrangers. En complément, il s'agit désormais de pouvoir attester l'identité d'une personne physique également sous forme électronique. Pour ce faire, le Conseil fédéral a chargé le DFJP de rédiger un concept pour les moyens d'identification électronique (e-ID) reconnus par l'Etat. De tels moyens reconnus par l'Etat permettent un enregistrement sûr pour accéder à des services en ligne et de s'y reconnecter ultérieurement en toute sécurité. D'autres services de confiance, tels que la signature électronique, peuvent être proposés par des fournisseurs de services d'identité, mais ils ne font pas partie des e-ID.

Le présent concept est fondé sur les travaux préalables entrepris par fedpol dans les années 2013-2015, au cours desquels des acteurs importants du marché ont été consultés. Il prend également en compte les enseignements tirés des solutions existantes pour des systèmes e-ID, les directives (EU, 2014) (Kommission, 2015) en matière de compatibilité avec l'UE[1] ainsi que les développements sur le plan international pour des solutions de systèmes e-ID solidement établies et proches de la pratique (FIDO Alliance, 2014) (Lindemann, R., FIDO Alliance and Nok Nok Labs Inc., 2013) (800-63-3, 2016) (eCH, eCH-0107 IAM Gestaltungsprinzipien v2.0, 2013) (8149, 2016). Dans la mesure du possible, un recoupement a aussi été effectué avec les exigences liées au dossier électronique du patient (LDEP) (Bundesamt für Gesundheit) et à la signature électronique (SCSE) (Schweizer Parlament, 2003).

Le concept prévoit que la Confédération ne publie pas ses propres e-ID, mais reconnaisse plutôt officiellement des systèmes e-ID appropriés disponibles sur le marché à trois niveaux de sécurité différents et exerce une surveillance idoine. Pour cela, la Confédération instaure un nouvel *Organisme de reconnaissance des fournisseurs d'identité (ORFI)*. En outre, la Confédération fait office de repère fiable pour l'identité de la détentrice ou du détenteur d'un e-ID en transmettant par voie électronique des données d'identification personnelle disponibles (nom, prénom, date de naissance, photo, etc.) à des émetteurs d'e-ID reconnus par l'Etat. Cette seconde tâche incombera au *Service d'identité électronique suisse (SIE)* qu'il convient de mettre sur pied au sein des autorités fédérales.

Pour garantir la sécurité du droit en matière d'e-ID, la Confédération édicte une *loi fédérale sur les unités d'identification électronique reconnus par l'Etat (loi e-ID)*, y compris les dispositions d'exécution requises. Celles-ci contiennent des directives techniques et organisationnelles con-

[1] Elles permettent une reconnaissance réciproque des systèmes e-ID. Toutefois, la notification requiert en tous les cas la conclusion d'un accord bilatéral avec l'UE.

crètes pour les systèmes e-ID reconnus par l'Etat, afin de créer les bases solides d'une confiance indispensable en la matière. Il s'agit aussi, notamment, de garantir l'interopérabilité entre les divers émetteurs de systèmes e-ID. Le présent concept fournit les bases substantielles pour la rédaction de la loi e-ID.

Table des matières

Répertoire des illustrations

Répertoire des tableaux

Répertoire des termes

A l'échelon national et international, un certain nombre de termes ont été adopté en matière d'e-ID. Veuillez vous référer au répertoire des termes ci-après ainsi qu'au glossaire en annexe.

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'Etat (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'Etat (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	Identity Attribute
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

1 Introduction

1.1 Structure et contenu

Le présent document décrit les réflexions fondamentales ayant mené au concept «e-ID» et au projet de loi correspondant relatif aux moyens d'identification électronique reconnus par l'Etat. Il s'agit de présenter les fonctions des participants à l'écosystème e-ID, les processus d'obtention et d'utilisation des e-ID reconnus par l'Etat, les considérations sur la sécurité et le rôle de la Confédération ainsi que les conséquences financières. Un chapitre est consacré à la présentation de la structure, de la fonctionnalité et des coûts du nouveau **Service d'identité électronique suisse (SIE)** et du nouvel **Organisme de reconnaissance des fournisseurs d'identité (ORFI)** au sein des autorités fédérales. Le premier opère comme service électronique de transmission aux fournisseurs de services d'identité (IdP) des attributs d'identité gérés par les autorités, alors que le second est principalement un organe de contrôle. Le présent document contient également, en annexe, une introduction aux rapports et termes en matière de gestion des identités, qui constitue la base du présent concept.

1.2 Moyens d'identification électronique

1.2.1 De quoi s'agit-il?

Pour que des processus commerciaux puissent se dérouler en ligne, les partenaires commerciaux (ci-après **parties utilisatrices [PU]**) doivent pouvoir se fier à l'identité fournie ainsi qu'à l'identification en ligne de l'autre partie, à l'échelon tant national qu'international. Dans le monde réel, les documents d'identité relevant de la puissance publique, tels que le passeport ou la carte d'identité, sont les moyens permettant de prouver de manière fiable son identité, fonction qui incombe, dans le monde numérique, aux **moyens d'identification électronique (e-ID)**. Un e-ID permet aux PU d'identifier et d'authentifier des personnes avant de fournir un service de confiance. Des e-ID fiables sont donc des éléments indispensables pour que des processus commerciaux électroniques puissent être implémentés.

L'e-ID est délivré par un **fournisseur de services d'identité (Identity Provider, IdP)** officiel ou privé, qui assigne au cours d'un processus d'enregistrement l'e-ID à une personne identifiée de manière fiable (ci-après **détentrice ou détenteur**). Un e-ID contient un **identifiant**[2] numérique unique ainsi qu'une fonction qui lie de manière sûre l'e-ID à une personne et qui est désignée par le terme d'**authentifiant**[3]. Grâce à un e-ID, la détentrice ou le détenteur peut transmettre à une PU, p. ex. le portail Internet d'une boutique en ligne, des **attributs d'identité** tels que le nom, l'âge, la nationalité, etc. (**identification**) et prouver qu'elle ou il est la personne à laquelle les attributs d'identité indiqués appartiennent (**authentification**). La PU la ou le connaît dès lors sous l'identifiant numérique unique de l'e-ID ou sous un pseudonyme assigné[4].

A l'usage, l'e-ID identifie la détentrice ou le détenteur grâce à l'identifiant numérique et fournit une

---

[2] L'identifiant est un code numérique lié de manière sécurisée à l'e-ID; au cours d'une identification en ligne, il représente la détentrice ou le détenteur d'un e-ID.

[3] Lors de l'utilisation d'un e-ID, l'authentifiant vérifie la présence physique de la détentrice ou du détenteur en contrôlant par exemple que le bon code NIP ou la bonne caractéristique biométrique de la détentrice ou du détenteur ont été saisis. Le support physique d'un e-ID (smartcard, smartphone, etc.) en possession d'une détentrice ou d'un détenteur a aussi la fonction d'un authentifiant.

[4] L'identifiant de l'e-ID peut aussi être utilisé sous forme cryptée et être défini de manière sectorielle pour chaque PU, voire de manière transitoire pour un bref contact.

preuve numérique[5] de la présence de la personne. L'e-ID permet ainsi à la PU une identification et une authentification de la détentrice ou du détenteur à un certain **niveau de sécurité**. Celui-ci dépend de la sécurité du processus d'enregistrement[6], de la sécurité avec laquelle l'e-ID fonctionne sur le terrain, de la sécurité avec laquelle la présence de la détentrice ou du détenteur est vérifiée lors de l'utilisation de l'e-ID et de la sécurité avec laquelle le résultat d'une identification ou d'une authentification est communiquée à la PU[7]. Les attributs d'identité transmis sont alors également définis selon un certain niveau de fiabilité, les attributs d'identité constatés par l'Etat, ou **données d'identification personnelle**, jouissant à cet égard d'un niveau de fiabilité très élevé. L'Etat est donc prédestiné à mettre de telles données à la disposition des IdP reconnus par l'Etat, qui peuvent ensuite les transmettre aux PU sur mandat des détentrices et détenteurs.

Grâce aux données d'identification personnelle sous-jacentes, un e-ID devient le lien numérique entre la personne physique et son identité définie officiellement (ci-après **identité civile[8]**), utilisée par les PU pour l'organisation des processus commerciaux. Pour simplifier ces opérations, un **identifiant personnel unique (IPU)** est en plus introduit en Suisse en matière d'e-ID en tant qu'attribut supplémentaire de l'identité civile.

Les rapports et termes valables en matière de gestion numérique des identités sont présentés en détail en annexe. Seuls les termes les plus importants sont expliqués ici.

L'ensemble des personnes morales et physiques, les PU, les IdP et les instances publiques, les moyens d'identification électronique et les services de confiance correspondants, tels que les signatures numériques, la protection des transactions, etc. qui utilisent ou contribuent à son exploitation sont désignés par le terme générique d'**écosystème e-ID**. Font également partie de l'écosystème e-ID les services officiels suisses et européens (UE) chargés de l'exécution de la réglementation légale ainsi que, éventuellement, d'autres services fournissant des prestations de soutien au marché numérique, par exemple un **service d'attribut** ou les services paneuropéens prévus de services proxy pour l'utilisation des e-ID à l'échelon international. La **gestion électronique des identités (eGId)** et les **systèmes e-ID** y afférents et exploités par les IdP forment la colonne vertébrale de l'écosystème e-ID.

Les instances et relations les plus importantes d'un écosystème e-ID pour les systèmes e-ID suisses reconnus par l'Etat sont illustrées schématiquement dans le Schéma 1[9].

---

5 Normalement, l'e-ID ne peut être utilisé que si la personne autorisée active elle-même l'e-ID et prouve ainsi implicitement sa présence physique.

6 Au cours du processus d'enregistrement lors de l'établissement d'un e-ID, la personne est, d'une part, liée à l'e-ID (p. ex. par la définition d'un code NIP que la personne devra par la suite saisir pour utiliser l'e-ID), d'autre part, son identité est vérifiée (p. ex. sur présentation d'un document d'identité officiel).

7 Les niveaux de sécurité sont définis par des standards et règles communs («Trust Framework» [28] [8]) que tous les intervenants d'un écosystème e-ID sont tenus de respecter. La confiance globale en matière de sécurité est composée des trois domaines partiels Robustesse de l'enregistrement initial et de l'identification, Robustesse de l'authentification à l'usage de l'e-ID et Robustesse de la transmission des résultats d'un examen aux PU [6].

8 L'identité civile regroupe l'ensemble des données d'identification personnelle enregistrées dans les registres officiels de l'état civil pour une personne. Seuls quelques-uns de ces attributs ou l'identifiant personnel unique nouvellement introduit suffisent pour déterminer indubitablement une identité civile.

9 Un exemple de modèle de référence complet d'un écosystème e-ID figure sous (Fachhochschule, Wirtschaft, & Institut, 2015). Pour le positionnement et la présentation compréhensible des interactions fondamentales d'un e-ID officiel, le modèle restreint aux instances déterminantes convient toutefois mieux.

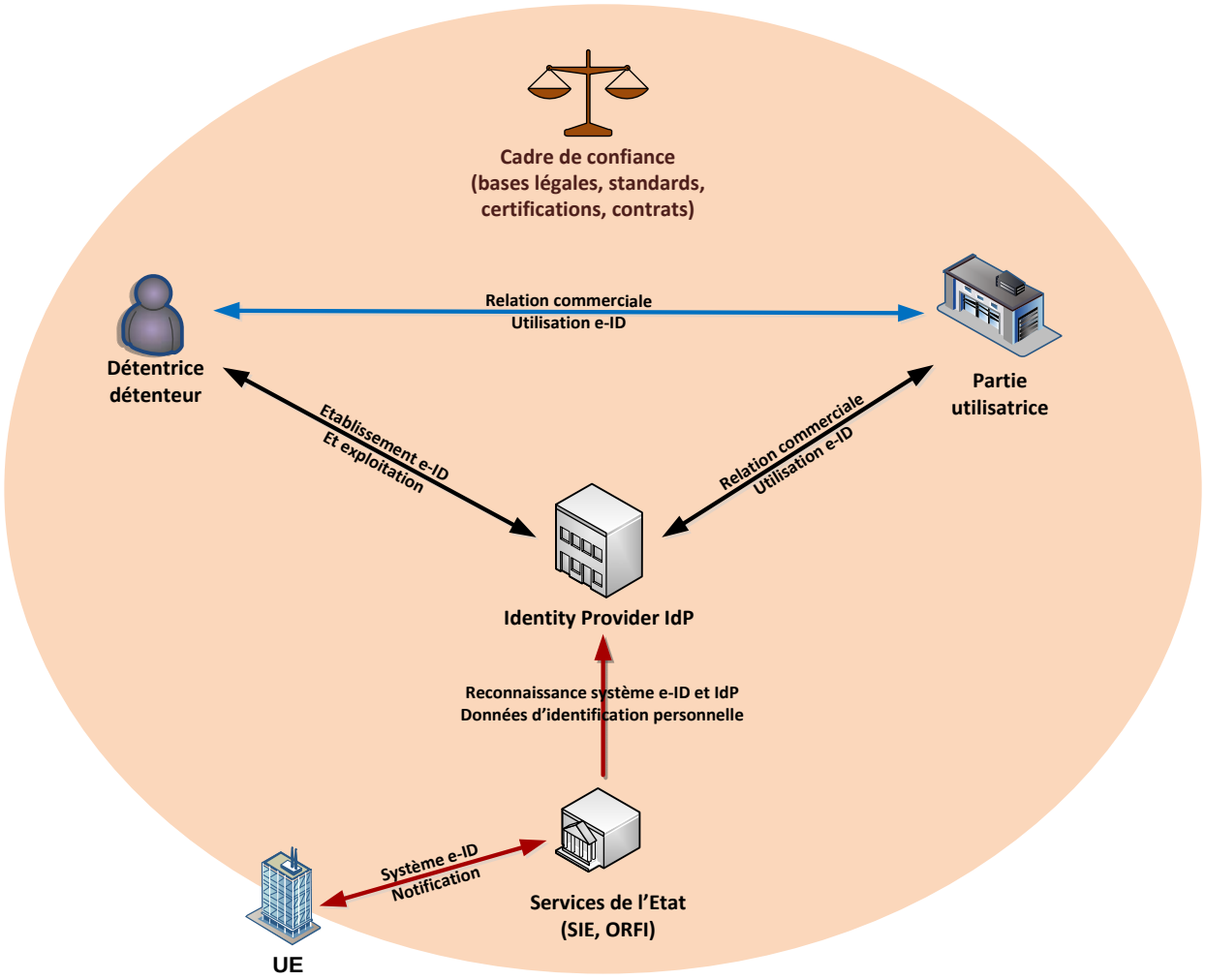


Schéma 1: Instances et relations les plus importantes d'un écosystème e-ID

1.2.2 Fiabilité

Un e-ID est fiable si les processus et procédures d'établissement et d'utilisation de l'e-ID ainsi que la transmission des résultats des vérifications par l'IdP à la PU sont sûrs et si le système e-ID dans son ensemble est régulièrement vérifié pour déterminer s'il satisfait les critères de sécurité standardisés et actuels.

A cet égard, l'enregistrement, la technologie utilisée pour le système e-ID, l'organisation de l'IdP, la véracité des attributs enregistrés, la sécurité de l'e-ID sur le terrain et les protocoles d'utilisation en mode d'interopérabilité des e-ID sont déterminants:

- Au cours de l'**enregistrement** d'une personne dans le système e-ID, l'IdP enregistre, d'une part, des attributs de l'identité civile identifiant la détentrice ou le détenteur parmi la **population**, d'autre part, des **attributs personnels** en tant que **facteurs d'authentification** pour l'authentification ultérieure de la détentrice ou du détenteur de l'e-ID. Les attributs personnels ne sont alors le plus souvent pas enregistrés de manière centrale, mais uniquement dans l'appareil servant de support à l'e-ID. Au cours du **processus de liaison**, ces éléments sont

fermement liés à l'authentifiant de l'e-ID[10]. Ces deux processus partiels doivent se dérouler selon un protocole technique et organisationnel sûr et déterminé par les exigences envers le niveau de sécurité de l'e-ID. Après l'enregistrement, l'identifiant unique de l'e-ID est assigné par l'IdP aux données d'identité de la détentrice ou du détenteur enregistrées.

- La **technologie** utilisée et l'**organisation** de l'IdP doivent satisfaire les exigences relatives au niveau de sécurité du système e-ID défini[11]. L'IdP répond de l'enregistrement correct et du fonctionnement correct de l'e-ID sur le terrain ainsi que de la transmission correcte des données d'identité et des résultats de l'authentification aux PU dans l'écosystème e-ID dans son ensemble. L'IdP doit pour cela implémenter des systèmes et processus sûrs, standardisés, transparents et certifiés[12]. La garantie en est donnée au cours du processus de reconnaissance du système e-ID et de l'IdP d'établissement, et des audits périodiques en assurent le contrôle. Les IdP reconnus par l'Etat doivent disposer d'un siège en Suisse et garantir qu'ils sont en mesure de répondre à d'éventuelles prétentions en responsabilité résultant des réglementations légales. Ils doivent en outre prouver qu'ils conservent toutes les données d'identification personnelle en Suisse exclusivement.
- L'IdP répond de l'**assignation correcte des attributs d'identité à l'e-ID**. Il a besoin de sources d'attribut sûres et fiables[13], le plus souvent possible garanties par l'Etat. Avec l'accord de la détentrice ou du détenteur, il reçoit du SIE les données d'identification personnelle garanties par l'Etat. Il n'est autorisé à transmettre ces données à des PU qu'avec l'accord exprès de la détentrice ou du détenteur.
- Le ***Service d'identité électronique suisse (SIE)*** répond de l'assignation correcte des données d'identification personnelle à l'**identifiant personnel unique (IPU)** lors de la transmission à l'IdP reconnu[14]. Ces données également ne peuvent être transmises du SIE à l'IdP qu'avec l'accord exprès de la détentrice ou du détenteur. Le SIE consulte les données d'identification personnelle directement dans les registres de la Confédération (Infostar, ISA, SYMIC, CdC-UPI). Le niveau de sécurité de l'e-ID détermine quelles données officielles d'identification personnelle sont transmises à l'IdP (cf. 2.6.3)[15].
- La **sécurité de l'e-ID** sur le terrain est pour l'essentiel définie par le nombre et la qualité des facteurs d'authentification indépendants vérifiés par l'authentifiant lors de l'utilisation d'un e-ID. De tels facteurs sont la «possession d'un objet personnalisé», la «connaissance d'un secret» ou une «caractéristique inhérente à la personne» pouvant être mesurées de manière

---

10 Lors de l'enregistrement, l'authentifiant de l'e-ID enregistre les facteurs d'authentification en tant que données de référence. Lors d'une authentification ultérieure en cas d'utilisation de l'e-ID, celui-ci enregistre à nouveau les facteurs d'authentification et les compare aux données de référence avant d'accepter ou de rejeter la personne enregistrée comme étant ou non authentifiée.

11 Les systèmes e-ID suisses peuvent être reconnus à trois niveaux de sécurité. Ces trois niveaux de sécurité correspondent à ceux précisés dans le Règlement eIDAS de l'UE et dans les directives pour l'authentification numérique des USA.

12 Pour les systèmes e-ID, des profils de protection adéquats, conformes à la norme ISO/IEC 15408, sont définis pour chaque niveau de fiabilité. Pour la reconnaissance, des certifications doivent être réalisées conformément à ces profils de protection.

13 Tous les Etats étrangers dont les ressortissants vivent en Suisse en tant qu'étrangers autorisés à disposer d'un e-ID ne tiennent pas des registres de personnes à un niveau de qualité habituel pour les registres suisses. Toutefois, dès que des données sont saises dans SYMIC, celles-ci sont considérées par définition comme source valable pour des attributs de l'identité civile.

14 Lors de l'enregistrement, l'IdP saisit le numéro d'un document d'identité officiel ou l'identifiant personnel unique de la personne et demande au SIE, sur la base de cette information, la transmission des données d'authentification personnelle pour l'e-ID.

15 Les attributs qui ne sont pas communiqués sans autre dans la vie commerciale normale sont réservés aux niveaux de sécurité supérieurs des e-ID; la signature numérisée, par exemple, n'est fournie que pour le niveau de sécurité le plus élevé.

biométrique. L'e-ID doit être sécurisé sur le plan technique de manière à pouvoir être identifié de manière univoque par son identifiant, à ce que l'authentification de la personne se déroule conformément aux exigences du niveau de sécurité de l'e-ID et à ce que d'éventuels messages envoyés à l'écran du support de l'e-ID et le retour d'information de la détentrice ou du détenteur soient authentiques.

- Tous les e-ID doivent pouvoir être utilisés, indépendamment de l'émetteur, auprès de toutes les PU qui acceptent une identification ou une authentification au niveau de sécurité de l'e-ID. Cette **interopérabilité** est une condition importante pour l'acceptation d'un e-ID dans la vie commerciale numérique. Elle est obtenue par la définition de protocoles, formats de messages et devoirs de collaboration entre les IdP. Que ce soit pour les PU ou pour les détentrices et détenteurs d'un e-ID, l'utilisation d'un e-ID reconnu doit être partout pareil et transparent.

Une PU considérera toujours l'utilisation d'un E-ID par rapport à ses besoins commerciaux en tenant compte de ces aspects de sécurité. En effet, le niveau de sécurité requis pour un processus commercial spécifique est déterminé dans la pratique par la PU. Celle-ci n'accepte que les systèmes e-ID qui satisfont ses exigences en matière d'identification et d'authentification du partenaire commercial. Elle obtient les services d'identité souhaités auprès du ou des IdP qui ont établi les systèmes e-ID appropriés reconnus par l'Etat. Les systèmes e-ID reconnus par l'Etat devant être interopérables et standardisés, la PU n'est quasiment pas limitée par des obstacles d'ordre technique dans son choix, et le marché peut opérer librement. Divers modèles commerciaux sont possibles entre la PU, la détentrice ou le détenteur et l'IdP. Le marché décide des modèles fructueux.

Les détentrices et détenteurs, à l'instar des PU, doivent pouvoir se fier au fait que les systèmes e-ID reconnus par l'Etat satisfont le niveau de sécurité déclaré. Ils répondent cependant des aspects sécuritaires pour lesquels ils sont compétents:

- la détentrice ou le détenteur répond de l'utilisation correcte de l'e-ID et ne doit en particulier pas le confier à des tiers;
- la PU doit garantir l'identification et l'authentification correcte par le système e-ID de l'IdP en suivant les processus techniques et organisationnels définis par l'IdP pour l'utilisation de l'e-ID.

Les compétences et la répartition de la responsabilité entre l'Etat et l'IdP sont illustrées ci-après. Les dispositions fondamentales sont inscrites dans la loi, et les modalités sont précisées dans l'ordonnance.

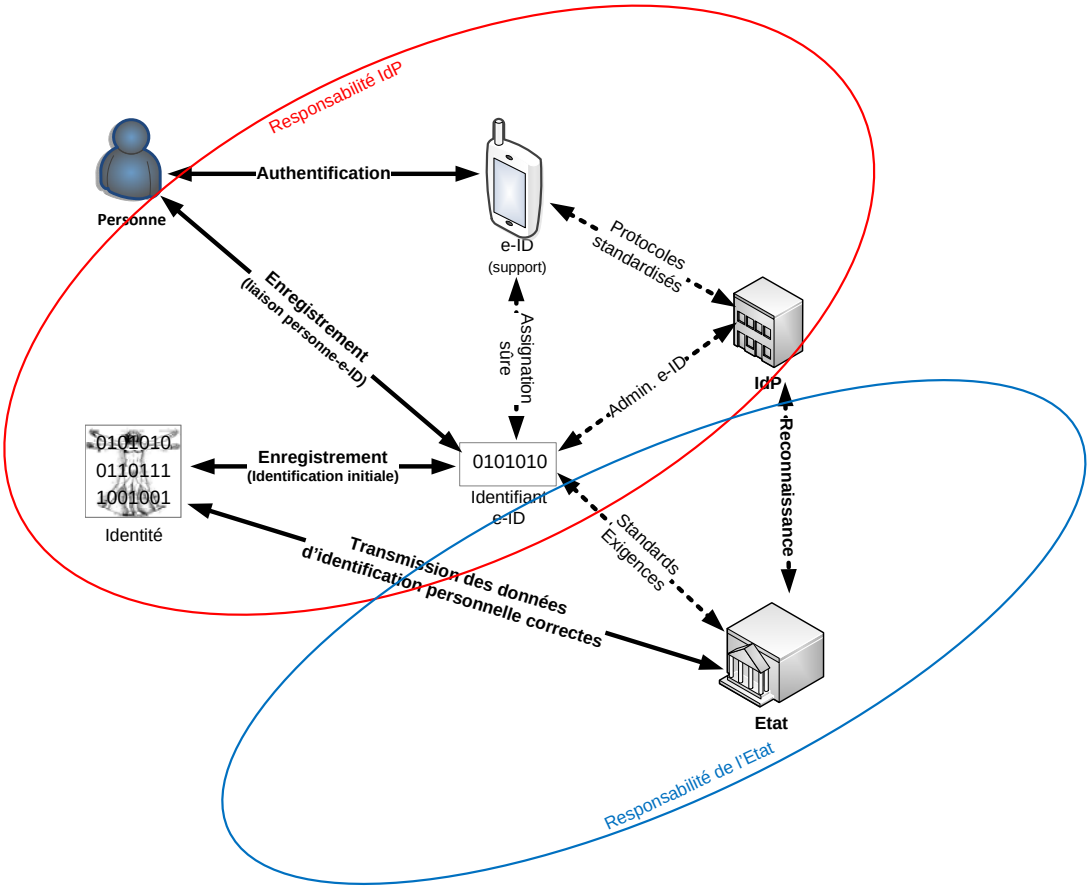


Schéma 2: Répartition de la responsabilité entre Etat et IdP

1.2.3 Convivialité d'utilisation

Le comportement des utilisateurs sur les marchés numériques est étroitement lié aux innovations et à l'évolution technologique internationale du marché informatique global. Le marché évolue rapidement et il est difficile de l'influencer durablement par des réglementations rigides ou des impératifs officiels. Pour faire simple, un système est convivial s'il est accepté par le marché et inversement. En matière de systèmes sécuritaires justement, ce qui inclut un système e-ID, les exigences en termes de sécurité et de protection de la sphère privée sont souvent des plus élevées. Il y a toutefois de fortes divergences entre de telles exigences idéalisées et le comportement concret des utilisateurs dans la pratique. Il arrive très fréquemment que des mesures de sécurité en théorie optimales mais souvent assez incommodes aboutissent à un comportement d'évitement de la part des utilisateurs et donc à des lacunes de sécurité substantielles qui pourraient être éludées grâce à des mesures de sécurité plus simples et plus conviviales.

Principales caractéristiques d'une convivialité d'utilisation élevée pour les systèmes e-ID:

- **Nombreuses offres en ligne** d'organisations connues, fiables et bien établies sur le marché et auprès desquelles l'e-ID peut être utilisé. Un e-ID doit pouvoir être utilisé par toutes les PU, indépendamment de l'IdP ayant émis l'e-ID. Seul le niveau de sécurité requis pour l'offre doit être satisfait par l'e-ID.
- **Etablissement aisé et mise en service simple**, toutes les étapes devant, autant que faire se peut, pouvoir être réalisées en ligne au cours d'un processus d'un seul tenant; toute présentation en personne éventuellement requise doit pouvoir être possible de manière souple et à proximité ou, mieux, être remplacée par des alternatives sécurisées, par exemple une vidéoconférence.
- **Déroulement partout semblable** lors de l'utilisation de l'e-ID à un certain niveau de sécurité. Il est capital que les détentrices et détenteurs connaissent leur e-ID et l'utilisent volontiers et le plus souvent possible. Cela ne peut être obtenu que par une expérience d'utilisation simple, uniforme et compréhensible à chaque utilisation. La standardisation des systèmes e-ID reconnus doit donc également formuler des exigences en matière d'interface utilisateurs et de protocole d'utilisation.
- **Utilisation universelle de l'e-ID**, autant que possible à tout moment depuis le terminal personnel (ordinateur, smartphone). Toutefois, et dans le même temps, indépendance la plus forte possible par rapport aux technologies actuelles et appareils présentant une durée de vie brève, de manière à ce que l'e-ID puisse être transféré sans problème d'un support à un autre.
- **Mesures de sécurité compréhensibles**, de manière à ce que les détentrices et détenteurs comprennent le sens d'une étape du protocole de sécurité et n'essaient pas de le contourner.
- **Coûts acceptables et durée de validité importante**. Un e-ID doit être valable et pouvoir être utilisé plusieurs années. Si la détentrice ou le détenteur d'un e-ID doit participer aux coûts lors de l'utilisation de son e-ID, il convient d'opter pour un modèle de «paiement selon l'utilisation» (pay-per-use) avec un prix pour l'ensemble de la prestation en ligne. Les coûts globaux liés à un e-ID devraient donc être calculés de telle manière que la possession d'un e-ID reconnu par l'Etat est perçue comme étant intéressante et avantageuse. L'établissement initial d'un e-ID devrait être gratuit dans la mesure du possible.

Le système e-ID doit être simple à utiliser non seulement pour les détentrices et détenteurs, mais aussi et en particulier pour les PU qui acceptent un e-ID et créent ainsi de nombreuses possibilités d'utilisation d'un e-ID. Les principaux critères d'implémentation d'un système e-ID pour le processus de connexion d'un **service de confiance** sont les suivants:

- L'**intégration des protocoles du système e-ID** dans, si possible, tous les processus commerciaux d'une PU nécessitant une identification et une authentification, doit être simple. La PU installe alors dans son portail (ou **service de confiance**) une application d'interface pouvant être intégrée de manière standard pour l'utilisation des services d'identité du système d'e-ID (ou **interface e-ID**). Cette interface e-ID est définie par l'IdP avec lequel la PU collabore, et elle contient en particulier également l'interface utilisateur standardisée pour l'utilisation en ligne de l'e-ID. L'exécution de l'identification et de l'authentification est alors déléguée par le service de confiance au système e-ID par le biais de l'interface e-ID. Le résultat du service d'identité est retourné par celui-ci au service de confiance, par le biais de l'interface e-ID sous forme d'un ticket sécurisé. La plupart des systèmes e-ID disponibles actuellement sur le marché fonctionnent selon ce principe et autorisent une intégration la moins invasive possible d'un système e-ID à une application d'e-commerce existante. Grâce à la standardisation, par exemple l'authentification selon les spécifications FIDO (FIDO Alliance, 2014) et la gestion des attributs selon les normes eCH correspondantes (eCH Verein), l'intégration ainsi que le passage d'un système e-ID à un autre peuvent être réalisés simplement.

- L'**interopérabilité** requise entre les systèmes e-ID reconnus par l'Etat permet d'utiliser chaque e-ID indépendamment de l'IdP d'établissement et auprès de chaque PU, pour autant que l'e-ID réponde au niveau de sécurité requis. Pour cela, l'IdP auprès duquel la PU obtient le service d'identité transmet le mandat d'identification ou d'authentification de la PU à l'IdP ayant délivré l'e-ID spécifique. Ce processus peut toujours être suivi, car les IdP doivent mettre en place entre eux des interfaces d'interopérabilité. L'IdP compétent exécute l'ordre et retourne le ticket de réponse par le même biais à la PU. De cette manière, ni les PU, ni les détentrices ou détenteurs ne sont limités dans l'acceptation ou l'utilisation d'un e-ID.
- L'utilisation de l'e-ID ne nécessite qu'un **modeste ajustement des processus commerciaux,** de manière à ne pas freiner l'opération en ligne. Grâce à la standardisation requise, les PU peuvent utiliser les systèmes e-ID sans bouleverser leur infrastructure informatique ou modifier leur modèle commercial. L'identification et l'authentification au moyen d'un e-ID ne doivent générer que des avenants simples aux protocoles des processus commerciaux existants. Les IdP sont encouragés à orienter leur offre conformément à ce besoin du marché. L'Etat aide les IdP à satisfaire cette exigence en édictant des prescriptions de standardisation et en instaurant un modèle d'indemnisation simple pour la transmission des données d'identification personnelle.
- La **protection des données commerciales** doit être garantie. L'intégration d'un e-ID pouvant être utilisé partout ne doit en aucun cas aboutir à la transmission de données commerciales ou confidentielles des PU, de l'IdP ou de la détentrice ou du détenteur. Un cahier des charges idoine en matière de protection des données et de surveillance permet à la Confédération de garantir que les systèmes e-ID reconnus par l'Etat et les IdP exploitants répondent à cette exigence.
- L'utilisation d'un e-ID reconnu par l'Etat doit déboucher sur un **avantage économique** et être, au final, plus intéressant de ce point de vue que le déploiement et l'exploitation d'une propre solution d'authentification (système en silo), voire la renonciation à une identification en ligne sûre. Les modèles économiques des IdP proposant des systèmes e-ID reconnus par l'Etat doivent prendre en compte ce critère économique. L'Etat, quant à lui, incite les PU à utiliser des systèmes e-ID dignes de confiance pour leurs prestations en ligne par le biais d'une réglementation appropriée en matière de responsabilité.

Conformément au Règlement eIDAS (art. 7), seuls des systèmes e-ID aussi utilisés par des pouvoirs publics pour l'identification en ligne peuvent recevoir de telles notifications. Voilà pourquoi la loi e-ID oblige fondamentalement les portails en ligne de la Confédération à utiliser des systèmes e-ID reconnus, pour autant que ceux-ci soient d'un niveau de sécurité suffisant pour le service en question En contrepartie, l'utilisation d'un e-ID par des services publics doit être proposée par les IdP à un tarif unique selon le modèle «pay-per-use».

1.3 Contexte

1.3.1 Evolution socio-économique

La popularisation d'Internet et la disponibilité importante d'appareils mobiles performants permettent un transfert de plus en plus facile des processus commerciaux vers le numérique. Les jeunes générations, au bénéfice d'une bonne formation et d'une certaine affinité avec les nouvelles technologies, sont très bien connectées et souvent en permanence en ligne, ce qui favorise cette évolution socio-économique.

Selon les indications de l'Office fédéral de la statistique (Bundesamt für Statistik, Informationsgesellschaft, 2016), 88% de la population âgée de 14 ans et plus a utilisé au moins une fois Internet en 2015, les 14-19 ans étant 99% et les plus de 70 ans, 43% tout de même à

avoir utilisé au moins une fois par semaine ou quotidiennement Internet. En comparaison européenne, la Suisse est au-dessus de la moyenne de 76%, mais encore loin derrière les pays leaders que sont l'Islande (97%) et le Danemark (93%). 42% des internautes passent 1-5 heures par jour sur Internet et 15% déjà sont plus de 15 heures par jour en ligne.

L'utilisation mobile d'Internet a fortement augmenté ces dernières années. En 2015, ce mode a été utilisé par 42% de l'ensemble de la population. Pour surfer de manière mobile, le téléphone portable a été utilisé à 95% et la tablette, à 23%. A l'inverse, l'utilisation de l'ordinateur (42%) a quasiment diminué de moitié depuis 2010.

En 2015, 56% de la population a utilisé Internet pour des achats en ligne, 49% pour l'e-banking, 48% pour des services liés à un voyage, 48% pour remplir en ligne un formulaire officiel et 35% pour des activités politiques. Pour prendre contact avec les autorités, 79% des internautes ont passé par Internet. En une décennie (chiffres 2014), les dépenses en e-commerce des ménages ont passé à plus de sept milliards de francs.

1.3.2 Contexte international

La Suisse est loin d'être isolée dès lors qu'il s'agit d'introduire un moyen d'identification électronique reconnu par l'Etat. Cette question figure depuis une quinzaine d'années à l'ordre du jour de la plupart des pays développés.

Il y a de nombreuses raisons valables d'étudier la situation prévalant dans d'autres pays ainsi qu'à l'international, et d'en tenir compte pour définir un propre concept. La problématique en matière d'e-ID dans des pays comparables est en grande partie similaire à celle à laquelle est confrontée la Suisse; il est donc possible de bénéficier des expériences réalisées par d'autres pays. Compte tenu de la nature globale des services en ligne proposés par Internet, il est important de concevoir sur les plans technique et juridique un moyen d'identification électronique reconnu par l'Etat pouvant être utilisé à l'international, notamment dans l'espace européen. En fin de compte, il est important de miser sur les dernières tendances dans des domaines fortement influencés par la technique. Un seul pays, à plus forte raison la Suisse, ne peut à lui seul influer de manière déterminante sur les tendances technologiques.

