Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Document de travail concernant le projet d'identité électronique (e-ID)

Base de discussion pour une vision commune d'une identité électronique reconnue par l'État en vue de la décision de principe qui sera prise par le Conseil fédéral

Résumé

Le présent document de travail concernant le projet d'e-ID sert de base à la discussion publique. Le but n'est pas ici de décider d'une variante de nouvelle e-ID reconnue par l'État. La discussion publique vise essentiellement à identifier les avantages offerts par l'e-ID, ses applications et les exigences relatives à une e-ID étatique. Le résultat de cette discussion publique servira ensuite de fondement à la décision de principe que le Conseil fédéral devra prendre d'ici à la fin de 2021.

Pour la Suisse, la recherche d'une solution d'identification électronique est relancée. La première étape consiste à discuter la vision d'une nouvelle e-ID. Les questions centrales qui se posent sont les suivantes:

- L'e-ID est-elle un document d'identité numérique établi par l'État permettant à son titulaire de prouver son identité et pouvant être utilisé dans le monde tant analogique que numérique?
- Est-ce qu'un écosystème plus étendu de preuves numériques de tous types provenant de divers émetteurs publics et privés pourrait être plus avantageux et susciter ainsi une utilisation plus large par les titulaires? Quels seraient les risques?

Les avantages de l'e-ID pour son titulaire doivent être au centre de la discussion. Quelques exemples d'application sont présentés, sachant qu'il n'existe pas *une seule et unique* application possible, mais que ce sont les avantages cumulés de toutes ses applications qui feront le succès de l'e-ID. En même temps, il convient de reconnaître également que ce sont probablement les différents fournisseurs publics et privés et non les titulaires mêmes de l'e-ID qui auraient le plus grand besoin dans l'immédiat d'un écosystème e-ID conçu de manière ouverte et facile à intégrer. Il est ainsi crucial de montrer, grâce à des exemples d'application pertinents, les avantages concrets aussi pour les titulaires. Dans ce contexte, l'État remplit les fonctions complémentaires d'initiateur, de facilitateur (*enabler*) et de garant.

Depuis le lancement de la loi fédérale sur les services d'identification électronique (LSIE), qui a été rejetée, la situation initiale a évolué dans les domaines suivants:

- La protection des données et, en particulier, la protection de la sphère privée sont des sujets de débat qui ont gagné en importance auprès du grand public.
- Les systèmes d'identité futurs reposent sur des approches axées sur l'utilisateur.

S'agissant des variantes de mise en œuvre technologique, diverses solutions possibles sont exposées et soumises à discussion:

- l'identité souveraine (SSI);
- l'infrastructure à clé publique;
- le fournisseur d'identité central étatique.

Des questions restent en suspens concernant toutes ces approches, ces dernières ne couvrant pas de la même manière l'ensemble des exigences. L'évaluation des solutions possibles n'aura pas lieu dans le cadre du présent document de travail, mais prendra place à l'occasion de la discussion publique. Il s'agira alors de définir dans les grandes lignes la vision commune d'une e-ID, son utilisation et les exigences relatives à l'écosystème. Cette discussion publique contribuera de manière significative à la décision de principe que le Conseil fédéral devrait prendre fin 2021. Il sera ensuite possible d'élaborer les bases légales, que le Parlement devra approuver.

Glossaire

Agent institutionnel	Terme du domaine de la SSI introduit par IDunion, projet pilote allemand en matière de SSI, qui désigne une application logicielle permettant de créer et de contrôler des données vérifiées.
Attribut	Donnée spécifique (par ex. prénom ou date de naissance).
Base de données "de secours" relative à l'identité	Dispositif électronique de sauvegarde de preuves d'identité, qui permet de récupérer les données et de les transférer sur d'autres appareils. Ce dispositif peut être géré par l'utilisateur lui-même à l'aide de son propre matériel informatique ou mis à disposition par un fournisseur de stockage sur le cloud.
Communication entre pairs	Communication directe sans intermédiaire décrivant, dans le contexte de la SSI, le flux de données entre l'émetteur et le détenteur ou le détenteur et le vérificateur.
Cryptographie à clé publique	Technologie de chiffrement asymétrique avec laquelle une clé est rendue publique alors que l'autre doit rester privée.
Détenteur (*holder*)	Dans le contexte d'une SSI et d'une infrastructure à clé publique: propriétaire d'un portefeuille de preuves numériques.
Données vérifiées (*verified credentials*)	Jeu de données d'un ou plusieurs attributs, vérifié et signé par l'émetteur, puis transmis à l'utilisateur; le nom de l'émetteur, la date d'émission et les preuves cryptographiques font partie, outre les données principales, des données vérifiées.
Écosystème e-ID	Interaction entre une grande variété d'acteurs (publics et privés) caractérisée par différentes utilisations et offres possibles qui a lieu au moyen et dans le contexte de l'e-ID sur la base d'une infrastructure numérique de confiance commune.
e-ID	Identité électronique reconnue par l'État, autrement dit un type de preuve numérique pouvant être utilisée pour justifier son identité.
Émetteur (*issuer*)	Institution, organisation ou particulier qui établit une preuve numérique et la délivre à un utilisateur.
Enregistrement décentralisé des données	Action de conserver les données non dans une seule mémoire centrale, mais de les répartir dans un réseau de systèmes de stockage ou de les délocaliser sur les appareils des utilisateurs finaux.
Fournisseur d'identité (IdP)	Élément technique du système servant à *garantir* l'identité de l'utilisateur au moyen d'une connexion. Au sens plus large, le terme peut également désigner par exemple un document d'identité ou un portefeuille.
Gestion des identités	L'abréviation GIA désigne la gestion des identités et des accès, ces deux termes allant souvent de pair. La gestion des identités consiste à administrer des identités et à assigner des caractéristiques (attributs techniques) – indépendamment des rôles et des autorisations associés. Dans ce contexte, une identité peut également être comprise simplement comme un login ou un compte.
Identité autogérée	Équivalent de l'identité souveraine; dans le domaine de la SSI, c'est l'utilisateur qui est responsable de l'administration de ses preuves numériques établies par des émetteurs et donc fiables.
Identité décentralisée	Identité électronique qui n'est pas gérée par un système central et n'a pas besoin uniquement de ce dernier pour être utilisée, mais qui est enregistrée sur le smartphone de l'utilisateur et peut être utilisée directement à l'aide de cet appareil.
Identité souveraine (SSI)	Ensemble de principes axés sur la protection des données et l'utilisateur qui a donné lieu ces dernières années à une technologie dérivée pour les e-ID.
Infrastructure à clé publique	Système global d'un réseau de confiance bâti sur la base d'une technologie de chiffrement asymétrique.
Infrastructure numérique de confiance	Ensemble de règlements, de processus, de concepts et d'éléments d'infrastructure qui garantissent la confiance dans les processus numériques et leur conformité et sont acceptés et utilisés par un large public.
Justificatif d'identité (*credential*)	Dans le domaine de l'identité souveraine: jeu de données composé d'un ou plusieurs attributs. Dans le domaine des fournisseurs d'identité (au sens d'identifiant): caractéristiques de l'identité permettant l'authentification d'une personne; synonyme de facteurs d'authentification (par ex. nom d'utilisateur, mot de passe ou NIP).
Liste de révocation	Liste lisible publiquement de numéros d'identification de preuves et de certificats établis puis retirés.
Minimisation des données	Action de réduire au minimum nécessaire les attributs lors de la transmission de données à des tiers et d'éviter les flux de données superflus ainsi que les données secondaires associées.
Niveau d'ambition	Terme tiré de la modification du règlement eIDAS (*ambition level*) visant à clarifier le champ d'application d'une infrastructure d'identification électronique.
Nœud (*node*)	Nœud de stockage dans un réseau de stockage distribué (*distributed ledger technology,* DLT).
Partie utilisatrice	Terme du domaine des fournisseurs d'identité désignant un vérificateur analogique, soit un participant au système qui tire profit de l'écosystème e-ID pour contrôler les preuves de l'identité et utiliser les données personnelles fournies par l'e-ID.
Portefeuille	Application logicielle, souvent conçue pour smartphone, qui stocke les preuves numériques et permet la communication avec les émetteurs et les vérificateurs.

Registre	Terme du domaine de la SSI désignant une mémoire lisible publiquement où sont stockées les preuves cryptographiques nécessaires pour contrôler la validité des données vérifiées
Règlement eIDAS	Règlement de l'Union européenne définissant des règles uniformes dans les domaines de l'identification électronique et des services de confiance électroniques; eIDAS (*electronic identification, authentication and trust services*) signifie identification électronique, authentification et services de confiance.
Répertoire des clés publiques	Registre central où les clés publiques (*public keys*) des émetteurs de preuves sont déposées. Dans une infrastructure à clé publique hiérarchique dotée d'une ancre de confiance, un tel répertoire n'est pas nécessaire.
Respect de la vie privée dès la conception	Principe de conception qui prévoit la protection des données et, en particulier, la minimisation de ces dernières dès la conception. Ainsi, la confiance peut être instaurée sans avoir à établir une sécurité par des bases légales et les contrôles qui en découlent.
Trust over IP (ToIP) Framework	Directives visant à définir les niveaux décisionnels concernant les questions de mise en œuvre en matière de gouvernance et de technologie, élaborées par des groupes de travail de la Trust over IP Foundation.
Vérificateur	Terme du domaine de la SSI désignant une partie utilisatrice analogique, soit un participant au système qui tire profit de l'écosystème e-ID pour contrôler les preuves et utiliser les données fournies par l'utilisateur.

Sommaire

1 But

Le présent document de travail concernant le projet d'e-ID constitue la base de la discussion sur la vision commune d'une e-ID reconnue par l'État, sa conception, le champ d'application de l'écosystème e-ID et nombre d'autres aspects. Ce document évite délibérément de décrire et d'évaluer une solution définitive. L'orientation que prendra l'e-ID pourra être précisée grâce à une large discussion, dont le résultat servira à préparer la décision de principe du Conseil fédéral concernant une nouvelle solution d'e-ID officielle.

2 Contexte

2.1 Votation populaire sur la LSIE

Le 27 septembre 2019, le Parlement a approuvé la LSIE à une large majorité. Le référendum ayant abouti, cette loi a été nettement rejetée lors de la votation populaire du 7 mars 2021.

2.2 Motions

Après le rejet de la LSIE, six motions de teneur identique ont été déposées le 10 mars 2021[1]:

*Le Conseil fédéral est chargé de mettre en place un système géré par l'État qui permette de prouver son identité en ligne, de la même manière que la carte d'identité ou le passeport permettent de le faire dans le monde réel. Il convient de respecter certains principes: prendre en compte la protection de la vie privée dès la conception du produit (*privacy by design*), ne collecter que les données nécessaires et enregistrer celles-ci de manière décentralisée (par exemple auprès de l'utilisateur en ce qui concerne les données d'identification). La solution pourra s'appuyer sur des produits et services développés par le secteur privé. En revanche, l'octroi des e-ID et le fonctionnement du système devront être assumés par des services publics spécialisés.*

Principales exigences formulées dans les six motions:

- moyens d'identification électronique reconnus par l'État, de manière comparable au passeport;
- minimisation des données et respect de la vie privée par le design;
- enregistrement décentralisé des données;
- processus d'émission et exploitation globale confiée aux autorités publiques.

