e-ID en SUISSE

CONSULTATION PUBLIQUE SUR LA LOI SUR l'e-ID, LeID

Réponse de SICPA

Octobre 2022

Présenté par:
SICPA SA
AV DE FLORISSANT 41,
1008 PRILLY
Suisse

SICPA

Enabling trust

TABLE DES MATIÈRES

1 LE CONTEXTE & OBJECTIFS DU DOCUMENT

Lors de sa séance du 29 juin 2022, le Conseil fédéral a envoyé en consultation un avant-projet de loi fédérale sur l'identité électronique et autres moyens de preuve électroniques (LeID).

L'objectif de ce document est d'apporter des propositions de modification de cet avant-projet et de poser quelques questions concernant la mise en œuvre de ce dernier afin d'éclairer les différents intervenants qui évaluent les impacts sur les systèmes d'identité digitale et les processus existants.

2 PROPOSITIONS DE MODIFICATION

L'avant-projet de loi sur l'e-ID (LeID) détaille bien les aspects applicatifs, les besoins d'interopérabilité avec nos voisins européens (Art19 et Art27) et la répartition des rôles et responsabilités de la Confédération, de la Fedpol et des Cantons (Art4 et Art8). Il est important qu'il reste neutre technologiquement parlant (Art25) afin de garantir les possibles évolutions en la matière. Par conséquent, de notre point de vue, cet avant-projet sous sa forme actuelle satisfait aux besoins législatifs qui permettraient une introduction harmonieuse de l'identité numérique dans notre pays.

Néanmoins, nous souhaitons soulever les points ci-dessous, qui méritent d'être approfondis.

2.1 ACCESSIBILITÉ POUR TOUS

Le premier point qui vient à l'esprit dans la définition même de l'e-ID est la question de l'accessibilité de ces outils pour chaque citoyen, quel que soit leur âge ou leur situation de handicap (inclusion sociétale). Les technologies mis en place devraient bénéficier à chacun et il semble important que les aspects d'ergonomie soient pris en compte par les fournisseurs de technologie et de service dès la conception. Par exemple, le 28 mai 2019, le gouvernement du Luxembourg a décidé d'inscrire dans la loi un tel principe[1].

L'OFJ pourrait garantir l'accessibilité pour tous en spécifiant ce principe dans le cadre de cette loi, ce qui obligerait les différents prestataires à se conformer aux normes existantes aujourd'hui en Suisse en la matière et à utiliser tous les outils mis à disposition par exemple par les fournisseurs de systèmes d'exploitation des téléphones portables pour faciliter la vie aux personnes en situation de handicap. Il est de plus également important de prendre en considération l'inclusion technologique, pour les personnes ne possédant pas de téléphone portable ou de Smartphone.

2.2 IDENTIFICATION (ART1)

L'Art. 1, Al2a stipule :
"Elle vise à garantir une identification sûre, à l'aide d'une e-ID, entre personnes privées et entre personnes privées et autorités ;"

En vue de satisfaire le niveau d'ambition 3, pourquoi ne pas inclure également les personnes morales ? En effet, l'e-ID sera un moyen très utile pour les entreprises pour identifier de manière sûre leurs clients ou leurs partenaires commerciaux par exemple.

PROPOSITION

a. *" Elle vise à garantir une identification sûre, à l'aide d'une e-ID, entre personnes privées et autorités et entre personnes privées ou morales ;"*

[1] https://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a373/jo

2.3 SYSTEME DE CONFIRMATION DES IDENTIFIANTS (ART18 AL1 ET AL2)

Selon l'article 18 Al1, « *dès le début, la Confédération se voit déléguer la compétence de confirmer l'identité des autorités fédérales, cantonales et communales qui agissent en tant qu'émetteurs et vérificateurs. Elle charge une entité au sein de l'administration fédérale de gérer et d'entretenir le système de confirmation d'identité. Cette entité maintient une liste d'autorités agissant en tant qu'émetteurs et vérificateurs qu'elle publie sur son site et la met régulièrement à jour* ».