Nombre de pays européens et un nombre considérable de pays émergents ont déjà introduit des e-ID officiels, très souvent intégrés dans des smartcards à contact. L'acceptation par la population et les milieux économiques est encore timide, notamment dans les Etats européens n'ayant pas introduit d'obligation d'utiliser un e-ID. Les systèmes déployés parfois à grands frais n'ont pas encore fait leurs preuves. Mentionnons à titre d'exemple la nouvelle carte d'identité allemande, introduite il y a déjà quelques années et qui contient un e-ID conçu de manière très sûre. Il s'est cependant avéré que l'e-ID dans cette carte d'identité était peu accepté, car il s'avérait compliqué à utiliser au quotidien et onéreux pour l'Etat chargé de son exploitation, alors que le niveau de sécurité était excellent (Fromm & et al., 2013). L'Allemagne essaie désormais de mettre à disposition l'e-ID sur des supports mobiles également, tels que des smartphones. D'autres solutions de systèmes e-ID exigeant des composantes d'infrastructure supplémentaires de la part des utilisateurs finaux sont mal acceptés; ainsi, l'e-ID belge (Belgische Regierung) n'est le plus souvent utilisé que pour remplir la déclaration d'impôt, car les citoyens y sont obligés, alors qu'en Autriche, l'e-ID de la carte d'identité n'est utilisé que par une très faible minorité (BRZ-Presseservice, 2014) (contrairement à la solution sur smartphone également proposée).

Les premières réflexions des Etats en matière d'e-ID ont porté sur le moment à partir duquel un Etat ajouterait un e-ID à sa carte d'identité, en faisant appel à quelle technologie et avec quelles fonctions. Les principales questions ont porté sur la technologie de microprocesseur à utiliser, sur le système d'exploitation du microprocesseur le plus adéquat et sur le mode de communication entre le microprocesseur et son milieu environnant, à savoir par contact ou par ondes radio (NFC). Un sujet important sur le plan juridique et politique était la question de savoir si l'e-ID

devait se référer à un identifiant personnel existant et si oui, auquel. D'un point de vue fonctionnel, il a fallu décider si le microprocesseur contenant dans le même temps une clé pour la signature électronique et si, ultérieurement, la fonction de passeport électronique avec technologie radio, entre-temps standardisée par l'ICAO (fonction e-passeport) (International Civil Aviation Organisation (ICAO)) , devait être incluse.

De telles réflexions ont conduit, au cours des 15 dernières années environ, de nombreux pays européens à introduire un e-ID lié à la carte d'identité en tant qu'élément central d'un système e-ID national. La Finlande a fait office de pionnier en introduisant en 1999 une carte d'identité avec un e-ID. Ont suivi l'Estonie, la Belgique, l'Espagne et le Portugal. L'Allemagne a lancé en 2010 sa carte d'identité électronique (ePA / nPA) (Bundesministerium des Innern). Ces dernières années, ce sont avant tout les pays du Proche-Orient et d'Asie qui ont lancé de nouvelles cartes d'identité avec une fonction e-ID. Il n'est pas rare que l'idée sous-jacente soit celle de ne pas prendre de retard compte tenu des cycles de production longs des cartes d'identité par rapport à l'évolution très rapide de la technique (mainstream). A contrario, ni les USA, ni le Royaume-Uni n'ont introduit d'e-ID officiel, ce qui est dû à la méfiance généralisée qui prévaut dans ces pays vis-à-vis des cartes d'identité. Aux USA du moins, le permis de conduire fait souvent office de pièce d'identité. Certains Etats aux USA ont commencé à introduire, ou envisage de le faire, un e-permis de conduire (Government Technology) (CNET).

Une des premières configurations typiques voyait des smartcards munies de certificats X.509 être dotées de microprocesseurs fonctionnant par contact, misant pour l'essentiel sur la technologie des cartes à signature. Les cartes e-ID finnoises, estoniennes et belges sont des exemples d'une telle solution, ainsi que, sur le fond, la SuisseID. Ces cartes ont entre-temps souvent été remplacées par des cartes de deuxième génération.

Une autre situation fréquente a résulté des efforts des milieux industriels européens spécialisés en microprocesseurs pour définir des standards pour une carte de citoyen européen (ECC). Ces cartes disposent de la fonction d'e-passeport conformément à l'ICAO ainsi qu'une fonction s'appuyant sur la fonction d'e-passeport pour l'identification électronique en ligne. La Suède, Monaco, la Lettonie, la Finlande (2^{e} génération) et les Pays-Bas disposent de telles cartes d'identité. Le standard ECC n'a toutefois jamais réussi à s'imposer totalement. A l'échelon européen, il est toutefois entré dans le domaine des livrets pour étrangers (permis de séjour pour les ressortissants d'Etats tiers), car l'UE peut légiférer dans ce domaine, ce qui n'est pas le cas pour les cartes d'identité. Le permis suisse pour les ressortissants d'Etats tiers respecte cette norme.

Un des points culminants, en quelque sorte, de cette phase de développement des e-ID est le document d'identité personnel électronique (epA) introduit en 2010 en Allemagne. Il comprend pour l'essentiel les composants mentionnés précédemment, mais a été amélioré sur certains points et inclut désormais notamment plusieurs procédures techniques exigeantes visant à renforcer la protection de la personnalité. Ainsi, les fournisseurs de prestations (Service Provider) doivent toujours se faire enregistrer par l'Etat pour recevoir certains attributs et également se faire authentifier auprès de l'e-ID lors de l'utilisation. Une fonction d'attribution d'un pseudonyme («Restricted Identity») veille à ce que le document d'identité s'annonce auprès de chaque fournisseur de prestations avec un identifiant différent, ce qui rend plus difficile l'établissement de profils d'utilisateurs. Grâce à une stratégie globale, les autorités allemandes sont parvenues à ce que les titres de séjour des ressortissants étrangers soient équipés de «fonctions d'identification en ligne» compatibles. Au cours des dernières années, l'ePA allemand est devenu en bonne partie une référence pour les nouveaux e-ID officiels dans le monde entier. Depuis lors, près de la moitié de la population allemande dispose d'un ePA et il n'est pas encore clair si l'e-ID sera effectivement utilisé à large échelle avec le nPA.

Un facteur décisif pour l'utilisation de l'e-ID par la détentrice ou le détenteur est la diversité de l'offre en services permettant de se servir de l'e-ID. Il s'avère ainsi que le taux d'activation de l'e-ID de l'ePA est nettement plus élevé dans les grandes agglomérations allemandes proposant

activement des offres en ligne. Ou à l'inverse, le scepticisme par rapport à l'eID intégré à l'ePA est nettement plus prononcé dans les régions ne disposant que d'une offre en ligne restreinte.

Le système e-ID estonien est le plus développé. Il est en service depuis plus de dix ans et il comprend aujourd'hui la plupart des services, de l'e-banking au vote électronique, pour toute la population. Le modèle suédois avec identifiant bancaire (BankID) jouit également d'un grand succès. Il repose sur la coopération des banques avec l'Etat et d'un point de vue conceptuel, il est très proche du modèle présenté ici pour la Suisse. Les critères déterminants pour le succès des e-ID dans ces pays sont (Gemalto, C. Mesnard, 2016)

- l'acceptation ininterrompue des e-ID pour tous les services publics en ligne,
- la coopération entre les secteurs public et privé,
- un modèle commercial fonctionnant bien pour toutes les parties concernées,
- une même expérience utilisateur tout au long de l'utilisation d'un e-ID, et ce, quelque soit l'application concernée,
- un identifiant personnel unique disponible de manière générale, et
- des règles contraignantes en tant que base de confiance ainsi que des standards uniformes pour l'infrastructure.

1.3.3 Derniers développements

L'optimisation ponctuelle de la sécurité de certains composants du déroulement des processus commerciaux électroniques ne peut améliorer la sécurité générale; cela vaut également pour l'e-ID (Steier, 2010). La SuisseID prouve que la sécurité à elle seule ne constitue pas un critère conceptuel déterminant pour atteindre l'objectif visé. Les attentes à son égard étaient importantes, mais elle n'a pour l'heure réussi à s'implanter en Suisse qu'en tant que produit de niche. Les faiblesses de la SuisseID ou les motifs pour sa diffusion limitée sont, notamment, son installation malaisée, la durée de vie limitée à trois ans des certificats, le manque d'applications et d'interopérabilité internationale ainsi que les frais d'acquisition importants (Quade & Wölfle, 2010) (Müller, 2011). A l'inverse, les ID mobiles les plus récents n'engendrent pas de frais directs pour l'utilisateur – qui sont facturés à la PU par le biais d'un accord d'utilisation – et l'établissement ainsi que l'utilisation sont plus conviviaux. Hors de Suisse également, presque tous les systèmes e-ID qui mettent unilatéralement l'accent sur la sécurité uniquement et délaissent la convivialité d'utilisation indépendamment de cas commerciaux concrets doivent faire face à des problèmes d'acceptation (Strauß & Aichholzer, 2010) (Riedl, R., E-Government Institut Bern, BFH, 2014) (Horsch, 2013).

Le concept de solution e-ID prévu pour la Suisse doit par contre satisfaire le mieux possible et de manière équilibrée les principaux critères. A cet égard, des examens étendus à différents niveaux ont déjà été réalisés au cours des travaux préparatoires pour le présent concept. Des services privés et publics d'établissement d'e-ID, des PU potentielles et des avant-gardistes en matière d'évolution technologique pour la gestion électronique des identités ont été consultés. Le présent concept e-ID a permis de réaliser de plus amples simplifications et améliorations pour des systèmes e-ID reconnus, qui devraient toutes aboutir à une amélioration de l'acceptation par le marché. Outre la base de confiance dans la sécurité juridique, technique et organisationnelle, les critères décisifs pour un e-ID accepté et pouvant être utilisé sont la convivialité d'utilisation, l'utilisation standardisée et la variété des possibilités d'utilisation (Gemalto, C. Mesnard, 2016) (Nok Nok Labs Inc., 2013). Les fonctions de l'e-ID les plus fréquemment utilisées sont l'enregistrement auprès d'une PU et, ultérieurement, l'annonce auprès du service de confiance si l'on est déjà enregistré en tant qu'utilisatrice ou utilisateur. Ces procédures doivent donc être particulièrement conviviales et du dernier cri technologique (Richter, 1997).

Ces dernières années, les considérations ont par conséquent davantage porté sur la promotion par l'Etat de l'e-ID plutôt que sur la question «quel e-ID sur la carte d'identité?» et l'ont amené vers une nouvelle dimension. Les principales raisons en sont la durée nettement trop longue du cycle de production d'une carte d'identité officielle par rapport à la vitesse de développement du monde numérique et la nécessité de disposer d'une infrastructure coûteuse et fiable pour lire l'e-ID sur les cartes. Certes, ces lecteurs ne sont souvent pas si onéreux à l'acquisition, mais compliqués et coûteux à l'utilisation et pour la maintenance. De plus, les plateformes en vigueur, notamment les appareils mobiles qui dominent actuellement le marché, ne disposent pas toutes de lecteurs ou connexions correspondants.

Parallèlement au projet étasunien de développement commun d'un écosystème d'identité (NIST), de nombreux pays ont commencé une réflexion de fond sur la nature d'une bonne architecture pour l'écosystème global à l'échelon national et international en matière d'e-ID, en impliquant tous les intervenants, et quelle pourrait être la contribution de l'Etat à un tel écosystème e-ID. Les pays concernés sont parvenus à des conclusions différentes.

Aux USA, le rôle de l'Etat est limité à celui d'un organisateur et d'un promoteur de l'écosystème e-ID; l'Etat lui-même ne met pas à disposition de tels services, mais il exerce une forte influence sur le marché en tant que bénéficiaire d'e-ID pour ses employés et en tant qu'exploitant de services de confiance pour des offres de cyberadministration. En Suède, en Norvège et au Danemark, les banques ont été identifiées comme les principaux fournisseurs d'e-ID pour tous les secteurs, dans la mesure où elles utilisent déjà depuis longtemps de tels produits pour leurs services. Des exigences officielles minimales garantissent une certaine qualité et une certaine interopérabilité.

Le règlement eIDAS de l'UE susmentionné a dû, en définitive, accepter cette évolution et valider à un même niveau également, pour la reconnaissance mutuelle, des systèmes e-ID reconnus par l'Etat en plus des e-ID délivrés par l'Etat. Cette conception trouve son expression à l'article 7 formulé comme suit:

> **Éligibilité pour la notification des schémas d'identification électronique**
>
> Un schéma d'identification électronique est éligible aux fins de notification en vertu de l'article 9, paragraphe 1, si toutes les conditions suivantes sont remplies:
>
> a) les moyens d'identification électronique relevant du schéma d'identification électronique sont délivrés
>
> i) par l'État membre notifiant;
>
> ii) dans le cadre d'un mandat de l'État membre notifiant; ou
>
> iii) indépendamment de l'État membre notifiant et sont reconnus par cet État membre.

Le même article précise ensuite la responsabilité du service d'établissement d'un e-ID ainsi que les devoirs auxquels il ne peut en aucun cas, donc pas non plus dans le cas précisé à l'article 7, lettre a) iii), se soustraire.

1.3.4 Conséquences pour la Suisse

A l'heure actuelle, de nombreux fournisseurs de services d'identité opèrent déjà dans l'écosystème e-ID suisse et proposent un e-ID, p. ex. SuisseID, Mobile ID, Google ID, AppleID, Open ID, etc. Des solutions internes à l'administration ont aussi été lancées avec une smartcard personnelle, par exemple celle permettant l'authentification auprès du portail SSO du DFJP. Le projet IAM de la Confédération ambitionne même de réaliser une solution uniforme pour toute l'administration fédérale. En outre, des entreprises telles que des banques ou sociétés d'assurance confient à leur clientèle des moyens d'identification dédiés servant uniquement à réaliser leurs propres opérations. De tels moyens d'identification limités à une seule utilisation sont appelés

des «solutions en silo», contrairement aux solutions dont il a été question plus haut, qui sont utilisées avec de multiples contacts («solutions fédérées ou interopérables»). Tous ces systèmes ont une diffusion, une convivialité d'utilisation, une fonctionnalité et une sécurité diverses, et le plus souvent, ils ne sont pas compatibles entre eux. A l'échelon international, la tendance s'oriente toutefois vers une authentification et une identification centrées sur l'utilisateur, sûres et interopérables pour servir de base à tous les services de confiance correspondants.

Si l'on compare le concept présenté ici et celui mis en œuvre dans le projet de loi pour la reconnaissance par l'Etat des moyens d'identification électroniques avec les développements, les expériences et les réflexions actuelles sur le plan national et international, il en résulte ce qui suit:

- La Suisse, grâce à son concept d'e-ID reconnu par l'Etat se situe dans la tendance, resp. a tiré les leçons des expériences réalisées ces 15 dernières années par d'autres pays.
- Le concept suisse est par principe conforme à celui de l'eIDAS de l'UE.
- Le concept suisse est très souple et doit pouvoir subsister même en cas d'évolution technique et économique majeure.

Le concept présenté est tout à fait compatible avec le modèle de référence d'écosystème e-ID développé en Suisse (Fachhochschule, Wirtschaft, & Institut, 2015).

1.3.5 Compatibilité européenne

Si la possibilité d'utiliser à l'échelon international un document d'identité classique avec des données visibles est capitale, elle l'est tout autant pour l'e-ID. Il est utilisé comme document d'identité en ligne sur Internet, qui est par nature sans limites. Pour l'UE, qui s'est engagée à réaliser un marché intérieur européen unique et sans barrières, cette exigence revêt une importance particulière.

Le 23 juillet 2014, l'UE a donc adopté le Règlement (UE) N° 910/2014 (EU, 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). Outre la réglementation et la certification des prestataires en signature électronique et d'autres services de confiance, le règlement précise désormais la question de la notification et, par voie de conséquence, la reconnaissance mutuelle des systèmes nationaux d'identification électronique. Tous les Etats membres ont l'obligation d'autoriser également tout e-ID étranger de chaque système notifié lorsqu'ils demandent un e-ID pour accéder aux services officiels (art. 6). Cette obligation vaut même pour un Etat membre qui ne dispose pas lui-même d'un système e-ID avec notification.

La loi e-ID prévue ainsi que les systèmes e-ID reconnus par l'Etat en Suisse doivent être compatibles avec les systèmes e-ID européens (cf. également les Remarques liminaires).

1.4 Stratégies et mandat

1.4.1 Stratégie du Conseil fédéral pour une Suisse numérique

La stratégie «Suisse numérique» du Conseil fédéral d'avril 2016 (Bundesrat, 2016) a notamment pour objectif qu'«un système simple et sécurisé de gestion de l'identité soit disponible dans toute la Suisse». Sur la base de normes internationales, il s'agit d'élaborer une solution numérique de certification d'identités simple, sécurisée et sans barrières, valable dans toute la Suisse.

1.4.2 Stratégie suisse de cyberadministration

La «**Stratégie suisse de cyberadministration**» (E-Government Schweiz, 2007) (E-Government

Schweiz, 2015) a pour objectif de permettre aux acteurs économiques et à la population de régler des affaires importantes par voie électronique avec les autorités. Le projet prioritaire «B2.15 Identité électronique sans barrières reconnue à l'échelon national et dans l'UE» (E-Government Schweiz, 2015) est l'un des éléments de la mise en œuvre de cette stratégie du Conseil fédéral, qui doit être préparée par le biais du présent concept e-ID.

1.4.3 Mandat du Conseil fédéral pour des moyens d'identification reconnus par l'Etat

Conformément à la note de discussion du DFJP du 23 décembre 2015, le Conseil fédéral a pris connaissance le 13 janvier 2016 notamment des points-clés précisés ci-après pour le développement ultérieur des e-ID reconnus par l'Etat. Il a en outre chargé le DFJP de lui soumettre d'ici fin 2016 un projet pouvant être soumis à consultation:

- La Confédération définit un cadre juridique et normatif ainsi que l'organisation structurelle pour la reconnaissance par l'Etat des systèmes e-ID et des fournisseurs de services d'identité chargés de l'établissement. Il y a lieu de veiller à ce que ce cadre autorise ultérieurement une reconnaissance mutuelle des systèmes e-ID reconnus par l'Etat entre la Suisse et l'UE.
- Des systèmes e-ID pouvant être reconnus par l'Etat seront proposés par des fournisseurs de services d'identité (IdP) privés et publics. La Confédération renonce à publier son propre e-ID officiel.
- Des systèmes e-ID adéquats doivent pouvoir être reconnus par l'Etat conformément à l'un des trois niveaux de fiabilité.
- Des systèmes e-ID reconnus par l'Etat sont par principe accessibles à toute personne de nationalité suisse ainsi qu'aux ressortissants étrangers en Suisse.
- Les données d'identification personnelle figurant dans les registres fédéraux sont transmises par le biais d'une interface électronique aux IdP pour les systèmes e-ID reconnus par l'Etat.
- Un identifiant personnel unique (IPU) est créé pour l'identification d'une personne.
- Le NAVS13 doit être pris comme attribut d'identité, sa transmission à des tiers non autorisés à en faire un usage systématique devant toutefois être empêchée techniquement.
- Une simplification plus poussée des procédures en lien avec la transmission des données d'identification personnelle sera évaluée au cours des travaux conceptuels ultérieurs
- A titre de mesure de protection de l'investissement, tous les services fédéraux doivent par principe avoir l'obligation d'utiliser des systèmes e-ID reconnus par l'Etat dans leurs applications de cyberadministration nécessitant une authentification de l'utilisateur, et ce, au niveau de sécurité requis dans chaque cas.

1.5 Délimitations

Le présent concept ne porte pas sur d'autres services de confiance tels que la gestion des rôles et des droits dans l'espace numérique, les signatures ou cachets numériques ou les preuves de fonctionnalité de transactions à réaliser en ligne. Les systèmes e-ID ne sont qu'un outil pour la gestion électronique des identités (eGId) et donc seulement un élément central des systèmes de gestion de l'identité et de l'accès globaux. A la différence de la gestion des accès, qui doit être conçue de manière individuelle par chaque PU conformément à son offre de services, l'eGId peut être réalisée de manière interinstitutionnelle et donc très efficacement.

2 Concept des e-ID reconnus par l’Etat

2.1 Introduction

Les bénéficiaires directs des systèmes e-ID reconnus par l’Etat, conviviaux et pouvant être utilisés de manière variée sont les PU de l’économie privée et des autorités (Schweizerische Bundeskanzlei, 2011). Mais les détenteurs d’un e-ID bénéficient eux aussi d’une offre en ligne plus large grâce à leur e-ID.

L’approche suivie dans le présent concept pour l’exploitation de l’écosystème e-ID avec une solution appropriée pour l’e-ID se différencie des systèmes déployés jusqu’à présent dans d’autres pays européens (cf. 1.3.2.). Considérant que les systèmes e-ID mis en place jusqu’à maintenant ont presque tous été confrontés à des problèmes d’acceptation, une nouvelle approche pour la mise en œuvre semble non seulement judicieuse, mais également impérative. La force d’innovation du marché en matière de prestations numériques en général et de moyens d’identification électroniques en particulier ne doit pas être limitée par des solutions étatiques obtuses. La mise à disposition de systèmes e-ID reconnus par l’Etat en particulier ne doit pas être réalisée de manière monopolistique par l’Etat. Les modèles commerciaux doivent être développés et validés par le marché afin qu’ils puissent être acceptés. Les émetteurs et exploitants de systèmes e-ID fournissent des services de confiance permettant au marché numérique de fonctionner correctement.

Des systèmes e-ID fructueux (NSTIC- National Strategy for Trusted Identities in Cyberspace) …

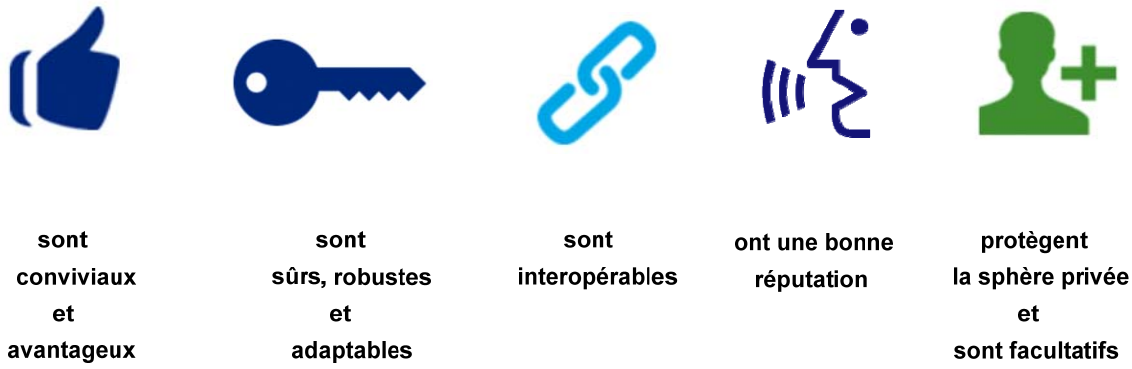


Schéma 3: Principes directeurs pour des systèmes e-ID fructueux

Dans le présent concept, les IdP et leurs systèmes e-ID respectent volontairement les prescriptions pour la reconnaissance par l’Etat et reçoivent ainsi le label de qualité officiel pour la reconnaissance, ce qui favorise la confiance, et, directement de l’Etat, des données d’identification personnelle des détentrices et détenteurs de leurs e-ID reconnus par l’Etat.

2.2 Objectifs

La contribution centrale de l’Etat à l’écosystème e-ID suisse est la mise à disposition d’un cadre juridique et normatif («Trust Framework») pour les systèmes e-ID reconnus par l’Etat. Ce cadre permet de constituer la base de confiance croissante requise par rapport aux prestations en ligne et régule le marché de manière à promouvoir l’interopérabilité, la reconnaissance internationale, la convivialité d’utilisation, l’applicabilité à large échelle, la sécurité et la protection de la sphère

privée.

Un e-ID reconnu par l'Etat peut être délivré

- à toutes les Suissesses et tous les Suisses qui disposent au moment de l'établissement de l'e-ID d'un document d'identité valable conformément à la loi fédérale sur les documents d'identité, et
- aux ressortissantes et ressortissants étrangers qui, au moment de l'établissement, disposent d'un titre de séjour valable conformément à la loi fédérale sur les étrangers (LEtr).

Les besoins différents en matière de sécurité de l'identification et de l'authentification des détentrices et détenteurs par les PU doivent être couverts par des niveaux de sécurité échelonnés des systèmes e-ID reconnus par l'Etat. Les niveaux de sécurité sont définis à trois niveaux correspondant à ceux définis pour les e-ID européens et américains.

Indépendamment de l'IdP d'établissement, les e-ID reconnus par l'Etat doivent pouvoir être utilisés par les PU de manière la plus variée possible. Le protocole d'utilisation est donc partout pareil et simple à intégrer dans les processus commerciaux des PU. A cet égard, la signature d'un accord d'utilisation d'un système e-ID entre les PU et un seul IdP doit suffire. L'interopérabilité pour les e-ID étrangers au système auprès d'une partie utilisatrice est réalisée par les IdP reconnus qui mettent leurs systèmes en réseau interopérable. Les e-ID reconnus par l'Etat à un niveau de sécurité suffisant doivent notamment pouvoir être utilisés auprès des autorités sans autre restriction lors de l'enregistrement ou de l'inscription à un service de confiance.

Par ailleurs, la Confédération exploite en tant que prestation un service d'attribut pour la transmission de données d'identification personnelle enregistrées par l'Etat aux IdP exploitant des systèmes e-ID reconnus par l'Etat. Les détentrices et les détenteurs enregistrent leurs données d'identification personnelle auprès de l'IdP qui leur délivre un e-ID. Après l'enregistrement, ils peuvent charger l'IdP auprès duquel leurs données d'identification personnelle sont enregistrées de fournir les attributs de leur identité civile à la partie utilisatrice de leur choix.

2.3 Principes

Les principes les plus importants de la solution proposée sont résumés ci-après:

- Bon nombre de services de confiance sont intégrés à la vie économique et sont fournis le plus souvent par des acteurs du marché privés et de droit public et non par l'Etat. Cela vaut logiquement aussi pour la mise à disposition de systèmes e-ID.
- L'Etat fait cependant office de régulateur pour un marché digne de confiance en reconnaissant officiellement des systèmes e-ID adéquats et des IdP prestataires. Les IdP sont alors tenus de respecter les standards et réglementations applicables en matière de sécurité, protection des données et interopérabilité. L'Etat renonce explicitement à émettre son propre e-ID officiel (p. ex. sur la carte d'identité), qui ferait concurrence à des solutions innovantes du marché.
- Un e-ID n'est pas un passeport, du moins du point de vue actuel, et il n'est donc acquis que lorsque l'e-ID est utilisé en ligne à des fins économiques, sociales ou administratives. Les systèmes e-ID doivent faire leurs preuves dans le jeu de l'offre et de la demande sur les marchés numériques. Cela signifie que les modèles commerciaux des IdP doivent être développés et validés par la pratique des marchés numériques afin d'être acceptés.
- Le marché des fournisseurs de service d'identité propose des e-ID de qualité variée en matière de fiabilité (sécurité) et de convivialité d'utilisation (seuil d'entrée bas, utilisation simple, nombreuses possibilités d'utilisation). L'Etat reconnaît des systèmes e-ID à trois niveaux de sécurité (le niveau faible est aussi désigné par le terme «argent», le niveau

substantiel, par le terme «or», et le niveau élevé, par «platine»), qui sont définis de manière équivalente aux niveaux de sécurité des systèmes e-ID de l'UE (EU, 2014).

- Par principe, tout ayant-droit en Suisse peut obtenir gratuitement un e-ID reconnu par l'Etat auprès d'un IdP reconnu par l'Etat de son choix. L'e-ID est choisi pour répondre à des besoins spécifiques en matière de niveau de sécurité et de convivialité d'utilisation. L'utilisateur doit par conséquent suivre le processus prescrit d'enregistrement et valider la transmission à l'IdP par le Service d'identité électronique suisse (SIE) des éléments permettant la reconnaissance par l'Etat, notamment ses données d'identification personnelle.
- L'IdP d'établissement est l'interlocuteur privilégié pour toute demande relative à l'e-ID, que ce soit pour les détentrices et détenteurs ou pour les PU avec lesquelles il a signé un accord d'utilisation. L'IdP met à disposition un support adéquat et des services de gestion des cas spéciaux (exception handling). Il répond des dysfonctionnements conformément aux obligations légales valables pour le niveau de sécurité de son système e-ID. L'IdP répond également de l'actualité et de l'assignation correcte des attributs d'identité ainsi que de leur livraison aux PU autorisées uniquement sur accord de la détentrice ou du détenteur.
- L'intégrité des données d'identification personnelle utilisées avec les e-ID reconnus par l'Etat est importante. La Confédération dispose déjà, avec le Système d'information relatif aux documents d'identité (ISA), le Système d'information central sur la migration (SYMIC) et le registre informatisé de l'état civil (Infostar), de registres de données d'identification personnelle tenus par l'Etat, qui se fondent sur une identification de la personne relevant de la puissance publique. Pour les systèmes e-ID reconnus, la Confédération fournit aux IdP des données d'identification personnelle enregistrées dans ces registres lors de la dernière identification par l'Etat, sous forme cryptée. L'étendue des attributs transmis est définie de manière différente pour les trois niveaux de sécurité (cf. 2.6.3). La date de l'identification fondamentale est fournie à chaque transmission. L'Etat répond des erreurs contenues dans ces données.
- La Confédération définit comme élément de l'identité civile qu'elle administre un identifiant personnel unique (IPU), qui est fourni conjointement et à chaque niveau de sécurité de l'e-ID avec les données d'identification personnelle transmises à l'IdP.
- Les exploitants de systèmes e-ID décident librement s'ils souhaitent obtenir une reconnaissance par l'Etat de leurs systèmes e-ID et bénéficier ainsi d'un avantage concurrentiel. Il n'y a aucune obligation à faire reconnaître par l'Etat un système e-ID. La Confédération définit la réglementation de manière à ce que les systèmes e-ID reconnus le soient aussi à l'échelon européen, c'est-à-dire qu'ils puissent être notifiés de la manière qui correspond au niveau de sécurité atteint.
- Les systèmes e-ID reconnus par l'Etat doivent être interopérables. L'interopérabilité est réalisée, d'une part, par des composants d'interface électronique standardisés simples (interface e-ID) auprès des services de confiance des PU et, d'autre part, par l'interopérabilité des systèmes e-ID entre eux. De plus, les IdP des systèmes e-ID reconnus doivent mettre à disposition de tous les autres IdP disposant de systèmes e-ID reconnus des interfaces standardisées pour l'utilisation interopérable de leurs e-ID. Des e-ID interopérables qui peuvent être utilisées auprès de toutes les PU conformément au niveau de sécurité exigé favorisent une diffusion rapide de systèmes e-ID reconnus dans l'écosystème e-ID.
- Les PU qui utilisent des systèmes e-ID reconnus par l'Etat disponibles sur le marché pour l'identification et l'authentification de leurs clients conformément à leurs exigences (confiance, sécurité, réglementations, cas commercial, responsabilité), peuvent alors compter

sur le respect de standards interopérables par tous les exploitants de systèmes e-ID. Ils répondent toutefois de l'utilisation conforme des e-ID par leur service de confiance lors de l'identification ou de l'authentification des détentrices et détenteurs.

- Les ayants-droit décident librement s'ils souhaitent obtenir un e-ID reconnu par l'Etat. Pour une reconnaissance par l'Etat de leur e-ID, ils doivent toutefois donner à l'IdP d'établissement l'autorisation expresse d'obtenir auprès du service d'attribut officiel des données d'identification personnelle correspondant au niveau de sécurité. En leur qualité de détentrice ou détenteur, ils peuvent décider au cas par cas si et quels attributs de l'identité civile doit être transmis de l'IdP à la PU.
- Les détentrices et détenteurs ont l'obligation d'utiliser leur e-ID avec précaution et de manière sûre dans leur sphère d'influence. Ils répondent des dommages causés par une utilisation inadéquate. Les PU également répondent des dommages résultant de l'utilisation erronée des e-ID lors de l'identification ou de l'authentification de leurs clients.

La Confédération met à disposition l'infrastructure requise pour la mise en œuvre de la réglementation légale et pour le service visant à transmettre les données d'identification personnelle (cf. ch. 3). Elle gère également un service administratif, intitulée **Organisme de reconnaissance des fournisseurs d'identité (ORFI)**, chargé de réaliser le processus de reconnaissance des IdP et systèmes e-ID reconnus par l'Etat et d'exercer la surveillance sur les IdP reconnus. Elle gère en outre une unité administrative, intitulée **Service d'identité électronique suisse (SIE)**, qui exploite un système d'information pouvant consulter des données d'identification personnelle dans les registres de personnes officiels correspondants tenus par la Confédération et les transmettre, avec l'accord des détentrices et détenteurs, à des IdP reconnus par l'Etat exploitant des systèmes e-ID.

2.4 Architecture et processus

La situation de départ est la création d'une relation commerciale en ligne entre une détentrice ou un détenteur et une PU. En matière de gestion électronique des identités (eGId), quatre rôles sont identifiés: celui de la détentrice ou du détenteur, celui des PU identifiant et authentifiant les détentrices et détenteurs, celui du fournisseur de services d'identité (IdP), qui exploite le système e-ID, et celui de l'Etat régulateur. Ce dernier définit les règles de collaboration entre les parties concernées ainsi que les exigences envers les systèmes e-ID reconnus par l'Etat, de manière à ce qu'une base de confiance sécurisée en résulte. En tant que tel, l'Etat est également l'administrateur de l'identité civile de toutes les personnes dans l'écosystème e-ID. Dans l'écosystème e-ID, les PU délèguent les processus d'identification et d'authentification électronique des détentrices et détenteurs d'un e-ID aux IdP. Chaque PU exploite en sus une application informatique en tant que service de confiance, qui est liée à un système e-ID d'un IdP par le biais d'une interface e-ID. Après réalisation d'un mandat pour un service d'identité, le système e-ID fournit au service de confiance ayant attribué le mandat le résultat de l'identification ou de l'authentification.

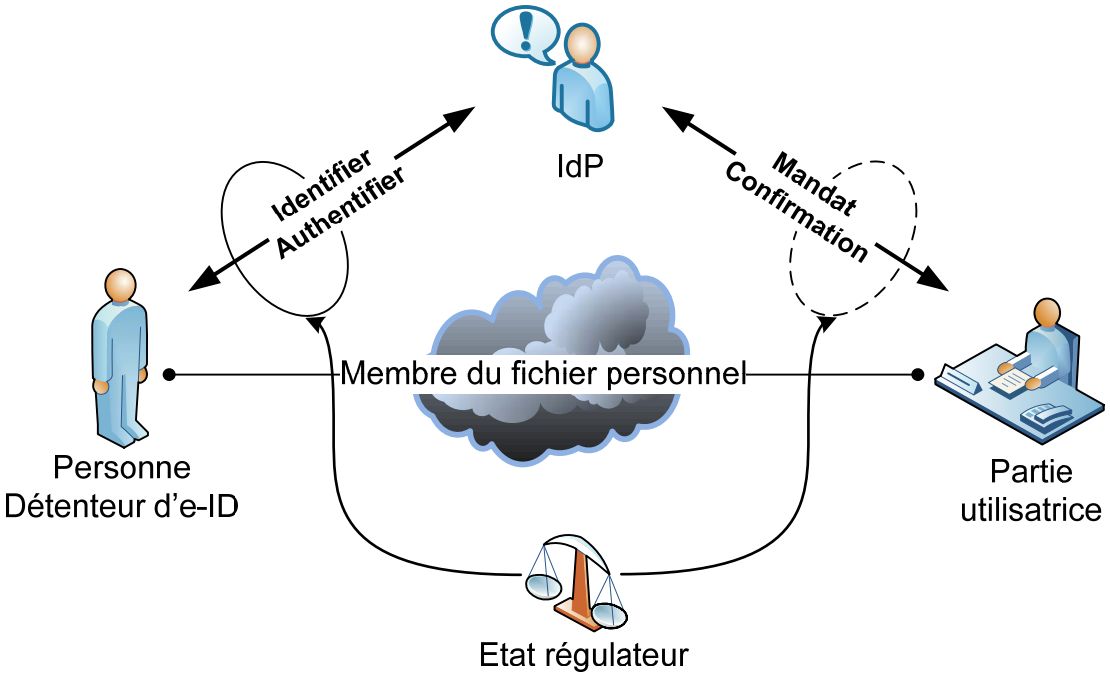


Schéma 4: Les rôles en matière de gestion électronique des identités

2.4.1 Systèmes de gestion électronique des identités

Les systèmes numériques d'eGId liés aux rôles sont les suivants:

- L'authentifiant, le plus souvent sous la forme de l'appareil personnel[16] de la détentrice ou du détenteur intégrant l'application e-ID sûre et digne de confiance. Cette application a un identifiant, une fonction d'authentification avec les données de référence pour l'identification de la détentrice ou du détenteur, un secret fermement lié à l'identifiant et une interface de communication sécurisée avec le système central de l'IdP. Facultativement, l'affichage du support peut également être sécurisé sous le contrôle de l'application e-ID installée.
- Le système de gestion et de prestation des PU pour le règlement en ligne des opérations en tant que service de confiance avec une interface intégrée et standardisée avec le système e-ID. Cette interface e-ID est composée de processus et de protocoles standardisés, qui sont utilisés lors de l'enregistrement ou de l'annonce d'une détentrice ou d'un détenteur auprès du service de confiance et qui génère le mandat pour le service d'identité. Elle reçoit de la détentrice ou du détenteur et du service de confiance les indications requises pour le mandat, qu'elle transmet au système e-ID de l'IdP. En retour, elle reçoit le ticket de réponse avec le résultat du mandat exécuté et transmet le résultat au service de confiance.
- Les composants du système e-ID de l'IdP gèrent tous les attributs d'identité enregistrés[17] des détentrices et détenteurs, reçoivent les mandats des services de confiance par le biais des interfaces e-ID, réalisent au moyen des e-ID sur le terrain les identifications et authentifications sûres des détentrices et détenteurs et établissent les tickets de réponse

16 L'authentifiant est un terme à comprendre au sens large (en anglais authenticator ou précédemment token), qui est susceptible de ne pas uniquement se rapporter aux appareils électroniques. L'important est qu'il permette de fournir une preuve de l'identité du détenteur en procédant au contrôle personnel de celui-ci.