2.3 Définir la vision d'une e-ID

Il existe actuellement de multiples conceptions de l'e-ID, chacun y allant de son opinion. Le présent document aidera à préciser et à développer une vision fondamentale. Il s'agira ainsi de clarifier si l'e-ID pourra être utilisée également dans le monde physique (de manière similaire aux certificats de vaccination numériques), si elle pourrait revêtir la même force probante que les documents d'identité physiques et si elle doit servir, en tant que facteur d'authentification, à un login national reconnu par l'État.

[1] https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213129

Prouver l'identité par des moyens numériques est la fonction première de l'e-ID. Cette dernière peut être conçue comme un *document d'identité* et le login comme l'*une* de ses applications possibles. Par ailleurs, l'État assume ici les rôles d'émetteur et d'exploitant. L'e-ID pourrait donc être définie comme suit:

"Une e-ID est un document d'identité numérique émis par l'État pour prouver l'identité de son titulaire".

Afin d'éviter une conception trop étroite, l'e-ID est présentée ici en lien direct avec la vision d'une infrastructure numérique suisse de confiance, que l'on pourrait notamment énoncer comme suit:

"La Suisse possède une infrastructure numérique de confiance gérée par l'État qui permet et favorise des processus sécurisés sans rupture de média".

Une telle infrastructure numérique de confiance pourrait grandement bénéficier de l'e-ID reconnue par l'État, bien que sa concrétisation nécessiterait bien davantage (cf. ch. 2.4). Sont considérés comme ayant droit à une e-ID – comme défini dans la LSIE – les ressortissants suisses titulaires d'un document d'identité reconnu et les étrangers titulaires d'une pièce de légitimation valable (ci-après "utilisateurs"). Les personnes morales agissant toujours par le biais de leur organe, autrement dit des personnes physiques, elles ne peuvent pas être titulaires d'une e-ID et sont identifiées au moyen d'un numéro d'identification unique des entreprises (IDE)[2].

2.4 Exigences concernant la numérisation

Les efforts de numérisation doivent souvent répondre à des exigences élevées, alors que les attentes et les conceptions sont des plus variées. La technique n'est plus perçue aujourd'hui comme un facteur limitant dans le domaine de la transmission de données: techniquement, tout est possible ou presque. Néanmoins, l'aspect immatériel complique parfois la compréhension commune des situations, des fonctions et des rôles.

La numérisation va toujours de pair avec une incitation à repenser les processus et les rôles. Lorsque les processus existants sont transférés sans vérification vers des canaux numériques, on n'obtient en principe pas une numérisation de qualité ni de processus numériques efficaces. Idéalement, il convient de supprimer les étapes des processus analogiques qui étaient nécessaires au préalable. L'automatisation associée à la numérisation des processus (dans le sens où ces derniers sont remaniés selon des principes numériques) permettra d'économiser des ressources et rend possible une grande extensibilité du système, qui, avec quasiment les mêmes ressources, peut traiter une quantité beaucoup plus importante de données de manière plus qualitative et rapide.

Les utilisateurs doivent être au centre du développement. Il s'agit là non seulement de particuliers, mais également d'utilisateurs issus de l'économie (agissant pour le compte de leur entreprise), qui peuvent bénéficier de processus numérisés à des degrés divers. Une numérisation de qualité améliore directement les conditions économiques, simplifiant les procédures, de sorte que l'économie est en mesure d'offrir de nouvelles possibilités aux utilisateurs. C'est donc l'ensemble de l'économie suisse qui en profite.

[2] Cf. https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises.html.

L'appel à la création d'une e-ID reconnue par l'État peut être compris comme une attribution de tâches à la Confédération. Les compétences exactes de cette dernière et donc les possibilités de faire avancer la numérisation à l'aide d'une infrastructure numérique étatique doivent cependant encore être examinées plus en détail. Cela dit, l'e-ID n'est pas la solution miracle que beaucoup attendent, tout en espérant qu'elle permettra de résoudre tous les problèmes de numérisation. L'e-ID ne numérisera pas la Suisse, mais contribuera à la poursuite de la numérisation, car elle constitue un élément d'infrastructure important de notre pays.

Enfin, il reste à préciser ici que de nombreuses exigences sont en conflit et qu'il n'y en a pas *une seule juste*, mais qu'il convient de trouver, à la faveur de la discussion, la voie du consensus au point de jonction par exemple des éléments suivants:

- convivialité ↔ protection des données ↔ sécurité des données
- responsabilité individuelle ↔ possibilité d'assistance
- orientation utilisateur ↔ confiance
- environnement contrôlé difficile d'accès ↔ système ouvert facile d'accès
- peu de possibilités d'application contrôlées ↔ de nombreuses possibilités d'application non contrôlées
- rapidité de mise en œuvre ↔ perfection
- flexibilité ↔ protection de l'utilisateur

3 Évolutions dans le domaine des identités numériques

3.1 Évolutions techniques

En raison des exigences en matière de protection renforcée des données et de décentralisation de leur stockage, également formulées dans les motions citées au ch. 2.2, une discussion au sujet de l'identité décentralisée s'est engagée à l'échelle mondiale ces dernières années. Il en a résulté toute une série de technologies et de nouvelles procédures et normes cryptographiques pouvant être utilisées pour créer des systèmes de confiance. La SSI, qui repose sur des principes et des moyens technologiques centrés sur l'utilisateur, est ainsi actuellement au cœur de la plupart des discussions. La raison en est notamment la simplicité de sa conception, la proximité de sa technologie et de la réalité physique et l'universalité de son application.

L'un des fondements techniques de la technologie SSI est la cryptographie à clé publique, qui permet déjà depuis des décennies de fournir des preuves d'origine techniques décentralisées sous forme de certificats (par ex. X.509). Ceux-ci sont entre autres utilisés pour signer des données dans le passeport biométrique, établir le certificat COVID, mettre en place une communication protégée sur un site Web ou dans le domaine de la signature électronique.

La tendance à utiliser l'e-ID sur smartphone est visible au niveau international, étant donné la très forte pénétration actuelle de ce dernier. Les solutions développées autrefois avec des cartes à puce sont remplacées par des solutions conçues pour les smartphones. Les portefeuilles numériques, en tant que dispositifs de stockage de preuves numériques gérées de manière décentralisée, sont en tête de l'agenda numérique également dans l'Union européenne (UE). Il reste cependant que de nombreuses solutions d'e-ID continuent d'être à l'heure actuelle en Europe des solutions de *fournisseurs d'identité classiques*, cela dit sous des formes très diverses (fournisseurs d'identité étatiques, privés, fédérés).

Relancer l'e-ID est une occasion pour la Suisse de profiter des connaissances et des développements les plus récents. La technologie évoluant très rapidement, il est nécessaire de choisir une solution dont la mise en œuvre technique soit souple. À l'étranger, les cycles de renouvellement des solutions en matière d'identité numérique vont de cinq à dix ans. Une solution parfaite et définitive n'existera jamais et ne doit donc pas être recherchée. L'objectif serait plutôt de choisir une voie qui puisse sous-tendre de nombreux processus de création de valeur et favoriser la numérisation de la Suisse. Le cadre juridique qui devra être créé pour une solution d'identification électronique reconnue par l'État devrait être le plus neutre possible du point de vue technologique afin de permettre explicitement des développements ultérieurs.

3.2 Évolution du droit européen

Le 3 juin 2021, la Commission européenne a soumis une proposition[3] de modification du règlement eIDAS[4] et de création d'un cadre juridique pour l'identité numérique européenne (EUid). Si le nouveau projet de règlement devait être adopté, les États membres seraient tenus de mettre à la disposition des citoyens et des entreprises des portefeuilles numériques leur permettant d'associer leur identité numérique nationale aux attestations d'autres attributs personnels (par ex. permis de conduire, diplômes, compte bancaire). De cette identité numérique nationale est tirée une EUid. Les portefeuilles peuvent être créés par des autorités ou des institutions privées, pour autant que ces dernières soient reconnues par un État membre.

Afin que la proposition puisse être mise en œuvre dès que possible, elle est assortie d'une recommandation où la Commission enjoint aux États membres de créer des instruments communs jusqu'à septembre 2022 et de commencer immédiatement les travaux préliminaires nécessaires. Ces instruments doivent inclure l'architecture technique, les normes, les lignes directrices et les meilleures pratiques.

Le cadre fourni par la Commission est neutre du point de vue technologique, mais repose sur les principes de la SSI. Dès septembre 2021, les États membres négocieront eux-mêmes les normes techniques. Afin que la future e-ID suisse puisse être notifiée conformément au règlement eIDAS, il est avantageux de se référer au cadre défini par la Commission.

4 Écosystème e-ID

4.1 Faire partie du quotidien

Toutes les initiatives visant à introduire avec succès une e-ID nationale sont constamment confrontées au paradoxe de l'œuf et de la poule: sans e-ID, il n'y a pas d'exemples d'application et sans exemples d'application, l'e-ID n'est pas nécessaire. Outre l'utilisation de l'e-ID pour accéder à des services de cyberadministration, on mise souvent dans le contexte européen sur des utilisations secondaires, telles que la signature électronique ou l'e-banking, afin d'en promouvoir la diffusion et l'utilisation fréquente. L'intérêt d'une plus grande fréquence d'utilisation réside dans une meilleure maîtrise de l'opération, une compréhension accrue et la possibilité de créer une habitude pour le grand public.

---

[3] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

[4] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

Si l'on souhaite permettre le plus grand nombre d'applications possible, il est nécessaire de créer un écosystème opérationnel, autrement dit une infrastructure partagée, avec des règles conjointement définies et offrant de nombreuses possibilités aux acteurs du système les plus divers. Idéalement, l'e-ID fonctionnera ici dans un écosystème doté d'interfaces ouvertes et normalisées, soumis à une gouvernance coordonnée, n'appliquant pas de réglementations bureaucratiques et inhibitrices, et permettant la mise à jour pratique et automatisable des données e-ID. La base serait ainsi créée pour que des entreprises du secteur privé puissent y participer et développer de nouveaux processus et activités – ce qui permettrait des applications supplémentaires. Du moment qu'il existe des applications pratiques et que l'on y voit une utilité personnelle, l'intérêt des utilisateurs potentiels sera éveillé.

La convivialité et la satisfaction des utilisateurs sont également des critères importants à prendre en compte. Les interactions de l'écosystème avec l'e-ID doivent être aisées, transparentes et cependant compréhensibles. Dans le même temps, il doit en résulter une confiance fondamentale dans le système, ses participants et la force probante de l'e-ID. Son utilisation ne devrait pas nécessiter des appareils supplémentaires et devrait probablement être gratuite, car même de petits montants peuvent avoir un effet dissuasif sur les utilisateurs. Il faudrait expressément veiller à ce qu'il y ait le moins possible d'obstacles à l'accès. Enfin, l'e-ID doit satisfaire aussi les attentes des participants en matière de protection et de sécurité.