En 2022, la Suisse compte 2'145[2] communes, plus de 570'000 sociétés et beaucoup de services et de registres cantonaux. Dans le cadre du fédéralisme, une décentralisation au niveau des cantons de la gestion des émetteurs et vérificateurs serait donc à étudier. En effet, une centralisation complète de cette fonction risque d'être très lourde à gérer par l'administration désignée alors qu'elle pourrait s'appuyer sur des systèmes existants comme les registres du commerce cantonaux ou des association faîtière par branche économique (banques, assurances, ...). Il serait bien également de clarifier quelles sont les conditions, notamment financières (Art26), pour faire partie de ce système de confirmation des identifiants (Art28 d).

PROPOSITION

Ajouter à l'Art 18. al 2. *"La Confédération pourra mettre en place un système de délégation de ces confirmations d'émetteurs et de vérificateurs auprès d'instances publiques et privées. Ces délégations seront sécurisées par un système de preuves électroniques associé".*

2.4 CODES SOURCE (ART23)

L'Art23 mentionne que la Confédération publiera le code source des composants de l'infrastructure de confiance qu'elle met à disposition. Sous sa forme actuelle, il semble rendre obligatoire la publication des codes source de tous les éléments, ce qui pourrait dans certains cas se révéler problématique au niveau de l'implémentation, de licences ou au niveau de la sécurité.

Dans le projet de loi fédérale sur l'utilisation des moyens électroniques pour l'exécution des tâches des autorités (LMETA)[3], l'article 9 Al.1 résout cette incertitude en formulant ce point de la manière suivante :
" *Dans la mesure où cela est possible et judicieux et pour autant que les droits des tiers soient préservés, les autorités fédérales soumises à la présente loi publient le code source des logiciels qu'elles développent ou font développer pour l'exécution de leurs tâches.*"

PROPOSITION

Afin de lever toute ambiguïté juridique quand à ce point et être aligné par rapport au projet de la LMETA, il est proposé par exemple de compléter l'Article 23 de la manière suivante (reprenant les termes de l'Art 9.1 de la LMETA) :
"*La Confédération publie le code source des éléments de l'infrastructure de confiance qu'elle met à disposition, dans la mesure où cela est possible et judicieux et pour autant que les droits des tiers soient préservés.*"

[2] https://www.agvchapp.bfs.admin.ch/fr/state/results?SnapshotDate=01.05.2022
[3] https://www.newsd.admin.ch/newsd/message/attachments/70501.pdf

3 QUESTIONS

En complément des points soulevés au chapitre 2 de ce document, SICPA a identifié quelques questions liées au côtés pratiques de l'implémentation de l'identité numérique. Ces questions trouveront certainement des réponses dans des ordonnance spécifiques à ces aspects plus techniques. Cependant, elles peuvent également conditionner certains articles de l'avant-projet de loi LeID. Vous trouverez donc ci-dessous une liste de ces questions :

3.1 PHOTOGRAPHIE (ART2 ET ART4 AL4)

Est-ce que la photographie est considérée comme « donnée personnelle » selon l'art5.a de la loi sur la protection des données (LPD)[4] au même titre que le nom et le prénom, ou est-ce qu'elle doit être considérée comme donnée biométrique et donc sensible selon l'art5.c.4 de la LPD ? En effet, si elle est considérée comme donnée biométrique ce qui nécessiterait un traitement particulier en termes de cryptographie et de sécurité. En effet, selon l'art5.c.4 de la LPD, une donnée biométrique permet d'identifier une personne physique de manière univoque et la photo pourrait être considérée comme tel. Pour rappel, la photographie est exposée sur la page de personnalisation du passeport et de la carte d'identité au même titre que le nom ou le prénom et à contrario des données biométriques qui ne sont accessibles que par l'autorité émettrice dans le passeport. Ceci est important dans la mesure où la photographie d'identité faisant partie des attributs de l'e-ID ne nécessiterait pas de traitement cryptographique particulier et serait ainsi au même niveau de protection que le nom, le prénom ou la date de naissance.