17 L'ensemble des attributs d'identité d'une détentrice ou d'un détenteur que l'IdP peut obtenir auprès de diverses sources est désigné par le terme d'identité partielle (cf. les explications à ce sujet en annexe).

pour les services de confiance. Chaque IdP dispose d'une interface sécurisée avec le service d'attribut officiel et d'un service pour la réalisation de l'interopérabilité avec les autres IdP reconnus. Il tient en outre une liste pouvant être consultée en ligne des e-ID provisoirement bloqués et de ceux désactivés de manière permanente.

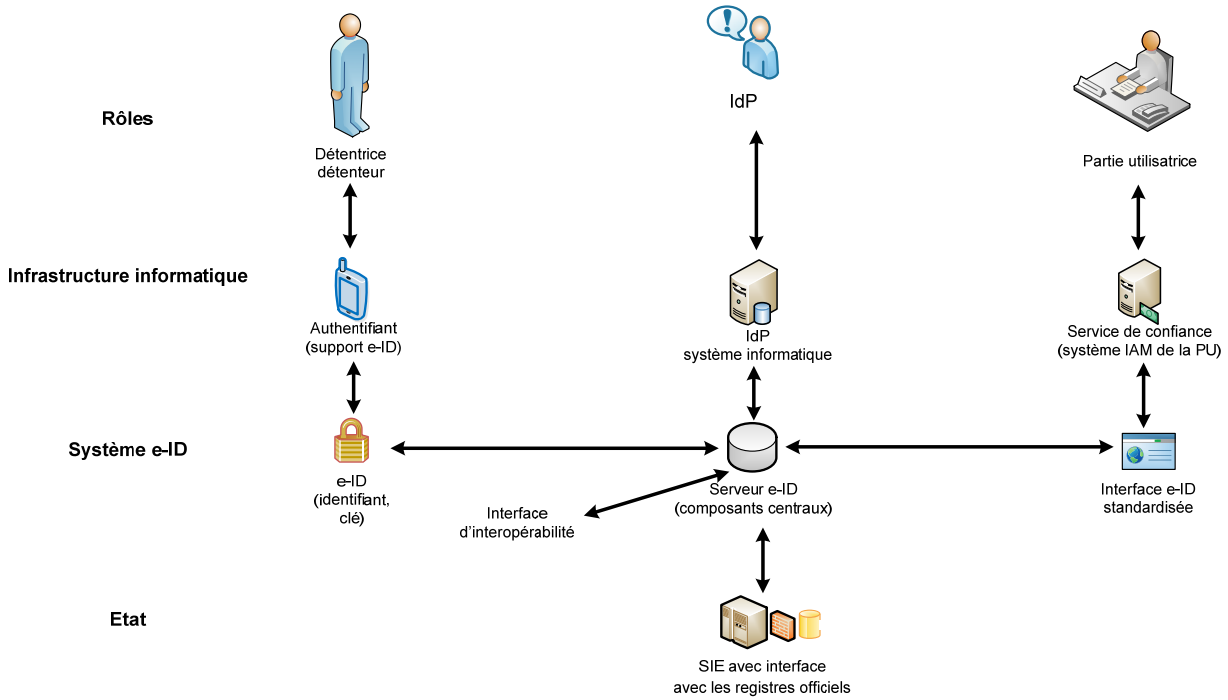


Schéma 5: Niveaux systémiques et composants eGId assignés

2.4.2 Authentifiant et e-ID

L'élément central d'un système e-ID est l'authentifiant, qui garantit le lien entre la personne physique et l'identité qui a été saisie pour elle dans le système e-ID. L'authentifiant peut revêtir diverses formes. Il peut s'agir, par exemple, d'un élément de sécurité intégré à une carte en plastique (microprocesseur), d'une application sur une carte SIM, d'une clé USB ou d'un appareil spécial, mais des variantes de logiciels, tels que des certificats liés à un mécanisme de déverrouillage ou d'autres formes sont envisageables. En principe, la combinaison d'un identifiant d'utilisateur et d'un mot de passe peut être considérée comme une forme abstraite d'un authentifiant. L'important est que l'authentifiant soit lié de manière univoque à une personne au cours d'un processus d'enregistrement, qu'il soit représenté par un identifiant intégré et qu'il puisse entrer en liaison avec le serveur e-ID de manière sûre. L'identifiant peut alors être défini différemment par secteur, PU ou période, mais doit toujours pouvoir indubitablement être assigné à un authentifiant dans le contexte du système e-ID.

Lors de l'enregistrement, l'authentifiant est, d'une part, lié à une personne, d'autre part (du côté du serveur), à ses données d'identité, ce qui en fait un e-ID. Ce n'est qu'avec l'e-ID mis ainsi à disposition que la personne enregistrée peut se faire authentifier et identifier numériquement.

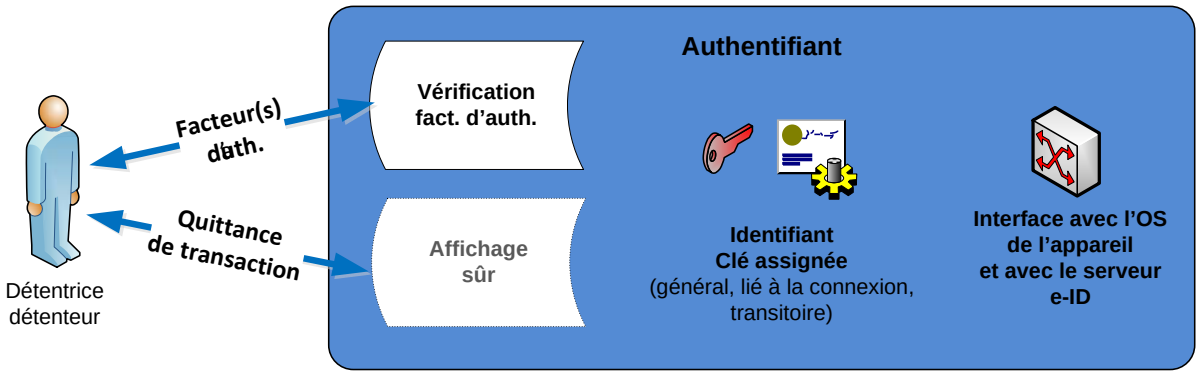


Schéma 6: Un e-ID est un authentifiant enregistré pour une personne avec les données d'identité assignées à la personne.

2.5 Cycles de vie dans le système e-ID

Chaque système e-ID dispose, d'une part, d'un cycle de vie en tant que système, d'autre part, administre le cycle de vie des e-ID et celui du client e-ID auprès des PU. A cette fin, des processus organisationnels et informatiques doivent être implémentés pour chacun des trois cycles de vie. A des fins d'illustration, ces cycles et processus sont décrits dans un système type. Dans la pratique, la diversité de ces cycles de vie et processus devrait vraisemblablement être importante, cette diversité n'étant restreinte que par des exigences légales impératives.

La description du système type est fondée sur le principe selon lequel l'e-ID est une application pour smartphone, qui peut être installée dans un espace sécurisé de l'appareil (TEE ou application SIM).

2.5.1 Constitution et exploitation d'un système e-ID

Un IdP souhaitant exploiter un système e-ID reconnu par l'Etat doit satisfaire les conditions d'une reconnaissance par l'Etat. Pour ce faire, il doit:

- Avoir ou ouvrir un siège commercial en Suisse et employer du personnel qualifié et à la réputation irréprochable pour l'exploitation du système e-ID;
- Prouver disposer de ressources financières suffisantes pour couvrir d'éventuels dommages pouvant résulter d'une violation de sa responsabilité;
- Mettre en place une infrastructure informatique certifiée selon des profils de protection idoines pour le système e-ID, avec sauvegarde des données en Suisse exclusivement. Cette infrastructure doit notamment comprendre les éléments suivants:
  - Des processus techniques et organisationnels certifiés et sûrs pour l'enregistrement de futurs détentrices et détenteurs d'e-ID et pour le traitement des mandats d'identification et d'authentification.
  - Une application e-ID sûre et certifiée avec un authentifiant pour l'identification de la détentrice ou du détenteur. Selon le niveau de sécurité visé pour le système e-ID, l'authentifiant intégré doit pouvoir identifier une personne par le biais de deux facteurs d'authentification indépendants (niveau or) ou par le biais de deux facteurs dont un de nature biométrique (niveau platine). L'application est développée pour les espaces sécurisés[18] des divers systèmes d'exploitation des smartphones sur lesquels l'e-ID peut être installé;

[18] Dans les smartphones modernes, les espaces sécurisés sont réalisés par le biais d'un Trusted Execution Environment (TEE) ou des Secure Elements (SE) pouvant être utilisés [58] [47]

- Un système de répartition sûr pour les applications e-ID avec la définition des identifiants e-ID dans un format standardisé, lié de manière fixe après installation avec le smartphone faisant office de support. Les identifiants e-ID doivent disposer d'une partie indicative permettant leur assignation par tous les systèmes e-ID de l'IdP d'établissement[19];
- Une application standardisée du client e-ID en tant qu'interface avec les services de confiance des systèmes IAM des PU, de sorte que ce soient toujours les mêmes protocoles d'utilisation qui se déroulent auprès de toutes les PU en cas d'utilisation d'un e-ID;
- Une interface d'interopérabilité standardisée avec tous les systèmes e-ID reconnus par l'Etat existants, à un niveau de sécurité similaire ou supérieur;
- Une interface standardisée sûre avec canal de communication protégé vers le SIE pour la transmission et la mise à jour périodique des données d'identification personnelle;
- Un service web pour la mise à disposition de listes de blocage et de révocation des e-ID sur le terrain;

- Une offre de soutien et d'assistance en ligne proposant, en fonction de la situation, des explications et une aide pour chaque action pouvant être réalisée avec l'e-ID.
- Un service clients auquel les dérangements, les abus et la perte d'un e-ID peuvent être signalés.

S'il satisfait ces conditions, l'IdP demande à l'ORFI sa reconnaissance par l'Etat, les preuves étant fournies principalement sous forme de certifications par profils de protection et rapports d'audit attestant que les conditions de reconnaissance sont remplies. Après avoir examiné ces moyens de preuve, l'ORFI reconnaît l'IdP ainsi que le ou les systèmes e-ID annoncés au niveau de sécurité atteint. L'ORFI publie les IdP et systèmes e-ID reconnus de même que les indicatifs assignés aux parties identifiantes des identifiants e-ID.

L'IdP reconnu par l'Etat doit passer tous les trois ans au moins un audit prouvant qu'il continue à satisfaire les conditions de la reconnaissance de ses systèmes e-ID; les rapports d'audit correspondants doivent être remis à l'ORFI. Celui-ci prolonge la durée de validité de la reconnaissance si le rapport d'audit confirme que lesdites conditions sont satisfaites et si l'IdP a réglé les émoluments dûs pour la transmission des données d'identification personnelle.

La reconnaissance par l'Etat peut être retirée si l'IdP enfreint les dispositions légales, s'il ne satisfait plus les conditions de reconnaissance, s'il arrête son activité commerciale ou s'il fait faillite. Dans un tel cas, le système e-ID peut être repris par un autre IdP reconnu par l'Etat.

Un IdP peut proposer ses systèmes e-ID reconnus par l'Etat aux PU ainsi qu'aux personnes autorisées à obtenir un e-ID. L'établissement d'un e-ID devrait être gratuit pour la personne concernée. L'IdP peut toutefois appliquer un modèle commercial de son choix pour la réalisation des mandats d'identification et d'authentification. La Confédération précise toutefois des plafonds pour les frais supplémentaires pouvant être facturés en cas d'utilisation de services d'interopérabilité. Tous les services fédéraux qui exigent une identification ou une authentification pour leurs services en ligne doivent accepter l'e-ID d'un système e-ID reconnu à un niveau de sécurité suffisant comme moyen d'identification. Les services fédéraux concernés doivent

[19] De manière similaire à l'identification d'un éditeur de cartes de crédit par une partie du numéro de carte de crédit, l'identifiant e-ID contient une partie qui permet d'identifier l'IdP d'établissement et le système e-ID. Cet identifiant facilite la réalisation de l'interopérabilité entre les systèmes e-ID.

tous signer un accord correspondant[20] avec au moins IdP, de sorte que tous puissent utiliser des e-ID reconnus par l'Etat et du niveau de sécurité appropriés.

Dès que la Suisse signe un tel traité international avec l'UE, un IdP peut faire notifier à l'UE, par l'intermédiaire de la Confédération, un système e-ID qu'il exploite et qui est établi sur le marché avec une part de marché suffisante. Le détail des conditions correspondantes ne pourra être défini que dans le cadre des négociations internationales.

2.5.2 Cycle de vie de l'utilisation d'un système e-ID

Si une PU souhaite utiliser pour son système IAM un e-ID reconnu par l'Etat à des fins d'identification et d'authentification des membres de son fichier personnel, elle doit conclure avec au moins un IdP un accord d'utilisation pour un système e-ID du niveau de sécurité requis. Elle peut choisir librement l'IdP prestataire et se décider en fonction de considérations d'ordre commercial. Les interfaces techniques et organisationnelles par contre sont dans une large mesure standardisées pour tous les systèmes e-ID proposés. Pour qu'une PU puisse utiliser un e-ID, elle doit intégrer un client e-ID à son service de confiance qui propose les fonctions suivantes:

- Un portail d'enregistrement et d'annonce standardisé pour les détentrices et détenteurs d'e-ID pour la saisie de l'identifiant e-ID ou d'un pseudonyme assigné par l'IdP à l'identifiant. En cas de nouvelle admission d'une détentrice ou d'un détenteur dans le fichier personnel de la PU (enregistrement), le portail indique en plus à la détentrice ou au détenteur quels attributs d'identité sont exigés auprès de l'IdP pour la transmission.
- Une interface standardisée avec le service de confiance qui réceptionne les mandats d'enregistrement ou de connexion du service de confiance et qui émet les tickets de réponse établis sur la base des composants du système e-ID. Chaque mandat et chaque ticket est défini dans un format standardisé et contient toujours l'identifiant e-ID correspondant resp. l'identifiant déduit appartenant au mandat. L'interface e-ID est typiquement un service web avec les éléments de sécurité nécessaires pour la transmission du mandat et la réception des réponses.
- Réception des données d'identification personnelle fournies par le système e-ID sur demande du service de confiance et avec l'accord de la détentrice ou du détenteur sous forme standardisée et sécurisée. La détentrice ou le détenteur donne son accord en saisissant un code à usage unique qu'elle ou il reçoit de l'IdP et qu'elle ou il renvoie à l'IdP par le client e-ID en passant par le portail d'enregistrement du service de confiance.

[20] Une procédure d'appel d'offres public sera ouverte, à laquelle tous les IdP disposant d'un système e-ID du niveau de sécurité approprié pourront participer.

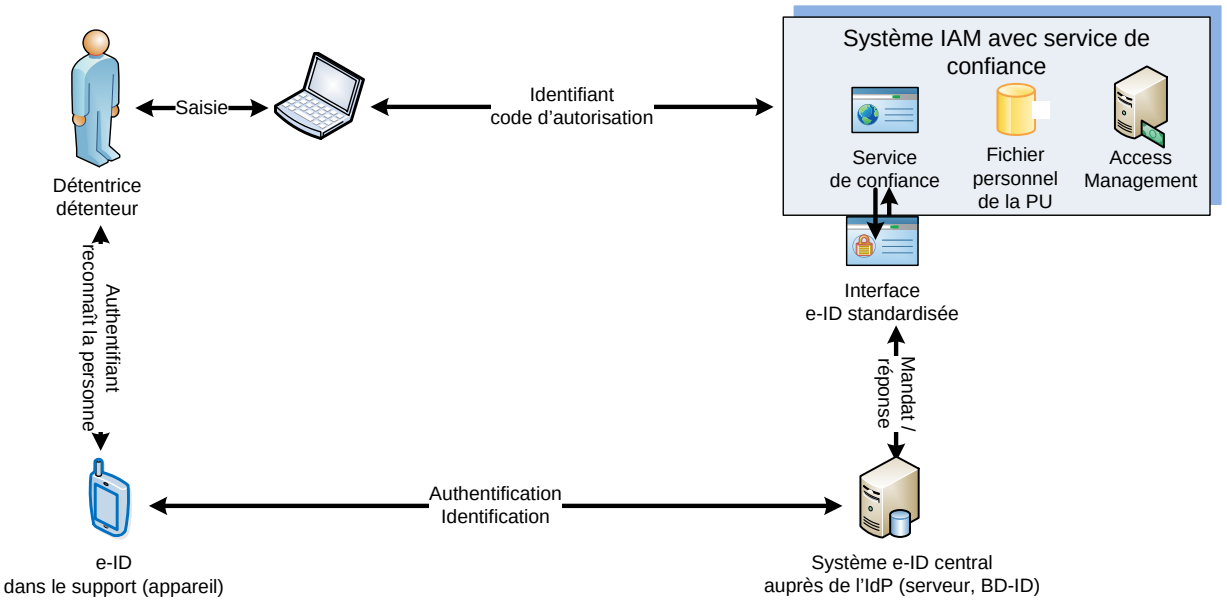


Schéma 7: Interfaces du système e-ID

Le service de confiance est modifié par la PU en cas de besoin pour répondre au développement du propre système IAM mais également pour améliorer l'acceptation de nouvelles générations d'e-ID. Le service de confiance a l'obligation d'accepter tous les e-ID du niveau de sécurité exigé, indépendamment de l'IdP d'établissement. L'interface e-ID est standardisée de manière à pouvoir traiter tous les identifiants e-ID, tickets et codes de réponse.

Une PU peut facturer aux détentrices et détenteurs les frais directs résultant de l'utilisation de l'e-ID auprès de son service de confiance.

2.5.3 Cycle de vie de l'e-ID

Pour la mise en service et l'utilisation d'un e-ID, qui est conçu pour l'un des trois niveaux de sécurité selon le système e-ID, les étapes suivantes sont réalisées:

- **Etablissement d'un authentifiant e-ID** L'établissement d'un authentifiant est effectué de manière intégrée au support ou en tant qu'application pour un terminal idoine du futur détenteur et de la future détentrice, voire seulement sous forme d'une instruction procédurale que la détentrice ou le détenteur doivent savoir, si elle peut utiliser une infrastructure générale disponible en tant qu'authentifiant. L'authentifiant e-ID dispose d'interfaces sécurisées permettant la saisie de facteurs d'authentification, la communication avec les composants centraux du système e-ID (serveur e-ID) auprès de l'IdP et l'affichage des codes à usage unique. Dans la mesure du possible, l'authentifiant peut même gérer une option confortable d'affichage et de saisie sécurisée et permettre ainsi certaines transactions sécurisées. Après installation sûre dans l'appareil, l'authentifiant e-ID génère un identifiant unique et des éléments de sécurité pour la communication avec le serveur e-ID de l'IdP. A titre alternatif, l'authentifiant e-ID peut être fournie dans un support sécurisé dédié avec identifiant préinstallé et éléments de sécurité. L'authentifiant e-ID est prêt pour l'enregistrement de la détentrice ou du détenteur lorsque la communication sécurisée est établie avec le serveur e-ID et l'identifiant est enregistré dans le serveur e-ID central.

- **Enregistrement de la détentrice ou du détenteur auprès de l'IdP** L'enregistrement de la détentrice ou du détenteur auprès de l'IdP passe par l'établissement d'une liaison fixe entre la personne et l'authentifiant e-ID et l'identification initiale de la personne qui a réalisé une liaison avec l'e-ID, par la saisie de ses données d'identification personnelle.
  - La liaison est instaurée par la saisie d'attributs personnels en tant que données de référence pour les facteurs d'authentification, à savoir
    - Définition d'un élément secret, par exemple par la saisie d'un code NIP par la détentrice ou le détenteur,
    - Saisie de caractéristiques biométriques de la détentrice ou du détenteur dans l'authentifiant e-ID, la mesure permanente de plusieurs caractéristiques comportementales typiques par les capteurs de l'appareil, par exemple la mesure des mouvements lors de la saisie sur un écran tactile, pouvant compter comme caractéristique biométrique,
    - Prise de possession de l'authentifiant e-ID au titre d'appareil personnel sevrant de support. Une smartcard personnelle par exemple, mais aussi un smartphone personnel avec carte SIM enregistrée, est un tel support personnel qui est toujours en possession de la détentrice ou du détenteur.
  - L'identification initiale est effectuée par la saisie de données d'identification personnelle attribuées avec un niveau de sécurité défini à la personne qui a généré la liaison avec l'authentifiant e-ID. Cela peut se produire à l'occasion d'une présentation en personne auprès d'un service de l'IdP habilité à procéder à l'identification mais aussi par identification vidéo. Il est alors impératif que la personne prouve que l'authentifiant e-ID la reconnaît avec les facteurs d'authentification définis et qu'elle atteste son identité civile au moyen d'un document d'identité officiel. A cette étape, il est vérifié que les facteurs d'authentification personnels, intégrés à l'authentifiant e-ID, sont correctement affectés aux attributs de l'identité civile. Le serveur central e-ID enregistre les données d'identification personnelle avec l'identifiant e-ID remplaçant les attributs personnels, qui sera vérifié par l'authentifiant. Normalement, aucun autre attribut personnel[21] ne sera saisi dans le serveur e-ID central.
- **La consultation de données officielles d'identification personnelle** Dans le cas des e-ID reconnus par l'Etat, l'affectation de l'identité civile à l'e-ID, qui doit en principe aussi être effectuée pour les e-ID non reconnus par l'Etat, est renforcée. A l'occasion de l'identification initiale de la personne, l'IdP saisit le numéro du document d'identité présenté ainsi que les indications pour l'établissement d'une connexion avec la détentrice ou le détenteur par un canal de communication indépendant. Il s'agit de préférence d'un numéro de téléphone, mais il peut aussi s'agir d'une adresse e-mail, voire d'une adresse postale. L'IdP transmet ces deux renseignements au SIE et demande que les données officielles d'identification personnelle lui soient remises, conformément aux numéros du document d'identité et au niveau de sécurité de l'e-ID. Le SIE demande ensuite par le biais du canal de communication indépendant à la détentrice ou au détenteur son accord pour transmettre les données requises. Pour cela, il lui envoie un code à usage unique pour confirmer son accord, que la détentrice ou le détenteur peut communiquer à l'IdP. L'IdP transmet la confirmation de l'accord au SIE, qui lui envoie les données officielles d'identification personnelle de la détentrice ou du détenteur, y compris l'IPU assigné par l'Etat. L'IdP active ensuite l'e-ID. Si la détentrice ou le détenteur refuse de donner son accord, l'e-ID peut malgré tout être activée, en fonction de la politique commerciale de l'IdP. Elle n'est toute-

[21] Contrairement aux données d'identification personnelle, les attributs personnels sont des attributs non publics de la personne, par exemple des données biométriques (cf. les explications en annexe).

fois alors pas un e-ID reconnu par l'Etat, ce qui doit être communiqué à chaque identification ou authentification ultérieure au service de confiance mandant. Si, à l'occasion de l'introduction d'e-ID reconnus par l'Etat, un système e-ID existant est dès lors reconnu par l'Etat, les e-ID du système déjà activés peuvent être exploités comme e-ID reconnus par l'Etat si seul le retrait des données d'identification personnelle est en suspens pour la reconnaissance par l'Etat. Le processus de retrait doit alors être effectué dans un certain délai.

- **Enregistrement de la détentrice ou du détenteur auprès d'une PU** Avec un e-ID reconnu par l'Etat et activé, une détentrice ou un détenteur peut s'enregistrer en ligne auprès de tous les services de confiance de PU acceptant des e-ID reconnus par l'Etat, à condition que le niveau de sécurité de l'e-ID soit suffisant pour le service de confiance. Elle ou il demande depuis le portail du service de confiance de la PU un nouvel enregistrement dans le fichier personnel de la PU. Le service de confiance de la PU affiche la page d'enregistrement avec les indications sur les informations d'inscription requises. La détentrice ou le détenteur indique dans le formulaire d'inscription[22] l'identifiant de l'e-ID[23] et demande un enregistrement. Elle ou il démarre l'authentifiant e-ID à ce moment, si celui-ci n'est pas de toute façon actif en permanence. Une attestation d'authentification peut alors éventuellement déjà être fournie parallèlement à l'identifiant, en fonction de l'e-ID. Le service de confiance établit un **mandat d'enregistrement** pour l'e-ID désigné par l'identifiant et envoie celui-ci à son IdP par le biais de l'interface e-ID. Celui-ci vérifie s'il gère cet e-ID et s'il doit transmettre le mandat en question à un autre IdP compétent par le biais de l'interface d'interopérabilité. L'IdP compétent demande à la détentrice ou au détenteur de s'authentifier par rapport à l'e-ID. Si la détentrice ou le détenteur s'est authentifié-e, un message lui est envoyé avec prière d'autoriser la transmission des données exigées par le service de confiance[24]. Le message contient un code à usage unique pour confirmer l'autorisation. En fonction de la situation de communication, la détentrice ou le détenteur donne son accord directement par le biais de son e-ID ou en saisissant le code à usage unique dans le formulaire correspondant du service de confiance, qui le transmet à l'IdP à titre de complément au mandat d'enregistrement. Si l'accord est donné, l'IdP transmet un ticket de réponse à l'interface e-ID du service de confiance avec la confirmation de l'identification ainsi que les données validées pour la PU. Si la validation n'a pas lieu, l'IdP envoie après échéance d'un délai (timeout) uniquement un ticket de réponse avec la confirmation de l'authentification. La PU doit alors décider si elle souhaite ou non enregistrer dans son fichier personnel le nouveau membre sous le seul identifiant indiqué[25]. Elle ne pourrait que constater à chaque fois qu'il s'agit toujours de la même détentrice ou du même détenteur en cas de connexion ultérieure avec cet e-ID, sans disposer de données de l'identité civile de la personne.
- **Nouvelle annonce auprès d'une PU (connexion)** La détentrice ou le détenteur s'annonce au service de confiance sur un portail avec l'identifiant e-ID ou le pseudonyme correspondant et indique, si cela est exigé, d'autres données identifiantes. Elle ou il démarre pour cela l'authentifiant e-ID si l'e-ID n'est pas de toute façon actif en permanence. Le service de confiance établit pour son IdP un **mandat de connexion**. Celui-ci vérifie s'il gère cet e-ID et s'il doit transmettre le mandat en question à l'IdP compétent par le biais

---

22 Les formulaires d'inscription des PU devront satisfaire certaines exigences en matière de standardisation de manière à ce que le schéma de base soit identique pour tous les portails.

23 Selon le portail du service de confiance, la saisie est effectuée grâce à un clavier ou par voie électronique si l'e-ID et le support du portail disposent par exemple d'une interface NFC.

24 Pour administrer son fichier personnel, la PU peut demander des attributs des données officielles d'identification personnelle mais aussi d'autres attributs gérés par l'IdP.

25 L'identifiant peut alors être publié sous forme déduite de manière sectorielle ou transitoire. Il ne serait alors identifiant que pour la PU et évtl. pendant un certain laps de temps uniquement.

de l’interface d’interopérabilité. L’IdP compétent demande à la détentrice ou au détenteur de s’authentifier par rapport à l’e-ID. En cas d’authentification réussie, l’IdP envoie un ticket de réponse au client e-ID auprès du service de confiance avec la confirmation de l’authentification.

- **Interopérabilité de l’e-ID** La remise interopérable des mandats de la PU à l’IdP et des tickets de réponse de l’IdP à la PU dans l’écosystème e-ID est effectuée dans un format fixe et de manière sécurisée par le biais de services web. Les messages contiennent l’identifiant unique de l’IdP compétent. Un IdP qui reçoit un tel message examine s’il est le bon destinataire et, le cas échéant, il envoie le message au bon destinataire (IdP) pour traitement. Il suffit donc que l’infrastructure d’interopérabilité relie tous les IdP reconnus. En cas de standardisation, des services d’interfaces supplémentaires sont inutiles. A défaut d’introduction de certains standards, l’interopérabilité pourrait encore être réalisée par le biais d’un hub central, ce qui engendre des frais supplémentaires et en principe évitables, qui devraient, en tous les cas à moyen terme, être assumés par les IdP.
- **Suppression d’un e-ID par la détentrice ou le détenteur** La détentrice ou le détenteur peut demander à l’IdP la suppression de son e-ID. Pour cela, elle ou il se connecte au service clients en ligne de l’IdP et lui présente une demande correspondante. L’IdP demande une authentification avec l’e-ID et envoie après authentification fructueuse un code à usage unique qui s’affiche sur l’e-ID. Avec ce code, la détentrice ou le détenteur peut confirmer la suppression. L’IdP désactive alors l’e-ID et supprime de son fichier personnel les données saisies sur la détentrice ou le détenteur. La suppression de l’e-ID peut également être demandée en cas d’abus constaté ou de perte. Dans ce cas, la détentrice ou le détenteur doit s’authentifier par un autre biais comme ayant-droit.
- **Verrouillage** Un verrouillage temporaire ou permanent de l’e-ID par l’authentifiant ou par l’IdP peut être déclenché par trois événements différents:
    - La détentrice ou le détenteur tente à plusieurs reprises de s’authentifier auprès de la fonction d’authentification de l’e-ID de manière erronée. Si le nombre maximum d’essais autorisés est dépassé, l’e-ID est verrouillé en local sur le support. Selon le type d’e-ID et la politique de sécurité de l’IdP, un tel verrouillage peut être annulé ou a un caractère permanent.
    - Si l’IdP est amené à penser de manière crédible par un biais quelconque qu’un certain e-ID est corrompu ou en de mauvaises mains, il le verrouille et place l’identifiant de l’e-ID sur une liste des blocages. Il informe la détentrice ou le détenteur en conséquence.
    - Lors de la vérification périodique de la validité de l’IPU, l’IdP constate qu’un certain IPU a été signalé par le SIE comme étant temporairement ou de manière permanente non valable. Si un e-ID a été établi pour une personne avec cet IPU, il doit la bloquer ou la révoquer et placer l’identifiant e-ID correspondant sur la liste de blocage.
- **Réactivation** L’IdP peut annuler le verrouillage et réactiver l’e-ID si la détentrice ou le détenteur est en mesure de prouver que l’e-ID fonctionne correctement et qu’il est en sa possession. L’e-ID doit être redémarré afin de procéder au déverrouillage en local.

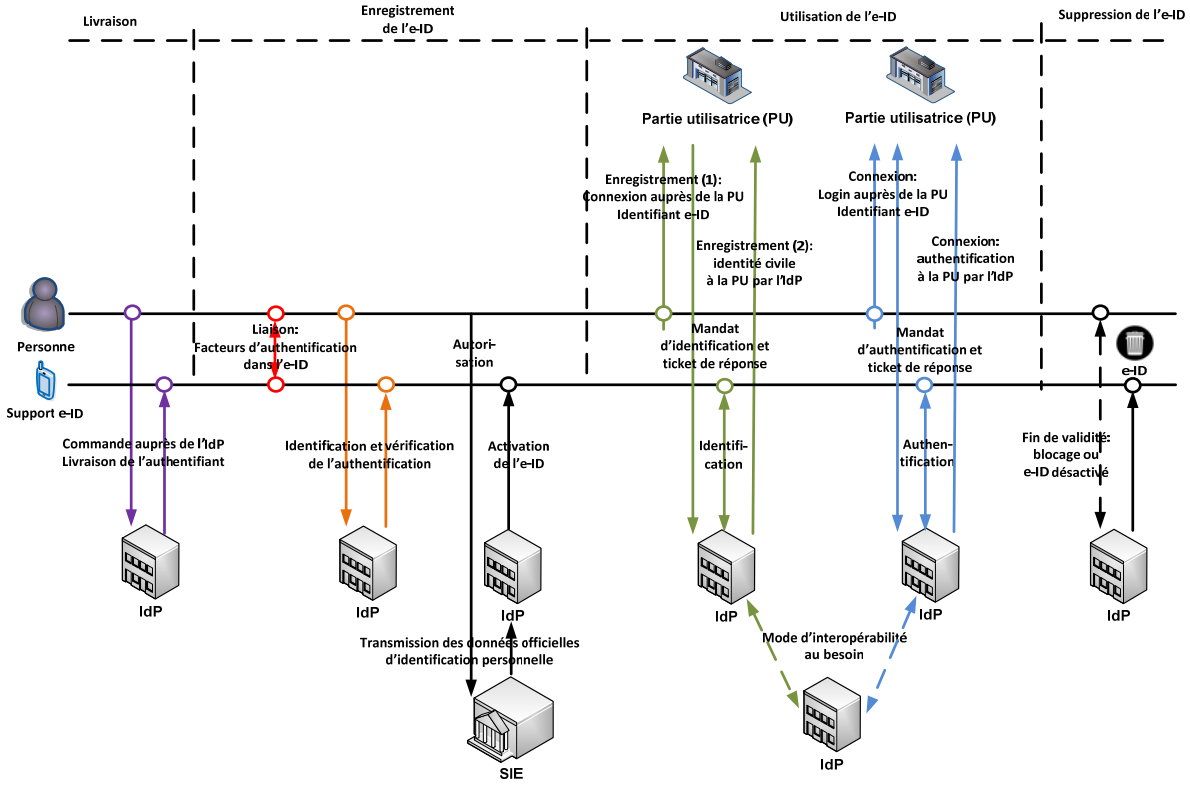


Schéma 8: Processus du cycle de vie de l'e-ID avec établissement (livraison, enregistrement), utilisation et révocation

Niveau de sécurité de l'e-ID	**Argent**	**Or**	**Platine**
Etape 1: Commander, recevoir et installer l'authentifiant de l'e-ID	Envoi de l'authentifiant e-ID par courrier postal comme unité physique ou en ligne comme application Installation automatique sur le support Test de fonctionnement avec l'identifiant e-ID à l'IdP		
Etape 2: enregistrement auprès de l'IdP (1) Liaison de la personne à l'e-ID	Saisie d'un facteur d'authentification (évtl. possession seul.)	Saisie de 2 facteurs d'authentification	Saisie de 2 facteurs d'authentification avec biométrie
Etape 3: enregistrement auprès de l'IdP (2) Vérification de l'identité de la personne avec validation de la validité du document d'identité, identité de la personne et liaison de la personne à l'e-ID	Numéro du document d'identité	Présence personnelle ou identification vidéo sur la base du document d'identité	
	-		Vérification photo du visage
Etape 4: Enregistrement auprès de l'IdP (3) Transmission des données d'identification personnelle du SIE à l'IdP	Demande d'autorisation par un canal indépendant Code d'autorisation à l'IdP par la détentrice ou le détenteur Livraison des données d'identification personnelle à l'IdP		

Etape 5 Activer l'e-ID	L'IdP active l'e-ID pour utilisation Communication à la détentrice ou au détenteur

Tableau 1: établissement d'un E-ID par l'IdP

Niveau de sécurité de l'e-ID	**Argent**	**Or**	**Platine**
Première annonce auprès de la PU avec enregistrement			
Etape 1: Enregistrement auprès de la PU	Annonce avec identifiant e-ID ou pseudonyme auprès du service de confiance de la PU (interface e-ID) Démarrage de l'authentifiant e-ID		
Mandat d'identification PU à IdP	Identifiant e-ID, niveau de sécurité et demande d'attribut par interface e-ID		
Etape 2: Authentification par l'IdP conf. Au niveau de sécurité	Saisie d'un facteur d'authentification	Saisie de 2 facteurs d'authentification	Saisie de 2 facteurs d'authentification avec biométrie
Etape 3: Transmission des attributs de l'identité civile de l'IdP à la PU	Affichage de la liste d'attributs et code à utilisation unique pour autorisation sur l'écran du support de l'e-ID Restitution du code par la détentrice ou le détenteur à l'IdP		
Etape 5 activer l'e-ID	L'IdP active l'e-ID pour utilisation Communication à la détentrice ou au détenteur		
Etape 4: Fin de l'enregistrement auprès du PU	La détentrice ou le détenteur accède au service de la PU		

Tableau 2: Processus d'exploitation Première annonce auprès de la PU

Tableau 3: Processus d'exploitation Nouvelle annonce auprès de la PU (connexion)

Niveau de sécurité de l'e-ID	**Argent**	**Or**	**Platine**
Nouvelle annonce			
Etape 1 Connexion à la PU	Connexion avec l'identifiant e-ID ou le pseudonyme auprès du service de confiance de la PU (interface e-ID) Démarrage de l'authentifiant e-ID		
Mandat d'authentification PU à IdP	Identifiant e-ID et niveau de sécurité		
Etape 2 Authentification par l'IdP conf. au niveau de sécurité	Saisie d'un facteur d'authentification	Saisie de 2 facteurs d'authentification	Saisie de 2 facteurs d'authentification avec biométrie
Ticket de réponse IdP à PU	Identifiant e-ID et confirmation de l'authentification		
Etape 3: Fin de la connexion à la PU	La détentrice ou le détenteur accède au service de la PU		

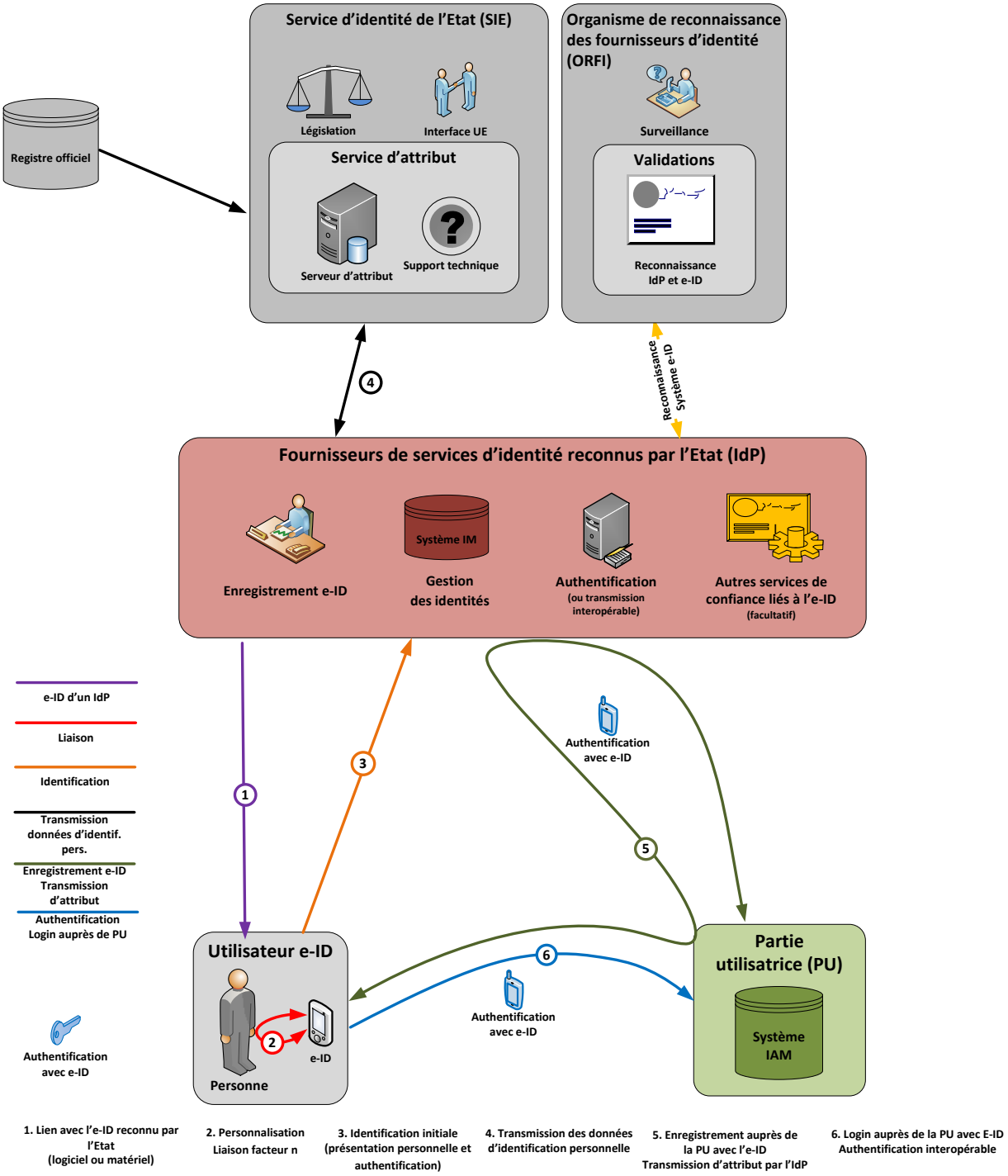


Schéma 9: établissement de l'e-ID et utilisation

2.6 Eléments importants de la mise en œuvre

Certains éléments importants pour la solution suisse, tels que le concept des niveaux de sécurité, le nouvel identifiant personnel unique et les données d'identification personnelle disponibles pour chaque niveau de sécurité, le processus de transmission des données officielles d'identification personnelle aux IdP et l'interopérabilité au sein du réseau des systèmes e-ID reconnus par l'Etat sont décrits plus en détail ci-après.