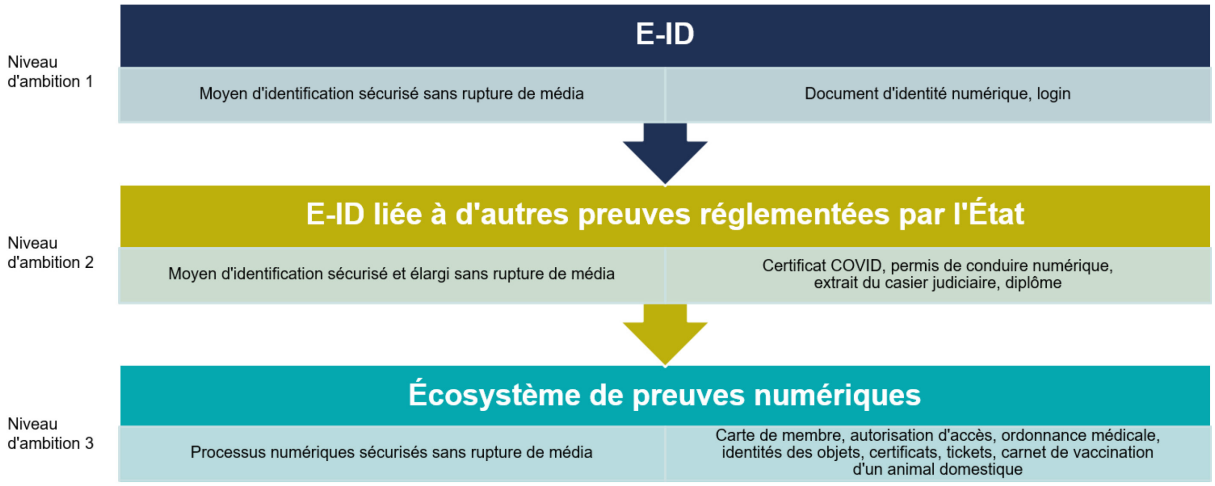
Cela est-il suffisant pour que l'e-ID fasse partie de notre quotidien? Suffit-il de bâtir un écosystème e-ID autour de l'e-ID ou la portée de l'écosystème devrait-elle être plus vaste et l'e-ID ne plus être qu'*une preuve numérique* parmi d'autres? Telles sont les questions traitées ci-après.

4.2 Portée de l'écosystème

Avant d'amorcer la réflexion sur la technologie, il est pertinent d'aborder également la question du champ d'application futur de l'e-ID (aussi appelé niveau d'ambition) et, par là même, de la portée de l'écosystème. Il existe des interdépendances entre, d'une part, le niveau d'ambition, la structure et la conception de l'écosystème et, d'autre part, les technologies pouvant être utilisées. La technologie devrait être choisie essentiellement en fonction du résultat souhaité, mais il importe également de savoir que diverses mises en œuvre techniques de complexité similaire permettent d'obtenir des résultats différents.

Comme base de discussion et compte tenu de la discussion menée par l'UE[5], les trois niveaux d'ambition ci-après sont définis:

[5] L'UE définit également trois niveaux d'ambition pour l'EUid.



Niveau d'ambition 1: une e-ID

Le niveau d'ambition 1 correspond à l'objectif minimal: l'e-ID est un document d'identité pouvant être utilisé dans le monde numérique pour prouver l'identité de son titulaire. La Confédération en est le seul émetteur. L'e-ID peut être complétée *par un* login ou être utilisée *pour un* login. Les avantages directs de l'e-ID en tant que moyen d'identification numérique résident pour l'essentiel dans les applications suivantes:

- confirmation de l'identité (par ex. compte bancaire, abonnement de téléphonie mobile, demande d'extrait du casier judiciaire, guichet postal, contrôle des personnes);
- confirmation de l'âge (avec des attributs dérivés).

Ce qui s'est passé lors de la votation sur la LSIE a donné l'impression que l'avantage offert par ces applications n'était pas totalement convaincant.

Niveau d'ambition 2: une e-ID liée à d'autres preuves réglementées par l'État

Le niveau d'ambition 2 vise un écosystème e-ID, où l'e-ID officielle constitue une identité de base sur laquelle reposent nombre d'autres preuves réglementées par l'État, comme le permis de conduire numérique. L'identité de base fournit ainsi les données personnelles, telles que le nom, la date de naissance et la photographie. Les données à ajouter au permis de conduire seraient des attributs complémentaires, comme la catégorie du véhicule et la date d'échéance.

Des liens cryptographiques permettraient le rattachement à l'identité de base. Grâce à des liens logiques, une autre preuve reconnue par l'État pourrait également fonctionner de manière autonome et ne serait pas affectée si, par exemple, l'identité de base devait être révoquée.

La portée de l'écosystème serait ainsi nettement plus large que celle du niveau 1, avec un nombre beaucoup plus élevé d'utilisations possibles. Un large éventail d'acteurs étatiques seraient autorisés à être émetteurs et garantiraient également le bien-fondé des liens établis.

Niveau d'ambition 3: un écosystème de preuves numériques

C'est avec le niveau d'ambition 3 qu'on a le plus de chances de résoudre le paradoxe de l'œuf et de la poule. En exploitant toute la portée de l'écosystème, l'e-ID devient une preuve numérique parmi d'autres. Bien qu'il soit possible d'établir un lien avec l'e-ID, une preuve numérique peut également fonctionner indépendamment (par ex. billet pour une manifestation, titre de

transports publics, carte de membre, carnet de vaccination d'un animal de compagnie, permis de circulation ou rapport du contrôle technique réussi d'un véhicule).

Ce niveau d'ambition permet à des services publics et privés d'émettre des preuves numériques. La compétence d'émission des services privés est ici également cruciale, les preuves émises entre ces derniers étant très nombreuses au quotidien. Ainsi, maints processus peuvent être mis en œuvre sans rupture de média en utilisant des moyens normalisés (par ex. dans la gestion des clients, des fournisseurs et du personnel, ainsi que partout où les document d'identité, les justificatifs et les certificats jouent un rôle important). L'intérêt pour l'utilisateur est que l'opération est toujours identique (réception, enregistrement, présentation) et qu'une compréhension collective des preuves numériques peut s'instaurer. L'e-ID ne se trouve plus au premier plan de l'écosystème, ce dernier devenant un dispositif de stockage décentralisé, sécurisé et réglementé par l'État, autrement dit un *portefeuille étatique* permettant d'obtenir des informations avec un haut degré de fiabilité.

Concernant l'EUid, l'UE se prononce en faveur de la variante complète de niveau 3, à savoir un portefeuille d'identités numérique personnel hautement sécurisé (*highly secure personal digital identity wallet*).

L'e-ID constitue indéniablement l'élément central d'un tel écosystème; elle pourrait favoriser la création au niveau national d'une infrastructure numérique de confiance ouverte. Un développement par étapes est en principe possible, mais le niveau d'ambition final doit être défini dès le départ, car toutes les solutions technologiques ne conviennent pas à un écosystème ouvert de preuves numériques (niveau d'ambition 3). Chaque niveau d'ambition est compatible avec une ou plusieurs technologies. Chaque implémentation entraîne des conséquences particulières. Or, avant de présenter les solutions possibles, il convient de décrire ci-après quelques exemples d'application.

4.3 Applications

Afin de comparer les solutions possibles, divers exemples d'application sont décrits ici, ainsi que la situation actuelle et la situation envisagée. Chacun est caractéristique d'un certain type d'application et fait ressortir des points spécifiques qui aideront à soulever des questions supplémentaires pour la discussion.

La liste d'applications qui suit n'a pas pour but d'être exhaustive. Afin d'analyser comme requis les avantages pour la population, il est essentiel de rechercher des applications (*use cases*) pertinentes et de les évaluer en fonction des avantages optimaux pour l'utilisateur. Comme expliqué plus haut, rien n'est définitif et il faudra découvrir de nouvelles applications au fur et à mesure. Par conséquent, selon le niveau d'ambition, il convient de mettre en place des processus agiles contrôlés permettant une telle adaptation. L'État doit jouer ici – comme exigé dans certaines motions – le rôle de facilitateur (*enabler*) proactif.

Les applications décrites visent à démontrer et questionner à l'aide d'exemples les avantages directs et concrets pour les utilisateurs de l'e-ID. Implicitement, il existe toujours en arrière-plan la possibilité de simplifier les processus, ce qui se traduit par des avantages indirects pour les utilisateurs, que ce soit par l'accélération des procédures, la baisse du prix des prestations ou la création de nouveaux services. Selon le niveau d'ambition, les fournisseurs de services eux-mêmes (également appelés *relying parties*, autrement dit parties utilisatrices) peuvent se considérer non seulement comme destinataires et vérificateurs de preuves, mais également comme émetteurs de ces dernières.

De nombreuses discussions sur ce thème montrent clairement qu'il n'existe pas *une seule et unique application possible*; ce sont la somme et la diversité des applications qui font leur valeur! Plus le niveau d'ambition est élevé, plus cette valeur et cette diversité augmentent. En Suisse, les acteurs économiques innovants pourraient considérablement accroître cette valeur et cette diversité dans le cadre d'un *écosystème de preuves numériques* ouvert – qui aurait ainsi des chances réelles de faire partie du quotidien des gens.

4.3.1 Contrôle de l'âge dans les mondes analogique et numérique

Le contrôle de l'âge vise à s'assurer qu'une personne a atteint un certain âge, son âge exact et sa date de naissance n'étant pas pertinents. L'avantage de l'e-ID pour ses utilisateurs réside dans l'utilisation aisée, ne nécessitant que peu de données et possible dans le monde tant analogique que numérique.

Situation actuelle dans le monde analogique, par exemple à l'entrée d'une discothèque:

- Le personnel de sécurité vérifie les documents d'identité physiques pour s'assurer par exemple qu'une personne a 18 ans révolus et peut entrer dans l'établissement.
- Le document d'identité comprend notamment la photographie, la date de naissance exacte, le nom complet et la nationalité.

Situation actuelle dans le monde numérique, par exemple sur un site de commerce en ligne:

- Dans de très nombreux cas, il n'y a pas de contrôle de l'âge et il est demandé aux utilisateurs de confirmer qu'ils sont majeurs. Ces mesures n'empêchent pas les mineurs d'acheter des articles non autorisés à leur âge.
- Le contrôle par photographie ou vidéo d'un document d'identité est relativement contraignant et n'est donc que rarement exigé.

Points principaux:

- Il n'y a pas de minimisation des données lors du contrôle de l'âge au moyen d'un document d'identité.
- Des données secondaires peuvent être divulguées pendant les procédures de contrôle.
- La protection des mineurs n'est pas suffisante, car elle est très exigeante sur le plan technique.

Situation envisagée dans le monde analogique, par exemple à l'entrée d'une discothèque:

- L'e-ID peut être utilisée dans le monde physique de la même manière que les documents d'identité existants.
- Pour contrôler l'âge d'une personne, deux informations suffisent: la preuve que la personne a l'âge autorisé et une photographie. Lors d'un contrôle, ces informations doivent pouvoir être présentées à partir de l'e-ID officielle, sans divulguer des données supplémentaires. La protection contre une utilisation ultérieure non autorisée de la photographie est réglementée dans la loi fédérale sur la protection des données (LPD).

Situation envisagée dans le monde numérique, par exemple sur un site de commerce en ligne:

- L'émetteur de l'e-ID n'est pas informé lorsque l'e-ID est utilisée.
- Pour garantir la fiabilité des données fournies, la demande d'information relative à l'âge est intégrée comme une étape du processus dans une e-ID (comme dans une opération de paiement).

Avantages concrets pour les utilisateurs de l'e-ID:

- Le nom et la date de naissance ne sont pas divulgués, ce qui contribue en fin de compte à la sécurité globale.
- Pour se rendre dans une discothèque, il n'est pas nécessaire de se munir d'un document d'identité physique.
- La protection des mineurs est renforcée lors des achats en ligne.

4.3.2 Ouverture d'un compte bancaire

Il n'existe guère de domaine aussi fortement réglementé que le secteur financier. L'ouverture d'un compte bancaire est soumise à un grand nombre de lois et de dispositions. Il est donc nécessaire d'être très au clair sur la personne qui souhaite ouvrir un compte (*know your customer* ou connaissance de la clientèle). L'avantage pour l'utilisateur de l'e-ID réside dans la transmission aisée de la preuve de l'identité. Par ailleurs, il serait possible de produire d'autres preuves sans avoir à scanner et à envoyer par e-mail des données critiques pour la protection des données.

