Les identités numériques (eID)

FICHE INFO DU PPDT

INTRODUCTION

Notre vie quotidienne migre progressivement du monde physique au monde numérique. Plusieurs démarches administratives ou bancaires, par exemple, peuvent se faire sur internet, plus efficacement qu'en optant pour la démarche physique. De nombreuses autres tâches se font exclusivement numériquement (abonnement à un journal en ligne, réseaux sociaux, etc.). Une grande partie de ces services/tâches exige l'utilisation d'identifiants, parfois liés à l'identité physique officielle et vérifiable. C'est pour cela que divers pays, dont la Suisse, proposent des identités numériques (eID) pour faciliter les tâches des citoyens tout en favorisant la croissance économique fortement liée au monde numérique.

Cette fiche est destinée aux lecteurs curieux, sans bagage technique nécessaire.

LES IDENTITES DANS LE MONDE PHYSIQUE

Avant d'aborder les détails des identités numériques, revisitons les identités physiques (et les cartes d'identité) pour voir leurs propriétés et utilités.

Les cartes d'identité servent, entre autres, à deux fonctions de base:

- l'**authentification** des personnes: pour vérifier que les données sur la carte correspondent vraiment à la personne qui la présente, en se servant par exemple de la photo d'identité, le sexe, l'âge, etc.
- vérifier les **autorisations** des personnes: une fois que la personne est authentifiée, l'étape suivante vérifie ses droits, ce qu'elle est autorisée à faire. Est-elle par exemple autorisée à entrer dans ce pays ? Est-elle autorisée à acheter du vin/de la bière ?

Lors de l'authentification d'une personne avec une carte d'identité "officielle", une banque s'assure que c'est la "bonne personne", pour vérifier ses autorisations, mais aussi pour s'assurer de pouvoir la poursuivre en cas de fraude. L'authentification sert aussi à la police pour vérifier qu'elle communique/arrête la "bonne personne".

Différentes identifications sont possibles, par d'autres moyens qu'avec les cartes d'identité officielles. Une carte de fidélité est en quelque sorte une identification pour créditer les points sur le bon compte, sans trop d'importance si elle correspond exactement à la personne qui la porte. Bien entendu, la police et la banque ne peuvent pas se baser sur cette identification/authentification "légère", non-officielle, pour arrêter ou ouvrir un compte pour la personne qui la porte: l'authentification de la personne qui la porte n'est pas assez forte.

PASSONS AU MONDE NUMERIQUE

Dans le monde numérique, nous utilisons une multitude d'identités: les adresses mail, les noms d'utilisateurs, les numéros de téléphone, les noms d'utilisateurs Facebook/Google etc.

En me connectant sur mon compte mail donald.trump@bluewin.ch, et en entrant le bon mot de passe, je m'authentifie comme le bon propriétaire de ce compte, sans pour autant prouver le lien avec la "bonne personne" derrière. Cela m'autoriserait à accéder à mes mails, mais pas à ouvrir un compte à la banque, ni à prouver au douanier que je suis autorisé à entrer en Suisse. Un peu comme la carte de fidélité dans le monde physique.

Les identités numériques (eID)

FICHE INFO DU PPDT

Nous n'avons pas encore en Suisse une identité numérique officielle. Ce moyen est en cours d'élaboration. En 2019, le Parlement a approuvé une loi pour une identité numérique en Suisse, avec les mêmes fonctions que l'identité du monde physique (créer un compte bancaire, prouver mes droits, etc.) Un référendum a abouti et la loi a été rejetée en mars 2021. Le Conseil fédéral a lancé une consultation publique sur la future identité numérique Suisse, terminée en novembre 2021. Sur cette base, une nouvelle loi est en cours de rédaction et prévue pour début 2023[1]. Mais quelle est la différence entre ces lois ? Pourquoi la nouvelle serait-elle meilleure que celle qui a été rejetée ? Nous allons aborder ces détails dans la suite de cette fiche.

LES DIFFERENTS TYPES D'IDENTITES NUMERIQUES

Avec une identité numérique officielle, l'utilisateur va pouvoir prouver son identité (ex. Jacques Panchaud) et recevoir les mêmes services dans le monde numérique (en ligne) que dans le monde physique, avec plus de rapidité/efficacité et plus de sûreté. Le support de l'identité numérique pourrait être une carte à puce, une clé USB, ou une application sur le smartphone ou l'ordinateur. Ouvrir un compte bancaire sans avoir à se présenter en personne, demander une hypothèque, prouver que j'ai plus de 18 ans, ou demander en ligne un extrait judiciaire ne sont que quelques exemples parmi des dizaines, voire des centaines d'utilités. Mais qui va présenter quoi exactement à qui ? Qui authentifie ? Comment ? Qui est le fournisseur de ces identités ? Il y a plusieurs configurations possibles.