2.6.1 Les trois niveaux de sécurité de l'e-ID

Un e-ID du niveau de sécurité le plus élevé ne s'impose pas pour toutes les opérations commerciales. Un niveau de sécurité élevé est souvent synonyme de convivialité moindre, notamment lors de l'enregistrement initial, et de frais plus élevés. Un niveau de sécurité relativement bas suffit souvent pour des transactions simples, qui peut être réalisé par une identification en ligne initiale simple (p. ex. pour l'AppleID ou le Google ID) et la saisie d'un facteur d'authentification. Ce n'est que pour des opérations plus critiques que l'e-ID doit garantir un niveau de sécurité plus élevé, qui requière alors une présentation en personne pour l'identification initiale (ce qui est le cas p. ex pour la SuisseID ou une mobile ID) et au moins une authentification par 2 facteurs à l'usage. Une limitation à un seul niveau de sécurité constituerait donc un obstacle pour la diffusion des e-ID reconnus par l'Etat. Voilà pourquoi les systèmes e-ID sont reconnus par l'Etat à l'un des trois niveaux de sécurité. Les trois niveaux de sécurité pour les systèmes e-ID reconnus par l'Etat en Suisse sont définis de manière à répondre aux mêmes exigences en termes de sécurité, qui sont requis pour les trois niveaux de sécurité e-ID définis dans le Règlement eIDAS édicté par l'UE (art. 8 du Règlement eIDAS (EU, 2014) et actes d'exécution correspondants (Kommission, 2015)). Les exigences en matière d'authentification du NIST prévoient aussi trois niveaux de sécurité (800-63-3, 2016). Chaque niveau de sécurité confère un niveau de confiance différent quant à l'identité et à l'authenticité de la détentrice ou du détenteur de l'e-ID. Le niveau de sécurité requis en fonction du type d'application est précisé dans les différents actes législatifs spécifiques aux applications de cybergouvernement ou définis par les PU privées. Ainsi, un niveau de sécurité différent peut être choisi pour la cyberéducation que pour le vote électronique ou pour les applications en cybersanté.

Outre la fiabilité des IdP et des sources d'attributs utilisées par les IdP pour établir l'identité civile de la détentrice ou du détenteur, l'enregistrement (identification initiale de la personne et liaison de l'e-ID à la personne) et l'authentification sur le terrain au moyen de l'e-ID (1 facteur, 2 facteurs, biométrie), de même que la transmission et le traitement des mandats et des réponses dans le réseau interopérable des systèmes e-ID exercent une influence déterminante sur le niveau de sécurité d'un e-ID. Les trois niveaux sont désignés par les termes Argent, Or et Platine à des fins de communication. Les principales caractéristiques des trois niveaux sont détaillées ci-après et dans le Tableau 3 (entre parenthèses, les désignations européennes pour le niveau de sécurité correspondant):

- ARGENT (faible): dans le cadre d'un système e-ID, l'e-ID a pour but de réduire le risque d'abus ou de falsification de l'identité. L'enregistrement peut être effectué en ligne sur la base d'un document d'identité officiel. Seules quelques données d'identification personnelle sont transmises du SIE aux IdP (nom, prénom(s), date de naissance et IPU). L'utilisation de l'e-ID exige au moins une authentification à un facteur. La gestion d'un tel e-ID est ainsi comparable avec un badge d'accès, une solution de paiement sans contact pour des montants modestes ou la connexion avec un identifiant et un mot de passe ou un NIP sûr. Le niveau de sécurité «ARGENT» se rapporte à un moyen d'identification électronique qui confère un niveau de confiance relativement faible mais tout de même d'une certaine importance quant à l'identité revendiquée ou prétendue d'une personne, plutôt qu'une simple autodéclaration avec identifiant d'utilisateur librement choisi et mot de passe à choix.
- OR (substantiel): dans le cadre d'un système e-ID, l'e-ID a pour but de réduire considérablement le risque d'abus ou de falsification de l'identité. L'enregistrement est effectué avec une présentation en personne auprès de l'IdP ou par vidéoidentification sur la base d'un document d'identité officiel. Outre les données d'identification personnelle de niveau moindre, le SIE transmet d'autres attributs (p. ex. sexe, état civil, photo du visage, etc.). L'utilisation de l'e-ID exige au moins une authentification à deux facteurs. La gestion d'un tel e-ID est donc comparable, par exemple, à celle des solutions proposées habituellement dans le secteur bancaire (cartes de compte, cartes de crédit, solutions d'e-banking). Le

niveau de sécurité «OR» désigne un moyen d'identification électronique conférant un niveau substantiel de confiance quant à l'identité revendiquée ou prétendue d'une personne.

- PLATINE (élevé): dans le cadre d'un système e-ID, l'e-ID a pour but d'empêcher tout abus ou falsification de l'identité. L'enregistrement est effectué avec une présentation en personne auprès de l'IdP ou par vidéoidentification sur la base d'un document d'identité officiel. En outre, l'authenticité du document d'identité ainsi qu'au moins une caractéristique biométrique sont vérifiées sur la base d'une source officielle indépendante (validité du document d'identité et photo du visage ou autre signe biométrique distinctif). Le SIE transmet toutes les données d'identification personnelle disponibles (p. ex. aussi la signature numérisée). L'utilisation de l'e-ID exige au moins une authentification à deux facteurs, l'un d'entre eux devant être biométrique («facteur inhérent» conf. à l'acte d'exécution du Règlement eIDAS (Kommission, 2015)).). La gestion d'un tel e-ID est comparable à celle d'un smartphone avec reconnaissance de l'empreinte digitale, du visage ou de la voix. L'authentification biométrique aboutit à un lien encore plus étroit entre l'e-ID et la détentrice ou le détenteur. Le niveau de sécurité «PLATINE» correspond à un moyen d'identification électronique conférant un niveau maximal de confiance quant à l'identité revendiquée ou prétendue d'une personne.

Tableau 3: Niveaux de sécurité de l'e-ID

Niveau	Argent (faible)	Or (substantiel)	Platine (élevé)
Authentification	Au moins 1 facteur	2 facteurs	2 ou 3 facteurs avec biométrie
Enregistrement: liaison d'une personne à l'e-ID	La personne procède à la liaison avec l'e-ID sans surveillance	La personne procède à la liaison avec l'e-ID avec vérification par l'IdP	La personne procède à la liaison avec l'e-ID avec vérification par l'IdP sur la base d'un facteur biométrique
Enregistrement: identification initiale	En ligne avec numéro du document d'identité et date de validité	Présentation en personne ou vidéoconférence avec document d'identité; test de l'authentification par e-ID	Présentation en personne ou vidéoconférence avec document d'identité; test de l'authentification par e-ID
Données d'identification personnelle	Jeu de données minimal et IPU; synchronisation annuelle avec le SIE	Toutes, sauf certaines données biométriques; synchronisation trimestrielle avec le SIE	Toutes, synchronisation hebdomadaire avec le SIE
Exigence envers l'IdP et le système e-ID conf. aux définitions eIDAS (Kommission, 2015), art. 2.4	Reconnaissance du système e-ID avec audit de sécurité pour le niveau de sécurité «faible», «substantiel» et «élevé» conf. à l'art 2.4.7 dans (Kommission, 2015)		

Ce modèle permet d'enregistrer dans un premier temps un e-ID approprié avec une authentification à 2 facteurs (actuellement, un standard industriel de facto) au niveau Argent et de le passer plus tard, au besoin, à un niveau de sécurité supérieur avec présentation en personne. Le niveau de sécurité Argent permet de maintenir simple l'accès à un e-ID reconnu par l'Etat, ce qui peut représenter un facteur de succès essentiel pour le prestataire de systèmes e-ID reconnus par l'Etat sur le marché. De plus, une personne peut posséder plusieurs e-ID de divers IdP ou à des

niveaux de sécurité différents.

2.6.2 Identifiant personnel unique (IPU)

Le concept suppose que la pratique actuelle en matière d'utilisation du NAVS13 restera identique et introduit donc en sus un nouvel identifiant personnel unique (IPU) qui doit être mis à disposition pour les e-ID mais aussi pour d'autres applications. Si, par contre, la pratique rigide relative à l'utilisation du NAVS13 est assouplie, le NAVS13 pourrait être utilisé aussi directement pour l'e-ID en tant qu'IPU. Des examens sont en cours pour déterminer si cela est possible.

L'Etat définit pour toutes les personnes enregistrées dans les registres de personnes déterminants tenus par la Confédération avec un document d'identité officiel délivré et un statut de séjour un nouvel identifiant personnel unique (IPU), qui est indépendant des autres données d'identification personnelle telles que le nom ou le NAVS13. Il sert de balise pour toutes les données d'identification personnelle liées à une personne, qui sont transmises par le SIE à l'IdP, ainsi que pour tout autre attribut affecté à une personne par un IdP ou une PU. Les données d'identification personnelle transmises par le SIE à l'IdP sont jumelées sous forme cryptée à l'IPU, de sorte que l'intégrité et l'authenticité d'un attribut transmis peuvent en tout temps être vérifiées par l'IdP. L'IdP a l'obligation de mettre à jour périodiquement les données d'identification personnelle relatives à un e-ID délivré, par une demande correspondante au SIE dont la fréquence dépend du niveau de sécurité. Dans son eGId, l'IdP attribue notamment aussi l'identifiant de l'e-ID à l'IPU de la détentrice ou du détenteur. Cela vaut également pour les identifiants ou les identifiants éventuellement déduits d'un deuxième e-ID, de manière à ce qu'une PU puisse toujours attribuer de manière univoque à une seule personne les éventuelles connexions multiples avec des e-ID différents avec l'aide de l'IdP. L'IPU permet aux PU de simplifier leurs processus administratifs, les rendre plus fiables et donc réaliser des économies. Si l'IdP le définit ainsi, un identifiant personnel déduit peut être utilisé pour chaque PU, si l'IdP de définit ainsi, afin qu'aucune instance ou secteur ne puisse dresser un profil général.

2.6.3 Données d'identification personnelle

Pour chaque personne autorisée, le SIE tire des données d'identification personnelle des registres de personnes pertinents tenus par la Confédération (cf. ch. 4). Les données d'identification personnelle sont administrées par la Confédération et les attributs enregistrés correspondent aux valeurs constatées lors de la dernière identification par l'Etat de la personne pour l'établissement d'un document d'identité relevant de la puissance publique ou d'un autre acte officiel ayant conduit à un enregistrement dans les registres de personnes tenus par la Confédération (ISA, SYMIC, Infostar, CdC-UPI)[26].

D'autres attributs d'identité officiels peuvent être ajoutés ultérieurement, si un écosystème e-ID en a besoin et qu'une base légale correspondante existe. Il est important de bien comprendre que ni un IdP, ni une PU ne peut accéder à ces attributs sans accord exprès de la personne concernée. Il s'agit toujours de la personne qui fait transmettre de manière explicite, consciente et exclusive les données d'identification personnelle d'un certain niveau de sécurité à l'IdP reconnu, auprès de laquelle elle obtient un e-ID reconnu par l'Etat. Une transmission ultérieure de certains attributs des données officielles d'identification personnelle par l'IdP à une PU également ne peut elle aussi avoir lieu que sur accord exprès de la détentrice ou du détenteur.

[26] Pour des raisons de consistance, les mêmes attributs seront toujours transmis pour l'e-ID également, comme enregistrés dans les derniers documents d'identité relevant de la puissance publique établis ou dans Infostar. Des cas particuliers tels que le retrait du document d'identité, le décès ou les changements d'identité suite à des programmes de protection des témoins seront réglés dans le concept détaillé.

Tableau 4: Données d'identification personnelle disponibles

Attribut	Argent	Or	Platine
IPU	X	X	X
Nom officiel	X	X	X
Prénoms	X	X	X
Date de naissance	X	X	X
NAVS13 (pour les ayants-droit uniquement)		X	X
Sexe		X	X
Lieu de naissance		X	X
Etat civil		X	X
Nationalité		X	X
Statut de séjour		X	X
Photo du visage		X	X
Type et numéro de document		X	X
Signature numérisée			X

Date de la dernière constatation des attributs pour tous les attributs

2.6.4 Transmission de données d'identification personnelle

La transmission des données d'identification personnelle à un IdP est déclenchée par une demande de l'IdP. Dans sa demande, l'IdP communique au SIE pour quelle personne ces données sont demandées, en indiquant le numéro d'un document d'identité relevant de la puissance publique et valable délivré en Suisse. La communication de l'IdP au SIE contient en plus la date d'établissement du document d'identité avec lequel la personne s'est identifiée la première fois, le niveau de sécurité du système e-ID pour lequel les données d'identification personnelle sont demandés, et les indications permettant de contacter la détentrice ou le détenteur par un canal indépendant.

Par le canal indiqué (p. ex. numéro de téléphone portable, adresse e-mail ou adresse postale), le SIE communique à la détentrice ou au détenteur le fait que l'IdP requérant souhaite que les données d'identification personnelle correspondant au niveau de sécurité pour la reconnaissance par l'Etat de l'e-ID délivré soient transmises. Le SIE communique à la personne concernée un code d'autorisation qu'elle doit transmettre à l'IdP si elle approuve cette transmission.

L'IdP renvoie ce code d'autorisation au SIE dans un laps de temps défini. La durée dépend du canal de communication avec la personne concernée utilisé par le SIE. Dès que le SIE reçoit le code d'autorisation, il transmet à l'IdP les données d'identification personnelle correspondant au niveau de sécurité. La date de la dernière identification, qui est aussi toujours communiquée, n'est pas nécessairement identique à la date du document d'identité transmise par l'IdP. Une personne peut disposer de plusieurs documents d'identité valables et les données d'identification personnelle correspondent toujours aux valeurs qui ont été constatées lors de la dernière identification par l'Etat.

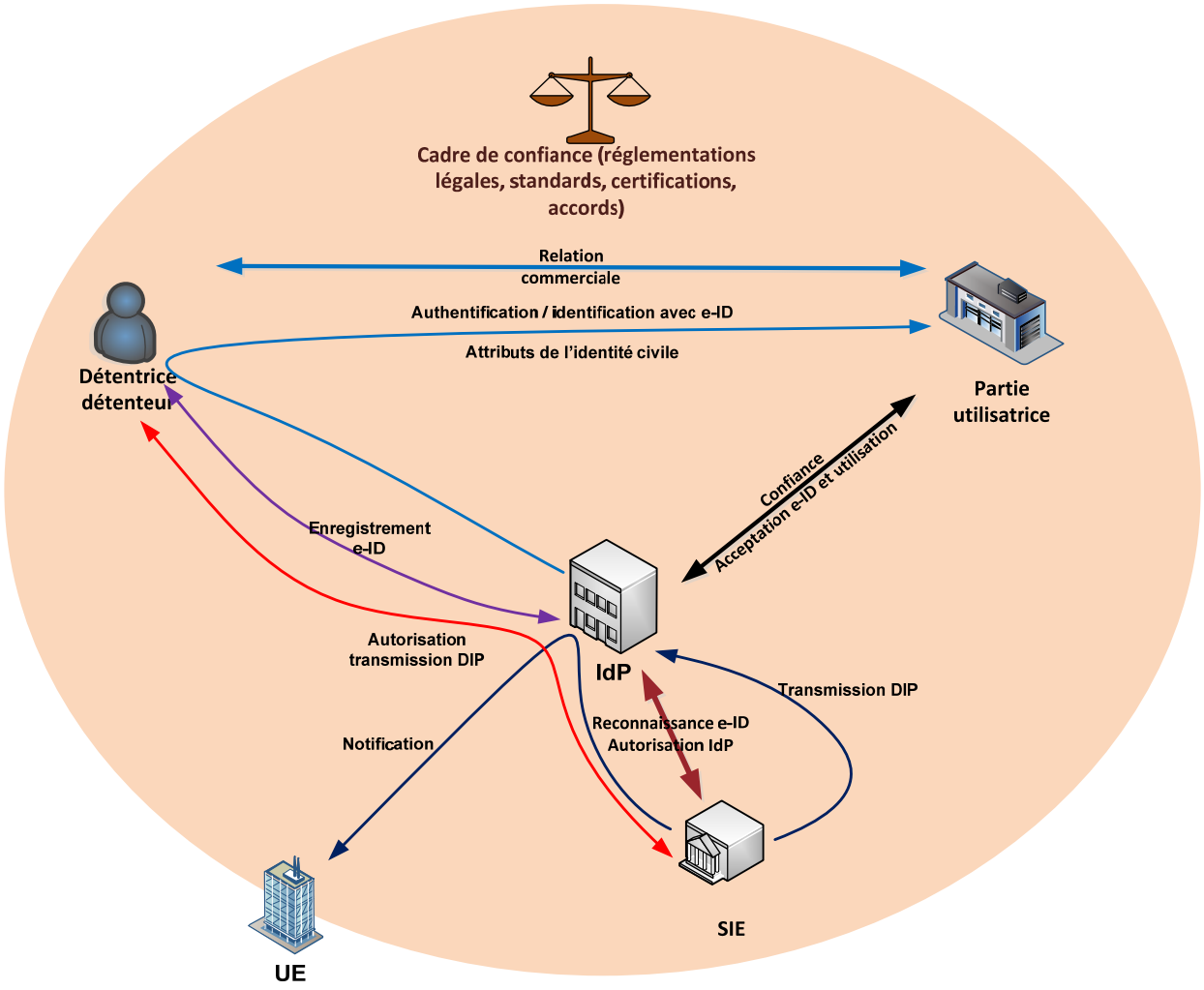


Schéma 10: Relations et processus lors de l'établissement et au cours de l'utilisation d'un e-ID

L'IdP doit mettre à jour régulièrement les données transmises en les comparant avec les données les plus récentes du SIE. La fréquence de mise à jour dépend du niveau de sécurité de l'e-ID correspondant. L'IdP doit aussi consulter quotidiennement les listes publiées par le SIE présentant les modifications des données d'identification personnelle, qui ont été saisies pour certains IPU[27]. Une nouvelle autorisation par la détentrice ou le détenteur n'est pas nécessaire pour la mise à jour.

2.6.5 Interopérabilité des systèmes e-ID

L'interopérabilité entre systèmes e-ID à un niveau de sécurité similaire est un facteur décisif pour la diffusion rapide et l'acceptation des systèmes e-ID reconnus par l'Etat dans l'écosystème e-ID. Il est toutefois peu judicieux que chaque PU doive signer des accords d'utilisation avec chaque IdP reconnu par l'Etat pour les systèmes e-ID pouvant être utilisés. Voilà pourquoi le concept précise que chaque e-ID atteignant ou dépassant le niveau de sécurité requis puisse être utilisé auprès de tous les services de confiance des PU indépendamment de l'IdP d'établissement.

Le protocole pour l'utilisation d'un e-ID lors de l'enregistrement ou de l'annonce à un service de

[27] Des changements d'attribut peuvent p. ex. résulter d'un mariage, si une nouvelle carte d'identité ou un nouveau passeport a été délivré dans l'intervalle. Le décès d'une personne doit bien évidemment également entraîner la révocation de son e-ID.

confiance est toujours identique dans son déroulement et dans sa structure par média (appareils mobiles, PC, kiosque Internet, etc.) et confère à la détentrice ou au détenteur un sentiment d'utilisation connu. Les services de confiance intègrent à leurs portails les pages d'enregistrement et d'annonce correspondantes sous forme d'une interface client e-ID en grande partie standardisée. Ils établissent les mandats d'identification et d'authentification de manière identique pour tous les e-ID et les envoient à l'IdP, avec le système e-ID auquel ils sont raccordés.

Les exigences en matière d'interopérabilité ne constituent pas non plus une charge supplémentaire pour les services de confiance. Ils établissent les mandats d'identification et d'authentification de manière identique pour tous les e-ID et les envoient à l'IdP, avec le système e-ID auquel il est raccordé. Ils reçoivent aussi toujours en retour, dans un format standard, les tickets de réponse par l'intermédiaire de cet IdP.

L'interopérabilité est exclusivement réalisée par les systèmes e-ID des IdP. Chaque mandat comprend l'identifiant de l'e-ID. Une partie de l'identifiant identifie le système e-ID et l'IdP d'établissement (correspond aux identifiants des systèmes e-ID reconnus par l'Etat publiés dans la liste de l'ORFI). L'IdP transmet un mandat d'identification ou d'authentification à l'IdP compétent et il reçoit de lui, après réalisation du ticket de réponse qu'il restitue au service de confiance.

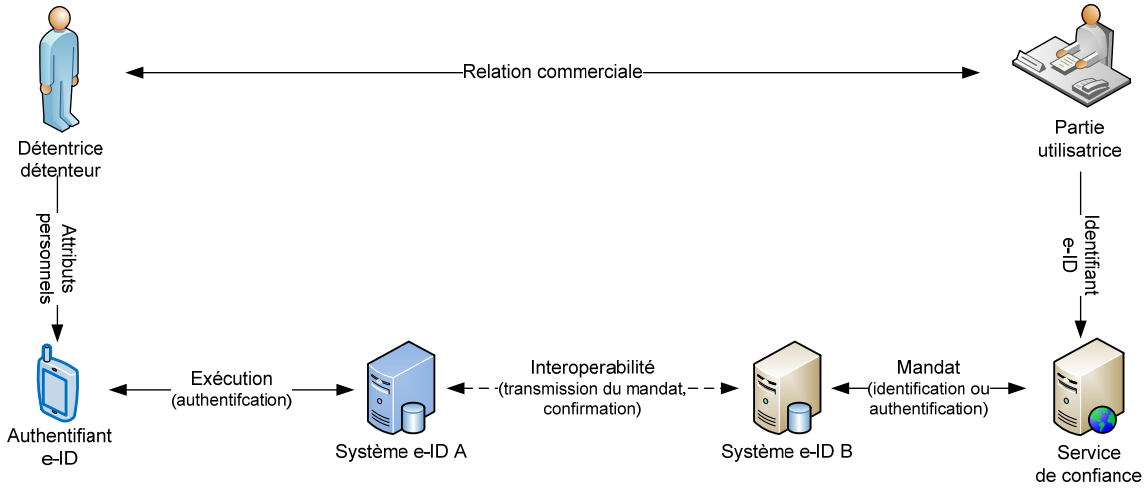


Schéma 11: réalisation de l'interopérabilité par la fédération

2.7 Possibilité de notification

Le 23 juillet 2014, l'UE a adopté le Règlement (UE) N° 910/2014 (EU, 2014) du Parlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. A partir de septembre 2015, les actes d'exécution correspondants ont ensuite été adoptés (EU, Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung) (EU, Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen) (EU, Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus) (EU, Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung).

Ci-après sont brièvement présentés les exigences à formuler pour un système e-ID suisse afin

que celui-ci soit conforme au Règlement e-ID afin de pouvoir éventuellement être notifié ultérieurement. Il va de soi que la Suisse n'est aucunement obligée sur le plan juridique de reprendre le Règlement de l'UE. Considérant toutefois la forte imbrication sociale et commerciale avec la plupart des Etats membres de l'UE, il est supposé que la Suisse a un intérêt à s'intégrer tôt ou tard dans le système européen d'interopérabillité des identités électroniques. Bien qu'il soit pour l'heure totalement ouvert si la Suisse va s'intégrer dans ce système international, quand et comment, le système suisse e-ID doit être conçu dès le départ de manière à pouvoir fondamentalement être notifié.

Pour qu'un système national puisse être notifié, il doit satisfaire les conditions énoncées à l'article 7 du Règlement eIDAS. La lettre a) chiffre iii) admet aussi les e-ID tels que définis en l'espèce, où l'Etat reconnaît des systèmes proposés par des particuliers. Les autres exigences principales sont précisées aux lettres c) à f) et sont les suivantes:

c) Le schéma d'identification électronique et les moyens d'identification électronique délivrés dans ce cadre répondent aux exigences d'au moins un des niveaux de garantie prévus dans l'acte d'exécution visé à l'article 8, paragraphe 3.

d) L'État membre notifiant veille à ce que les données d'identification personnelle correctes au moment de l'établissement soient assignés à l'e-ID et il en répond impérativement également conformément à l'article 11, chiffre (1).

e) La partie délivrant le moyen d'identification électronique relevant de ce schéma veille à ce que l'e-ID ne soit assigné qu'à la bonne personne conformément au niveau de sécurité.

f) L'Etat notifiant lui-même s'assure qu'une authentification en ligne est disponible à tout moment, dans toute l'UE, pour chaque service de confiance, sa responsabilité étant à nouveau engagée conformément à l'article 11, ch. (1) en cas de dommage.

Ces exigences impactent la réglementation suisse. La loi e-ID prévue doit notamment définir un cadre juridique et de standardisation pour la reconnaissance par l'Etat des systèmes e-ID et la reconnaissance des IdP. Ceci doit être conçu de manière à ce que la reconnaissance réciproque ultérieure des systèmes e-ID reconnus par l'Etat reste possible entre la Suisse et l'UE ou certains Etats membres. La compatibilité du présent concept avec les actes d'exécution du Règlement eIDAS a été examinée dans la mesure du possible, et considérée comme étant réalisée.

3 Contribution de l’Etat à l’e-ID

3.1 En bref

Les autorités suisses tiennent actuellement plusieurs registres des personnes contenant des données d’identification personnelle. Mentionnons ici notamment le registre électronique de l’état civil (Infostar), le registre des habitants et le registre central de la Centrale de compensation de l’AVS (CdC). En matière de documents d’identité, les données d’identification personnelle pour les Suissesses et les Suisses figurent dans le Système d’information relatif aux documents d’identité (ISA) et celles pour les ressortissants étrangers, dans le Système d’information central sur la migration (SYMIC). Le registre UPI de la Centrale de compensation également sert à l’identification officielle des personnes physiques et à l’attribution d’un numéro AVS univoque (UPI est l’acronyme de «Unique Person Identification»).

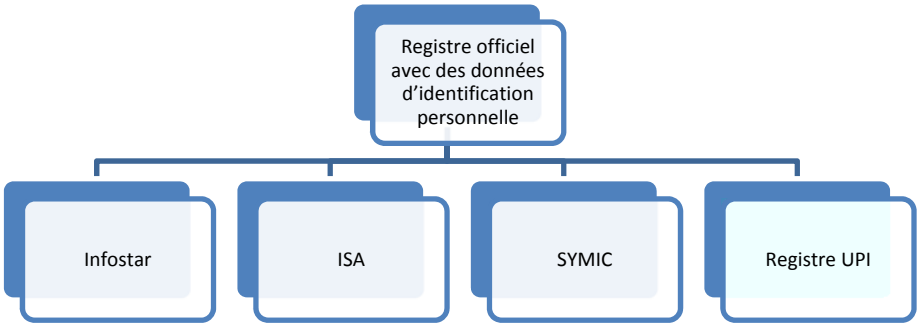


Schéma 12: Registres des personnes tenus par la Confédération

La loi fédérale sur l’harmonisation de registres (LHR) a fait du nouveau numéro AVS (NAVS13) un identifiant personnel unique et univoque dans les registres concernés par le recensement. Parmi ces registres se trouvent les registres de personnes de la Confédération ainsi que les registres cantonaux et communaux des habitants. La carte d’assuré délivrée par les assureurs-maladie conformément à l’ordonnance du 27 juin 1005 sur l’assurance-maladie (OAMal) comprend elle aussi le numéro AVS en tant qu’identifiant personnel unique. Le NAVS13 n’est pas évocateur et il est composé d’une suite de 13 chiffres (3 chiffres pour le code de pays selon ISO 3166, 9 chiffres aléatoires, 1 chiffre de contrôle).

Sur la base des données d’identification personnelle dans ISA ou SYMIC, la Confédération délivre actuellement des moyens d’identification conventionnels, à savoir le passeport suisse, la carte d’identité et le livret pour étrangers. La Confédération fait à cet égard office de repère fiable pour l’identité officielle d’une personne. L’introduction d’e-ID reconnus par l’Etat doit permettre de délivrer également, sur la base des données d’identification personnelle disponibles auprès de la Confédération, des moyens d’identification électronique avec des données d’identification personnelle officielles enregistrées et transmises.

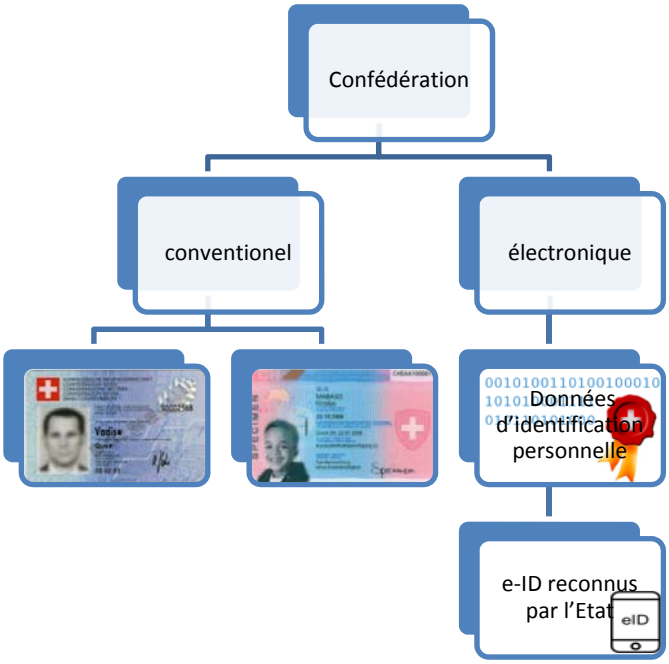


Schéma 13: Moyens d'identification officiels

La Confédération s'acquitte à cet égard de quatre tâches: premièrement, elle crée et préserve un cadre juridique transparent, deuxièmement, elle exploite une interface électronique par le biais de laquelle les IdP reconnus peuvent obtenir des données officielles d'identification personnelle, troisièmement, elle peut reconnaître des IdP et leurs systèmes e-ID, et quatrièmement, elle exerce la surveillance sur les IdP reconnus par l'Etat et leurs systèmes e-ID. Au sein de la Confédération, ces tâches doivent être réalisées par deux services administratifs: le «Service d'identité électronique suisse (SIE)» et l'«Organisme de reconnaissance des fournisseurs d'identité (ORFI)».

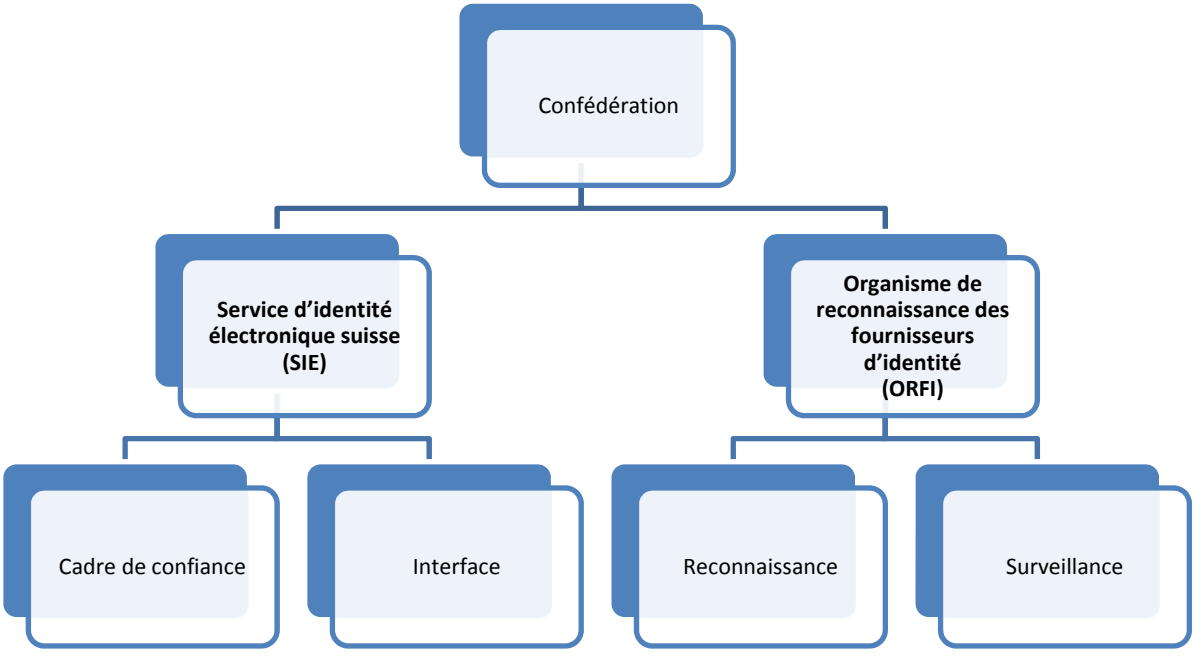


Schéma 14: Tâches du SIE et de l'ORFI

3.2 Service d’identité électronique suisse (SIE)

3.2.1 Cadre juridique

En collaboration avec l’ORFI, le SIE (aussi appelé service d’identité) gère au niveau opérationnel les prescriptions juridiques, organisationnelles et techniques. Il définit notamment les standards des interfaces pour l’interopérabilité des systèmes e-ID et ajuste les exigences techniques et organisationnelles en matière de reconnaissance des IdP et des systèmes e-ID aux progrès socio-économiques et techniques.