Comme une photographie d'identité peut être échangée comme attribut et visible pour permettre une identification lors d'un contrôle en présentiel, au même titre que le nom et le prénom, il semble que cet attribut de l'e-ID ne doit pas être considéré comme élément sensible au même titre que des données biométriques. Également, si compromise, une photographie d'identité peut être facilement remplacée par une autre photographie du détenteur, alors que les données biométriques sont en principe et par définition invariants. Il serait judicieux de clarifier cette ambiguïté à l'art2 de la LeID.

3.2 REVOCATION EN CAS DE DECES (ART5)

L'article 5 définit que Fedpol est responsable de révoquer l'e-ID s'il prend connaissance du décès de son titulaire. Il serait judicieux de pouvoir clarifier le processus de transmission de la notification de décès de bout en bout (p.ex via le numero AVS).

3.3 EQUIVALENCE PHYSIQUE-NUMÉRIQUE (ART9)

Cet avant-projet établi une équivalence légale d'une identité électronique fourni par l'état et d'un document d'identité reconnu comme la carte d'identité ou le passeport (Art9) ce qui couvrirait le niveau d'ambition 1. Ceci permettrait par exemple à la FINMA d'adapter les règlements relatifs à la connaissance des titulaires de comptes bancaires en Suisse et de simplifier les processus et l'expérience utilisateur dans le domaine bancaire. Cependant, cet avant-projet ne couvre que l'équivalence du document d'identité et pas tous les autres certificats émis par les autorités fédérales, cantonales ou communales pour couvrir le niveau d'ambition 2. Ceci risque de ralentir considérablement l'adoption de l'identité électronique car cela nécessiterait probablement une modification de loi pour chaque

[4] https://www.fedlex.admin.ch/eli/fga/2020/1998/fr

document. Selon l'art9, « *toute autorité ou tout service qui accomplit des tâches publiques doit accepter l'e-ID lorsqu'il recourt à l'identification électronique* ». De même, il faudrait que tous certificats électroniques émis par les autorités fédérales, cantonales ou communales ait valeur légale et doive également être accepté en tant que tel.

Au Luxembourg par exemple, le seul document qui bénéficie d'une équivalence légale physique-numérique est le certificat de résidence[5]. Seul ce document peut être reconnu et utilisé par les banques sous sa forme numérique ce qui limite la transition vers une digitalisation de la société. Le règlement européen eIDAS est en train d'être adapté pour palier à ce problème en fournissant un cadre de confiance et une validité légale de l'identité numérique permettant l'équivalence de tous les certificats émis par les états membres à l'intérieur et au-delà des frontières[6]. Ce nouveau règlement éviterait ainsi à tous les états membres de devoir adapter leur législation pour couvrir l'équivalence de tous les certificats émis par l'état. La Suisse ne faisant pas partie de l'union européenne, ce nouveau règlement ne bénéficiera pas au cadre législatif Suisse. Les objectifs de la LMETA semblent couvrir une partie de ces besoins et il serait judicieux que cette loi puisse être une base légale pour adapter les règlements fédéraux et cantonaux rapidement après l'introduction de la LeID.

Par ailleurs, l'art1 al2.d fait mention de normalisation de l'e-ID. De même, il serait nécessaire que toutes les attestations émises par l'état comme par exemple les attestations de domicile émises par les communes, les certificats de naissance ou les permis de conduire soient normalisés. Il serait judicieux que la définition de ces attestations soit réglementée par un organisme au niveau fédéral afin de garantir une interopérabilité et une équivalence intercantonale et intercommunale.

3.4 UNICITE DE L'EID (ART5 E)

L'Article 5e semble indiquer qu'une personne ne peut avoir qu'une seule e-ID. S'il est évident qu'une personne n'a qu'une seule identité, on constate dans le monde physique que cette personne peut posséder plusieurs déclinaisons de son identité, comme son passeport et sa carte d'identité. De même, il arrive fréquemment qu'une personne possède également plusieurs téléphones portables. Est-ce que chaque appareil pourrait avoir un portefeuille/wallet qui contiendrait une version (ou instance) de l'e-ID ?