Situation actuelle:

- Le contrôle de l'identité sur place se fait en présentant une carte d'identité ou un passeport. Une copie du document d'identité est effectuée et ajoutée aux dossiers.
- Le contrôle de l'identité en ligne se fait par exemple en photographiant un document d'identité et en procédant ensuite à une identification par vidéo au moyen de processus en ligne parfois automatisée.
- Le contrôle de l'identité par virement d'un montant se fait à partir d'un compte bancaire libellé au nom du titulaire.

Points principaux:

- L'identification est très contraignante (sur le plan financier, technique et du personnel).
- L'attribution de l'identité au titulaire est très fiable; elle permet d'imputer de manière certaine les actes réalisés sous une identité à son titulaire (possibilité de les faire valoir devant un tribunal).

Situation envisagée:

- L'e-ID permet une identification aisée, sans rupture de média et sécurisée.
- Il se peut que la banque procède à des opérations de comparaison complémentaires en raison d'exigences spécifiques au secteur (par ex. contrôle de la personne devant l'écran au moyen de la photographie tirée du document d'identité numérique transmis pour l'identification).

4.3.3 Extrait du registre des poursuites

Pour louer ou acheter un appartement ou conclure un contrat de travail, un extrait du registre des poursuites est souvent demandé d'office. Celui-ci doit être obtenu auprès de l'office des poursuites compétent. L'avantage de l'e-ID pour ses utilisateurs réside tant dans la fourniture aisée d'une preuve de l'identité au moment de commander l'extrait auprès de l'un des quelques 400 offices des poursuites existants que dans l'obtention d'un extrait du registre des poursuites numérique (preuve) pouvant être présenté aussi souvent que souhaité.

Situation actuelle:

- D'abord, il faut trouver l'office des poursuites compétent. Le portail de la Confédération EasyGov propose à cette fin une fonction de recherche et aide à remplir correctement le formulaire de demande.
- Ensuite, la demande est généralement imprimée, signée et expédiée par voie postale (accompagnée d'une copie du document d'identité). Selon l'office des poursuites, il peut être nécessaire de payer au préalable un émolument.
- L'office envoie l'extrait sur support papier.
- L'utilisateur transmet le document (l'original ou une copie) au destinataire concerné.
- Des processus numériques sont également proposés si la personne demandant l'extrait dispose d'une signature qualifiée ou si elle charge un tiers d'obtenir son extrait en justifiant d'un intérêt.
- Dans ce cas, l'office des poursuites compétent envoie un PDF signé. Le destinataire peut en contrôler l'authenticité au moyen de l'application du validateur.

Points principaux:

- Transmission de l'extrait: le document original est souvent exigé.
- Les processus sont contraignants pour le destinataire en raison de la rupture de média et de la nécessité de contrôler la validité de la signature du PDF au moyen de l'application du validateur.
- Les extraits sur support papier manipulés passent inaperçus auprès des destinataires qui n'exigent pas un original identifiable.

Situation envisagée:

- La personne demandant l'extrait peut être identifiée au moyen de l'e-ID.
- L'extrait numérique faisant office de preuve est envoyé à l'utilisateur par un canal sécurisé.
- L'extrait numérique peut être directement transmis par l'utilisateur au destinataire.
- Le système du destinataire peut automatiser des processus de contrôle.

Avantages concrets pour les utilisateurs de l'e-ID:

- Il n'est plus nécessaire de se rendre à un office ou à un guichet postal.
- La confirmation de l'original peut être présentée aussi souvent que souhaité. Aucun coût supplémentaire n'est généré lorsque le même document doit être remis à différents services.

4.3.4 Login officiel

Un login est nécessaire pour accéder à de nombreux services de cyberadministration. À cet effet, un service d'authentification de l'État pourrait utiliser l'e-ID comme facteur d'authentification. L'avantage de l'e-ID pour ses utilisateurs résiderait dans l'utilisation des mêmes identifiants de login sur différentes plates-formes de cyberadministration.

Situation actuelle:

- La diversité des fournisseurs d'identité ou des systèmes de gestion de l'identité (*identity management systems*) sur différents portails engendre une multitude d'identifiants de login.
- De nombreux cantons ne disposent pas encore d'une gestion des identités pour d'éventuels services de cyberadministration.
- Il n'existe pas de login officiel qui soit utilisé dans toute la Suisse.

Points principaux:

- Le fonctionnement en parallèle des solutions existantes en service est rendu possible.
- L'authentification est sécurisée à l'aide de facteurs d'authentification supplémentaires.

Situation envisagée:

- L'e-ID est un facteur d'authentification (multiple), soit un élément que la personne possède, éventuellement aussi une information secrète et un élément biométrique.
- Un service d'authentification étatique met un mécanisme d'authentification sécurisé à la disposition de tous les portails de cyberadministration de l'État.
- Il est possible de séparer l'identité des droits d'accès, ce qui simplifie considérablement la structure et la maintenance des applications.

Avantages concrets pour les utilisateurs de l'e-ID:

- Les mêmes identifiants de login peuvent être utilisées sur différentes plates-formes de cyberadministration.
- Le processus de login est sécurisé, ce qui renforce la protection de l'accès.

4.3.5 Signatures électroniques

Les signatures électroniques sont régies depuis 2005 par la loi sur la signature électronique (SCSE), bien qu'elles n'aient été que peu utilisées par la population jusqu'à présent. L'avantage pour les utilisateurs de l'e-ID réside dans l'accès facilité à la signature électronique qualifiée.

Situation actuelle:

- Des fournisseurs de services reconnus proposent les services de signature électronique nécessaires.
- Les fournisseurs de services procèdent tout d'abord à l'identification de l'utilisateur; pour accéder à la signature qualifiée, l'utilisateur doit se présenter en personne. Un certificat qualifié lui est ensuite délivré.
- Le certificat qualifié permet de signer électroniquement et valablement des documents.

- Les documents signés électroniquement peuvent être contrôlés à l'aide de l'application du validateur.

Point principal:

- L'accès à la signature qualifiée est moins aisé en raison de l'obligation de se présenter en personne.

Situation envisagée:

- La création de signatures électroniques qualifiées est facilitée.
- L'échange numérique de documents contractuels est favorisé.

Avantage concret pour les utilisateurs de l'e-ID:

- Grâce à la signature électronique qualifiée, les contrats numériques garantis juridiquement deviennent la norme et permettent de gagner du temps et de l'argent.

4.4 Bases légales

L'analyse des bases légales de la loi future et l'élaboration du projet de loi ne font pas l'objet du présent document de travail. Afin de créer les bases légales de l'identification électronique reconnue par l'État, il convient d'abord de définir le niveau d'ambition visé et de retenir une solution d'e-ID.

4.5 Communication

Pour créer une e-ID reconnue par l'État, une bonne communication est nécessaire dès le début entre tous les acteurs concernés: utilisateurs potentiels, cantons, secteur privé, organisations et administration fédérale devront être inclus de la même manière pour contribuer à façonner cette vision commune et la porter ensuite. Les avantages sociétaux possibles doivent toujours être placés en première ligne, suivis des éventuels exemples et formes d'application. La discussion relative à la technologie à mettre en œuvre aura lieu ultérieurement.

Outre les processus participatifs habituels, il sera tenu compte – dans la mesure du possible – des autres avis exprimés via des plates-formes de discussion interactives et des tests publics d'intrusion.

5 Différentes solutions d'e-ID possibles

5.1 Solution d'e-ID basée sur l'identité souveraine

5.1.1 Approche

L'identité souveraine (*self-sovereign identity*, SSI) est la plus récente des solutions possibles d'écosystème e-ID proposées dans le présent document de travail concernant le projet d'e-ID. En 2016, Christopher Allen a formulé dix principes centrés sur l'utilisateur et la protection des

données, qui devraient présider à la conception des "identités autogérées"[6], soit des identités sur lesquelles l'utilisateur exerce le plus grand contrôle possible. Cette évolution est dans l'air du temps, qui fait la part belle aux préoccupations relatives à la protection et à la sécurité des données et à la dépendance vis-à-vis de systèmes d'identification centraux, comme le reflètent les motions mentionnées au ch. 2.2. Dans le même temps, on cherche aussi à relier numériquement des systèmes de façon universelle au lieu de devoir toujours concevoir de nouvelles interfaces.

En quelques années ont vu le jour des normes ouvertes, des cadres techniques et une architecture unique propres à étayer la mise en œuvre d'une SSI. Cette évolution n'a pas réinventé la roue, mais s'est nourrie de la connaissance des infrastructures à clé publique et des procédés avancés de cryptographie. Ainsi, on trouve déjà aujourd'hui des écosystèmes SSI en service, même si aucun État n'a encore créé d'e-ID sur la base de la SSI. Les récents développements survenus dans l'UE vont également dans ce sens.

L'approche SSI se situe en principe au niveau d'ambition 3, qui correspond à un écosystème de preuves numériques. Elle est toutefois aussi appropriée à tous les niveaux d'ambition, la différence résidant dans la gouvernance, puisque les moyens techniques engagés sont les mêmes.

5.1.2 Description des fonctions

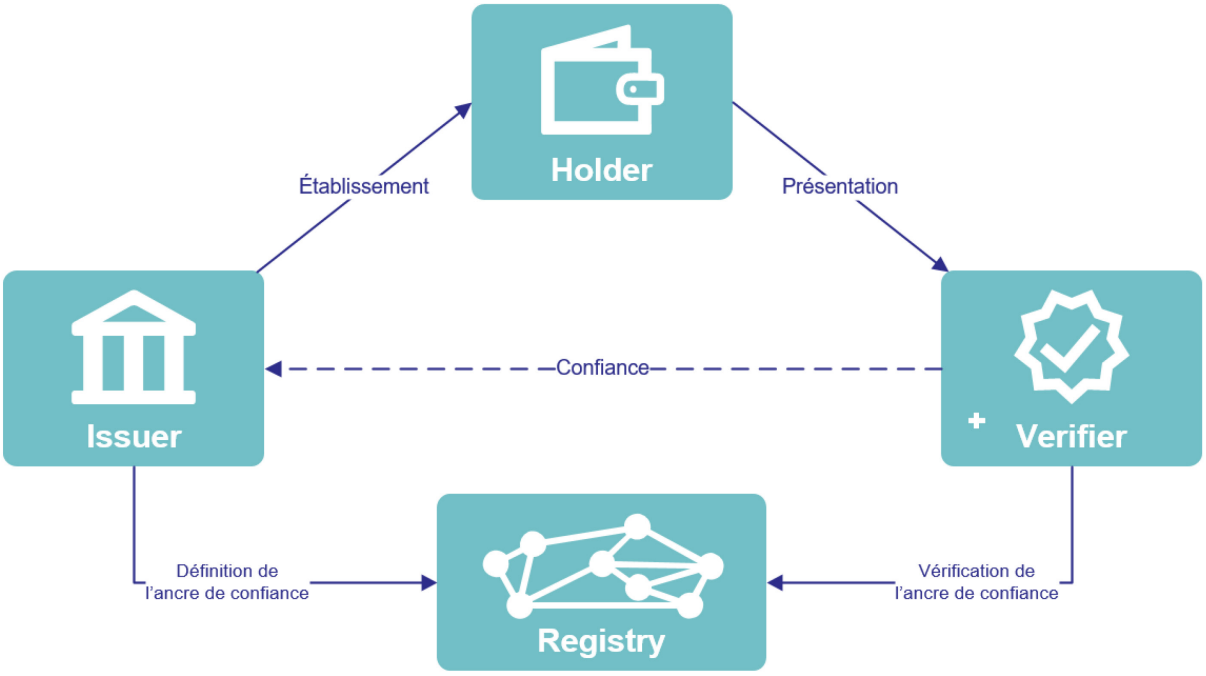


Illustration 1: architecture de base de la SSI

[6] *Self-sovereign identity* est fréquemment traduit par *identité souveraine*, ce qui prête souvent à confusion. En effet, une pièce d'identité officielle est établie par l'État, qui la remet aux utilisateurs pour qu'ils la gèrent et l'utilisent; ce n'est donc pas eux qui l'émettent, contrairement à ce que laisse penser la notion de souveraineté.