Pour qu’un système e-ID de l’UE puisse être notifié ultérieurement, il doit satisfaire les prescriptions du Règlement eIDAS de l’UE. Il convient donc de veiller à ce que les prescriptions pour les systèmes e-ID reconnus par l’Etat en Suisse recoupent celles du Règlement eIDAS, comme l’a stipulé le Conseil fédéral dans son mandat.

3.2.2 Interface

Par le biais d’une interface électronique, le SIE met à disposition des IdP reconnus des données d’identification personnelle tenues par la Confédération. L’établissement et la transmission d’un IPU permettent de garantir l’intégrité de l’assignation des données d’identification personnelle à la bonne personne. Cette interface B2B n’est accessible qu’aux IdP reconnus.

Lors de l’établissement d’un e-ID reconnu par l’Etat, la personne s’identifie auprès de l’IdP au moyen d’un document d’identité conventionnel. L’IdP transmet au SIE le numéro du document. Le SIE détermine en consultant ISA ou SYMIC l’IPU correspondant et le transmet à l’IDP accompagné des données d’identification personnelle correspondant au niveau de sécurité de l’e-ID.

Dans l’optique de la migration des jeux de données existants, les systèmes d’identifiant actuels (p. Ex. NAVS13) pourront être utilisés pour l’assurance-qualité.

Toute transmission fait l’objet d’un procès-verbal par le SIE et est identifiée de telle manière qu’une demande de mise à jour d’un IdP peut indubitablement être rapportée à une première transmission précédente.

Le SIE perçoit les données d’identification personnelle, tels que le nom d’une personne, en premier lieu à partir d’Infostar et p. ex. le numéro du document d’identité ou photo subsidiairement auprès d’ISA et de SYMIC. Le tableau ci-après présente une sélection possible de données d’identification personnelle avec indication du registre d’où elles sont tirées.

Nom de l'attribut	**Registre utilisé comme source**
IPU	UPI, SYMIC, ISA
Nom officiel	Infostar
Prénoms	Infostar
Date de naissance	Infostar
Numéro d'assuré (NAVS13)	Infostar
Sexe	Infostar
Lieu de naissance	Infostar
Etat civil	Infostar
Nationalité	Infostar
Statut de séjour	SYMIC
Photo du visage	ISA, SYMIC
Numéro(s) de document Passeport	ISA
Numéro(s) de document Carte d'identité	ISA
Numéro(s) de document Livret pour étrangers	SYMIC
Signature numérisée	ISA, SYMIC

Tableau 5: Sources officielles des données d'identification personnelle

Ces registres doivent être complétés par le NAVS13 avant le lancement d'e-ID reconnus par l'Etat et migrés en conséquence. Pour améliorer encore la qualité des données, il est en outre recommandé de procéder à une comparaison systématique des registres avec les données d'Infostar, comme c'est déjà le cas actuellement au sein d'ISA.

Les données d'identification personnelle peuvent être complétées par des métadonnées, par exemple l'indication des sources ou la date de relevé. De plus, elles sont toujours liées de manière cryptée à l'IPU. La première transmission des données d'identification personnelle à l'IdP ne doit avoir lieu qu'avec l'accord exprès et documenté de la personne concernée.

Les IdP sont tenus de mettre à jour périodiquement les données d'identification personnelle liées à un IPU. Cela passe aussi par l'interface du SIE, mais pour des raisons de convivialité d'utilisation, une nouvelle autorisation expresse de la personne n'est alors plus nécessaire. Selon le niveau de sécurité, les IdP doivent procéder à une mise à jour annuelle (argent), trimestrielle (or) ou hebdomadaire (platine). La mise à jour peut être déclenchée par l'IdP sur la base de l'IPU, le SIE examinant alors si une première transmission de l'IPU à l'IdP concret a tout simplement eu lieu avec accord exprès de la personne.

Afin de pouvoir bloquer rapidement un e-ID dans des circonstances particulières, le SIE met à disposition, par le biais de son interface, une liste des IPU bloqués. Le décès d'une personne peut, par exemple, être une circonstance particulière. Les IdP sont tenus de bloquer immédiatement tous les e-ID qui ont été délivrés pour un IPU listé. La liste peut être consultée gratuitement par les IdP par le biais de l'interface susmentionnée. Ils sont tenus de le faire régulièrement (quotidiennement).

3.2.3 Organisation

Le SIE s'acquitte de tâches juridiques et notamment opérationnelles. Des ressources correspondantes sont requises au sein du SIE pour rédiger puis veiller aux prescriptions juridiques, organisationnelles et techniques pour les systèmes e-ID.

Le SIE répond en outre de l'exploitation de l'interface pour la transmission des données d'identification personnelle. Il est le point de contact unique (Single Point Of Contact, SPOC) pour toute question spécialisée et technique des registres connectés et des IdP en lien avec ladite interface.

Les examens sur des données d'identification personnelle supposées ou effectivement inconsistantes ou erronées ne sont pas réalisés par le SIE lui-même mais par le service clearing de la CdC-UPI, qui répond d'ores et déjà aujourd'hui de cette tâche en matière de NAVS13 (Zentrale Ausgleichsstelle).

Selon les estimations actuelles, 300 pour cent de postes à durée indéterminée sont nécessaire pour le SIE afin de s'acquitter de ces tâches (gestion continue et ajustement régulier des prescriptions techniques aux derniers développements, prise en charge du SPOC). Considérant que les bases de données pertinentes pour les e-ID reconnus par l'Etat (à l'exception du registre UPI) sont de la responsabilité du DFJP, le SIE doit logiquement être mis en place au sein du DFJP.

3.3 Organisme de reconnaissance des fournisseurs d'identité (ORFI)

3.3.1 Reconnaissance

Les IdP établis (issus de l'économie privée ou aux mains des pouvoirs publics) peuvent obtenir de l'ORFI une reconnaissance par l'Etat pour eux et leurs systèmes e-ID à l'un des niveaux de sécurité prévus. Un IdP peut demander la reconnaissance de plusieurs systèmes e-ID à des niveaux de sécurité différents.

Tant l'IdP que le système e-ID concret doivent demander une reconnaissance au niveau de sécurité souhaité au moins. A cette fin, des obligations d'ordre juridique, organisationnel et technique sont définis par le SIE en accord avec l'ORFI, dont la réalisation par l'IdP est vérifiée par l'ORFI. A cet égard, les certifications et reconnaissances existantes (p. ex. dans le cadre de SCSE ou de plateformes de remise) sont intégrées autant que possible au processus de reconnaissance afin d'éviter des doublons.

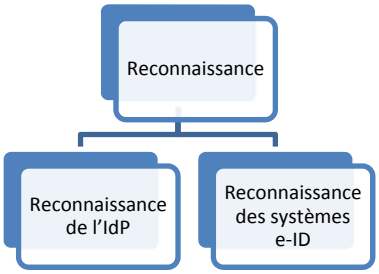


Schéma 15: Reconnaissance de l'IdP et du système e-ID

La reconnaissance doit par principe être fondée sur des certificats de conformité à des normes internationales et des profils de protection nationaux. L'IdP doit pour cela prouver à l'ORFI la conformité de son organisation et de ses systèmes e-ID par des certifications. L'ORFI contrôle les documents de certification remis et se prononce quant à la reconnaissance par l'Etat.

L’éventuelle notification d’un système e-ID vis-à-vis de l’UE représente un cas particulier de la reconnaissance. Avec la notification, un système e-ID est reconnu au sein de l’UE et peut y être utilisé au niveau de sécurité correspondant. Réciproquement, tous les systèmes e-ID des Etats membres de l’UE déjà notifiés doivent être reconnus en Suisse également au niveau de sécurité correspondant. La Suisse doit conclure un accord bilatéral avec l’UE pour la notification.

Enfin, l’ORFI publie une liste des IdP et systèmes e-ID reconnus, sur la base de laquelle les PU et les personnes physiques peuvent vérifier le statut d’un IdP concret et du système e-ID.

3.3.2 Surveillance

L’ORFI exerce la surveillance des IdP reconnus et des systèmes e-ID et il réagit en cas de divergence par rapport aux prescriptions et incidents relatifs à la sécurité informatique. De plus, l’ORFI surveille le marché, réceptionne et évalue des messages sur la sécurité informatique en matière d’e-ID et les transmet si nécessaire au SIE. L’ORFI demande en outre aux IdP reconnus, à des intervalles prédéfinis, les certificats de conformité nécessaires et les contrôle. Enfin, l’ORFI peut retirer à un IdP ou à un système e-ID la reconnaissance par l’Etat.

3.3.3 Organisation

L’ORFI reconnaît et exerce la surveillance sur les systèmes e-ID reconnus par l’Etat. Ces tâches présentent des possibilités de synergie avec d’autres tâches de la Confédération dans le domaine informatique:

DFF: L’UPIC répond de la mise en place du système IAM au sein de la Confédération. Dans ce domaine, tant une surveillance qu’un pilotage des systèmes IAM intégrés sont nécessaires.

De plus, une unité organisationnelle a pu être créée en lien avec la loi fédérale sur la sécurité de l’information, et celle-ci s’acquitte de telles tâches de surveillance.

DETEC: L’OFCOM peut se targuer d’un niveau de compétence élevé et d’expériences significatives en matière de surveillance du marché. De plus, l’OFCOM est déjà engagé en ce qui concerne les signatures électroniques (SCSE).

DEFR: Le SECO exerce également une fonction de surveillance en lien avec la Fédération suisse d’identités, projet dont il est le responsable.

Une première analyse révèle qu’il semble judicieux de mettre en place l’ORFI au sein du DFF (UPIC), car IAM-Confédération et la sécurité des TIC sont des sujets étroitement liés aux systèmes e-ID reconnus par l’Etat. Pour l’accomplissement des tâches citées, 100 pour cent de poste à durée indéterminée sont nécessaires pour l’ORFI.

3.4 Conséquences financières pour la Confédération

3.4.1 Hypothèses sur le modèle

Si l'on analyse les avantages financiers générés sur le marché par les e-ID, il apparaît que ceux-ci sont principalement réservés aux PU. En effet, celles-ci peuvent simplifier leur processus en utilisant des e-ID et peuvent baisser leur tarif (p. ex. moins de guichets, papier et changement de support, procédure plus rapide, modèles commerciaux innovants, identifiant personnel unique, etc.). Le modèle de financement doit tenir compte de cet aspect fondamental.

Il s'ensuit que le modèle «pay-per-use» est le mieux qualifié pour la facturation des prestations officielles aux acteurs du marché. Le modèle prévoit aussi que les services concernés assument eux-mêmes leurs frais d'investissement et d'exploitation (donc, de fait, qu'ils n'assument pas de garantie de déficit), mais qu'ils peuvent à moyen terme compenser les dépenses par des recettes. Le modèle le plus prometteur ne perçoit pas de redevance élevée mais un émolument pour l'utilisation concrète de l'e-ID. La Confédération ne devrait donc facturer des émoluments à un IdP que lorsque celui-ci fait effectivement appel à des attributs. A titre d'incitatif supplémentaire, il serait possible d'envisager que la Confédération renonce à percevoir des émoluments pour la première transmission des données d'identification personnelle si un IdP, en contrepartie, délivre l'e-ID gratuitement.

Il appartient à l'IdP de déterminer ensuite comment il facture ces coûts à l'utilisateur (p. ex. «pay-per-use» ou «flat rate»). Les IdP peuvent nettement réduire leurs coûts s'il est possible d'éviter une visite de la personne concernée lors de l'établissement de l'e-ID. Cela pourrait par exemple être réalisé par le fait que les IdP utilisent la photo du visage transmise par la Confédération pour les niveaux de sécurité Or et Platine afin de procéder à une vérification biométrique de l'identité.

Au cours des travaux, d'autres modèles ont été examinés, mais ils ont été rejetés. Il en va ainsi du modèle «prepaid», mis en œuvre par exemple par la SuisseID. Dans ce modèle, l'utilisateur doit s'acquitter au préalable d'un émolument couvrant le plus possible les coûts de l'éditeur. Il s'avère que cet émolument, dont une personne doit s'acquitter sans possibilité manifeste et importante d'utilisation de l'e-ID, représente un obstacle majeur pour que la solution soit acceptée. Le modèle «promotion», dans lequel la Confédération propose gratuitement les prestations du SIE pendant une durée illimitée, a lui aussi été examiné et rejeté, car il fait totalement abstraction des coûts réels. Ce modèle aurait toutefois l'avantage d'abaisser encore le seuil d'admission pour les autres participants et d'annuler la charge pour l'encaissement des émoluments.

Pour estimer les coûts incombant à la Confédération, il faut se fonder sur un modèle dont les paramètres sont difficiles à pronostiquer. A titre d'estimation générale, il est attendu que près de la moitié de la population suisse disposera à moyen terme d'un e-ID reconnu par l'Etat et que la Confédération recevra donc quelque 10 millions de demandes d'attributs. La charge liée à ces demandes ne nécessitera pas, du point de vue actuel, d'augmenter les capacités des bases de données existantes.

3.4.2 Frais d'investissement et d'exploitation SIE et ORFI

Compte tenu des hypothèses formulées au ch. 3.4.1, il faut s'attendre à des coûts globaux de quelque CHF 6,5 millions pour la mise en place et l'exploitation du SIE. Les coûts d'exploitation annuels, y compris les coûts de personnel, sont estimés à CHF 2,2 millions de francs environ.

Pour l'exploitation du SIE, 300 pour cent de postes sont requis, et pour celle de l'ORFI, 100 pour cent de postes. Au sein du SIE, ces ressources en personnel sont prévues pour les tâches suivantes: a) support spécialisé pour les fournisseurs de données internes à la Confédération concernés, b) support spécialisé pour les IdP reconnus par l'Etat concernés, c) responsabilité de

l'application et gestion de l'infrastructure informatique requise au sein du SIE (interface B2B et raccordement aux sources de données telles que ISA, Infostar, etc.), d) élaboration et gestion des consignes organisationnelles et techniques pour la reconnaissance des IdP et des systèmes e-ID reconnus par l'Etat, e) acquisition (mise au concours publique) des services IdP requis au sein de la Confédération, f) gestion et publication de la liste des IdP reconnus et g) obtention d'informations sur les développement technologiques actuels en matière d'e-ID et les questions de sécurité informatique correspondantes. Au sein de l'ORFI, les ressources en personnel sont prévues pour les tâches suivantes: a) reconnaissance des IdP (vérification des attestations de conformité) et b) surveillance de la conformité en continu des IdP et systèmes e-ID reconnus.

Le montant des coûts d'exploitation est susceptible de varier au cours de l'élaboration future du concept informatique détaillé.

3.4.3 Dépenses de la Confédération pour des prestations IdP

La Confédération devant acquérir pour ses portails des services d'identité auprès d'IdP reconnus par l'Etat, il en résulte des dépenses. Ces dépenses seront plus que compensés par les économies réalisées suite à la suppression des solutions IM isolées, en place ou futures, de la Confédération ainsi que par les économies réalisées par la simplification des processus commerciaux.

3.4.4 Recettes e-ID pour la Confédération

Le SIE percevant dès la mise en service des émoluments pour la transmission et la mise à jour des données d'identification personnelle transmises aux IdP, il en résulte des recettes pour la Confédération. Avec quelque 10 millions de demandes par année, l'émolument devrait se situer dans une fourchette basse de quelques dizaines de centimes par transmission. Avec quatre mises à jour des attributs par année, les coûts d'un e-ID au niveau de sécurité Or sont donc nettement inférieurs à un franc. De plus, la Confédération peut prélever des émoluments pour la reconnaissance et la vérification périodique des attestations de conformité des IdP et de leurs systèmes e-ID.

3.4.5 Compte de pertes et profits d'exploitation

L'introduction de systèmes e-ID reconnus par l'Etat est un projet stratégique sur plusieurs années. En ce qui concerne la diffusion des e-ID, il y a ainsi lieu de ne pas formuler des attentes irréalistes, comme le prouvent les expériences réalisées dans d'autres pays voisins. L'e-ID est un outil novateur, à l'instar du vote par correspondance il y a quelques années, qui doit d'abord susciter la confiance de la population.

Par ailleurs, un nombre suffisant d'applications en ligne attrayantes doivent être mises à disposition par les PU en plus de l'établissement des e-ID. A titre de mesure de protection des investissements, la Confédération doit donc inscrire dans la loi le principe selon lequel tous les services fédéraux qui demandent une authentification sur leur portail Internet ont par principe l'obligation d'accepter des systèmes e-ID reconnus par l'Etat.

A moyen terme, les coûts d'exploitation de la Confédération devraient être entièrement compensés par les recettes des émoluments perçus pour la transmission des attributs et des émoluments pour la reconnaissance des IdP, de sorte que le projet est neutre en termes de coûts pour le budget fédéral. Au début, un «financement de lancement» ou la «garantie de déficit» susmentionnée sera toutefois nécessaire.

4 L’e-ID dans la pratique

4.1 Introduction

Le présent chapitre doit fournir un aperçu des applications futures possibles pour les e-ID reconnus par l’Etat. Il recourt sciemment à des termes simplifiés (p. ex. «données officielles» plutôt que «données d’identification personnelle enregistrées par la Confédération» ou «émetteur» plutôt que «fournisseur de services d’identité IdP»).

4.2 Etablissement d’un e-ID

Dans un premier temps, la cliente ou le client peut choisir parmi les produits à disposition celui qui répond le mieux à ses besoins. Les e-ID proposés se différencient par exemple par leur niveau de sécurité, le média faisant office de support (smartphone, clé USB, smartcard, etc.) ou par les services supplémentaires proposés conjointement, par exemple la signature électronique ou le verrouillage. Il est autorisé de posséder en même temps plusieurs e-ID reconnus par l’Etat.

Dans un deuxième temps, la cliente ou le client obtient l’e-ID choisi. Celui-ci contient un processus d’enregistrement auprès de l’émetteur et peut être effectué en ligne dans le cas le plus simple; en règle générale, il est cependant requis de se présenter en personne à l’émetteur, ou du moins d’effectuer une identification vidéo. Sur place, la cliente ou le client est identifié au moyen d’un document d’identité officiel, ses données officielles sont consultées auprès de la Confédération avec son accord, l’e-ID est personnalisé et remis à la cliente ou au client et activé par l’émetteur.

Dans un troisième temps, la détentrice ou le détenteur peut déjà utiliser l’e-ID. Les e-ID reconnus par l’Etat fonctionnant en grande partie de manière identique sur les portails grâce aux prescriptions de standardisation, les détentrices et détenteurs s’habituent vite à les utiliser. Cela vaut notamment en cas de changement d’émetteur également.

4.3 Restitution ou perte d’un e-ID

En cas de perte d’un e-ID ou si celui-ci ne doit plus pouvoir être utilisé pour d’autres raisons, la détentrice ou le détenteur peut à tout moment en demander le blocage à l’émetteur. Tous les émetteurs d’e-ID reconnus par l’Etat ont l’obligation de proposer des services correspondants chargés de réceptionner de telles demandes et de tenir une liste des e-ID bloqués. Cette liste doit être consultée par les PU lorsqu’une personne se connecte avec un e-ID.

4.4 Utilisation d’un e-ID

4.4.1 Cyberdémocratie et cyberparticipation

Le développement d’Internet influence également l’opinion publique et la volonté populaire. En 2011, la Chancellerie fédérale a rédigé, sur mandat du Conseil fédéral, un rapport sur la cyberdémocratie et la cyberparticipation (Bundeskanzlei, E-Demokratie und E-Partizipation). Ce rapport analyse l’influence d’Internet sur l’exercice des droits populaires et met en évidence diverses perspectives. Les domaines auxquels les détentrices et détenteurs d’e-ID pourraient participer à moyen terme aux affaires politiques par le biais des médias numériques sont les suivants:

- Votations populaires

- Elections fédérales
- Initiatives populaires et référendums fédéraux
- Pétitions fédérales[28]
- Consultations et auditions[29]
- Parlement - autorités - tribunaux

Conformément au processus démocratique, l'information et la consultation sont suivies de la prise de décision. Le vote électronique (Bundeskanzlei, Vote électronique) est promu de manière progressive depuis la première votation par Internet, qui s'est déroulée le 19 janvier 2003 à Anières (GE), par la Chancellerie fédérale et les cantons. Après une première étape comprenant des essais-pilote dans les cantons de Genève, Neuchâtel et Zurich, réalisés en étroite coopération avec la Confédération, le Conseil fédéral s'est exprimé le 31 mai 2006 en faveur de l'introduction par étapes du vote électronique. A l'occasion des votations populaires du 5 juin 2016, 5 cantons ont ainsi proposé une solution électronique pour la votation.

En 2009, le référendum contre l'introduction du passeport biométrique a fait parler de lui, car il n'avait pas été annoncé dans les délais par un parti établi avant d'être organisé de manière habituelle, mais parce que le comité référendaire avait utilisé Facebook pour mobiliser le corps électoral. Par motion[30], une conseillère nationale avait déjà chargé le Conseil fédéral, une année plus tôt, «de créer les bases légales permettant de récolter des signatures pour des initiatives populaires et des référendums par voie électronique, dans le cadre de projets pilotes. Ce projet sera mené en parallèle avec le projet de vote électronique et celui de cyberadministration.»

Dans sa réponse à cette motion, le Conseil fédéral a appuyé sa proposition de procéder en plusieurs étapes pour la numérisation des droits populaires. Etape 1: votation électronique. Etape 2: élection électronique. Etape 3: récolte électronique de signatures. Etape 4: listes électroniques de candidats.

4.4.2 Cyberadministration

Bien que le terme de cyberadministration présente quelques similitudes avec d'autres éléments du présent chapitre 4, diverses possibilités d'utilisation d'un e-ID reconnu par l'Etat, qui sont déjà partiellement en ligne par le biais de procédures propres, sont présentées ci-après:

- Compléter des formulaires en ligne auprès des autorités, p. ex. en cas de déménagement, pour obtenir des autorisations ou pour demander des documents d'identité.
- Accès à des dossiers fiscaux et décomptes de TVA
- Accès à des portails comme E-VERA pour les Suisses de l'étranger
- Accès aux portails des services de contrôle des véhicules automobiles
- Commande d'un extrait du casier judiciaire

Les détentrices et détenteurs d'e-ID reconnus par l'Etat peuvent se connecter de manière sûre à

[28] Toute personne – donc pas uniquement les électeurs – a le droit de s'adresser par écrit aux autorités compétentes pour leur présenter des requêtes ou des suggestions ou pour lui adresser des réclamations, et ce, pour toute activité officielle.

[29] Au cours de la procédure de consultation, les documents sont publiés sous forme numérique par la Chancellerie fédérale. Il est autorisé de remettre une prise de position sous forme électronique, mais il n'est pas encore possible de procéder à l'entier de la procédure, ni d'évaluer les prises de position sous forme électronique.

[30] 08.3908. Motion Jacqueline Fehr. Renforcer la démocratie. Autoriser la récolte électronique de signatures. 17.12.2010 Classement, car en suspens depuis plus de deux ans.

tous les portails des autorités acceptant l'identifiant personnel unique prévu, et ce, sans enregistrement fastidieux préalable. Au vu du projet de loi actuel, il s'agira de tous les portails de la Confédération exigeant une connexion électronique.

4.4.3 Cybersanté

Le dossier électronique du patient devrait être lancé en 2017 déjà (Bundesamt für Gesundheit). Les détentrices et détenteurs d'un dossier électronique du patient, resp. leur représentant légal, doivent pouvoir s'y annoncer de manière sûre, ce qui sera possible grâce à des e-ID reconnus par l'Etat.

Un tel dossier devrait être ouvert pour chaque enfant à sa naissance ou lors du premier contrôle médical; il suffira ensuite de le tenir à jour au fur et à mesure. En cas d'hospitalisation éventuelle, le personnel spécialisé peut obtenir l'accès au dossier électronique, et après le séjour à l'hôpital, le médecin peut consulter les données médicales pour les traitements de contrôle. Au moyen d'applications spécifiques, la patiente ou le patient pourrait à l'avenir enregistrer des données relatives à sa santé et, au besoin, les mettre à disposition du personnel spécialisé.

Il n'est pas exclu que le patient reçoive à l'avenir une cyberordonnance, avec laquelle il pourrait commander les médicaments requis pour son traitement auprès d'une pharmacie de vente par correspondance. Par ailleurs, les conditions pourraient être réunies pour un service de conseil médical en ligne (cyberconsultation).

4.4.4 Cyberéducation

La numérisation est depuis longtemps une réalité au sein de l'école obligatoire et des hautes écoles. Il y a actuellement de plus en plus de moyens didactiques numériques à disposition, souvent accessibles uniquement après connexion au portail de l'établissement scolaire ou de l'éditeur. Les certificats et informations scolaires sont eux aussi de plus en plus souvent mis à disposition sous forme électronique. Avec un e-ID, les élèves peuvent accéder à ces ressources.

Les parents aussi peuvent accéder aux informations scolaires grâce à leur e-ID et confirmer en ligne qu'ils ont pris connaissance des résultats de leur(s) enfant(s), afin de s'acquitter de leurs droits et obligations pendant la période de scolarité et de formation.

A un niveau scolaire plus élevé, l'immatriculation et l'inscription pédagogique des branches sont d'ores et déjà possibles par voie électronique. Pour cela, une inscription électronique est aussi requise, qui peut être effectuée de manière sûre avec un e-ID reconnu par l'Etat. En ce qui concerne les hautes écoles, l'utilisation d'un e-ID peut même être envisagée à l'échelon international.

4.4.5 E-commerce

Les détentrices et détenteurs d'un e-ID peuvent utiliser celui-ci pour réaliser des achats dans des boutiques en ligne, s'y enregistrer et se reconnecter ultérieurement à leur compte de manière sûre. Les boutiques en ligne ne peuvent ni ne doivent être légalement tenues d'accepter des e-ID reconnus par l'Etat. Les détentrices et détenteurs d'e-ID verront toutefois un avantage certain à ce qu'elles le fassent. En effet, ils pourront alors utiliser leur e-ID reconnu par l'Etat de manière universelle, sans devoir procéder à de nombreuses reprises à des enregistrements de nom d'utilisateur et mot de passe. Un cadre légal transparent devant en outre être fixé pour les e-ID reconnus par l'Etat, les droits et obligations en la matière sont aussi réglés de manière claire. Il y a ainsi lieu d'interdire aux boutiques en ligne, en leur qualité de PU de commercer avec les données d'identification personnelle transmises par les IdP, ce qui favorise la protection des données personnelles. De telles données ne seront transmises par les IdP d'établissement que si les détentrices et détenteurs l'approuvent expressément.

De plus, l'e-ID permet de manière simple et fiable de prouver son âge, ce qui peut être utile pour

des offres réservés à des jeunes d'un certain âge, ou à l'opposé pour des offres réservées à des adultes ou des retraités.

4.4.6 Cyberpaiement

Payer avec une solution mobile jouit d'une popularité croissante. Avec l'e-ID, il est encore plus simple de prouver son identité numérique afin d'obtenir une solution de paiement numérique. Lors de l'enregistrement, la preuve de l'identité peut être fournie de manière numérique sans discontinuité, l'application étant alors rapidement validée afin d'être utilisée immédiatement. Le paiement mobile est possible en ligne mais aussi hors ligne et représente une solution porteuse d'avenir pour l'ensemble des acteurs en e-commerce.

4.4.7 E-banking

L'e-banking gagne sans cesse en importance. Selon l'Office fédéral de la statistique, 49% de la population a tiré parti en 2015 des possibilités offertes par l'e-banking (Bundesamt für Statistik, Informationsgesellschaft, 2016). Dans ce domaine également, un enregistrement sûr, de même qu'une connexion au portail, sont impératifs pour un déroulement fiable des opérations. Un e-ID reconnu par l'Etat au niveau de sécurité Or ou Platine pourrait remplacer les solutions propriétaires des banques et, à moyen terme, permettre ainsi de réaliser des économies importantes.

4.4.8 Cyber documents d'identité

Si l'on considère l'avenir en portant le regard un peu plus loin, bien que certaines entreprises (Österreichische Staatsdruckerei) (MORPHO) les aient déjà proposés à titre d'essai, on aperçoit les «documents d'identité électroniques relevant de la puissance publique», en bref, les cyber documents d'identité. Ils sont pour ainsi dire le pendant électronique des documents d'identité physiques relevant de la puissance publique tels que le passeport, la carte d'identité ou le permis de conduire.

De tels cyberdocuments peuvent être utilisés pour attester de son identité en cas de rencontre physique avec une PU, par exemple pour prouver son âge dans un magasin ou en cas de vérification de l'identité. Une image lisible de la photo du cyberdocument est alors présentée à la détentrice ou au détenteur d'un e-ID par le biais d'un écran d'un support approprié, et une application de lecture appropriée permet ensuite de la vérifier de manière électronique auprès des IdP. Cela facilite l'établissement de liens conceptuels entre les e-ID purement électroniques et les documents d'identité conventionnels.

Il va de soi qu'il ne s'agit pas simplement de «photos» de documents d'identité qui sont contrôlées avec les cyber documents d'identité, mais qu'en arrière-plan, les procédures et mécanismes de sécurité d'un e-ID reconnu par l'Etat classique sont respectés. Les fonctions requises pour les cyber documents d'identité peuvent être mises en œuvre assez facilement par les IdP et les PU.

4.4.9 Signatures électroniques

Suite à la révision de la loi fédérale sur la signature électronique (SCSE) (Bund), il est possible de proposer en ligne des signatures électroniques en tant que «service de confiance». Les détentrices et détenteurs d'un e-ID reconnu par l'Etat peuvent donc s'enregistrer en ligne auprès d'un prestataire correspondant et d'utiliser immédiatement, par exemple, les signatures électroniques qualifiées basées sur un serveur. L'e-ID reconnu par l'Etat étant disponible au niveau de sécurité requis, il est inutile de se présenter en personne auprès du prestataire du service de signature, ce qui permet de gagner du temps et de l'argent.

4.4.10 Abonnements

Les e-ID reconnus par l'Etat prévus pouvant aussi transmettre la photo du visage des individus (photo du document d'identité) à partir du niveau de sécurité «or», des documents d'identité nécessitant une photo pourraient aussi être commandés en ligne. Cette possibilité pourrait intéresser les entreprises de transport public ainsi que les milieux touristiques. Les détentrices et détenteurs d'un e-ID ne devrait ainsi pas attendre au guichet mais valider en ligne et avec une photo les pièces d'identité requises et les recevoir, par exemple, sur une application mobile ou par courrier postal à domicile.

Les e-ID pourraient aussi compter des fonctions supplémentaires grâce à des applications mobiles. L'e-ID peut alors être utilisé pour l'enregistrement et la connexion et des abonnements et billets peuvent être achetés en ligne par le biais de l'application mobile et attestés, ce qui permet d'économiser les coûts d'émission d'un abonnement ou billet distinct.

4.4.11 Economie collaborative

L'économie collaborative (European Commission) joue un rôle de plus en plus important, et son potentiel est loin d'être épuisé. L'économie collaborative (partage de voiture ou d'appartement, plateformes pour freelance, etc.) fait alors souvent appel à une identification sûre des partenaires commerciaux. Ce besoin peut être couvert à divers niveaux de sécurité grâce à des e-ID reconnus par l'Etat.

4.4.12 Informatique en nuage

A l'instar de la virtualisation, l'informatique en nuage promet des économies par rapport aux systèmes conventionnels. L'informatique en nuage permet d'optimiser nettement l'utilisation des systèmes TIC par rapport à des systèmes individuels dédiés, ce qui permet une planification et une utilisation durable des ressources informatiques. Un e-ID, combiné à d'autres méthodes cryptographiques, peut être utilisé pour protéger les données stockées dans le nuage d'un accès non autorisé.

4.4.13 Réseaux sociaux

Bien qu'un individu puisse très bien utiliser les réseaux sociaux sous un pseudonyme, certaines applications requièrent un enregistrement sûr et fiable, par exemple des forums avec des conditions à remplir pour devenir adhérents. Pensons aux forums destinés aux enfants et aux jeunes, à «protéger» des adultes. Un e-ID reconnu par l'Etat facilite ce travail, puisqu'il livre de manière fiable l'âge de la personne.

5 Protection de l’information et des données

5.1 Introduction

La protection de l’information et des données, de même que la sécurité informatique en général, sont des éléments importants pour pouvoir se fier aux e-ID reconnus par l’Etat. Le comportement des utilisateurs constaté actuellement sur le marché indique toutefois que la convivialité d’utilisation d’une solution est capitale pour que celle-ci soit acceptée. Les milieux industriels déploient des efforts importants pour commercialiser des appareils finaux sûrs et conviviaux, aptes à servir de supports à des e-ID (p. ex. téléphones portables avec Trusted Execution Environment (The Trusted Execution Environment, Delivering Enhanced Security at a lower cost to the mo-bile market, 2011)). Il convient donc de trouver un équilibre réaliste entre sécurité et convivialité d’utilisation.

Le présent concept est fondé sur une répartition des tâches entre l’Etat et le marché, la condition préalable implicite étant la confiance fondamentale dans les services d’identité fournis de manière économiquement viables. Bien que la sécurité de tous les composants, systèmes et organisations concernés de l’écosystème e-ID soit importante, l’Etat ne peut assumer la responsabilité, ni implémenter toutes les mesures de sécurité requises pour faire face à toutes les menaces dans l’ensemble de l’écosystème e-ID. Ainsi, un IdP reconnu par l’Etat peut, par exemple, enregistrer et administrer d’autres attributs d’autres sources en plus des données d’identification personnelle. La responsabilité en incombe donc à l’IdP lui-même.

Conformément à la loi fédérale sur la protection des données (LPD), l’ordonnance concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI), l’ordonnance sur l’informatique et la télécommunication dans l’administration fédérale (ordonnance sur l’informatique dans l’administration fédérale, OIAF), les directives du Conseil fédéral concernant la sécurité informatique dans l’administration fédérale et les lignes directrices relatives à la sécurité informatique dans l’administration fédérale, les menaces et risques que présente l’environnement e-ID doivent être identifiés, et les mesures requises, être prises. En outre, une analyse des besoins en matière de protection (y compris le processus d’audit GRAES) ainsi que les concepts SIPD sont élaborés et les exigences relatives à la sécurité informatique fondamentales, mises en œuvre.

En instaurant une base légale formelle pour les e-ID reconnus par l’Etat, il s’agit d’édicter des prescriptions complémentaires en matière de sécurité et de protection des données pour les organismes concernés et les systèmes techniques.

5.2 Identifiant personnel unique

Dans l’écosystème e-ID, l’IPU a une importance capitale pour l’intégrité des données – comprenez par là l’assignation correcte des données d’identification personnelle à la personne concernée – et la confiance envers l’e-ID. Dans le domaine des assurances sociales, la CdC[31] a déjà réalisé précisément cet objectif en instaurant l’UPI («Unique Person Identification», NAVS13) et peut ainsi garantir un déroulement correct des opérations.

Au besoin, des identifiants sectoriels peuvent être formés avec l’IPU, que cela soit par une fonction «à usage unique» ou par une assignation tabulaire, à l’image de ce qui est déjà une réalité pour le cybernuméro du patient, qui est enregistré par la CdC conjointement au NAVS13.

[31] La Centrale de compensation (CdC) est une division principale du Département fédéral des finances. Elle exploite le service «CdC-UPI», qui attribue aux personnes physique un NAVS13, ainsi qu’un service clearing pour la rectification des données.