Une question qui concerne l'implémentation technique de manière importante est de savoir à quoi sera lié le credential eID émis (au téléphone portable (eg IMEI number), autres …) ?

3.5 MANDAT (ART 15 AL1)

Une question liée au point précédent est la question du mandat (Art4 Al2 et Art15). En effet, dans plusieurs cas de figure une personne physique peut être appelé à agir au nom d'une autre personne physique ou morale et aurait besoin soit de détenir une attestation électronique appartenant à cette autre personne dans son portefeuille ou tout du moins d'avoir accès à son portefeuille. Il s'agit notamment des cas de parents et de leurs enfants (<14 ou même <18), de représentants légaux en cas de deuil ou d'incapacité de tout type ou représentant d'une personne morale. Il s'agit de clarifier du point de vue de la loi le principe et si possible les processus qui pourraient régir de tels cas de figure afin que les fournisseurs technologiques puissent répondre de manière adéquate à cette problématique. Notamment, est-il envisageable pour le représentant légal (p.ex des parents) d'avoir l'eID dans leur

[5] https://legilux.public.lu/eli/etat/leg/rgd/2016/03/29/n2/jo
[6] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

portefeuille ? Si oui, dans le cas des parents par exemple, est-ce que cette eID peut être stockée chez deux personnes différentes (p. ex père et mère) ? Où est-ce que l'enfant doit avoir son propre téléphone et son propre portefeuille, ce qui pose le problème de l'accès au portefeuille) (Art14)?

3.6 IDENTITÉ D'ORGANISATIONS (ART15 AL2)

En même temps que l'e-ID pour les citoyens, une identité pour organisations (personnes morales) serait à envisager. En effet, la commission européenne travaille sur ce sujet car les deux concepts d'identité sont liés notamment dans le cas de mandat où une personne physique (référent d'une entreprise) représente une personne morale pour des transactions légales ou financières par exemple. La Suisse a tout intérêt à mettre en place une identité pour organisation en parallèle d'un e-ID pour citoyens qui soit compatible avec les schémas mis en place par la commission européenne. Il s'agit notamment de clarifier les conditions d'utilisation de l'e-ID dans le cadre d'un mandat et de clarifier le rôle décentralisé des registres du commerce cantonaux dans ce processus.

3.7 IDENTIFICATION DES EMETTEURS ET DES VERIFICATEURS (ART17 AL3)

Selon l'article 17 Al3, « la vérification de l'identité des émetteurs ou des vérificateurs n'est pas nécessaire avant qu'ils ne puissent utiliser le registre de base. Cela impliquerait une procédure d'autorisation nécessitant des ressources importantes, ce qui conduirait inévitablement à un goulot d'étranglement coûteux et inutile. Certes, il existe un risque que des émetteurs ou des vérificateurs puissent délivrer des preuves électroniques en usurpant leur identité. Ce risque est toutefois atténué par la publication d'informations sur les cas de soupçons fondés d'utilisation abusive de l'infrastructure de confiance, conformément à l'art. 22, et exclu par le système de confirmation des identifiants prévu à l'art. 18. L'exclusion d'émetteurs ou de vérificateurs enregistrés n'est techniquement pas possible dans le registre de base, mais elle l'est dans le système de confirmation des identifiants selon l'art. 18 ».
D'autre part, l'article 7 Al1 décrit le devoir de diligence d'un titulaire d'une e-ID. « Il doit prendre les mesures nécessaires et raisonnablement exigibles au vu des circonstances pour empêcher toute utilisation abusive de son e-ID. »