Le triangle de confiance reliant **émetteur** (*issuer*), **utilisateur** (*holder*) et **vérificateur** (*verifier* ou *relying party*) existe dans de nombreuses architectures de confiance. S'agissant de la SSI, il est essentiel que les relations décrites reflètent aussi directement les flux de communication – sans instances intermédiaires supplémentaires. Le flux de données entre l'émetteur et l'utilisateur ou entre l'utilisateur et le vérificateur prend la forme d'une communication cryptée entre pairs. Le canal de communication est en règle générale établi au moyen d'un mécanisme utilisant un code QR.

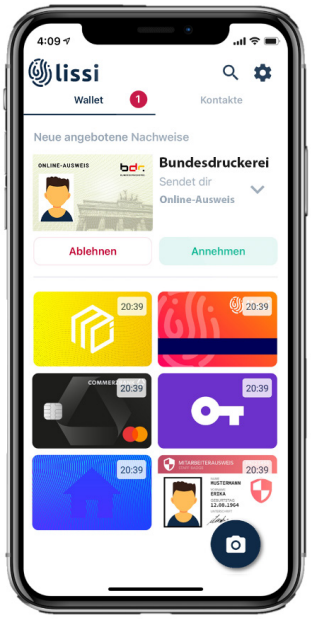


Illustration 2: exemple d'un portefeuille électronique permettant à l'utilisateur de recevoir, de gérer et de présenter des données vérifiées (source: IDunion, lissi)

L'émetteur transmet les données vérifiées (*verified credentials*) à l'utilisateur, qui les sauvegarde dans un portefeuille électronique sur son téléphone portable. Le vérificateur peut demander à l'utilisateur de lui fournir des données via le canal de communication sécurisé. En réponse, l'utilisateur peut décider quelles données il transmet effectivement au vérificateur: les données vérifiées dans leur intégralité, certains éléments de ces données ou des données qu'il a lui-même saisies.

Pour contrôler l'authenticité des données vérifiées, on utilise les preuves cryptographiques – pas les données elles-mêmes – conservées dans un registre contenant des ancres de confiance électroniques (aussi appelé *registry*). Ce registre est une mémoire en général décentralisée (par ex. DLT, *blockchain*) où chaque émetteur dépose son identité ainsi que ses clés publiques. Un vérificateur peut ainsi vérifier sans contact avec l'émetteur et sans instance tierce les données présentées par l'utilisateur. La relation de confiance entre le vérificateur et l'émetteur repose soit sur un contact personnel, soit sur une référence publique (par ex. une information figurant sur un site Internet).

Les données vérifiées peuvent être conçues pour être annulables ou révocables. L'émetteur a ainsi la possibilité d'annuler un justificatif d'identité établi à tout moment et sans entrer en contact avec l'utilisateur. Cette information est répertoriée dans une liste de révocation du registre.

Le cas d'application minimal de l'e-ID est le suivant:

- L'État (*issuer*) établit l'e-ID à titre de données vérifiées pour l'utilisateur (*holder*) selon un processus entièrement automatisé.
- L'utilisateur gère ces données vérifiées dans un portefeuille électronique.
- Tel ou tel tiers (*verifier*) peut demander à consulter cette e-ID ou certains de ses éléments et vérifier leur authenticité après en avoir contrôlé la transmission autorisée par l'utilisateur.

5.1.3 Éléments exploités par l'État

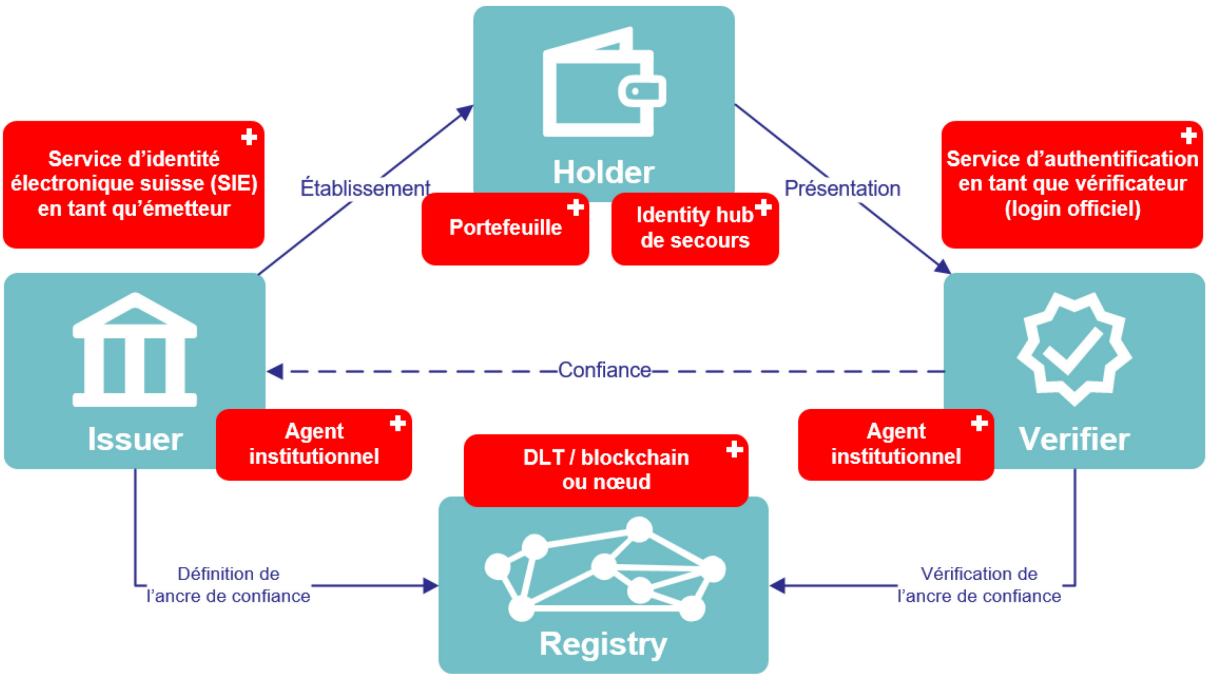


Illustration 3: vue d'ensemble des éléments exploités ou fournis par l'État (en rouge) dans une architecture SSI

L'illustration 3 présente en rouge les éléments techniques individuels ci-après, qui devraient, comme l'exigent les motions, être exploités sous la responsabilité de l'État ou fournis par lui en tant que logiciels libres d'accès:

- **Service d'identité électronique suisse (SIE):** processus numérique entièrement automatisé de validation, de décision et de vérification concernant une personne. Le résultat de ce processus (avec l'aide d'un agent institutionnel) est l'établissement et la transmission de données vérifiées, qui constituent l'e-ID.
- **Agent institutionnel:** logiciel d'établissement et de vérification de données vérifiées, qui comprend une interface de programmation (API) pour couvrir toute l'étendue des fonctions.
- **Portefeuille électronique:** application de smartphone servant à gérer en toute sécurité les données vérifiées.
- **Registre:** mémoire de données contenant des ancres de confiance électroniques qui est utilisée par tous les participants de l'écosystème e-ID et généralement concrétisée sous forme de registre distribué (*distributed ledger technology*, DLT), par exemple à l'aide de la *blockchain*. Le registre contient des preuves cryptographiques, des identités et des clés publiques d'émetteurs, des définitions des justificatifs d'identité et un système d'identification, mais jamais de données personnelles ou matérielles.
- **Base de données "de secours" relative à l'identité:** éléments servant à simplifier la portabilité et la sauvegarde des justificatifs d'identité personnels. Une base de données relative à l'identité (*identity hub*) n'est pas nécessaire pour le fonctionnement de base de l'e-ID, mais est recommandée pour en assurer la convivialité et la satisfaction des utilisateurs sur la durée dans un écosystème où les justificatifs d'identité sont nombreux.

- **Service d'authentification:** service de login pour les plates-formes étatiques et éventuellement aussi privées. Le justificatif d'identité est utilisé à cet effet comme facteur d'authentification (multiple).

Les motions citées au ch. 2.2 exigent que la solution d'e-ID soit gérée sous la responsabilité d'une autorité étatique. Le cas d'application minimal devrait par conséquent être réalisable en utilisant des éléments produits ou gérés exclusivement par l'État. L'ouverture technique qui sous-tend l'écosystème permettrait toutefois aussi à des prestataires privés de fournir certains éléments – surtout l'agent institutionnel, le portefeuille électronique et la base de données relative à l'identité. Quant au registre, l'État a la possibilité de fournir une partie du système (nœud ou *node*) ou la totalité, par exemple en sollicitant les cantons.

Les éléments que sont le SIE, le fournisseur d'identité et la base de données relative à l'identité sont des systèmes externes à la SSI que l'écosystème SSI utilise pour établir et transmettre les e-ID et en vérifier l'authenticité.

Des normes sont en voie d'élaboration pour régir ces interactions. Les différents éléments peuvent ainsi être mis au point indépendamment les uns des autres et pour le compte de l'État. L'interdépendance technique des différents éléments est limitée à la définition des normes.

5.1.4 Avantages et inconvénients de l'approche SSI

Avantages:

- L'esprit de la SSI repose sur la protection et la minimisation des données et le respect de la vie privée dès la conception (*privacy by design*). Il respecte les exigences des motionnaires.
- Cette approche générale permet d'envisager beaucoup de possibilités d'application et de scénarios d'utilisation, tout en restant très près de la réalité d'un portefeuille physique.
- Elle offre à l'utilisateur une vue d'ensemble de toutes les transactions reçues et envoyées.
- Elle s'inscrit dans le droit fil de l'évolution internationale; de nombreux projets et initiatives adoptent la même approche.
- Des interfaces libres et normalisées permettent de relier des systèmes tiers.
- Cette approche crée un canal de communication direct et crypté entre pairs, qui permet de transmettre des justificatifs d'identité, mais aussi d'autres messages.
- Les technologies de base sont disponibles sous forme de logiciels libres.

Inconvénients:

- Cette approche est relativement récente, certaines questions fondamentales ne sont pas encore résolues de manière concluante et les normes sont encore incomplètes.
- L'opinion publique doit d'abord être sensibilisée au potentiel de cette approche globale, qui diffère d'un login.
- La responsabilité de la gestion des données vérifiées est pleinement confiée à l'utilisateur, ce qui rend toute aide de l'émetteur quasiment impossible.