Nous estimons qu'un IPU, contrairement à ce qui est parfois prétendu, ne conduit pas à un affaiblissement de la protection des données personnelles. Au contraire, un IPU réduit le risque de confusion ou d'inconsistance des données d'identification personnelle, ce qui pourrait nuire à la personne concernée. En outre, un IPU évite de devoir publier d'autres données d'identification personnelle telles que le nom, le prénom ou la date de naissance, pour une identification univoque, alors que c'est souvent le cas habituellement, ces attributs pouvant être rattachés sans autre dans la vie quotidienne par tout un chacun à une personne physique.

5.3 Besoins en matière de protection

L'analyse des besoins en matière de protection a révélé que des systèmes e-ID reconnus par l'Etat traitent des données personnelles conformément à la LPD, qui peuvent être, dans le cas particulier, particulièrement dignes de protection. Il s'agit par exemple des informations sur l'appartenance à une race ou à une religion, voire sur l'état de santé, pouvant être déduites de la photo d'une personne transmise aux niveaux de sécurité or et platine.

Conformément à l'OPrI, les données d'identification personnelle ne doivent être classifiées ni comme étant confidentielles, ni comme étant secrètes, mais comme des données internes. En ce qui concerne la disponibilité de l'infrastructure de la Confédération, les exigences ne sont pas plus élevées, contrairement à ce qui est le cas en matière d'intégrité et de transparence. La Confédération s'apprêtant à faire appel à des services IAM auprès d'IdP reconnus par l'Etat pour ses portails, comme le précise le présent concept, et ceux-ci pouvant être aussi pertinents en matière de BCM selon le portail, des mesures de sécurité particulières doivent être prises conformément au processus d'audit GRAES. Ces mesures de sécurité sont précisées dans la législation correspondante.

5.4 Objets dignes de protection

Du point de vue de la protection des données, l'être humain est l'objet digne de protection et la technique, le risque. Du point de vue de la sécurité informatique, la technique est l'objet digne de protection et l'être humain, le risque. Dans le premier cas, la priorité dans la définition des mesures de protection va du droit à la technique en passant par l'organisation, alors que c'est exactement l'inverse dans le second cas.

L’illustration ci-après fournit une vue d’ensemble des objets dignes de protection des systèmes e-DI reconnus par l’Etat, pour lesquels des mesures doivent être définies du point de vue de la protection des données et de la sécurité informatique (légende du schéma ci-dessous):

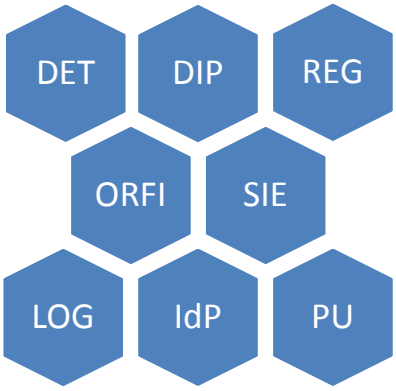


Schéma 16: Objets dignes de protection

Abr.	Détails
DET	La détentrice ou le détenteur d’un e-ID reconnu par l’Etat, y compris l’infrastructure technique qu’elle ou il utilise, par exemple un smartphone, une tablette ou un ordinateur.
REG	Registres de personnes tenus par la Confédération contenant des données d’identification personnelle (Infostar, ISA, SYMIC, CdC-UPI), y compris le personnel et les systèmes techniques.
DIP	Jeu de données unique avec des données d’identification personnelle telles que le nom, le prénom, la date de naissance, la photo, etc.
LOG	Données de la journalisation de la transmission des données d’identification personnelle et de l’utilisation des e-ID reconnus par l’Etat, qui sont (impérativement) collectées par les services concernés.
ORFI	Organisme de reconnaissance des fournisseurs d’identité, y compris le personnel et les dispositifs techniques.
SIE	Service d’identité électronique suisse, y compris le personnel et les dispositifs techniques.
IdP	Fournisseurs de services d’identité, y compris le personnel et les dispositifs techniques utilisés pour éditer les e-ID reconnus par l’Etat
PU	Partie utilisatrice, y compris le personnel et les dispositifs techniques liés à l’utilisation d’un e-ID reconnu par l’Etat.

Tableau 6: Légende des objets dignes de protection

5.5 Risques

Les menaces et points faibles entraînent des risques qui peuvent aboutir à des dommages. Un risque est la vraisemblance qu'une menace se réalise, multipliée par le potentiel de dommage. Les menaces pour la sécurité informatique sont, par exemple, des actes intentionnels commis de l'extérieur ou de l'intérieur, un cas de force majeure et des problèmes d'ordre technique ou des erreurs humaines, telles que la négligence ou une faute. Les menaces pour la protection des données sont, par exemple, des réglementations légales insuffisantes, des actes intentionnels commis de l'extérieur ou de l'intérieur ainsi que des dysfonctionnements des systèmes informatiques.

Risques majeurs pour des systèmes e-ID reconnus par l'Etat:

Abr.	Risque
DET	Violation du devoir de diligence et abus d'identité Les e-ID reconnus par l'Etat doivent eux aussi être protégés conformément aux prescriptions et avec le discernement requis. Une violation du devoir de diligence serait, par exemple, le fait de noter le NIP d'un e-ID ou de renoncer totalement à une détection de la présence de virus informatiques. Un abus d'identité consisterait à une utilisation par des tiers de son propre e-ID, p ex. en autorisant l'utilisation de celle-ci par des tiers (p. ex. le partenaire).
REG	Vol de données Les données enregistrées dans les registres de personnes tenus par la Confédération doivent notamment être protégées contre le vol massif de données et la falsification des données dans le cas particulier.
DIP	Falsification de données La falsification d'un jeu de données contenant des données d'identification personnelle peut entraîner des dommages.
LOG	Abus de données L'utilisation de moyens informatiques, tels que les e-ID, génère des journaux de données qui peuvent être analysées. Ces données doivent être protégées de toute utilisation abusive, p. ex. l'établissement non autorisé d'un profil des utilisateurs.
ORFI	Violation du devoir de diligence La reconnaissance et la surveillance exercée sur les IdP doivent être réalisées avec le soin et l'indépendance qui s'imposent. Il faut pour cela des profils de protection soigneusement élaborés par le SIE.
SIE	Vol de données et falsification de données, manque de connaissances en sécurité informatique Les données traitées par le SIE doivent être protégées contre le vol et la falsification. Le vol de données comprend une transmission non autorisée des données d'identification personnelle à un IdP. Les profils de protection mis à disposition par le SIE pour la reconnaissance des systèmes e-ID doivent être du dernier cri technologique et contrer les menaces actuelles.
IdP	Vol de données Les systèmes e-ID des IdP reconnus par l'Etat doivent en particulier être protégés contre le vol massif de données et la falsification des données dans le cas particulier. Un dysfonctionnement technique de l'e-ID ou un enregistrement erroné d'une personne sont considérés comme une falsification de données.

Abr.	Risque
PU	Vol et abus de données Les processus techniques et organisationnels appliqués par la PU doivent permettre une utilisation irréprochable d'un e-ID reconnu par l'Etat. Une authentification réalisée de manière non correcte constituerait par exemple une erreur. Les données auprès de la PU doivent en particulier être protégées contre le vol massif de données et l'abus de données.

Tableau 7: Risques majeurs

Autres risques fondamentaux:

Abr.	Risque
NUL	Manque de fournisseurs de services d'identité Si aucun fournisseur d'e-ID reconnu par l'Etat ne s'impose sur le marché, le concept de la répartition des tâches entre l'Etat et le marché tourne court. Si l'on considère qu'un e-ID reconnu par l'Etat doit tout de même être introduit, une solution de rechange doit être définie.
FIN	Monopole d'un fournisseur de services d'identité Le concept repose sur l'hypothèse que plusieurs fournisseurs d'e-ID officiels s'établissent dans l'écosystème e-ID et qu'il en résulte donc une situation concurrentielle. A défaut de concurrence, il y a lieu d'éviter que les prix entraînent un développement raté des e-ID reconnus par l'Etat.
KET	Enchaînement d'incidents dommageables De nombreux systèmes individuels (p. ex. Infostar, ISA, IdP, etc.) participent aux e-ID reconnus par l'Etat, et sont intégrés au niveau organisationnel et technique. Il convient d'empêcher que la défaillance d'un système partiel entraîne la défaillance des autres systèmes partiels.
KOV	Perte de contrôle sur les systèmes e-ID reconnus par l'Etat Un contrôle des systèmes e-ID reconnus par l'Etat par des instances étrangères serait politiquement indéfendable. Ces systèmes doivent être «en mains suisses».
AUS	Espionnage des systèmes e-ID reconnus par l'Etat En tant que tels, les e-ID reconnus par l'Etat ne disposent d'aucune autre caractéristique sur une personne, hormis les données d'identification personnelle. Ils ne fournissent notamment aucun renseignement sur les adhésions, fonctions, orientations politiques et aptitudes d'une personne. Un e-ID peut toutefois être utilisé pour obtenir de telles informations, notamment en cas d'abus d'identité.

Tableau 8: Autres risques

Une analyse approfondie des risques conformément au «Manuel de gestion des risques de la Confédération du 29 avril 2013» sera réalisée lors de la rédaction du concept détaillé et des dispositions d'exécution de la loi e-ID.

5.6 Mesures de sécurité

Compte tenu de l'analyse sur les besoins en matière de sécurité (ch. 5.3), la liste des objets dignes de protection (ch. 5.4) ainsi que les risques (ch. 0), les principales mesures de sécurité sont mentionnées ci-après qui doivent être prises pour les systèmes e-ID reconnus par l'Etat:

Abr.	Mesures de sécurité
DET	Contre la violation du devoir de diligence et l'abus d'identité Prescriptions légales (p. ex. gestion, devoir d'annonce); information active des détentrices et détenteurs.
REG	Contre le vol de données Pas de mesures supplémentaires. Les registres des personnes sont d'ores et déjà tenus conformément aux prescriptions de la Confédération.
DIP	Contre la falsification de données Introduction systématique d'un IPU; signature des données d'identification personnelle.
LOG	Contre l'abus de données Prescriptions légales (p. ex. interdiction de faire commerce des profils); audits dans le cadre de la reconnaissance et de la surveillance.
ORFI	Contre la violation du devoir de diligence Processus contrôlés (évtl. certification ISO-27000); contrôle de sécurité relatif aux personnes.
SIE	Contre le vol de données et la falsification de données, manque de connaissances en sécurité informatique Données actuelles d'identification personnelle; processus contrôlés (évtl. certification ISO-27000); contrôle de sécurité relatif aux personnes; signature numérique; canal de communication sécurisé; économie des données; listes bloquées (p. ex. avec les détentrices et détenteurs décédés); formation continue systématique et collaboration avec les spécialistes en sécurité informatique.
IdP	Contre le vol de données Données actuelles d'identification personnelle; utilisation d'un IPU; prescriptions légales (p. ex. profils de protection selon ISO/IEC 15408, données conservées en Suisse, responsabilité, délais de suppression, listes bloquées); reconnaissance par l'Etat et surveillance; prescriptions techniques actuelles pour la reconnaissance; processus contrôlés (évtl. certification ISO-27000); contrôle de sécurité relatif aux personnes.
PU	Contre le vol de données et l'abus de données Prescriptions légales (p. ex. gestion, consignes pour la protection des données d'identification personnelle); transmission contrôlée des données d'identification personnelle par les IdP (p. ex. le NAVS13 sur la base d'une «white list»).
NUL	Contre le manque de fournisseurs de services d'identité Conditions-cadre attrayantes pour les IdP; solution de rechange (publication d'un e-ID par la Confédération).
FIN	Contre un monopole des prestataires Conditions-cadre attrayantes pour les IdP; prescriptions légales pour les prix.

Abr.	Mesures de sécurité
KET	Contre l’enchaînement d’incidents dommageables Raccordement à la légère des systèmes; analyse des risques et BCM; responsabilités réglementées.
KOV	Contre la perte de contrôle sur les systèmes e-ID reconnus par l’Etat Systèmes orientés sur les utilisateurs (p. ex. accord exprès pour la transmission des données d’identification personnelle); prescriptions légales et de sécurité («droit suisse et for», «traitement des données en Suisse», «pas d’obligation de publication des données»); responsabilités réglementées.
AUS	Contre l’espionnage des systèmes e-ID reconnus par l’Etat Prescriptions légales (p. ex. économie des données, interdiction de former des profils, délais de suppression); prescription de point («pas d’obligation de publication des données»)

Tableau 9: Mesures de sécurité

6 Législation

6.1 Généralités

La définition d'un cadre juridique clair doit permettre d'atteindre les buts suivants:

- Réduction ou empêchement des abus d'identités et des falsifications d'identité dans le monde numérique;
- Promotion d'un trafic commercial électronique sûr entre particuliers et autorités; et
- Interopérabilité et perméabilité des systèmes e-ID en Suisse et avec l'UE (notification).

Les prescriptions sont données par la loi e-ID à rédiger, les dispositions d'application correspondantes ainsi que les standards requis, et elles comprennent les indications d'ordre juridique, organisationnel et technique pour

- la teneur, l'établissement, l'exploitation, l'administration, le retrait et l'utilisation des e-ID reconnus par l'Etat;
- la reconnaissance par l'Etat des IdP ainsi que la surveillance sur les IdP reconnus et leurs systèmes e-ID;
- l'interface pour la transmission des données par l'Etat d'identification personnelle à l'IdP;
- l'interopérabilité des systèmes e-ID.

L'ensemble de la réglementation doit être conçue de manière à ce qu'il en résulte un cadre de confiance pour un écosystème e-ID pérenne, qui constitue la base pour le développement ultérieur des marchés numériques. Si possible et judicieux, il y a lieu de s'appuyer sur des standards internationaux ou des prescriptions déjà établies sur le marché. Dans l'environnement technique et dynamique existante des e-ID, il est tout à fait judicieux de procéder au réglage fin sur les plans techniques et opérationnels au niveau des dispositions d'exécution. La loi ne doit donc définir que les objectifs des catégories d'e-ID, en l'espèce les niveaux de sécurité. Le Conseil fédéral doit pouvoir définir les détails techniques et organisationnels, y compris les restrictions relatives à la transmission de certains attributs (p. ex. le NAVS13) à certaines PU. A l'inverse, la loi doit préciser les conséquences en cas d'abus de la part des PU. Il doit ainsi être possible de retirer l'autorisation à un IdP reconnu.

Par principe, les PU définissent le niveau de sécurité entrant en ligne de compte pour quel type d'application. Ainsi, un niveau de sécurité différent de l'e-ID peut être choisi pour le vote électronique que pour les applications recommandées en matière de cybersanté ou indispensables pour la cyberéducation.

6.2 Rapport à d'autres lois

Les travaux législatifs examineront et mettront en évidence en détail les points de contact avec d'autres lois. Le cas échéant, des modifications seront apportées lors de la «révision d'autres actes législatifs». Des réglementations claires en matière de responsabilité des IdP et/ou des services de certification sont visées.

7 Annexe

7.1 Définitions des termes

Le concept e-ID 2016 ainsi que le projet de loi (loi fédérale sur les unités d'identification électronique reconnus par l'Etat) font appel à divers termes qui sont expliqués ci-après et qui sont reliés d'un point de vue sémantique et logique. Les paragraphes suivants expliquent les termes utilisés autant que possible, sans entrer dans le détail du discours scientifique.

A. Termes de base

Le terme fondamental de l'identité est un terme qui a de nombreuses facettes, et qui a été analysé à de nombreuses reprises, et continuera de l'être, quant à ses nombreuses acceptions sur les plans philosophique, psychologique, juridique, économique et technique. Le réseau européen Network of Excellence - Fidis en constitue un bon exemple ((Eds), 2009). Dans le contexte de la procédure législative, le terme d'identité est utilisé dans un sens un peu plus restrictif sur les plans juridique et technique, à l'image de ce qui a été fait par NIST (NIST Hildegard Ferraiolo, Larry Feldman and Greg Witte, 2014) et l'UE (EU, 2014). Notre logique de définition est aussi fondée sur les normes eCH tirés du modèle d'information (eCH, eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID, 2014) (eCH, eCH-0107 IAM Gestaltungsprinzipien v2.0, 2013) (eCH, 2014).

1. Entités, ensemble d'entités et attributs

Cette approche est fondée sur une vue externe adoptée par une administration[32] sur une quantité d'unités matérielles ou immatérielles dans le monde réel, désignées par le terme d'**entités**. La totalité des entités pertinentes est définie par le contexte administratif et est désigné par le terme d'**ensemble d'entités**[33]. Du point de vue et dans le contexte de l'administration, une **entité** va avoir une série de caractéristiques qu'elle pourra constater avec un certain degré de vraisemblance et qui représentent ensuite une entité en tant que jeu de données d'**attributs** dans un système d'information de l'administration.

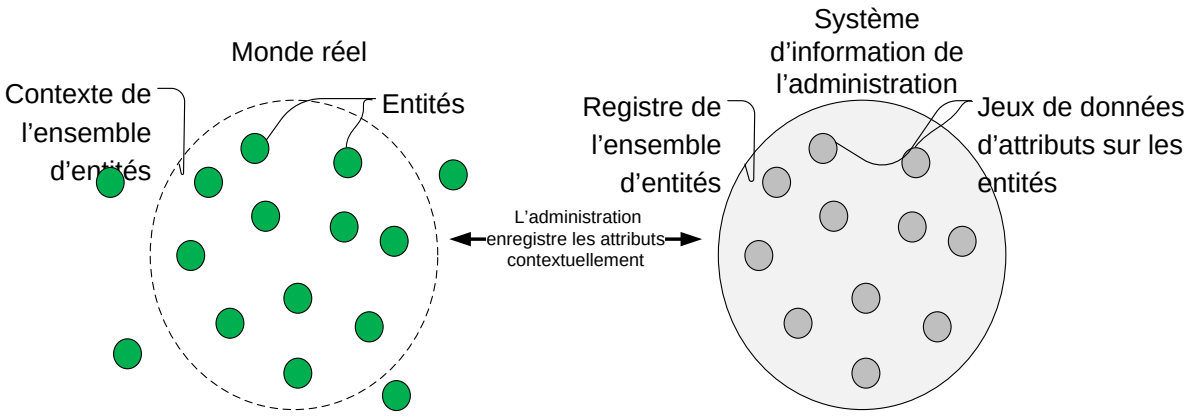


Schéma 17: Attributs comme caractéristiques pertinentes des entités pour l'administrateur

[32] L'administration est une instance qui administre les entités et qui peut leur assigner des rôles et des droits. Typiquement, il s'agit d'une PU, d'un fournisseur de services d'identité ou d'une organisation officielle.

[33] Dans les normes eCH [7] [51] [50], l'entité n'est comprise que comme une personne et est désignée ensuite comme *sujet*. L'ensemble d'entités et l'administration correspondante correspondent aux termes *espace nominatif* et *ressource.*

Un attribut est composé du **nom de l'attribut**, de la **valeur de l'attribut** et, éventuellement, d'autres métadonnées telles que, par exemple, un type de données ou une date de validité. Le nom définit la signification sémantique de l'attribut et, ainsi, le domaine des valeurs d'attribut possibles. La valeur de l'attribut résulte d'une définition de l'attribut pour une entité particulière.

Implicitement, la sécurité avec laquelle la valeur de l'attribut a été définie et sur la base de laquelle la confiance de l'administration repose quant à l'exactitude de l'assignation est aussi assignée à la valeur de l'attribut. La confiance de l'administration découle de la solidité de la liaison entre la caractéristique et l'entité, la garantie que la valeur d'attribut correspondante a été saisie correctement, resp. la fiabilité de la source à partir de laquelle l'attribut a été tiré, ainsi que la durée écoulée depuis la définition de l'attribut. Ainsi, la constatation de l'authenticité d'une carte SIM en particulier est très sûre, par contre le lien entre le téléphone portable en tant que support de la carte SIM et la personne est ténu. D'un autre côté, une caractéristique biométrique est fermement liée à une personne, mais lors de la mesure, une certaine incertitude demeure quant à savoir si la valeur de l'attribut a été constatée et assignée de manière correcte. Selon le contexte, la confiance qui en résulte dans la véracité de la valeur de l'attribut et son assignation à une personne suffit ou non. En général, la confiance dans la définition d'attribut réalisée une fois diminue au fil du temps, raison pour laquelle les attributs sont saisis à nouveau de temps à autre, afin de maintenir un degré de confiance élevé.

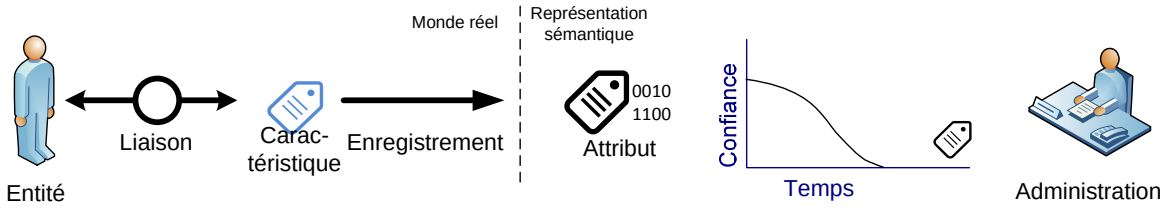


Schéma 18: Sécurité d'un attribut et confiance en fonction du temps

Si la valeur d'un attribut est définie avec suffisamment de sécurité pour toutes les entités, l'ensemble d'entités fondamentales peut être réparti en ensembles partiels, dans lesquels toutes les entités reçoivent la même valeur d'attribut[34]. Prenons pour exemple la partition d'un groupe de personnes en fonction de l'attribut *date de naissance*. Les divers ensembles partiels de cette partition sont formés par les personnes qui ont toutes la même date de naissance comme valeur d'attribut. Divers attributs indépendants les uns des autres ou seulement en faible corrélation aboutissent à des partitions différentes de l'ensemble des entités. A cet égard, il y a des attributs qui partitionnent fortement un ensemble d'entités et d'autres qui ne le font que de manière modeste, voire qui ne proposent aucune nouvelle information, par exemple l'année de naissance si la date de naissance est déjà connue.

2. Combinaison d'attributs

Un ensemble d'entités, ou plus exactement l'ensemble des jeux de données avec les attributs saisis appartenant aux entités, peut être partitionné plusieurs fois grâce à des plusieurs attributs le plus possible indépendants. Ce n'est que lorsqu'il ne reste plus qu'un seul jeu de données d'attribut assigné à une entité au maximum pour chacune des ces partitions d'attribut dans les ensembles d'entités que toutes les entités de l'ensemble d'entités peuvent être différenciées par les jeux de données avec les attributs saisis qui les représentent. Dans ce cas, la combinaison

[34] Formellement, la définition d'un attribut est une illustration de l'ensemble des entités dans l'espace des valeurs d'attribut. Il n'y a partition univoque de l'ensemble d'entités que si une valeur d'attribut est définie de manière univoque pour chaque entité au niveau de sécurité requis. La partition de l'ensemble d'entités résulte alors des représentations originelles des diverses valeurs d'attribut.

des attributs constatés est **identifiante** au niveau de confiance correspondant. De manière générale, un jeu de donnnées d'attributs pour une entité est désigné par le terme d'**identité partielle**. Si les attributs sont identifiants, il s'agit d'une identité partielle identifiante.

Si une identité partielle ne comprend que des attributs dont l'ensemble partiel ne sépare pas toutes les entités, un certain anonymat demeure, qui correspond à la plus importante partie de l'ensemble non séparé. Par exemple, l'identité partielle *nom* et *date de naissance* dans l'ensemble d'entités de la population résidant en Suisse laisse un certain anonymat, car il y a plusieurs personnes avec le même nom et la même date de naissance. S'il y a un seul attribut qui met déjà totalement fin à l'anonymat, il est désigné par le terme d'**identifiant[35].**

Le Schéma 19 présente symboliquement A) un ensemble d'entités avec les diverses entités (représentées par leurs jeux de données d'attribut) et B) une partition de cet ensemble par un attribut nominatif et l'ensemble partiel défini par une certaine valeur d'attribut. La combinaison d'attributs (ensemble des partitions d'une identité partielle) est présentée en C). Un attribut individuel qui sépare toutes les entités de l'ensemble d'entités est un identifiant en D).

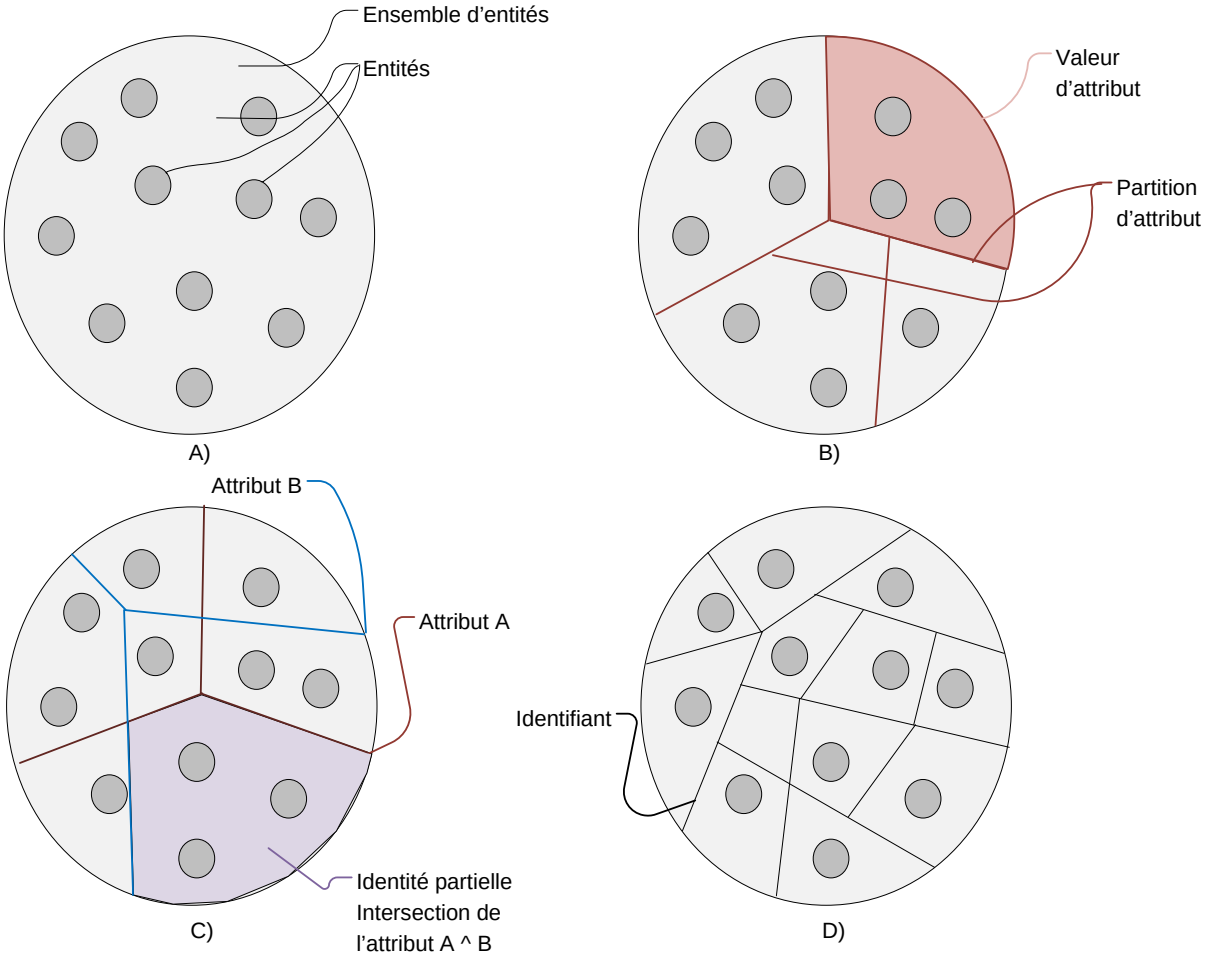


Schéma 19: jeu de données sur les ensembles d'entités et les identités partielles

[35] Une identité partielle identifiante en tant que représentation d'une entité sous forme d'attributs avec un identifiant est désigné par le terme *eIdentity* dans les standards eCH. Le terme eIdentiy est toutefois souvent utilisé avec des significations sémantiques différentes, raison pour laquelle nous lui préférons la notion d'identité partielle identifiante.

Un identifiant est souvent assigné par une administration à un ensemble d'entités et peut alors être utilisé par d'autres administrateurs, pour lesquels des ensembles partiels de l'ensemble d'entités plus vaste sont pertinents dans leur contexte, qui sont également utilisés comme attribut pleinement identifiant. Dans la population résidant en Suisse, un tel identifiant est par exemple le NAVS13, qui est attribué par la CdC aux personnes en Suisse et qui est utilisé comme identifiant par diverses instances.

3. Classes des ensembles d'entités

Un cadre légal divise les entités en sujets juridiques et en objets juridiques. Les **sujets juridiques** ont des devoirs et des obligations. A l'opposé, les **objets juridiques** sont des objets qui disposent d'un sujet juridique auquel ils peuvent prétendre eux-mêmes. Les sujets juridiques sont des **personnes physiques** (êtres humains) et des **personnes morales** (p. ex. entreprises ou institutions). Les objets juridiques sont des **biens matériels** (p. ex. immobilier ou mobilier) et des **biens immatériels** (p. ex. des brevets, des droits d'auteur, des créances monétaires ou des logiciels).

Bien qu'en principe l'identification électronique dans le contexte «Internet of Things (IoT)» soit pertinente pour tous les types d'entités, la loi e-ID se focalise, conformément au mandat, sur les sujets juridiques que sont les personnes (physiques). Logiquement, le concept porte sur les *personnes physiques*, qui, en matière d'e-ID suisse, forment les ensembles d'entités pertinentes.

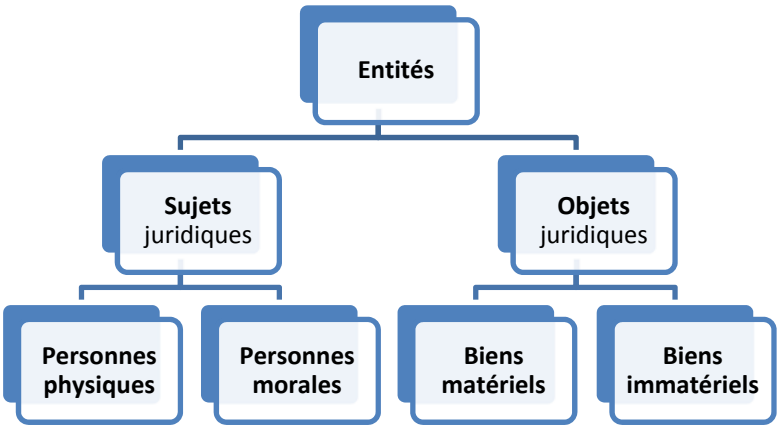


Schéma 20: Catégorisation des entités en sujets et objets juridiques

4. Personne – fichier personnel, écosystème e-ID

De par ses activités sociales et économiques, chaque personne est membre de nombreux ensembles d'entités contextuelles, que nous désignons par le terme de **fichier personnel** en référence au fichier de clients[36]. Une **personne** peut être citoyenne ou citoyen d'un Etat, collaboratrice ou collaborateur d'une entreprise, cliente ou client d'un magasin, membre d'un parti, d'un club ou d'autres groupes. Ensemble, tous ces groupes sont le fichier personnel des personnes concernées défini par un cadre réglementaire (loi, contrat, statuts, etc.) et géré par une organisation à définir selon le contexte. Si l'organisation est un Etat et le cadre réglementaire défini par une Constitution, des lois et des règles d'application, le fichier personnel ainsi défini est nommé **population.** Pour une certaine population, l'ensemble de toutes les personnes et des instances admnistratrices qui définissent de tels fichiers personnels en fonction du contexte au sein de la populaiton sont désignés par le terme **écosystème d'identité** ou **écosystème e-ID**.

[36] Un fichier personnel est à un certain moment défini de manière fixe par la quantité de jeux de données de l'identité partielle qui la représente auprès de l'administration. Au fil du temps, des jeux de données peuvent être saisis nouvellement ou supprimés pour des personnes. Le fichier personnel évolue en conséquence.

5. Identifiant personnel, données d'identification personnelle

Dans un contexte spécifique, une personne est déterminée de manière univoque par une identité partielle identifiante à un certain niveau de fiabilité. Un attribut qui identifie à lui seul toutes les personnes d'un fichier personnel est un **identifiant personnel**. Si un tel identifiant se rapporte à l'ensemble de la population d'un Etat, nous le désignons par le terme d'**identifiant personnel unique (IPU)**. Le NAVS13 est un exemple d'un attribut identifiant dans le fichier personnel de la population saisie par la CdC; il représente donc un IPU.

Les attributs enregistrées et administrés par l'Etat sont désignés par le terme de **données d'identification personnelle**. Les données d'identification personnelle permettent d'identifier de manière indubitable une personne dans la population. Le plus souvent un modeste échantillon de telles données suffit, par exemple les *nom, prénom* et *date de naissance*, qui sont de fait identifiantes en Suisse en tant qu'identité partielle[37].

Si un IPU est défini pour une population comme un fichier personnel défini par l'Etat, il est possible de déduire de cet IPU des identifiants personnels différents pour chaque fichier personnel subordonné (identifiants sectoriels), voire de limiter leur durée de validité (identifiants transitoires). Les identifiants déduits peuvent servir à empêcher une identification transversale par divers fichiers personnels subordonnés pour des raisons de protection des données. Les systèmes d'identifiants déduits doivent être administrés, ou pour le moins surveillés, par l'administration du fichier personnel officiel, car seule cette instance peut abolir l'anonymat relatif entre les fichiers personnels au moyen d'identifiants déduits différents.

6. Identité d'une personne

L'**identité** d'une personne est une généralisation idéalisée des identités partielles d'une personne. Elle est par principe composée de tous les attributs qui auraient pu être assignés dans tous les contextes possibles et pour lesquels une confiance suffisante existe dans l'ensemble quant au fait qu'au moment de la constatation, ils décrivaient exactement la bonne personne. En ce qui concerne un écosystème e-ID avec des données d'identité saisies par l'Etat pour l'ensemble de la population, l'identité est souvent utilisée comme synonyme pour l'identité partielle saisie par l'Etat avec les données d'identification personnelle, que l'on désigne plus exactement par le terme d'**identité civile** ou **officielle**.

7. Classes d'attribut

En matière d'attributs, il y a lieu de distinguer entre ceux qui sont assignés aux personnes par l'administration d'un fichier personnel, ceux dont la personne dispose en tant que caractéristique personnelle indépendamment d'une réglementation, et ceux qui sont souvent assignés pour la vie par la réglementation officielle prévalente, qui définit la population et l'identité civile des personnes.

i. Attributs assignés

Il s'agit en principe d'attributs d'une personne connus publiquement mais dépendant du contexte du fichier personnel, par exemple la licence d'adhésion à une association, le numéro de client d'une PU, le numéro personnel, la procuration d'une entreprise, un identifiant d'utilisateur pour accéder à un service, etc. Ils servent à identifier contextuellement les membres saisis dans le fichier personnel et à leur attribuer des rôles. Les organisations professionnelles tiennent de tels registres de personnes pour leurs membres, avec des attributs ainsi assignés, tels que la qualification, les spécialisations, les accréditations, les autorisations, etc. De tels attributs peuvent être assignés aux fichiers personnels de toutes les organisations administratrices. Le plus souvent,

[37] Les taux de méprise avec ces trois attributs sont à un niveau ppm au sein de la population suisse.

ils complètent des données d'identification personnelle et n'ont souvent une signification que dans un contexte spécifique.

ii. Attributs personnels en tant que facteurs d'authentification

Il s'agit des attributs appartenant à la personne, tels que les caractéristiques biométriques, des secrets inventés ou assimilés par exemple des codes NIP ou la possession d'un type d'outil personnel, par exemple une smartcard personnalisée ou un document d'identité. En principe, de tels attributs sont privés et ne peuvent être saisis par une administration et ajoutés à une identité partielle identifiante qu'avec l'accord et la coopération de la personne concernée[38]. Ils servent en particulier à vérifier l'authenticité d'une personne. Pour une authentification, la personne concernée révèle l'attribut personnel à l'administration du fichier personnel de manière à ce que cette dernière puisse ultérieurement vérifier que l'attribut personnel est disponible. Les attributs personnels ainsi saisis sont le plus souvent définis pour être vérifiés au sein du fichier personnel uniquement, pour lequel ils ont été saisis. La saisie et la vérification peuvent aussi être effectuées indirectement par le biais d'un appareil, qui enregistre les attributs personnels originaux et les vérifie avant de transmettre uniquement le résultat de la vérification. Un authentifiant e-ID est une réalisation typique d'un tel appareil. Dans le cas de l'authentifiant e-ID, l'identifiant et les éléments de sécurité de l'appareil font partie de l'identité partielle du détenteur de l'authentifiant enregistrée auprès de l'administration (IdP). D'autres exemples de tels appareils, mentionnons les authentifiants distribués par les établissements bancaires, qui enregistrent la présence de la personne au moyen d'un code NIP ou par biométrie, et qui génèrent un code à usage unique à titre de confirmation de la vérification réussie. Un attribut ainsi assigné représente alors les attributs personnels sous-jacents.