L'article (Art17 AL3) peut se révéler problématique pour la confiance du citoyen. En effet, compter que sur le devoir de diligence du citoyen (Art 7 Al1) tout en laissant la porte ouverte à l'usurpation d'identité en excluant les mauvais émetteurs/vérificateurs qu'à posteriori risque de freiner l'adoption du système par le citoyen. Il est donc essentiel que lors de toute vérification, le citoyen ait à disposition dans son portefeuille un moyen clair et facile d'identification du vérificateur qui lui demande le partage de certains attributs. Il doit pouvoir savoir sans effort si ce vérificateur fait bien partie du registre de confirmation des identifiants et que dans le cas contraire, une notice d'avertissement apparaisse. Ainsi le citoyen pourra avoir la certitude de partager ses données qu'à des vérificateurs légitimes.

3.8 VÉRIFICATION SANS RÉSEAU INTERNET (OUT OF BAND) (ART18 AL3 ET ART20)

Dans le monde réel, c'est-à-dire lors d'une vérification d'attestation en présentiel, est-ce que les attributs e-ID et les émetteurs/vérificateurs doivent pouvoir être vérifiables sans réseau internet (inclusion technologique) sachant que des solutions technologiques rendent cela possible ?

3.9 ACCÈS AU PORTEFEUILLE (ART19)

Est-ce que la Confédération pense fournir les outils nécessaires à la restriction d'accès au portefeuille (eg Biométrie, Login/Password, …)? Suivant la réponse du peuple concernant la LSIE, il semble opportun que la Confédération prenne cette responsabilité et n'utilise pas les fonctions similaires mises à disposition par les fabricants de téléphones ou les systèmes d'exploitation de ces derniers afin d'avoir le contrôle de bout en bout sur les aspects liés à la sécurité (exemple via utilisation des templates biométriques).

3.10 PRESTATAIRE DE SERVICE (ART24)

Est-ce que ce prestataire de services gardera la flexibilité de pouvoir déléguer, quand cela est nécessaire, l'exploitation d'une partie de l'infrastructure à un tiers, tout en garantissant que ce tiers opère sous le contrôle total de la Confédération ?

4 CONCLUSION

L'approche dite « Self-sovereign Identity » (SSI) a été reconnue par de nombreux protagonistes publiques et privés comme étant l'approche de choix pour une transition vers l'identité digitale du futur. Au vu des tendances de marché évoquées ci-dessus, des attentes de la population suisse et des contraintes techniques, l'approche dite « Self-sovereign Identity » (SSI) semble l'approche la plus adaptée pour garantir un taux d'adoption élevé de l'eID en Suisse. Même s'il s'agit d'une nouvelle approche et qu'un certain nombre de questions restent ouvertes, il y a de fortes chances qu'il devienne le système d'identité de la prochaine génération d'Internet. Comme d'autres pays comme le Canada, les États-Unis ou l'Union Européenne mènent actuellement des projets pilotes similaires pour évaluer les impacts sur leurs infrastructures et leurs processus existants, la Suisse pourrait également faire partie des pionniers du SSI qui façonnent les transactions numériques de demain.

L'avant-projet de la loi LeID soumis à consultation par l'Office Fédéral de la Justice (OFJ) permet de jeter les bases d'une implémentation d'identité numérique en Suisse basée sur le SSI. Cet avant-projet permet aux différents acteurs étatiques et du secteur privé de se préparer à l'adaptation et à la migration des processus et technologies existants. SICPA a soulevé quelques points qui pourraient se révéler critiques lors de la mise en place et pour la gestion opérationnelle de cette plateforme en Suisse. Nous espérons par cette démarche pouvoir initier des discussions ouvertes sur ces thèmes et pouvoir contribuer à une mise en œuvre réussie et harmonieuse de l'identité numérique en Suisse.

Nous restons volontiers à votre disposition pour partager notre expérience et vision dans le domaine ou toute information complémentaire.

SICPA SA
Headquarters
Av de Florissant 41
1008 Prilly
Switzerland

Tel +41 21 627 55 55
Fax +41 21 627 57 27
www.sicpa.com/contact
www.sicpa.com