- Les possibilités d'évaluation forensique sont réduites, car le système bénéficie d'une bonne protection décentralisée et cryptographique. En cas d'utilisation abusive de l'e-ID ou d'autres preuves, il peut donc être difficile de prouver qu'on "n'était pas" la personne en question.
- Les portefeuilles hautement sécurisés pour les applications spéciales devraient reposer sur les éléments de sécurité des smartphones. Tous les smartphones n'en sont pas encore équipés et les outils de développement nécessaires ne sont pas encore complets et faciles à se procurer.

5.1.5 Inclusion de plates-formes cantonales de cyberadministration existantes

Les plates-formes cantonales de cyberadministration permettraient d'une part d'intégrer des preuves de l'identité par l'e-ID en tant qu'étape d'un processus, comme lors d'un paiement, et d'autre part d'utiliser le service d'authentification étatique.

Un canton pourrait en outre exploiter l'écosystème pour remplir lui-même la fonction d'émetteur et établir ses propres preuves, comme une attestation de domicile ou un permis de circulation. Une commune pourrait faire de même.

Dans un écosystème de niveau d'ambition 3 où des acteurs de l'économie privée sont aussi émetteurs, les plates-formes cantonales de cyberadministration pourraient encore envisager de nombreuses simplifications supplémentaires: si les employeurs émettent les certificats de salaire et les banques les certificats d'intérêts sous forme de justificatifs d'identité, ceux-ci pourraient être transmis directement lors de la déclaration d'impôts en ligne, ce qui simplifierait les processus ultérieurs.

5.1.6 Questions ouvertes sur l'approche SSI

À ce jour, l'identité souveraine est quasi unanimement acceptée par la communauté SSI lors de ses discussions internes, qui portent avant tout sur les questions de gouvernance et les processus externes à la SSI:

- Quels niveaux de gouvernance existe-t-il et qui est compétent en la matière – par exemple niveaux de gouvernance selon un cadre de confiance sur Internet (*trust over IP framework*): écosystème, justificatifs d'identité, fournisseur, utilité?
- L'État doit-il avoir le monopole sur certains éléments? Doit-il certifier les portefeuilles électroniques? Le choix du portefeuille et de l'agent institutionnel est-il laissé à l'utilisateur? Une réglementation distingue-t-elle les parties qui doivent être conçues et exploitées de manière coopérative ou plutôt concurrentielle?
- Qui exploite le registre? Un registre national propre est-il nécessaire ou peut-on rejoindre un écosystème international existant? Les cantons, les villes ou les entreprises privées veulent-ils ou devraient-ils exploiter des nœuds de stockage (*nodes*)? Quelle technologie faudrait-il préconiser? Quel rôle joue la quantité de données? Comment résout-on les questions d'interopérabilité avec les autres registres? L'émetteur est-il même libre de choisir un registre?
- Qui peut être émetteur? Le système reste-t-il complètement ouvert à l'ajout de cas d'application supplémentaires ou les émetteurs sont-ils sélectionnés ou autorisés spécifiquement?

- Comment rendre possibles les sauvegardes et les transferts de justificatifs d'identité? Comment éviter les sauvegardes centrales et donc les cibles privilégiées des pirates? Quel rôle joue la possibilité d'une liaison cryptographique entre le portefeuille électronique et les données vérifiées?
- Quels mécanismes de sécurité faut-il pour accéder au portefeuille électronique?
- Comment utiliser les données vérifiées sur plusieurs appareils? Quand serait-ce nécessaire? Suffit-il de toujours établir une liaison avec le vérificateur sur un smartphone, même si l'on vient de lancer le processus demandant l'e-ID sur un autre appareil?
- Qui définit le système d'identification? Faut-il qu'une instance reconnue se charge de la définition et de la coordination (par ex. eCH) ou les définitions sont-elles développées en fonction de la branche concernée?
- Un service d'authentification étatique est-il vraiment nécessaire? Serait-il pertinent de réunir le processus d'établissement et la sauvegarde des facteurs d'authentification pour tirer profit du processus d'identification complexe lors de l'établissement et pour assurer un haut degré de sécurité lors du processus d'authentification?

5.2 Solution d'e-ID basée sur l'infrastructure à clé publique

5.2.1 Approche

L'État utilise déjà aujourd'hui une infrastructure à clé publique (*public key infrastructure*, PKI) afin de sécuriser et de valider les données de documents d'identité (passeports, livrets pour étrangers) munis d'une puce. À cet effet, la Confédération signe numériquement les données en qualité d'émetteur avant de les enregistrer sur la puce, puis, en rendant accessible la clé publique, elle permet à tous les vérificateurs de les valider. Normalisée depuis plus de trente ans, cette technique est utilisée dans le monde entier pour les technologies les plus variées. L'application la plus récente de cette solution est le certificat COVID.

L'approche PKI est très similaire à celle de la SSI. Une e-ID établie sous forme de certificat (X.509) est une identité décentralisée entièrement maîtrisée par l'utilisateur – et donc aussi placée sous son entière responsabilité. La sphère privée de l'utilisateur, lorsqu'il se sert de son e-ID, est protégée de l'émetteur, car ce dernier n'a pas connaissance de l'utilisation. Il est toutefois bien plus difficile de minimiser ici les données étant donné que l'e-ID est par principe signée dans son intégralité et ne peut donc aussi être transmise que dans son intégralité au vérificateur pour confirmer l'identité.

Cette approche couvre les objectifs d'une preuve numérique en application analogique et numérique. L'application en ligne de ce type de certificats est normalisée (authentification TLS mutuelle). Différentes procédures basées sur le code QR se sont imposées pour l'application dans un monde analogique (par ex. le SwissPass dans l'application des CFF, le certificat COVID), bien que l'application hors ligne ne soit pas encore normalisée.

L'approche générale de l'établissement de certificats permet de concrétiser tous les niveaux d'ambition. Il est possible d'établir une relation logique ou mathématique entre des preuves. S'il est aussi techniquement possible d'inclure des émetteurs issus de l'économie privée, l'approche PKI n'est utilisée en règle générale qu'avec les émetteurs d'un groupe contrôlé ou contrôlable.

5.2.2 Description des fonctions

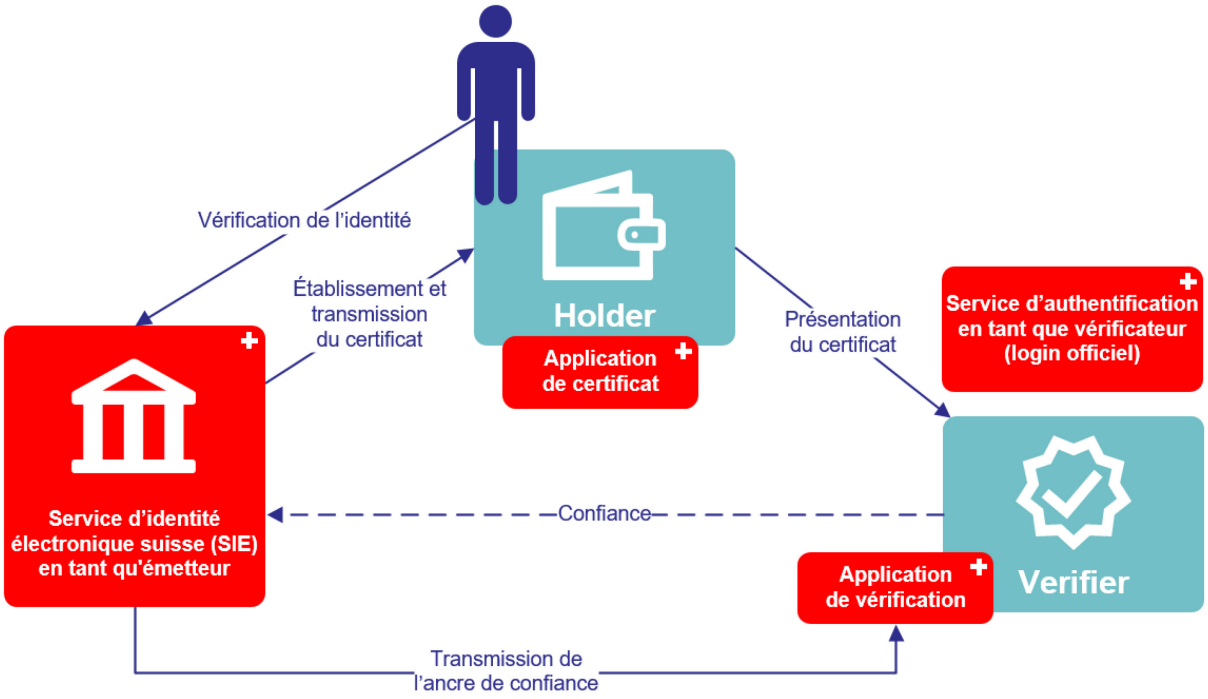


Illustration 4: architecture d'une solution PKI

Le triangle de confiance reliant **émetteur** (*issuer*), **utilisateur** (*holder*) et **vérificateur** (*verifier* ou *relying party*) est aussi présent ici. Les flux de communication se déroulent comme illustré, mais par rapport à l'approche SSI, différents canaux de communication sont possibles.

L'émetteur établit le certificat après avoir vérifié l'identité et le transmet à l'utilisateur. Celui-ci l'enregistre dans une application ad hoc destinée à le protéger contre la copie. Au besoin, l'utilisateur peut présenter le certificat à un vérificateur via un canal numérique ou, visuellement, via un code à barres, divulguant ainsi toutes les données signées. Après avoir reçu le certificat, le vérificateur peut en vérifier la validité à l'aide d'une application ad hoc. Cette application fournit directement la clé publique de l'émetteur et permet ainsi de procéder aussi à la vérification dans un lieu dépourvu de connexion Internet.

Pour invalider les certificats émis, l'émetteur tient une liste de révocation contenant tous les certificats retirés. Il existe à cet effet différents protocoles et procédures censés renforcer la protection des données lors de la consultation de la liste de révocation, afin que le vérificateur n'indique pas trop souvent à l'émetteur quand il procède à une vérification. La liste de révocation peut être consultée en ligne en temps réel, de manière périodique ou même de manière décentralisée et individuelle.

5.2.3 Éléments exploités par l'État

L'illustration 4 indique en rouge les éléments techniques individuels ci-après qui devraient être exploités sous la responsabilité de l'État ou fournis sous forme de logiciels libres, conformément aux exigences formulées dans les motions:

- **SIE:** système destiné au processus numérique entièrement automatisé de validation, de décision et de vérification concernant une personne. Le résultat de ce processus

est l'établissement et la transmission du certificat, qui constitue l'identité électronique. Ce système gère en outre la liste de révocation en vue de sa consultation.

- **Application de certificat:** application destinée à recevoir, sauvegarder et présenter les certificats.
- **Application de vérification:** application destinée à recevoir, afficher et vérifier les certificats.
- **Service d'authentification:** service de login pour les plates-formes étatiques et éventuellement aussi privées. L'e-ID est utilisée ici comme facteur d'authentification (multiple).

5.2.4 Avantages et inconvénients de l'approche PKI

Avantages:

- Cette approche fait appel à des techniques et des technologies éprouvées de longue date et largement diffusées.
- Elle permet de répondre aux caractéristiques et aux exigences les plus variées.
- Les identités et leur utilisation sont décentralisées. L'utilisation ne génère pas de données secondaires supplémentaires. L'exigence de respect de la vie privée par le design est remplie lors de la mise en œuvre.
- Cette approche respecte le principe selon lequel l'e-ID est un document d'identité, pas seulement un login.