Il arrive fréquemment que les attributs personnels soient aussi désignés par le terme de **facteurs d'authentification**, répartis entre les trois catégories **biométrique, basé sur le savoir** et **basé sur la propriété**. Des attributs isolés, qui se fondent sur une caractéristique pouvant être mesurée, par exemple les caractéristiques biométriques, ne peuvent que peu être utilisés comme identifiants pour des fichiers personnels de taille importante, car il y a presque toujours des personnes qui présentent des valeurs d'attribut ne pouvant être différenciées compte tenu de la précision des mesures et de la sécurité visée[39]. Pour des fichiers personnels de taille plus modeste et préalablement limités, des attributs mesurables peuvent cependant très bien être identifiants. Normalement, ils servent toutefois à confirmer une identité partielle prétendue à laquelle ils appartiennent par une nouvelle saisie et une vérification. Une administration, par exemple, vérifie si le mot de passe saisi par une personne lors de la connexion correspond au mot de passe enregistré conjointement à l'identifiant d'utilisateur se rapportant à cette personne. Ou le policier vérifie d'un regard rapide si le visage de la personne correspond à la photo qui figure sur la carte d'identité comme identité partielle.

iii. Attributs de l'identification officielle d'une personne

La troisième catégorie est constituée des attributs les plus souvent assignés à la naissance[40] à une personne selon des règles officielles et par un processus officiel de gestion des identités et qui permettent d'identifier, en tant qu'identité civile, l'individu au sein de la population en général.

---

38 En médecine légale, la coopération de la personne n'est pas consciente, mais exige de la part de la police, en sa qualité d'instance administratrice, des efforts supplémentaires importants pour relier une identité partielle identifiante à des attributs personnels enregistrés.

39 Il existe certaines exceptions: l'iris d'une personne est ainsi un attribut identifiant au sein de la population mondiale. Cela vaut également pour l'ADN, avec pour restriction les jumeaux monozygotes.

40 Il y a bien sûr des Etats qui ne saisissent que de manière lacunaire, voire inexistante, des données d'identification personnelle ou des personnes, qui pour une quelconque raison essaient de rompre la liason avec leurs données d'identification personnelle et donc se départir de leur identité civile. Dans de tels cas, un Etat peut assigner à une personne de nouvelles données d'identification personnelle valables au sein de sa population.

Ces données d'identification personnelle sont administrées dans des registres de personnes officiels. Citons à titre d'exemple les *nom*, *prénom*, *date de naissance*, *lieu de naissance*, etc. Elles sont attribuées de manière contextuelle par filiation, localisation et date à une nouvelle entité *personne* à la naissance, contrôlées à chaque fois qu'un document d'identité est établi et signalées de manière idoine lors du décès. Mais la *nationalité*, le *numéro de passeport* ou les *coordonnés* font aussi partie de ces attributs. Contrairement à la plupart des autres données d'identification personnelle, ils ne sont pas forcément valables durant toute la vie ou ont une durée de vie explicitement limitée.

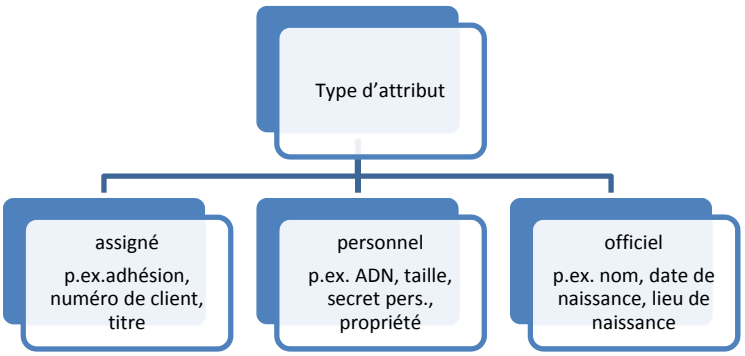


Schéma 21: Catégories d'attributs pouvant être saisis dans des identités partielles

8. Hiérarchie des fichiers personnels

Le fichier personnel défini contextuellement par un administrateur est dans la plupart des cas un ensemble partiel d'un fichier personnel plus important, pour lequel certains attributs ont déjà été constatés ou assignés. Au sommet d'une telle hiérarchie de fichiers personnels se trouve l'ensemble de la population d'un écosystème d'identité avec des données d'identification personnelle de l'identité civile. Les attributs de l'identité civile sont administrés au moyen des registres officiels d'état civil et la confiance dans l'assignation correcte des attributs saisis pour les personnes est, en Suisse, sans cesse renouvellée par une vérification réitérée de ces données à chaque fois qu'un document d'identité est établi.

Les attributs des données d'identification personnelle sont souvent enregistrés également dans des fichiers personnels subordonnés, de sorte que l'identité civile de l'état et l'identité partielle dans le fichier personnel subordonnés déterminent la même personne. Ainsi, une entreprise d'e-commerce va vouloir catégoriser son fichier de clients le plus possible dans le cadre juridique officiel et elle va donc aussi enregistrer des attributs qui sont importants pour une telle catégorisation et identifier la cliente ou le client en tant que personne avec son identité civile officielle.

Les divers fichiers personnels peuvent se recouper et sont donc partiellement représentés par des identités partielles identiques avec des attributs identiques. Ainsi, le nom et la date de naissance d'une personne sont, dans nombre de registres de fichiers personnels, une partie de l'identité partielle enregistrée. Pour des raisons de protection des données, il peut être judicieux de faire en sorte que des identités partielles de certains fichiers personnels se recoupent le moins possible, afin qu'aucun lien ne puisse être établi entre elles. Cela peut, par exemple, être réalisé par une réduction des attributs officiels à un identifiant personnel sectoriel déduit. L'IPU introduit par le présent concept constitue la base d'une telle option. Un IPU offre en tous les cas une meilleure protection de la sphère privée que l'alternative actuellement usuelle constituée des *nom, prénom* et *date de naissance*, qui peut en pratique être très simplement rapportés à une certaine personne, par exemple par le biais des réseaux sociaux. Le **Fehler! Verweisquelle konnte nicht gefunden werden.** présente des exemples de fichiers personnels différents inté-

grant des données d'identification personnelle dans leurs jeux de données d'attribut. De tels fichiers personnels se recoupent en partie, et leurs identités partielles sont le plus souvent centréees sur des attributs tirés des données officielles d'identification personnelle.

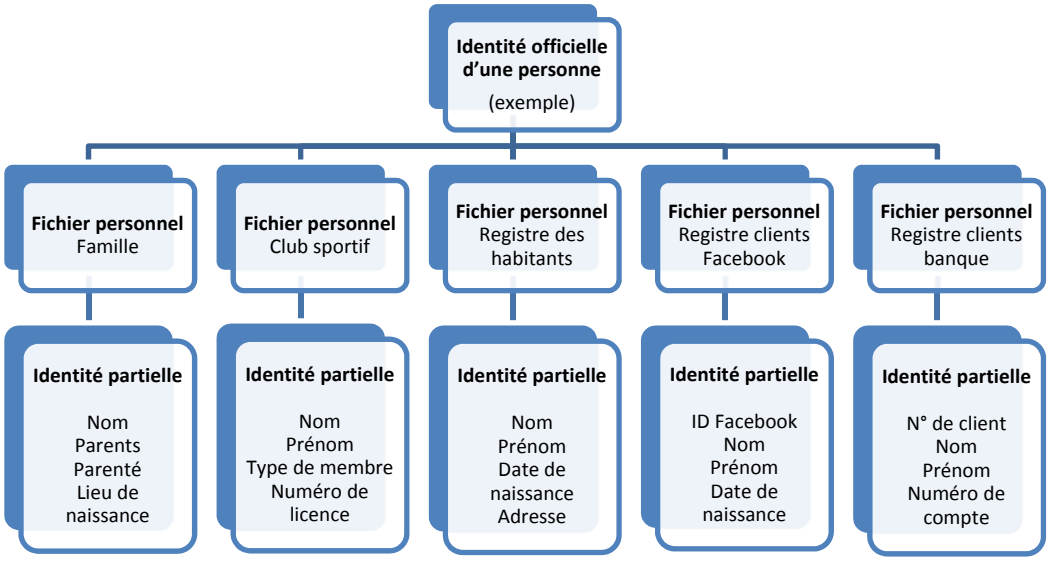


Schéma 22: Exemples de fichiers personnels différents

B. Gestion des identités (GId), système de gestion des identités (SGId)

La gestion des données des identités partielles d'un fichier personnel, sa sécurisation et sa maintenance, ainsi que la réalisation de l'identification et de l'authentification de certaines personnes sont désignés par le terme générique de **gestion des identités (GId)**. L'ensemble des outils permettant de s'acquitter de ces tâches est un **système de gestion des identités (SGId)**. Le cœur d'un SGId est composé du registre des personnes avec les attributs des identités partielles saisis et les processus définis pour gérer, utiliser et administrer le registre.

9. Cycle de vie d'une identité partielle en GId

Les principales phases du cylce de vie d'une identité partielle dans un GId sont l'**enregistrement** d'une nouvelle personne, la **reconnexion** d'une personne déjà saisie et la **suppression** de personnes sorties. La répartition des rôles et droits ne fait déjà plus partie des tâches centrales d'un GID, qui ne sont souvent considérés que comme une partie d'un système global[41]. Les registres des habitants, des impôts ou de l'état civil tenus par les autorités, les registres des clients des médias sociaux, entreprises et banques ainsi que les listes de membres d'association ou le répertoire des élèves d'un établissement scolaire sont des exemples de tels SGId.

i. Enregistrement d'une personne en GId

Pour enregistrer une nouvelle personne, son identité partielle doit être établie dans le contexte

[41] Souvent la répartition des rôles et donc la garantie des droits d'utiliser l'organisation exploitant un GId est décrite comme une partie d'un système global, désigné par le terme de système Identity and Access Management (IAM). Pour une répartition correcte des rôles selon les indications de l'organisation, il faut au préalable un enregistrement et, pour l'exercice d'un rôle, une connexion préalable et donc impérativement la fonctionnalité d'un GId. En ce qui concerne l'administration des droits d'accès, il s'agit toutefois de tâches supplémentaires qui sont regroupées sous le terme de gestion des accès. Pour une modélisation efficace du système, il est toutefois recommandé de séparer l'administration des droits d'accès au GId [7].

de l'organisation administratrice ou tirées du SGId d'un fichier personnel prévalent. Un identifiant spécifique au contexte est un élément de l'identité partielle, qui représente la totalité de l'identité partielle de la personne. L'identifiant également peut être défini de manière spécifique pour le SGId ou être tiré d'un fichier personnel prévalent.

Lors de l'enregistrement, l'identité partielle d'une personne dans le SGId est enregistrée au niveau de sécurité défini par l'administration. En font partie au moins un attribut personnel (secret) en tant que facteur d'authentification servant de référence (**liaison**), saisi sous forme protégée ou redéfini conjointement avec la personne. Certains facteurs d'authentification, par exemple les attributs biométriques, doivent alors ne pas être révélés chaque fois par la personne concernée, mais peuvent être remis sous forme indirecte comme données de référence dans un appareil fermé (authentifiant)[42]. Outre les facteurs d'authentification, d'autres attributs sont saisis, par exemple certaines données d'identification personnelle, qui sont comparées à des attributs connus d'un fichier personnel prévalent ou existant (**identification initiale)**. Le plus souvent, il s'agit d'attributs de l'identité civile. Après l'enregistrement fructueux, le système est activé pour utilisation par la personne autorisée.

ii. Nouvelle connexion au GId

Si une personne souhaite ultérieurement prouver son appartenance à un fichier personnel géré par GIdn, elle se connecte au moyen de l'identifiant personnel attribué ou un pseudonyme correspondant (identifiant d'utilisateur, etc.) et prétend ainsi être la bonne personne. Le SGId procède alors à une **authentification** au moyen des facteurs d'authentification enregistrés qui font partie de l'identité partielle prétendue d'une personne. Pour l'authentification, la personne doit prouver qu'elle dispose actuellement des mêmes facteurs d'authentification (attributs personnels) que ceux saisis lors de l'enregistrement de son identité partielle. En fonction du nombre de tels facteurs indépendants qui doivent être vérifiés, il est question d'une authentification à un, deux ou trois facteurs.

iii. Suppression ou blocage temporaire

Si une personne ne fait plus partie du fichier personnel administré par GId, l'identité partielle saisie lors de l'enregistrement est supprimée. Les tâches d'un GId comprennent également la surveillance de l'utilisation régulière de l'identité partielle enregistrée. En cas de doute sur la confiance encore à accorder à une identité partielle, son utilisation peut être provisoirement ou définitivement bloquée.

10. Processus de base d'un système de gestion des identités (SGId)

L'identification et l'authentification d'une personne sont des processus de base de la gestion des identités. L'exploitant d'un GId peut aussi fournir ces prestations à des tiers qui administrent un fichier personnel subordonné.

La différence entre ces deux processus est facilement illustrée à l'aune de l'exemple d'une connexion à un portail en ligne. Une utilisatrice ou un utilisateur procède lors du premier contact avec le portail à un enregistrement, par lequel elle ou il crée une identité partielle dans le SGId du portail. Celle-ci comprend notamment aussi un identifiant personnel librement choisi (pseudonyme) ou assigné (identifiant d'utilisateur, numéro d'inscription). Dans le même temps, elle ou il doit dévoiler auprès du SGId au moins un attribut personnel directement (p. ex. mot de passe personnel) ou par le biais d'un média intermédiaire (p. ex. les éléments de sécurité d'une carte SIM validés par un code NIP) en tant qu'élément de l'identité partielle.

[42] Un tel appareil fait partie du SGId et fournit avec une sécurité définie le résultat de la vérification des facteurs d'authentification.

Si la personne se reconnecte ultérieurement au portail, elle s'identifie au moyen de l'identifiant personnel pointant vers son identité partielle dans le SGId (**identification**). Elle prétend alors être l'utilisatrice ou l'utilisateur enregistré dans le SGId. Au cours d'une étape ultérieure, elle le prouve au moyen de l'attribut personnel enregistré dans le SGId sous la même identité partielle et s'authentifie ainsi (**authentification**). Cette preuve est fournie soit à nouveau directement, soit indirectement, de la même manière que l'attribut personnel a été saisi lors de l'enregistrement. L'authentification est donc un processus au cours duquel une confirmation de l'identité prétendue d'une personne est demandée. La reconnexion avec identification par un identifiant personnel avec authentification subséquente est, par rapport à l'identification initiale avec saisie de l'identité partielle lors de l'enregistrement, un processus très fréquent.

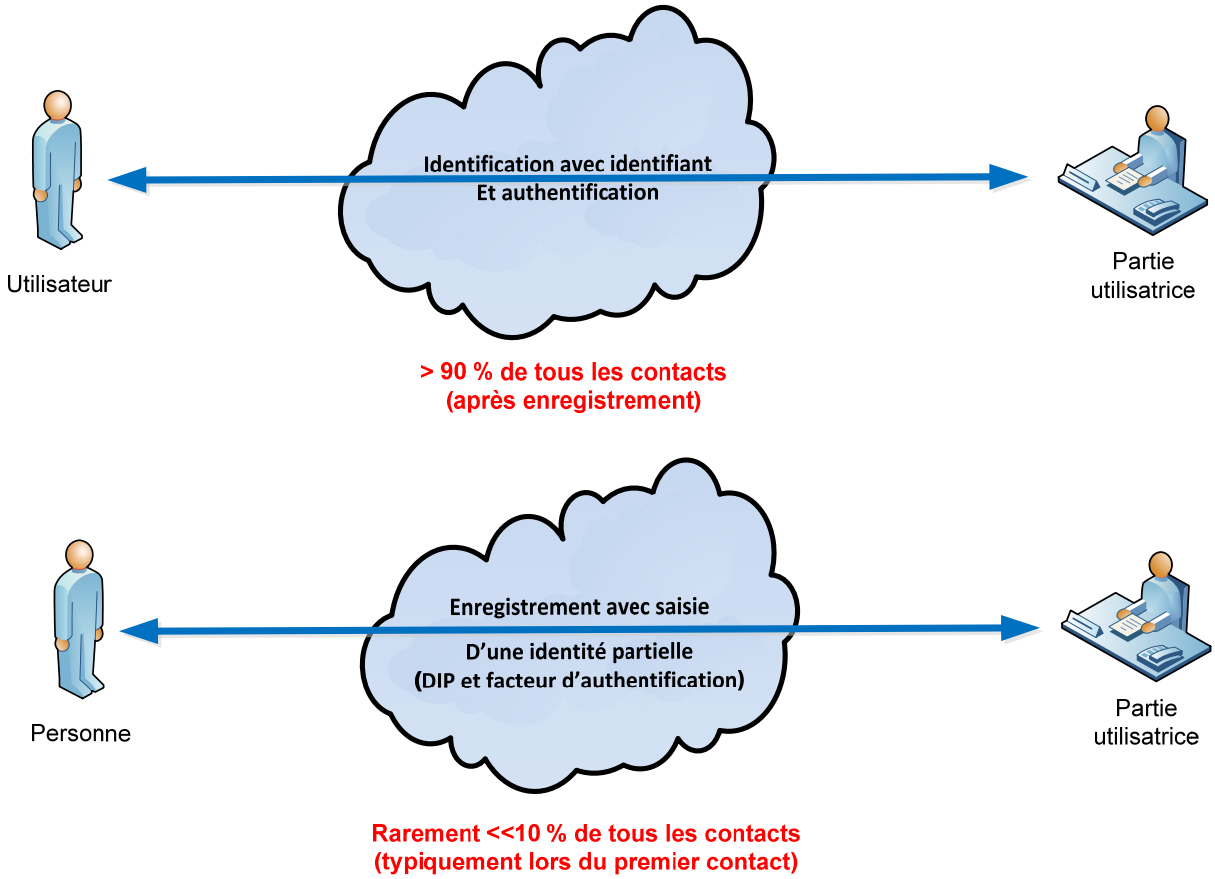


Schéma 23: Fréquence de la reconnexion par rapport à l'enregistrement

11. Identification d'une personne

La base de l'identification est la constatation et l'assignation sûre d'une identité partielle à une personne, au moins un attribut personnel devant alors être également saisi par la personne comme facteur d'authentification. En intégrant des données officielles d'identification personnelle, l'identification peut aussi se dérouler de manière relative à un fichier personnel prévalent (et officiel). En cas d'identification, un fichier personnel prévalent peut fournir également les données correspondantes directement au fichier personnel subordonnés. Cela se produit, par exemple, lorsque il convient de présenter un document d'identité officiel pour une identification, qui contient les principales données d'identification personnelle telles que *nom, prénom* et date de naissance, etc. En règle générale, un identifiant personnel unique d'un fichier personnel est aussi saisi dans une identité partielle identifiante. Celui-ci représente alors l'ensemble de l'identité partielle dans le fichier personnel et peut être utilisé pour la connexion en ligne et, partant,

pour l'identification. Si l'Etat définit un identifiant personnel unique pour tous les fichiers personnels subordonnés, celui-ci peut être utilisé pour l'identification dans toute la population et pour de nombreuses PU en tant qu'identifiant dans leur SGId.

12. Authentification d'une personne

L'authentification est le processus de vérification de l'appartenance d'une identité partielle à une personne, qui prétend l'être. Il est alors vérifié que les attributs personnels de l'identité partielle (facteurs d'authentification) enregistrés appartiennent effectivement et avec une certaine fiabilité à la personne du fichier personnel qui y prétend. La vérification a lieu par comparaison des attributs personnels fournis par la personne au moment de l'authentification avec les facteurs d'authentification saisis par la personne lors de l'enregistrement. La force d'une authentification dépend de la liaison des attributs personnels vérifiés à la personne et du nombre et du type des attributs vérifiés. Ainsi, la vérification de l'iris d'une personne est nettement plus significative pour la liaison que la requête d'un code NIP à quatre chiffres ou d'un mot de passe. Dans l'état actuel des connaissances, un iris est absolument unique, alors que nombre de personnes utilisent des codes NIP ou des mots de passe simples à deviner. Chaque facteur d'authentification indépendant vérifié en plus renforce l'authentification. La confiance dans une authentification résulte de la force de l'authentification et de la sécurité quant à l'impossibilité pour une personne malveillante d'avoir pu falsifier le processus. Une authentification est un instantané d'un certain niveau de sécurité, et la confiance à son égard faiblit au fil du temps.

13. Gestion électronique des identités

Si la gestion des identités se déroule par des médias électroniques, il est question de **gestion électronique de l'identité (eGId)** et du **système électronique de gestion des identités (eGId)** correspondant. En matière d'EGId, outre le rôle de la personne qui va être identifiée avec un **e-ID**, et qui est désignée par le terme de **détentrice ou détenteur**, et le rôle de l'administration qui identifie et authentifie les personnes et qui est désignée par le terme de **partie utilisatrice (PU)**, deux autres rôles s'y ajoutent, à savoir celui du **fournisseur de services d'identité (Identity Provider, IdP)**, qui établit les e-ID et exploite le système e-ID, et celui de l'**Etat régulateur**. La partie utilisatrice, qui doit se fier à l'IdP, charge l'IdP de procéder aux processus d'identification électronique et d'authentification des personnes. La PU exploite pour cela une application informatique, désigné par le terme de **service de confiance** qui est lié au système e-ID de l'IdP par une interface e-ID.

L'IdP exploite un système e-ID et enregistre un fichier personnel le plus largement étayé possible, de manière à couvrir les fichiers personnels du plus grand nombre possible de PU et donc fournir un service d'identité à un grand cercle de clients. Un moyen d'identification électronique (e-ID), que l'IdP délivre à toute personne enregistrée chez lui et qui lui permet d'authentifier toutes les détentrices et tous les détenteurs d'un tel e-ID partout dans l'espace virtuel. L'**Etat régulateur** définit les conditions-cadre d'un point de vue juridique, procédural, organisationnel au sein desquelles l'eGId se déroule avec participation de l'IdP et de ses systèmes e-ID. L'e-ID peut comprendre une fonction d'authentification liée avec sécurité à l'unité avec des données de référence intégrées pour les facteurs d'authentification personnelle de la détentrice ou du détenteur. Il définit ainsi le cadre de confiance requis pour le développement d'un écosystème e-ID fonctionnant.

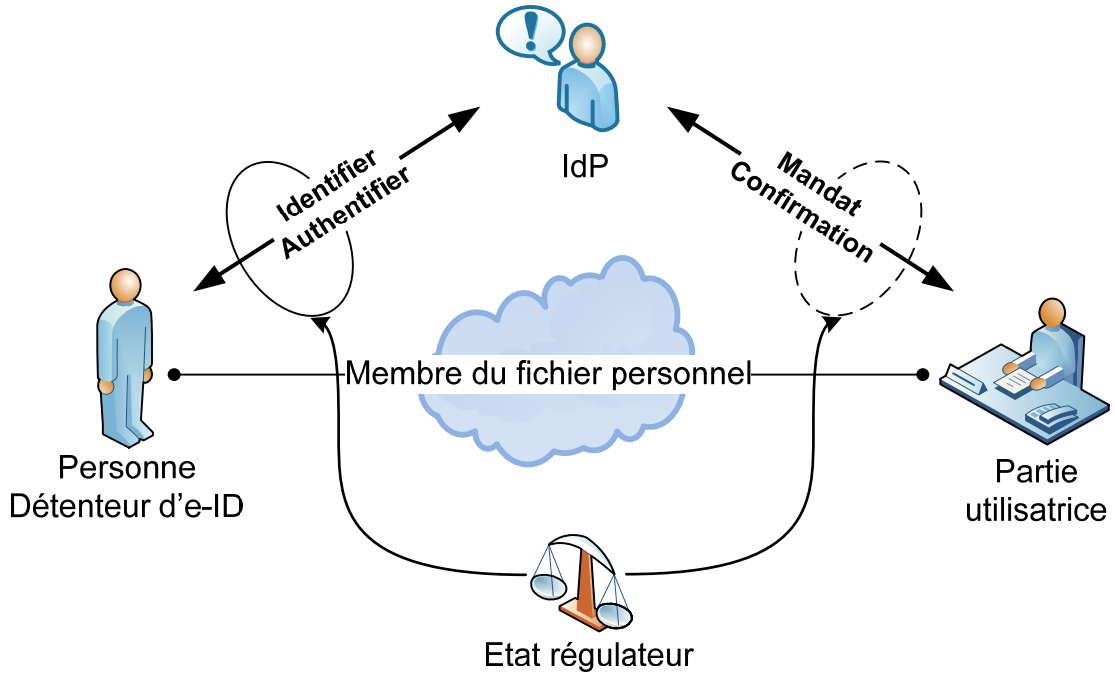


Schéma 24: Répartition des tâches dans la gestion électronique des identités

14. Moyen d'identification électronique (e-ID)

Un moyen d'identification électronique (e-ID) est une unité électronique matérielle et/ou immatérielle (authentifiant)[43], qui fait partie d'un système e-ID et qui est utilisée pour l'identification et l'authentification d'une personne dans le fichier personnel de l'exploitant du système e-ID. L'e-ID dispose d'interfaces qui permettent une communication directe sûre avec le serveur central du système e-ID et qui comprend un identifiant qui est affecté à la détentrice ou au détenteur lors de l'enregistrement. L'e-ID peut comprendre une fonction d'authentification liée avec sécurité à l'unité avec des données de référence intégrées pour les facteurs d'authentification personnelle de la détentrice ou du détenteur. Une telle fonction d'authentification compare les facteurs d'authentification de la détentrice ou du détenteur saisis lors de l'enregistrement avec les attributs personnels de la personne saisis et décide si ces éléments correspondent et s'ils proviennent donc de la détentrice enregistrée ou du détenteur enregistré. Outre l'identifiant évtl. dépendant de la connexion, l'e-ID peut comprendre d'autres attributs d'identité de la personne ou être lié de manière indubitable à de tels éléments par l'eGId du fichier personnel de l'IdP.

i. Niveau de sécurité d'un e-ID

Un moyen d'identification électronique peut être conçu pour répondre à divers niveaux de sécurité. Le Règlement eIDAS (EU, 2014) de l'UE définit pour l'essentiel trois niveaux de sécurité (faible, substantiel, élevé) supérieurs, qui pour l'essentiel correspondent aux trois niveaux supérieurs de la norme ISO/IEC 29115 (ISO, 2013) et aux niveaux de sécurité définis par le NIST pour l'authentification numérique (800-63-3, 2016). Dans le concept pour l'e-ID suisse, ces niveaux de sécurité correspondent aux niveaux de sécurité introduits (argent, or, platine). Les e-ID des trois niveaux de sécurité se distinguent notamment par le processus d'établissement lors de l'enregistrement d'une personne, par la force d'authentification de l'authentifiant intégré à l'e-ID, par des jeux différents de données d'identification personnelle transmis par l'Etat, et par l'étendue de

[43] Un authentifiant est pour l'instant uniquement une unité fonctionnelle électronique. Il devient un e-ID dès lors que l'unité est reliée au cours du processus d'enregistrement à une personne et à des données d'identité avec l'identifiant de l'unité au moyen de la fonction d'authentification.

diverses utilisations possibles.

ii. e-ID reconnus par l'Etat

La *loi fédérale sur les unités d'identification électronique reconnus par l'Etat (loi e-ID)* est la base légale pour la reconnaissance des systèmes e-ID et des e-ID proposés sur le marché par des IdP pour des personnes autorisées de la population suisse. La reconnaissance par l'Etat est fondée sur un processus de reconnaissance par lequel les aspects techniques et organisationnels de sécurité sont vérifiés conformément au niveau de sécurité de l'e-ID, la fiabilité des IdP d'établissement et l'interopérabilité du système e-ID pour satisfaire les critères légaux de reconnaissance.

iii. Interopérabilité

La standardisation appropriée des interfaces et des protocoles permet à un e-ID ou au système-ID correspondant d'être en principe utilisé par toutes les PU pour l'identification et l'authentification des détentrices et détenteurs. Pour cela, les systèmes e-ID doivent être interopérables. Grâce à l'interopérabilité, une PI peut confier un mandat d'identification ou d'authentification d'une détentrice ou d'un détenteur pour tous les e-ID au niveau de sécurité indiqué et indépendamment de l'IdP reconnu par l'Etat émetteur.

15. Interopérabilité dans les systèmes e-ID

Il suffit d'établir l'interopérabilité entre tous les exploitants de systèmes e-ID pour parvenir à une utilisation transparente d'un e-ID dans tout l'écosystème e-ID. Une détentrice ou un détenteur d'un e-ID de l'IdP A peut l'utiliser auprès d'une PU dont le service de confiance est raccordé au système e-ID de l'IdP B. A cette fin, elle ou il se connecte avec l'identifiant de l'e-ID auprès du portail du service de confiance, qui transmet la demande au système e-ID de son IdP B. Celui-ci constate que les éléments de sécurité de l'e-ID dans le système e-ID de l'IdP A sont disponibles et transmet le mandat d'authentification ou d'identification au système e-ID de l'IdP A. Celui-ci exécute lui-même le mandat et communique le résultat par le même chemin ou fournit les éléments de sécurité requis à l'IdP B, de manière à ce que celui-ci puisse ensuite exécuter le mandat avec l'e-ID de la détentrice ou du détenteur. Techniquement, cela peut être réalisé de la même manière que ce qui est le cas pour l'itinérance (roaming) pour les réseaux de télécommunication mobile. Pour que cela fonctionne, tous les systèmes e-ID reconnus par l'Etat doivent utiliser un système d'identifiant uniforme pour leurs e-ID. Cela peut, par exemple, consister directement en des adresses IP-V6, un système d'adresses e-mail standardisé ou une autre forme d'identifiants définis de manière uniforme.

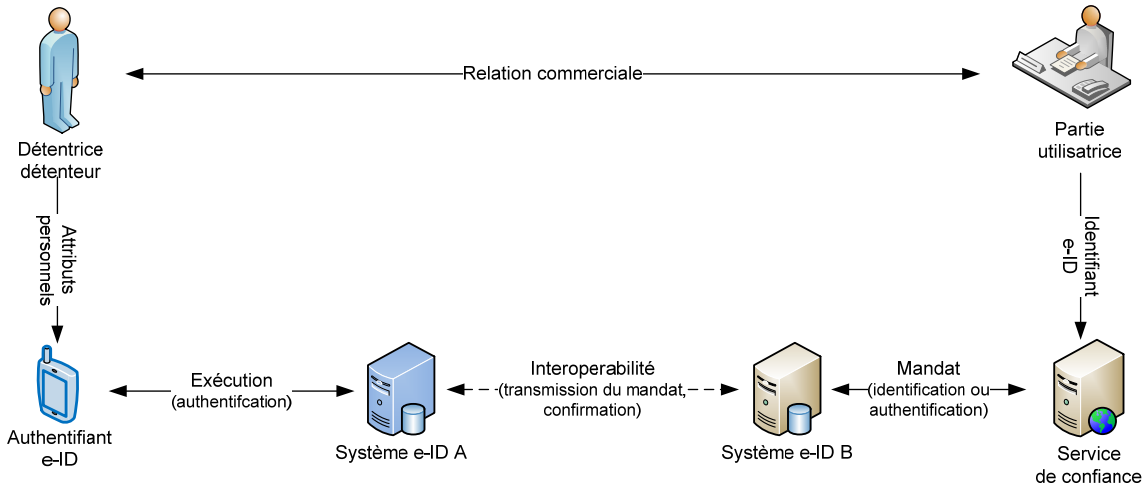


Schéma 25: Déroulement d'une authentification ou d'une identification interopérable

i. Utilisation interopérable de données d'identification personnelle

Compte tenu de l'interopérabilité entre les systèmes e-ID des IdP reconnus par l'Etat, chaque PU dont le service de confiance est raccordé au moins à un système e-ID reconnu peut utiliser les mécanismes d'identification et d'authentification de tous les e-ID reconnus par l'Etat pour son fichier personnel. La PU détermine alors le niveau de sécurité minimal exigé. Au cours du processus d'enregistrement, la PU, avec l'accord de la détentrice ou du détenteur de l'e-ID, peut reprendre également des données d'identité des fichiers personnels prévalents des IdP reconnus par l'Etat et, partant, des attributs de l'identité civile enregistrés par l'Etat. Cela permet de parvenir à une interopérabilité globale des données d'identification personnelle au sein de l'écosystème e-ID suisse pour tous les détentrices et détenteurs d'un e-ID reconnu par l'Etat. L'interopérabilité de l'identification et de l'authentification avec comparaison des attributs enregistrés par l'Etat atteint les PU en passant par la chaîne Etat et IdP.

Lorsqu'une PU enregistre une personne dans son fichier personnel, l'identification requise est effectuée par l'IdP, et le résultat est communiqué à la PU. Si l'e-ID est reconnu par l'Etat, l'IdP peut alors, si la détentrice ou le détenteur le souhaite, également transmettre à la PU des données d'identification personnelle et notamment aussi un IPU tiré des registres officiels. Même si une détentrice ou un détenteur souhaite se connecter à la PU, l'IdP réalisera lui-même l'authentification requise ou déléguera cette tâche à l'IdP compétent avant d'en communiquer le résultat à la PU.

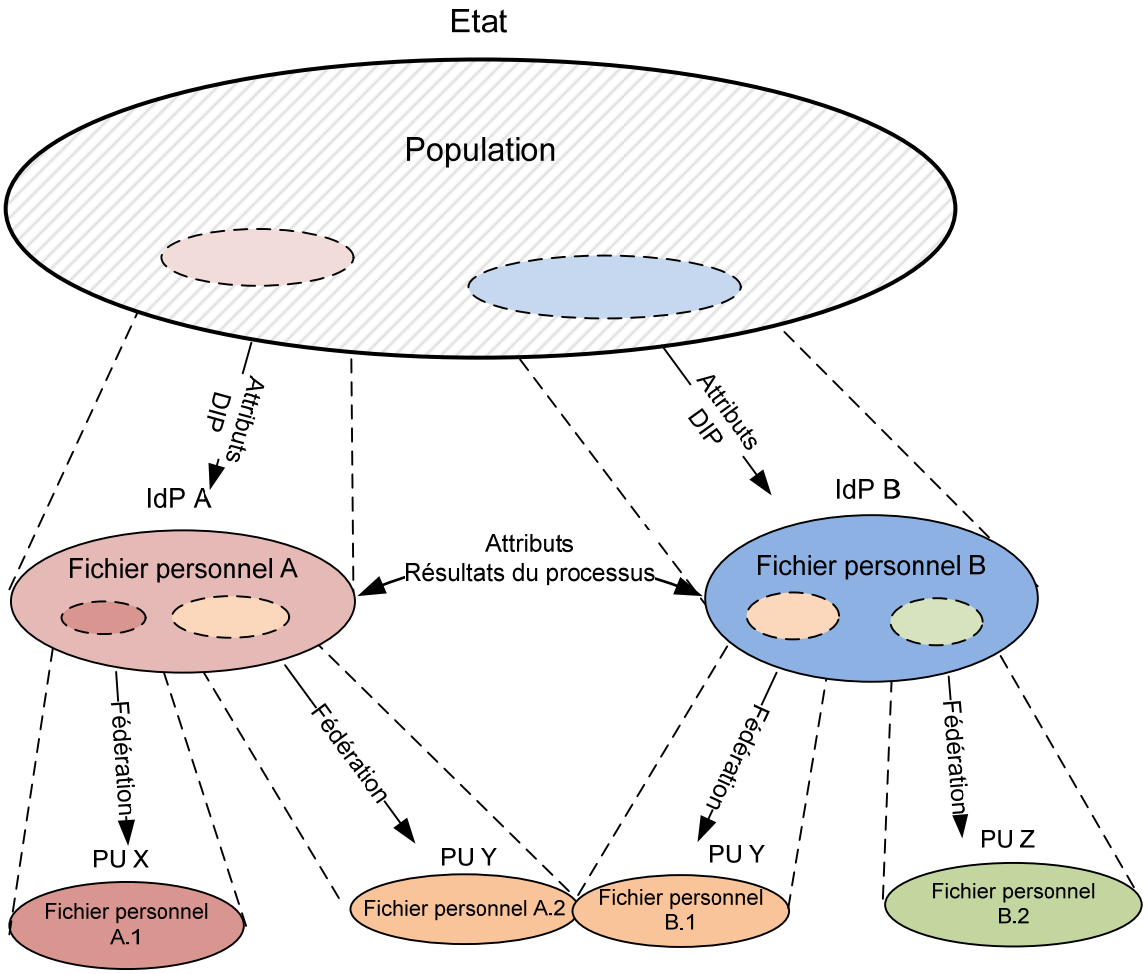


Schéma 26: Chaîne de transmission d'attributs

Le Schéma 26 montre la chaîne de transmission d'attributs d'un fichier personnel prévalent à des fichiers personnels subordonnés, avec pour exemple l'Etat – les fournisseurs de services d'identité (IdP) – les parties utilisatrices (PU). Au sommet se trouve le fichier personnel de la population dans son ensemble avec les données d'identification personnelle. L'interopérabilité à l'aide d'un e-ID permet de reporter entre les IdP non seulement des attributs mais aussi des résultats de processus d'identification et d'authentification.

16. L'Etat comme administrateur d'attribut et service de reconnaissance pour l'eGId

La Confédération exploite le GId officiel pour toutes les personnes enregistrées en Suisse en possession d'un document d'identité valable délivré par les autorités suisses. L'identification et l'authentification soutenues par l'Etat au moyen de ces documents d'identité sont d'ores et déjà possibles pour tous les fichiers personnels ainsi que leur SGId. L'introduction d'IdP reconnus par l'Etat en tant que fournisseurs de systèmes e-ID permet en plus la transmission électronique de données d'identification personnelle à partir des registres officiels par le biais d'un service proxy officiel. Les IdP proposant des systèmes e-ID reconnus par l'Etat peuvent tirer parti de cette offre. En matière de **systèmes e-ID reconnus par l'Etat**, le fichier personnel suprême est la population suisse dans son ensemble, dont les données d'identification personnelle sont gérées dans les registres officiels que sont Infostar, ISA, ISR, CdC et SYMIC.

i. Service d'identité électronique suisse (SIE)

Le SIE est une unité administrative du DFJP, qui transmet après accord explicite de la détentrice ou du détenteur d'un e-ID un jeu de données d'identification personnelle dépendant du niveau de sécurité de l'e-ID au système e-ID de l'IdP. Il a de plus accès aux registres de personnes déterminants tenus par les autorités fédérales (ISA, Infostar, SYMIC, CdC-UPI).

ii. Organisme de reconnaissance des fournisseurs d'identité (ORFI)

Pour qu'un IdP puisse exploiter un système e-ID reconnu par l'Etat, il doit se soumettre, lui et ses systèmes e-ID à un processus de reconnaissance. Celui-ci comprend la vérification des conditions de reconnaissance sur les plans techniques, organisationnels et juridiques. En font notamment aussi partie la vérification du respect de standards et la présence d'interfaces pour l'intégration interopérable du système e-ID à reconnaître dans l'écosystème e-ID suisse.
L'ORFI est une unité administrative au sein du DFF. La reconnaissance par l'Etat des IdP et de leurs systèmes e-ID lui incombe. L'ORFI exerce également la surveillance du respect des conditions d'une telle reconnaissance.

7.2 Glossaire

Considérant les termes expliqués précédemment et les liens mis en évidence, les définitions suivantes sont utilisées pour la législation et le concept des e-ID reconnus par l'Etat.

Terme	Abr.	Définition
Activation		Validation d'un e-ID pour l'exploitation par l'IdP après établissement fructueux avec enregistrement de la détentrice ou du détenteur
Attribut		Caractéristique définie nommément d'une entité. Un attribut a un nom, une valeur et d'autres caractéristiques, par exemple un type de données ou une date de validité
Attributs assignés		Attributs contextuels assignés à une personne dans son identité partielle dans le fichier personnel par une PU ou un IdP.
Attributs d'identité		Cf. attributs
Attributs d'identité identifiants		Identité partielle avec des attributs qui identifient de manière univoque une entité dans un ensemble d'entités
Attributs personnels		Attributs pouvant être utilisés pour l'authentification d'une personne, cf. facteurs d'authentification
Authentifiant		Unité électronique matérielle et/ou immatérielle qui appartient à un système e-ID. Elle dispose d'interfaces qui permettent une communication directe sûre avec le serveur central du système e-ID et contient un identifiant assigné à la détentrice ou au détenteur lors de l'enregistrement. Elle contient une fonction d'authentification liée de manière sûre à l'unité avec des données de référence pour les facteurs d'authentification personnelle de la détentrice ou du détenteur.
Authentification authentifier		Cf. annexe, paragraphe 12
Détentrice, détenteur		Personne pour laquelle un e-ID reconnu par l'Etat a été délivré par un IdP
Données d'identification personnelle	DIP	Attributs de l'identité civile d'une personne enregistrée dans les registres de personnes officiels. Les données d'identification personnelle sont en l'espèce limitées à une quantité partielle de ces attributs définis légalement.
Ecosystème d'identité		Cf. écosystème e-ID
Ecosystème e-ID		Ensemble de toutes les instances qui utilisent un e-ID pour la population d'un Etat ou qui contribuent à son exploitation.
Enregistrement		Enregistrement auprès d'un IdP: Liaison d'une personne à un e-ID, identification de la personne par l'IdP, transmission des données d'identification personnelle de la personne par le SIE à l'IdP lors de l'établissement d'un e-ID Enregistrement auprès d'une PU: Première inscription d'une détentrice ou d'un détenteur auprès d'une PU auprès de son SGId avec transmission des données d'identification personnelle par l'IdP ayant délivré l'e-ID

Ensemble d'entités		Ensemble d'entités dépendant du contexte
Entité		Unité pouvant être individualisée par des attributs constatés
Facteurs d'authentification		Attributs personnels pouvant être utilisés pour l'authentification d'une personne. Une distinction est souvent opérée entre les trois catégories que sont biométrique, basé sur le savoir et basé sur la possession.
Fichier personnel		Quantité de personnes dont l'identité partielle est enregistrée dans le GId d'un administrateur.
Fonction d'authentification		Fonction d'un e-ID, qui permet de saisir des attributs personnels (facteurs d'authentification) de la détentrice ou du détenteur et de les comparer avec des valeurs stockées en local. Cette fonction décide si la détentrice ou le détenteur est la bonne personne.
Fournisseur de services d'identités Identity Provider	IdP	Prestataires de services d'identité qui exploite et/ou utilise un système e-ID.
Gestion des identités	GId	Cf. annexe, chapitre B
Gestion des identités et des accès	IAM	GId avec administration raccordée des rôles et droits pour les personnes enregistrées dans le fichier personnel
Gestion électronique des identités	eGId	Gestion des identités au moyen de systèmes électroniques numériques
Identifiant		Désignation univoque d'une entité dans le système d'information d'un administrateur d'identités partielles
Identifiant personnel		Nom défini dans un contexte qui désigne de manière univoque une personne dans un contexte
Identifiant personnel unique	IPU	Identifiant unique attribué par l'Etat aux personnes de sa population. Le NAVS13 est un IPU utilisé en Suisse.
Identification identifier		Cf. annexe, paragraphe 11
Identité partielle		Jeu de données avec des attributs relatifs à une entité
Identité, identité civile		Ensemble de tous les attributs qui peuvent être saisis pour une personne (entité). L'identité civile correspond aux attributs d'une personne enregistrée dans les registres de personnes officiels.
Inactivation		Débranchement d'un e-ID dans le système e-ID d'un IdP
Inscription / connexion		Connexion (renouvelée) d'une détentrice ou d'un détenteur auprès d'un système eGId (ou IAM) d'une PU ou auprès d'un IdP avec un e-ID
Interfaces électroniques des applications et processus	Interface e-ID	Composants standardisés des systèmes e-ID qui opèrent au sein des services de confiance comme interfaces avec le système e-ID. Ils garantissent l'uniformité des formulaires et formats pour l'utilisation des e-ID.
Interopérabilité des e-ID		Réseau de systèmes e-ID qui se fient et se reconnaissent mutuellement avec un niveau de sécurité minimal défini.
Moyen d'identification électronique	e-ID	Authentifiant assigné à une identité partielle de la détentrice ou du détenteur auprès de l'IdP et dont la fonction d'authenti-

		fication est définie de telle manière à permettre l'authentification de la détentrice ou du détenteur.
Niveau de sécurité		Cf. 2.6.1
Nom de l'attribut		Nom sémantique de la caractéristique qui est enregistrée comme attribut
Organisme de reconnaissance des fournisseurs d'identité	ORFI	Cf. ch. 3.3
Partie utilisatrice	PU	Personne physique ou unité UID, qui exploite un service de confiance pour exercer son activité.
Personne		Sujet juridique, en l'espèce le plus souvent désignant une personne physique
Personne physique		Personne qui est un sujet agissant de manière autonome
Population		En l'espèce, les personnes enregistrées et administrées dans les registres de personnes officiels relevant de la souveraineté d'un Etat.
Protection de la transaction		Contrôle de la faisabilité d'une transaction
Service d'attribut		Service pour la transmission des attributs d'identité des personnes enregistrées dans les registres du service. Les IdP reconnus officiellement agissent en tant que service d'attribut pour les données d'identification personnelle, qui sont mises à leur disposition par le SIE. Le SIE est aussi un service d'attribut.
Service d'identité		Désigne en l'espèce toujours une authentification ou une identification avec transmission des données d'identification personnelle
Service d'identité électronique suisse	SIE	Cf. 3.2
Service de confiance		Application informatique utilisée par le service d'identité du système e-ID et qui pet à disposition les interfaces nécessaires entre les services de la PU et le système e-ID.
Sujet juridique		Porteurs de droits et de devoirs agissant de manière autonome; il s'agit des personnes physiques et morales
Support d'un e-ID		Unité électronique dans laquelle un authentifiant resp. un e-ID est intégré
Suppression		Inactivation définitive d'un e-ID
Système de gestion des identités	SGId	Cf. annexe, chapitre B
Système de gestion des identités et des accès	IAMS	Système électronique pour les procédures IAM
Systèmes de gestion électronique des identités	Système e-ID	Système dans lequel des e-ID sont délivrés, exploités et administrés.
Valeur d'attribut		Valeur constatée d'un attribut d'une entité spéciale (personne)

7.3 Bibliographie

Le répertoire bibliographique indique en premier lieu les documents cités, puis d'autres sources pour les sujets traités par le concept.

[1] Bundesamt für Statistik, «Informationsgesellschaft,» Schweizerische Eidgenossenschaft, 2016. [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04.html. [Zugriff am 20 Juli 2016].

[2] EU, «Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung),» 23. Juli 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&qid=1422521123960&from=EN. [Zugriff am 29. Oktober 2015].

[3] E. Kommission, «Technical Specifications and procedures for Assurance for eID,» in *2015/1502*, 2015.

[4] FIDO Alliance, «UAF Architectural Overview, Review Draft,» 09. Februar 2014. [Online]. Available: https://fidoalliance.org/specifications/download/. [Zugriff am 12. April 2015].

[5] Lindemann, R., FIDO Alliance and Nok Nok Labs Inc., «The evolution of authentication,» 2013. [Online]. Available: http://www.springer.com/cda/content/document/cda_downloaddocument/9783658033705-c1.pdf. [Zugriff am 12. April 2015].

[6] D. N. S. P. 800-63-3, «Digital Authentication Guideline,» 12 Mai 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3. [Zugriff am 15 Juni 2016].

[7] eCH, «eCH-0107 IAM Gestaltungsprinzipien v2.0,» 04. Dezember 2013. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0. [Zugriff am 12. April 2015].

[8] N. 8149, «Developing Trust Frameworks to Support Identity Federations,» NIST - National Institute of Standards and Technology; US DoC, 2016.

[9] Bundesamt für Gesundheit, «Bundesgesetz über das elektronische Patientendossier,» [Online]. Available: http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/index.html?lang=de. [Zugriff am 23 07 2016].

[10] Schweizer Parlament, «Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03,» 19. Dezember 2003. [Online]. Available: http://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Zugriff am 12. April 2015].

[11] eCH Verein, «eCH - E-Governement Standards,» [Online]. Available: http://www.ech.ch. [Zugriff am November 2015].

[12] J. Fromm und et al., «3-Jahre Online Ausweisfunktion – Lessons Learned,» *Fraunhofer Fokus,* Oktober 2013.

[13] Belgische Regierung, «Portal belgium.be - Online Dienste der Belgischen Behörden,» [Online]. Available: http://www.belgium.be/de/online_dienst/. [Zugriff am 12. April 2015].

[14] BRZ-Presseservice, «Handy-Signatur gräbt der Bürgerkarte langsam das Wasser ab (Seite 54),» 27. März 2014. [Online]. Available: https://www.brz.gv.at/presse/pressespiegel/Pressespiegel-2014-03.pdf. [Zugriff am 12. April 2015].

[15] International Civil Aviation Organisation (ICAO), «Document 9303,» [Online]. Available: http://www.icao.int/Security/mrtd/pages/Document9303.aspx. [Zugriff am 26 07 2016].

[16] Bundesministerium des Innern, «Personalausweis,» [Online]. Available: http://www.personalausweisportal.de/DE/Home/home_node.html. [Zugriff am 26 07 2016].

[17] Government Technology, «Louisiana Considers Electronic Driver's License,» [Online]. Available: http://www.govtech.com/state/Louisiana-Considers-Electronic-Drivers-License.html. [Zugriff am 26 07 2016].

[18] CNET, «The driver's license of the future is coming to your smartphone,» [Online]. Available: http://www.cnet.com/news/your-future-drivers-license-could-go-digital/. [Zugriff am 26 07 2016].

[19] Gemalto, C. Mesnard, «Trusted National Mobile ID Schemes,» in *Secure Document World Conference, London 2016*, London, 2016.

[20] H. Steier, «Uns blieb das Lachen im Hals stecken,» *20 Minuten,* Bd. 22. September 2010; 11:14, Nr. Digital News, Sicherheit, p. http://www.20min.ch/digital/hardware/story/17220624, 2010.

[21] M. Quade und R. Wölfle, SuisseID in der Praxis - Grundlagen und Fallbeispiele zum elektronischen Identitätsnachweis der Schweiz, Basel: edition gesowip, 2010, p. 88.

[22] P. Müller, «Die SuisseID als Unterstützung für E-Voting, eine Analyse der Möglichkeiten und Handlungsoptionen,» Berner Fachhochschule, Wirtschaftsinformatik, Bern, 2011.

[23] S. Strauß und G. Aichholzer, «National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design. International Journal on Advances in Intelligent Systems,» pp. 12-23, Vol. 3, Nrs. 1&2 2010.

[24] Riedl, R., E-Government Institut Bern, BFH, «Von unterschiedlichen nationalen eID-Strategien zum einheitlichen europäischen Identitäts-raum – ein Ländervergleich,» 03. Juni 2014. [Online]. Available: http://e-government.adv.at/2014/pdf/2_1100_Riedl_eGovernmentKonferenz_20140603.pdf. [Zugriff am 12. April 2015].

[25] M. Horsch, «Die Open eCard App für mehr Transparenz, Vertrauen und Benutzerfreundlichkeit beim elektronischen Identitätsnachweis,» in *13. Deutscher IT-Sicherheitskongress des BSI*, Bonn, 2013.

[26] Nok Nok Labs Inc., «Four Barriers To Adabpt Strong Authentication,» 2013. [Online]. Available: https://www.noknok.com/sites/default/files/whitepapers/4barrierswhitepaper_0.pdf. [Zugriff am 12. April 2015].

[27] M. Richter, «Kriterien der Benutzerfreundlichkeit,» Philosophische Fakultät der Universität Zürich, http://www.michaelrichter.ch/literat_97.pdf, 1997.

[28] NIST, «National Strategy for Trusted Identities in Cyberspace (NSTIC),» [Online]. Available: http://www.nist.gov/nstic/index.html. [Zugriff am 26 07 2016].

[29] B. Fachhochschule, F. Wirtschaft und E.-G. Institut, «eID- Ökosystem Modell,» Juni 2015. [Online]. Available: https://www.egovernment.ch/index.php/download_file/force/271/3343/. [Zugriff am 8 August 2016].

[30] Bundesrat, «Strategie des Bundesrates für eine digitale Schweiz,» Schweizerische Eidgenossenschaft, 20. April 2016. [Online]. Available: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/strategie.html. [Zugriff am 15 Mai 2016].

[31] E-Government Schweiz, «E-Government-Strategie Schweiz,» 24. Januar 2007. [Online]. Available: http://www.egovernment.ch/egov/00833/00834/index.html?lang=de. [Zugriff am 12. April 2015].

[32] E-Government Schweiz, «Roadmap E-Government Schweiz,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00852/index.html?lang=de. [Zugriff am 12. April 2015].

[33] E-Government Schweiz, «Katalog priorisierter Vorhaben,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00847/index.html?lang=de. [Zugriff am 12. April 2015].

[34] Schweizerische Bundeskanzlei, «E-Demokratie und E-Partizipation,» 2011. [Online]. Available: http://intranet.bk.admin.ch/themen/06367/index.html?lang=de. [Zugriff am 08 05 2015].

[35] NSTIC- National Strategy for Trusted Identities in Cyberspace, «The Identity Ecosystem: Use Examples;,» [Online]. Available: http://www.nist.gov/nstic/identity-ecosystem.html [Zugriff am 13. April 2015].. [Zugriff am 13 April 2015].

[36] EU, «Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185252017&uri=CELEX:32015D0296. [Zugriff am 29 07 2017].

[37] EU, «Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185296675&uri=CELEX:32015R1501. [Zugriff am 29 07 2016].

[38] EU, «Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185318253&uri=CELEX:32015R1502. [Zugriff am 29 07 2016].

[39] EU, «Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185344281&uri=CELEX:32015D1984. [Zugriff am 29 07 2016].

[40] Zentrale Ausgleichsstelle, «Verteilter Clearingprozess,» [Online]. Available: http://www.zas.admin.ch/org/00721/00758/00911/index.html?lang=de. [Zugriff am 25 07 2016].

[41] Bundeskanzlei, «E-Demokratie und E-Partizipation,» [Online]. Available: https://www.bk.admin.ch/themen/06367/index.html?lang=de. [Zugriff am 22 07 2016].

[42] Bundeskanzlei, «Vote électronique,» [Online]. Available: https://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de. [Zugriff am 22 07 2016].

[43] Österreichische Staatsdruckerei, «MIA (My Identity App),» [Online]. Available: https://www.staatsdruckerei.at/produkte/identitaetsmanagement/mia-my-identity-app/. [Zugriff am 26 07 2016].

[44] MORPHO, «Electronic Driver License,» [Online]. Available: http://www.morpho.com/en/now-your-smartphone-could-be-your-drivers-license-too. [Zugriff am 26 07 2016].

[45] Bund, «Bundesgesetz über die elektronische Signatur, ZertES,» [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Zugriff am 24 07 2016].

[46] European Commission, «Collaborative economy,» [Online]. Available: http://ec.europa.eu/growth/single-market/strategy/collaborative-economy/. [Zugriff am 23 07 2016].

[47] «The Trusted Execution Environment, Delivering Enhanced Security at a lower cost to the mo-bile market,» Februar 2011. [Online]. Available: http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf. [Zugriff am 12. April 2015].

[48] K. R. e. a. (Eds), The Future of Identity in the Information Society, Berlin - Heidelberg: Springer-Verlag, 2009.

[49] NIST Hildegard Ferraiolo, Larry Feldman and Greg Witte, «NIST Special Publication 800-157 - Guidelines for Derived Personal Identity Verification (PIV) Credentials,» Dezember 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf. [Zugriff am 12. April 2015].

[50] eCH, «eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,» 04. September 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0171. [Zugriff am 13. April 2015].

[51] eCH, «eCH-0170 Qualitätsmodell für elektronische Identitäten,» 06. Juni 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170. [Zugriff am 12. April 2015].

[52] ISO, «ISO Standard 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework,» 27. März 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138. [Zugriff am 13. April 2015].

[53] D. Hühnlein, «Identitätsmanagement-eine visualisierte Begriffsbestimmung,» *Datenschutz und Datensicherheit, Heft 3,* p. 163, 2008.

[54] M. Jakobsson und S. Taveau, «The Case for Replacing Passwords with Biometrics,» 2012. [Online]. Available: http://mostconf.org/2012/papers/3.pdf. [Zugriff am 12. April 2015].

[55] J. Grant, «Digital Identity in 2019: a vibrant identity ecosystem,» 2014. [Online]. Available: http://secureidnews.com/news-item/digital-identity-in-2019-a-vibrant-identity-ecosystem/#. [Zugriff am 12. April 2014].

[56] M. Schröder und F. Morgner, «Abgeleitete Identitäten,» 2013. [Online]. Available: https://www.bundesdruckerei.de/sites/default/files/documents/2013/08/fachartikel_dud_abgeleitete_identitaeten.pdf. [Zugriff am 12 April 2015].

[57] Meister, Gisela, Giesecke & Devrient, «Abgeleitete Identitäten – ein Überblick,» 25. September 2014. [Online]. Available: http://www.cast-forum.de/workshops/programm/194. [Zugriff am 12. April 2015].

[58] Global Platform Inc., «A new model: The consumer-centric model and how it applies to the Mobile ecosystem,» März 2012. [Online]. Available: http://www.globalplatform.org/documents/Consumer_Centric_Model_White_PaperMar2012.pdf. [Zugriff am 12. April 2015].

[59] «OASIS - Advancing Open Standards for the Information Society,» [Online]. Available: https://www.oasis-open.org/. [Zugriff am 12. April 2015].

[60] OASIS, «OASIS - SAML Wiki,» [Online]. Available: https://wiki.oasis-open.org/security/FrontPage. [Zugriff am 12. April 2015].

[61] Schweizer Bundesrat, «Informationsgesellschaft in der Schweiz,» März 2012. [Online]. Available: http://www.bakom.admin.ch/themen/infosociety/. [Zugriff am 12. April 2015].

[62] EU, «STORK,» 2015. [Online]. Available: https://www.eid-stork.eu/. [Zugriff am 12. April 2015].

[63] Schweizer Bundesrat, «Bundesratsbeschluss zur Ausarbeitung eines Gesetzgebungspaketes zur Förderung des elektronischen Geschäftsverkehrs,» 19. Dezember 2012. [Online].

[64] SuisseID, «SuisseID,» 2015. [Online]. Available: http://www.suisseid.ch/de. [Zugriff am 12. April 2015].

[65] Mondinis Workshop, «Mondinis Study on Identity Management in eGovernment; Common Terminological Framework for Interoperable Electronic Identity Management; V2.01,» DG Information Society and Media; EU Commission, 23 November 2005. [Online]. Available: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf. [Zugriff am 13 April 2015].

[66] D. Miessler, «Daniel Miessler Blog; Security: Identification, Authentication, and Authorization,» [Online]. Available: https://danielmiessler.com/blog/security-identification-authentication-and-authorization/ . [Zugriff am 13 April 2015].

[67] G. Doe, «Difference Between Identification & Authentication;,» Demand Media; , [Online]. Available: http://science.opposingviews.com/difference-between-identification-authentication-3471.html . [Zugriff am 13 April 2015].

[68] I. 1. Standard, «Common Criteria for Information Technology Security Evaluation».

[69] R. Dholakia, «A question of Scale,» NokNok Labs, 2012.

[70] D. O'Shea, «Fido U2F & UAF Tutorial,» in *World e-ID Congress, Marseille 2014*, Marseille, 2014.

[71] Bundesversammlung, «Ausweisgesetz (AwG, SR 143.1),» 01 Jan 2013. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19994375/index.html. [Zugriff am 08 Mai 2015].

[72] SkIDentity, «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Zugriff am 09. Mai 2015].

[73] Verein eGov-Schweiz, «Bürgerdossier,» 2015. [Online]. Available: http://www.egov-schweiz.ch/media/archive2/eGov_Flyer_Buergerdossier_def.pdf. [Zugriff am 09. Mai 2105].

[74] E-Government Schweiz, «Identititätsverbund Schweiz (IDV Schweiz),» 2015. [Online]. Available: http://www.egovernment.ch/b206/index.html?lang=de. [Zugriff am 09. Mai 2015].

[75] «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Zugriff am 12. April 2015].

[76] H. STORCK 2.0, «STORK - Secure idenTity acrOss boRders linKed 2.0,» STORK 2.0 project group, [Online]. Available: https://www.eid-stork2.eu/. [Zugriff am 9 11 2015].

[77] Bundesamt für Statistik, «Nutzungszwecke,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=302#302. [Zugriff am 22 07 2016].

[78] Bundesamt für Statistik, «Nutzungshäufigkeit von Online-Fomularen,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=335#335. [Zugriff am 22 07 2016].

[79] Bundesamt für Statistik, «Nutzung des Internets,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/03/key/ind16.indicator.30106.160204.html. [Zugriff am 22 07 2016].

[80] FINMA, «FINMA ermöglicht Video- und Online-Identifizierung,» 21 12 2015. [Online]. Available: https://www.finma.ch/de/news/2015/12/20151221-mm-videoidentifizierung/. [Zugriff am 15 7 2016].

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Berne, le 23 février 2017

Destinataires
Gouvernements cantonaux

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) : ouverture de la procédure de consultation

Mesdames et Messieurs les Conseillers d'Etat,
Mesdames, Messieurs,

Le 22 février 2017, le Conseil fédéral a chargé le DFJP de consulter les cantons, les partis politiques, les associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national, les associations faîtières de l'économie qui œuvrent au niveau national et les autres milieux intéressés sur le projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID).

Le délai imparti pour la consultation court jusqu'au **29 mai 2017**.

Afin que des transactions plus complexes puissent également être effectuées en ligne, les partenaires commerciaux doivent pouvoir se fier à l'identité de leur interlocuteur. Un e-ID reconnu permet d'identifier électroniquement une personne physique habilitée à utiliser un service.

L'avant-projet de loi prévoit une répartition des tâches entre l'État et les acteurs du marché. La Confédération habilitera les acteurs privés ou les fournisseurs d'identité (FI) du secteur public satisfaisant aux conditions requises à établir des e-ID reconnus par l'État. Pourra obtenir un e-ID toute personne dont l'identité est attestée par les systèmes d'information gérés par l'État, c'est-à-dire Infostar (registre informatisé de l'état civil), le SYMIC (système d'information central sur la migration), ISA (système d'information relatif aux documents d'identité) et le registre central de la centrale de compensation de l'AVS (CdC-UPI).

L'avant-projet de loi fixe un cadre législatif pour la reconnaissance étatique des systèmes e-ID et des FI. Ce cadre est conçu de manière 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. Des accords bilatéraux seront nécessaires.

La Confédération accomplit cinq tâches dans le domaine des e-ID reconnus :

1. elle élabore et met à jour un cadre légal qui garantit la transparence et la sécurité;
2. elle définit les normes ainsi que les exigences de sécurité et d'interopérabilité pour l'exploitation d'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 électronique suisse (service d'identité) et l'organisme de reconnaissance des FI (organisme de reconnaissance).

À moyen terme, l'objectif sera atteint sans incidence sur le budget puisque les frais d'exploitation seront couverts par des émoluments.

Le projet et le dossier mis en consultation sont disponibles à l'adresse Internet www.admin.ch/ch/f/gg/pc/pendent.html.

Conformément à la loi sur l'égalité pour les handicapés (RS *151.3*), nous nous efforçons de publier des documents accessibles à tous. Aussi nous saurions-vous gré de nous faire parvenir dans la mesure du possible votre avis sous forme électronique (**prière de joindre une version Word en plus d'une version PDF**) à l'adresse suivante, dans la limite du délai imparti :

copiur@bj.admin.ch

Nous vous prions d'indiquer le nom et les coordonnées de la personne à qui s'adresser en cas de question.

Urs Paul Holenstein (Tel. 058 463 53 36, urspaul.holenstein@bj.admin.ch) et Sandra Eberle (Tel. 058 465 47 77, sandra.eberle@bj.admin.ch se tiennent à votre disposition pour toute question ou information complémentaire.

Nous vous prions d'agréer, Mesdames et Messieurs les Conseillers d'Etat, l'expression de notre considération distinguée.

Simonetta Sommaruga
Conseillère fédérale

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Berne, le 23 février 2017

Destinataires
Partis politiques
Associations faîtières des communes,
des villes et des régions de montagne
Associations faîtières de l'économie
Autres milieux intéressés

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) : ouverture de la procédure de consultation

Madame, Monsieur,

Le 22 février 2017, le Conseil fédéral a chargé le DFJP de consulter les cantons, les partis politiques, les associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national, les associations faîtières de l'économie qui œuvrent au niveau national et les autres milieux intéressés sur le projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID).

Le délai imparti pour la consultation court jusqu'au **29 mai 2017**.

Afin que des transactions plus complexes puissent également être effectuées en ligne, les partenaires commerciaux doivent pouvoir se fier à l'identité de leur interlocuteur. Un e-ID reconnu permet d'identifier électroniquement une personne physique habilitée à utiliser un service.

L'avant-projet de loi prévoit une répartition des tâches entre l'État et les acteurs du marché. La Confédération habilitera les acteurs privés ou les fournisseurs d'identité (FI) du secteur public satisfaisant aux conditions requises à établir des e-ID reconnus par l'État. Pourra obtenir un e-ID toute personne dont l'identité est attestée par les systèmes d'information gérés par l'État, c'est-à-dire Infostar (registre informatisé de l'état civil), le SYMIC (système d'information central sur la migration), ISA (système d'information relatif aux documents d'identité) et le registre central de la centrale de compensation de l'AVS (CdC-UPI).

L'avant-projet de loi fixe un cadre législatif pour la reconnaissance étatique des systèmes e-ID et des FI. Ce cadre est conçu de manière 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. Des accords bilatéraux seront nécessaires.

La Confédération accomplit cinq tâches dans le domaine des e-ID reconnus :

1. elle élabore et met à jour un cadre légal qui garantit la transparence et la sécurité;
2. elle définit les normes ainsi que les exigences de sécurité et d'interopérabilité pour l'exploitation d'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 électronique suisse (service d'identité) et l'organisme de reconnaissance des FI (organisme de reconnaissance).

À moyen terme, l'objectif sera atteint sans incidence sur le budget puisque les frais d'exploitation seront couverts par des émoluments.

Le projet et le dossier mis en consultation sont disponibles à l'adresse Internet www.admin.ch/ch/f/gg/pc/pendent.html.

Conformément à la loi sur l'égalité pour les handicapés (RS *151.3*), nous nous efforçons de publier des documents accessibles à tous. Aussi nous saurions-vous gré de nous faire parvenir dans la mesure du possible votre avis sous forme électronique (**prière de joindre une version Word en plus d'une version PDF**) à l'adresse suivante, dans la limite du délai imparti :

copiur@bj.admin.ch

Nous vous prions d'indiquer le nom et les coordonnées de la personne à qui s'adresser en cas de question.

Urs Paul Holenstein (Tel. 058 463 53 36, urspaul.holenstein@bj.admin.ch) et Sandra Eberle (Tel. 058 465 47 77, sandra.eberle@bj.admin.ch se tiennent à votre disposition pour toute question ou information complémentaire.

Nous vous prions d'agréer, Madame, Monsieur, l'expression de notre considération distinguée.

Simonetta Sommaruga
Conseillère fédérale

Liste der ständigen Vernehmlassungsadressaten
Liste des destinataires consultés systématiquement
Elenco dei destinatari permanenti della consultazione

Art. 4 Abs. 3 Vernehmlassungsgesetz (SR 172.061)

Stand: 2.2.2017

1. Kantone / Cantons / Cantoni

Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich staatskanzlei@sk.zh.ch
Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch
Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
Chancellerie d'Etat du Canton de Fribourg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch relations.exterieures@fr.ch

Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen staatskanzlei@ktsh.ch
Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch
Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
Cancelleria dello Stato del Cantone Ticino	Palazzo delle Orsoline 6501 Bellinzona can-scds@ti.ch
Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch

Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancellerie@ne.ch
Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
Konferenz der Kantonsregierungen (KdK) Conférence des gouvernements cantonaux (CdC) Conferenza dei Governi cantonali (CdC)	Sekretariat Haus der Kantone Speichergasse 6 Postfach 3001 Bern mail@kdk.ch

2. In der Bundesversammlung vertretene politische Parteien / partis politiques représentés à l'Assemblée fédérale / partiti rappresentati nell' Assemblea federale

Bürgerlich-Demokratische Partei BDP Parti bourgeois-démocratique PBD Partito borghese democratico PBD	Postfach 119 3000 Bern 6 mail@bdp.info
Christlichdemokratische Volkspartei CVP Parti démocrate-chrétien PDC Partito popolare democratico PPD	Generalsekretariat Klaraweg 6 Postfach 3001 Bern info@cvp.ch
Christlich-soziale Partei Obwalden csp-ow	Frau Linda Hofmann St. Antonistrasse 9 6060 Sarnen ch.schaeli@gmx.net
Christlichsoziale Volkspartei Oberwallis	CSPO Geschäftsstelle Postfach 132 3930 Visp info@cspo.ch

Evangelische Volkspartei der Schweiz EVP Parti évangélique suisse PEV Partito evangelico svizzero PEV	Nägeligasse 9 Postfach 3001 Bern vernehmlassungen@evppev.ch
FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR.I Liberali Radicali	Generalsekretariat Neuengasse 20 Postfach 3001 Bern info@fdp.ch
Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
Grünliberale Partei glp Parti vert'libéral pvl	Laupenstrasse 2 3008 Bern schweiz@grunliberale.ch
Lega dei Ticinesi (Lega)	Via Monte Boglia 3 Case postale 4562 6904 Lugano lorenzo.quadri@mattino.ch
Mouvement Citoyens Genevois (MCG)	Case postale 155 1211 Genève 13 info@mcge.ch
Partei der Arbeit PDA Parti suisse du travail PST	Postfach 8640 8026 Zürich pdaz@pda.ch
Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC	Generalsekretariat Postfach 8252 3001 Bern gs@svp.ch
Sozialdemokratische Partei der Schweiz SPS Parti socialiste suisse PSS Partito socialista svizzero PSS	Zentralsekretariat Spitalgasse 34 Postfach 3001 Bern verena.loembe@spschweiz.ch

3. Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete / associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national / associazioni mantello nazionali dei Comuni delle città e delle regioni di montagna

Schweizerischer Gemeindeverband	Laupenstrasse 35 3008 Bern verband@chgemeinden.ch
Schweizerischer Städteverband	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch
Schweizerische Arbeitsgemeinschaft für die Berggebiete	Seilerstrasse 4 Postfach 3001 Bern info@sab.ch

4. Gesamtschweizerische Dachverbände der Wirtschaft / associations faîtières de l'économie qui œuvrent au niveau national/ associazioni mantello nazionali dell'economia

economiesuisse Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation	Hegibachstrasse 47 Postfach 8032 Zürich info@economiesuisse.ch bern@economiesuisse.ch sandra.spieser@economiesuisse.ch
Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
Schweizerischer Arbeitgeberverband Union patronale suisse Unione svizzera degli imprenditori	Hegibachstrasse 47 Postfach 8032 Zürich verband@arbeitgeber.ch
Schweiz. Bauernverband (SBV) Union suisse des paysans (USP) Unione svizzera dei contadini (USC)	Laurstrasse 10 5201 Brugg info@sbv-usp.ch
Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association	Postfach 4182 4002 Basel office@sba.ch

Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS) Unione sindacale svizzera (USS)	Monbijoustrasse 61 Postfach 3000 Bern 23 info@sgb.ch
Kaufmännischer Verband Schweiz Société suisse des employés de commerce Società svizzera degli impiegati di commercio	Hans-Huber-Strasse 4 Postfach 1853 8027 Zürich berufspolitik@kfmv.ch
Travail.Suisse	Hopfenweg 21 Postfach 5775 3001 Bern info@travailsuisse.ch

5. Weitere Interessierte / Autres intéressés / Altri interessati

asut	Schweizerischer Verband der Telekommunikation Klösterlistutz 8 3013 Bern info@asut.ch
Berner Fachhochschule	Falkenplatz 24 3012 Bern office@bfh.ch
Interessengemeinschaft Detailhandel Schweiz (IG DHS) Communauté d'intérêt du commerce de détail suisse (CICDS)	Geschäftsstelle IG DHS Postfach 5815 3001 Bern info@igdhs.ch
Post CH AG	Wankdorfallee 4 3030 Bern corporatecenter@post.ch
Privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten	Henric Petri-Strasse 15 Postfach 205 4010 Basel praesident@privatim.ch
Procivis Daniel Gasteiger	Seestrasse 329 8038 Zürich gasteiger@procivis.ch
Schweizerische Bundesbahnen SBB	Hilfikerstrasse 1 3000 Bern 65 meier.bernhard@sbb.ch

Schweizerische Informatikkonferenz	Haus der Kantone Speichergasse 6 3011 Bern info@sik.ch
Schweizerischer Anwaltsverband SAV	Marktgasse 4 Postfach 8321 3011 Bern info@sav-fsa.ch
Schweizerischer Notarenverband	Schwanengasse 5/7 3011 Bern info@schweizernotare.ch
Swico	Josefstrasse 218 8005 Zürich info@swico.ch
Swiss Fintech Innovations	Binzmühlestrasse 14 8050 Zürich office@swissfintechinnovations.ch
Swisscom (Schweiz) AG	Alte Tiefenaustrasse 6 3050 Bern Konzern.Rechtsdienst@swisscom.com
Trägerverein SuisseID	Geschäftsstelle Steinerstrasse 37 3006 Bern office@suisseid.ch