Inconvénients:

- La conservation des identités est entièrement du ressort de l'utilisateur et la fiabilité accrue de la conservation et du fonctionnement requièrent presque toujours du matériel informatique supplémentaire (par ex. pour la protection contre la copie ou une authentification multifactorielle forte).
- Les certificats ne peuvent par principe être présentés que dans leur intégralité. Des certificats partiels seraient envisageables pour minimiser les données, mais l'utilisateur devrait alors demander et gérer plusieurs certificats d'e-ID; il serait donc contraignant de sélectionner certains attributs selon la situation.
- Les différents canaux de transmission possibles entre l'émetteur, l'utilisateur et le vérificateur compliquent *l'utilisation sûre et correcte* des certificats.

5.2.5 Inclusion de plates-formes cantonales de cyberadministration existantes

Les plates-formes cantonales de cyberadministration permettraient d'une part d'intégrer des preuves de l'identité par l'e-ID en tant qu'étape d'un processus, comme lors d'un paiement, et d'autre part d'utiliser le service d'authentification de l'État.

Un canton pourrait en outre exploiter l'écosystème pour remplir lui-même la fonction d'émetteur et établir ses propres certificats, comme une attestation de domicile ou un permis de circulation. Une commune pourrait faire de même.

5.2.6 Solutions de PKI basées sur des cartes

Alternativement à l'approche PKI, il serait aussi possible d'utiliser une carte à puce pour sécuriser la sauvegarde du certificat au lieu de l'application de certificat sur un smartphone. Un lecteur de cartes est nécessaire pour présenter le certificat – dans le monde analogique, c'est le vérificateur qui doit en être équipé, alors que pour une utilisation en ligne, c'est l'utilisateur. De nombreux modèles actuels de smartphones sont capables de lire les cartes à puce, faute de quoi un lecteur de carte spécial est nécessaire.

SuisseID et la nouvelle carte d'identité électronique allemande (*neuer Personalausweis*, nPA) reposent toutes deux sur ce principe et offrent notamment une identification numérique. Ces deux applications n'ont pas connu un succès retentissant, même si l'utilisation de cartes en soi n'était qu'un obstacle parmi d'autres. Au niveau international, les systèmes d'e-ID utilisant des cartes à puce sont actuellement en perte de vitesse. Les systèmes prometteurs misent sur l'utilisation d'appareils mobiles et de smartphones avec des applications spéciales, qui assure avant tout une meilleure acceptation grâce à une grande convivialité. À titre d'exemple, l'Estonie, pionnière de la cyberadministration, a initialement lancé une carte à puce, puis introduit une identité mobile liée à des cartes SIM et offre aujourd'hui en premier lieu une application entièrement dématérialisée (Smart-ID). L'Allemagne est aussi à la recherche d'une solution pour conserver les données du nPA sur un smartphone, afin que la carte physique ne soit plus nécessaire. La Suisse devrait bénéficier de ces expériences.

D'autres raisons que celles précitées s'opposent à une mise en œuvre au moyen d'une carte d'identité officielle munie d'une puce, comme celle du nPA:

- S'il est certes prévu d'introduire une nouvelle carte d'identité dans les années à venir, la fonctionnalité d'e-ID n'était pas incluse dans l'appel d'offres public réalisé et devrait être ajoutée par la suite. Ce dernier aspect vaut aussi pour tous les livrets pour étrangers et les cartes diplomatiques.
- Il faut au moins dix ans pour lancer un document d'identité physique en Suisse en raison de la durée de validité (ainsi que du délai). Il n'est pas efficace de rendre l'adoption d'une e-ID dépendante du cycle de renouvellement de la carte d'identité.
- L'utilisation d'un support physique de transmission des données personnelles restreint le choix et la possibilité de concevoir une solution d'e-ID prometteuse.

5.2.7 Questions ouvertes sur l'approche PKI

- Des certificats spécifiques à des applications sont-ils nécessaires pour l'e-ID? Leur nombre peut-il être limité?
- Quels avantages un répertoire de clés publiques (*public key directory*), soit une instance administrative gérant les clés publiques et les listes de révocation, apporterait-il? Comment les différences par rapport à l'approche SSI devraient-elles être pondérées?
- Un service d'authentification étatique est-il vraiment nécessaire? Serait-il pertinent de réunir le processus d'établissement et la sauvegarde des facteurs d'authentification pour tirer profit du processus d'identification complexe lors de l'établissement et pour assurer un haut degré de sécurité lors du processus d'authentification?

5.3 Solution d'e-ID basée sur un fournisseur d'identité central étatique

5.3.1 Approche

La LSIE prévoyait une solution incluant des fournisseurs d'identité reconnus tant publics que privés. L'idée sous-jacente était de doter au plus vite d'une e-ID une base d'utilisateurs aussi large que possible et de fournir en même temps des possibilités d'application. L'inclusion des particuliers a toutefois été l'un des motifs du rejet de la loi en votation populaire.

L'idée initiale consistant à fournir aux utilisateurs une identité électronique vérifiée par l'État sur la base d'un login peut aussi être réalisée avec un fournisseur d'identité central étatique. Cette solution simplifiée résoudrait certaines questions d'interopérabilité et de flux de données, en comparaison avec l'architecture prévue par la LSIE rejetée, mais il serait difficile de la généraliser rapidement. C'est la Confédération qui a la responsabilité de gérer le système. Cette solution permet avant tout d'avoir un login uniforme officiel pour la cyberadministration.

Les bases et les protocoles technologiques (par ex. OpenID Connect) de cette approche sont établis et adaptés au niveau d'ambition 1. Pour couvrir des niveaux d'ambition plus élevés, des extensions sont nécessaires; elles sont actuellement en cours d'élaboration.

5.3.2 Description des fonctions

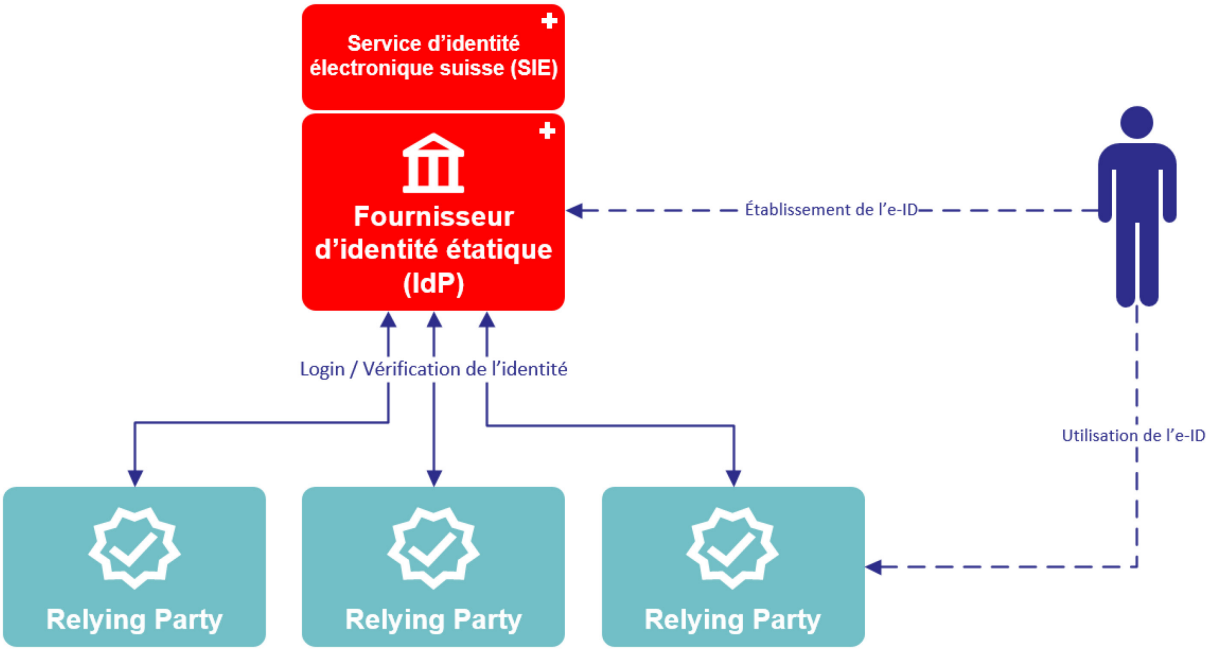


Illustration 5: vue d'ensemble de l'architecture d'une solution d'e-ID basée sur un fournisseur d'identité central étatique

Au centre de cette approche se trouve un fournisseur d'identité étatique gérant l'e-ID de l'utilisateur, qui peut être utilisée lors d'un processus de login. Toute partie utilisatrice, par exemple une plate-forme cantonale de cyberadministration, peut se connecter au fournisseur d'identité étatique, de deux manières:

- La partie utilisatrice se sert du service de fournisseur d'identité pour gérer activement les identités, de sorte que l'utilisateur se connecte à son compte par l'intermédiaire d'un fournisseur d'identité étatique.
- La partie utilisatrice ne recourt au service de fournisseur d'identité que comme un *service d'identification*: l'utilisateur peut divulguer à la partie utilisatrice certains attributs de l'e-ID à une certaine étape du processus sans que le fournisseur d'identité étatique se charge de la gestion des identités.

L'utilisateur déclenche l'établissement d'une e-ID directement auprès du fournisseur d'identité étatique. Ce dernier utilise le SIE pour effectuer la vérification complète (cf. ch. 5.4).

Les parties utilisatrices pourraient en principe fournir des preuves liées sur la base d'une e-ID connectée (niveau d'ambition 2). Une approche technologique indépendante du fournisseur d'identité serait possible, semblable par exemple à l'approche PKI (cf. ch. 5.2).

5.3.3 Éléments exploités par l'État

La portée réduite d'un écosystème avec un fournisseur d'identité central a une incidence sur la mise en œuvre. L'illustration 5 indique en rouge les éléments techniques individuels ci-après qui devraient être exploités sous la responsabilité de l'État ou fournis sous forme de logiciels libres, conformément aux exigences formulées dans les motions:

- **SIE:** système destiné au processus numérique entièrement automatisé de validation, de décision et de vérification concernant une personne. Au terme de ce processus, la confirmation de la vérification est transmise au fournisseur d'identité en vue de la création de l'e-ID.
- **Fournisseur d'identité:** fournisseur d'identité étatique qui gère l'e-ID et la rend utilisable pour les parties utilisatrices publiques et éventuellement aussi privées grâce à un processus de login.

5.3.4 Avantages et inconvénients de l'approche du fournisseur d'identité

Avantages:

- Cette approche présente une architecture simple et fournit une solution claire.
- Elle fait appel à des technologies et des protocoles largement utilisés.
- Le fait d'associer la vérification de personnes et le login par e-ID rend le login sûr.

Inconvénients:

- Cette solution n'est pas conforme aux principes exigés dans les motions. Elle n'est pas décentralisée et le respect de la vie privée par le design n'est pas garanti, étant donné que l'approche repose sur une confiance totale vis-à-vis du fournisseur d'identité. Les inquiétudes relatives à la minimisation des données et aux données secondaires seraient quelque peu atténuées du fait que la Confédération assume la responsabilité globale du système et peut ainsi exercer un contrôle précis.
- Le paradoxe de l'œuf et de la poule n'est pas résolu: les chances que les utilisateurs adoptent rapidement cette solution et que l'on puisse connecter rapidement et librement de nombreux services sont assez minces selon les expériences réalisées à l'étranger.

- Le scénario d'utilisation est limité et l'utilisation est plutôt difficile dans le monde analogique.
- L'écosystème ne peut que difficilement être étendu à des niveaux d'ambition plus élevés.
- L'établissement de l'e-ID et son utilisation ne sont pas séparés, ce qui est contraire à l'usage actuel des documents d'identité et ne correspond donc pas à ce qui se fait dans le monde analogique.
- Il n'est possible de relier l'e-ID et d'autres preuves que par l'intermédiaire de services associés, ce qui complique l'utilisation de ces preuves.
- Cette solution ne suit pas le principe selon lequel l'e-ID est un document d'identité numérique.
- Le système est dépendant d'un fournisseur d'identité.

5.3.5 Inclusion de plates-formes cantonales de cyberadministration existantes

Le fournisseur d'identité central est relié aux plates-formes cantonales de cyberadministration existantes. La gestion des accès et des rôles demeure auprès de la plate-forme concernée, mais l'identité viendrait du fournisseur d'identité fédéral, qui garantit un processus de login sûr. Cette caractéristique pourrait soulager les cantons qui n'ont pas encore leur propre solution de login et décharger les cantons qui disposent de leur propre fournisseur d'identité. Ces derniers pourraient aussi relier le fournisseur d'identité fédéral à leur plate-forme de cyberadministration. Concrètement, cela signifie que l'on relie une identité existant auprès de son propre fournisseur d'identité à celle transmise par le fournisseur de la Confédération, sans qu'il y ait donc d'exploitation parallèle. Notons à cet égard qu'une architecture comprenant plusieurs fournisseurs d'identité est précisément difficile à mettre en œuvre pour les applications mobiles (jetons d'actualisation, etc.). En cas d'utilisation d'un fournisseur d'identité fédéral pour une plate-forme cantonale, la question de l'assistance devrait aussi bénéficier d'une attention appropriée pour que les utilisateurs aient un point de contact précis en cas de problème.

Il serait en principe possible de fédérer les fournisseurs d'identité cantonaux existants. Une telle fédération permettrait une sorte de décentralisation (régionalisation) en raison de la répartition entre différents systèmes. Comparés à une solution centralisée, les systèmes fédératifs requièrent toutefois plus de moyens, de réglementation et de mécanismes de contrôle (normes, niveau de confiance de l'identité, protection des données, etc.). En outre, des normes devraient toujours être fixées avant de développer des fonctions supplémentaires, comme l'établissement de certificats d'âge, et chaque fournisseur d'identité serait ensuite obligé de les mettre aussi en œuvre. C'est seulement ainsi que tous les utilisateurs pourraient bénéficier des mêmes fonctions de l'e-ID, indépendamment du fournisseur d'identité cantonal. Même en utilisant à plusieurs reprises certains fournisseurs d'identité cantonaux, on estime que les moyens que doit fournir l'État sont considérablement plus élevés qu'avec un fournisseur d'identité central étatique relié à des plates-formes cantonales.

5.3.6 Questions ouvertes sur l'approche du fournisseur d'identité

- Qui est autorisé à utiliser le fournisseur d'identité central étatique comme fournisseur de login et pour confirmer certains attributs? Les plates-formes officielles sont-elles les seules à pouvoir s'y relier ou les systèmes privés le peuvent-ils aussi?
- Quelles plates-formes de cyberadministration seraient liées à un fournisseur d'identité étatique? Combien de cantons auront encore besoin d'une solution de fournisseur d'identité au moment de la mise en œuvre?
- Est-il vraiment pertinent de transférer le login aux cantons et autres parties utilisatrices?
- Qui est le partenaire contractuel vis-à-vis des parties utilisatrices et possède la compétence d'élaborer les contrats? Quelles conditions les parties utilisatrices devraient-elles remplir? Comment le contrôle est-il assuré?

5.4 Processus d'établissement de l'e-ID

Le processus d'établissement d'une e-ID est indépendant de l'approche retenue. Les étapes suivantes sont toutefois nécessaires:

- La personne qui fait la demande présente une pièce d'identité valable.
- La pièce d'identité est comparée avec cette personne.
- L'e-ID est remise à cette personne par l'État.

Un processus en ligne entièrement automatisé, comme il en existe en Italie, est l'objectif à atteindre pour une diffusion simple et rapide, ce qui n'exclut pas que des guichets physiques apportent une assistance. L'État exploite le système nécessaire et transmet la preuve numérique à la personne qui a fait la demande par un canal sécurisé.

Le principe visant à minimiser les données et à permettre les attributs dérivés permet de reconsidérer le contenu d'une e-ID. Ainsi, il n'est pas nécessaire de renoncer préventivement à des attributs par souci de protection des données, la transmission de chacun des attributs étant contrôlée par l'utilisateur. L'e-ID contiendrait les données qui se trouvent aussi sur un document d'identité physique: prénom, nom, date de naissance, photographie, lieu d'origine, lieu de naissance, nationalité, date d'établissement. Il serait envisageable d'ajouter le numéro AVS, qui est exigé pour de nombreuses démarches administratives et serait donc pratique pour l'utilisateur.

Pour assurer une grande interopérabilité au niveau international, il faut viser un niveau de garantie élevé lors de l'établissement des e-ID (identification et vérification). Le niveau de garantie d'une e-ID ne peut toutefois pas être examiné que sur le plan de l'établissement. Selon la mise en œuvre, différents niveaux de garantie sont possibles pour la sauvegarde et la présentation de la preuve ou pour l'utilisation du document d'identité numérique. Il n'est donc pas pertinent de limiter la discussion à un seul niveau de garantie – c'est la chaîne de confiance dans son intégralité qui doit être examinée pour chaque cas d'application, idéalement avec une solide ancre de confiance: l'e-ID.

Les détails relatifs à la mise en œuvre du processus d'établissement restent à élaborer et ne font donc pas partie du présent document de travail.

6 Planification de la mise en œuvre

6.1 Calendrier

Après que les différentes questions soulevées par le présent document de travail concernant le projet d'e-ID auront fait l'objet d'une discussion publique et d'une évaluation, le Conseil fédéral devrait prendre une décision de principe d'ici à la fin de 2021. Sur la base des exigences qui en découleront, un avant-projet de loi sur les services d'identification électronique sera élaboré, de façon que la procédure de consultation sur la loi puisse être ouverte au milieu de 2022. S'ensuivront l'élaboration du message, la délibération parlementaire, un éventuel référendum ainsi que l'édiction des dispositions d'exécution. La date d'introduction d'une e-ID officielle dépendra de ce processus.

Afin de gagner du temps, il est possible de démarrer la planification de la mise en œuvre et la mise en œuvre elle-même parallèlement au processus législatif. Les premières applications pilotes et la preuve de concept (*proof of concept*) pourraient déjà être réalisées lors de la planification afin de clarifier d'éventuelles questions dans la pratique. À la suite des premières discussions parlementaires indiquant la voie à suivre, des appels d'offres et des travaux de développement pourraient être lancés.

6.2 Évaluation des coûts des différentes solutions d'e-ID possibles

Comme pour le calendrier, de nombreuses inconnues pèsent sur l'évaluation des coûts. Une estimation précise n'est pas possible en raison des exigences encore complètement ouvertes. On peut partir du principe que la mise en œuvre de toutes les solutions possibles présentées ici se situe dans une fourchette similaire. C'est pourquoi aucune évaluation globale n'est avancée à ce stade. Les coûts peuvent être répartis en trois domaines:

1) coûts d'élaboration, d'exploitation et de développement des systèmes fonctionnels et techniques;
2) coûts servant à promouvoir l'utilité de l'e-ID et son emploi par les utilisateurs, les milieux économiques et l'État à l'aide de mesures de communication appropriées ainsi que de programmes pilotes et de soutien;
3) coûts destinés à garantir la compatibilité et, par là même, le développement de l'utilité (aux niveaux international et fédéral et selon les exigences des milieux économiques).

Il va de soi que les coûts sont plus élevés à mesure que le niveau d'ambition augmente, mais cette hausse est aussi directement liée à une plus grande attente quant à l'utilité.

6.3 Sources de financement

Si l'un des buts principaux est de créer une *plate-forme largement utilisée*, un financement subventionné par l'État serait à examiner: l'État prend en charge les coûts, qu'il considère comme une contribution de base à la numérisation de la Suisse. La population suisse attend de l'État qu'il lui fournisse comme prestation de base une identité numérique officielle.

Cette approche ne répond certes pas à l'exigence de fournir les prestations étatiques avec des émoluments couvrant les coûts, mais elle évite une charge bureaucratique dissuasive. Si le

financement subventionné par l'État est rejeté, des modèles tarifaires coûteux devraient être évités afin de ne pas entraver inutilement la diffusion.

L'expérience d'autres pays a montré que les utilisateurs ne sont pas prêts à payer pour une e-ID. Celle-ci et l'utilisation de l'infrastructure de confiance qui y est liée doivent être fournies gratuitement.

Quant à la question de savoir quels acteurs pourraient contribuer au financement, le vérificateur et la partie utilisatrice n'entrent pas en ligne de compte pour les systèmes décentralisés du fait des mesures de protection des données. Il reste les émetteurs, qui peuvent cofinancer une partie de l'infrastructure, par exemple dans l'approche SSI en réglant une taxe pour sauvegarder dans le registre leurs propres identités, système, définitions de données vérifiées ou de révocation (l'établissement effectif de données vérifiées serait gratuit, puisqu'il n'y a rien à écrire dans le registre). Avec une solution de fournisseur d'identité, les tarifs pourraient être fixés dans le cadre des contrats d'utilisation entre fournisseurs d'identité et parties utilisatrices.

7 Discussion publique sur le projet d'e-ID

Le présent document de travail concernant le projet d'e-ID est avant tout une base de discussion, même s'il présente trois solutions possibles. La Suisse doit prendre une décision de principe capitale, pour laquelle il faut récolter l'avis d'un public spécialisé. Quelle e-ID la Suisse veut-elle? Quel écosystème souhaitent les utilisateurs, les communes, les cantons et les milieux économiques? Quels cas d'application agitent les utilisateurs et les fournisseurs de services?

À titre indicatif, il faudrait que les prises de position rédigées sur ce projet d'e-ID abordent au moins les points suivants:

- Où voyez-vous une utilité particulière pour l'e-ID et quels cas d'application sont prioritaires pour vous?
- Quelles sont pour vous les trois exigences principales auxquelles doit répondre une e-ID officielle sous forme de document d'identité numérique?
- Quelle est pour vous l'utilité d'une infrastructure nationale qui permet à l'État et aux particuliers d'établir et de vérifier des preuves numériques (par ex. e-ID, permis de conduire numérique, badges d'accès, attestations de formation)?

Il va de soi que des commentaires supplémentaires peuvent être formulés sur tous les autres aspects de l'e-ID, tant dans les prises de position que dans la discussion. La discussion doit aussi permettre de poser des questions et de remettre en cause les approches. Cette discussion est l'occasion d'élargir le champ de vision et de réflexion. La Suisse doit-elle avoir le courage de miser sur une solution d'e-ID qui ait du potentiel sans connaître tous les détails? Ou une variante minimale utilisée uniquement par l'État suffit-elle? La discussion vise à fournir des éléments de réponse à ces questions.

La discussion publique a lieu au sein de différents organes de réflexion où sont représentés les milieux politiques, économiques et scientifiques, la société civile, les cantons et l'administration. Par ailleurs, une discussion publique sera organisée sous forme de conférence. Les résultats de ces différentes discussions ainsi que les exigences connues seront réunis et serviront de base à la décision de principe du Conseil fédéral. En fin de compte doit émerger un projet de loi susceptible d'obtenir la majorité politique, qui puisse être adopté par le Parlement et accepté par le peuple.