IdP ("ID Provider" en Anglais, ou "fournisseur d'identité")

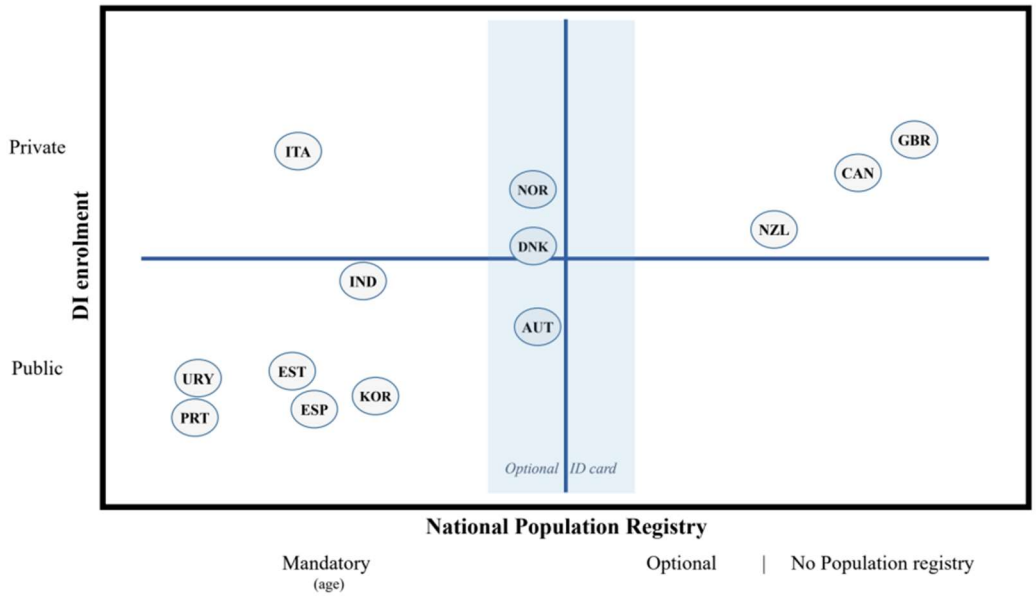
C'est la configuration dans laquelle une organisation (l'Etat ou des entreprises privées) fournit les identités numériques aux utilisateurs. Quand l'utilisateur demande un service (ex. demande d'un extrait judiciaire), l'authentification est faite par l'intermédiaire du fournisseur d'identité avant que le service soit fourni. Cela ressemble à ce que l'on observe maintenant avec plusieurs sites web qui demandent l'identification avec un compte Facebook ou Google. Ce ne sont pas des identifications officielles, mais pour certains services tels qu'un abonnement dans un journal, cela évite à l'utilisateur la création d'un compte supplémentaire, ainsi qu'au fournisseur de services (ex. journal) la gestion des comptes des utilisateurs. C'est pratique pour l'utilisateur et pour le journal, sauf que le fournisseur d'identité (ex. Facebook) va pouvoir tracer les abonnements de l'utilisateur, quand ce dernier s'y connecte, etc., permettant au fournisseur de profiler les utilisateurs (ex. quels sont ses intérêts ou orientations) et d'utiliser les données et profils à des fins publicitaires, influencer les opinions par l'envoi de recommandations, ou aussi les vendre à des tiers.

La loi sur l'identité numérique de 2019 suivait cette configuration (IdP) : c'est l'Etat qui établit et fournit les identités, mais ce sont des entreprises privées accréditées (La Poste, Swisscom, CFF, ou autres petits fournisseurs) qui s'occupent de la mise en œuvre et des opérations. Par exemple : l'utilisateur visite la page pour consulter son dossier médical, l'authentification est faite par "La Poste" avant qu'il puisse accéder à son compte (un peu comme l'identification par Facebook et Google pour visiter la page web de mon journal). Pour éviter le traçage des utilisateurs par les fournisseurs, le profilage, ou la vente des données, la loi limitait les utilisations possibles par les fournisseurs. A part le principe selon lequel les identités doivent rester dans les mains de l'Etat, les référendaires s'inquiétaient que les opérateurs privés puissent collecter des données et les utiliser au-delà de ce qui est permis par la loi.

Est-ce que ce problème de choix (entre secteur privé vs gouvernement pour gérer les identités numériques) se pose seulement en Suisse ? Non. Plusieurs paramètres entrent en considération et le choix n'est pas unique. Une étude[2] de l'OCDE montre, par exemple, que dans les pays où il n'y a pas de registre gouvernemental central pour les identités (physiques), le secteur privé, tel que les banques, est mieux placé pour gérer les identités numériques des citoyens d'une manière fiable (voir figure ci-dessous).

[1] Pour plus de détails sur le processus législatif: https://www.ejpd.admin.ch/ejpd/fr/home/themes/abstimmungen/bgeid.html, consulté le 13 septembre 2022.

[2] https://www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en, consulté le 13 septembre 2022.



PKI ("Public Key Infrastructure" en Anglais, ou "Infrastructure à Clés Publiques")

La PKI nous permet, entre autres, de résoudre le problème où "toute identification doit passer par un opérateur" (que l'opérateur soit l'Etat ou un opérateur privé). Dans une PKI, l'utilisateur est muni d'une identité signée cryptographiquement par l'Etat[3]. Avec ce certificat, l'utilisateur peut :

- s'identifier auprès d'un fournisseur de services, sans passer par un opérateur d'identité central (ni l'Etat, ni un privé)
- signer (cryptographiquement) un document tel qu'un contrat. Un fournisseur de services, tel qu'une banque, peut vérifier qu'un document est effectivement signé par une certaine personne, et la personne ne pourrait pas nier sa signature. Tout cela, sans passer par un fournisseur d'identité central.

Nous venons de voir que ces mécanismes se déroulent sans l'implication du fournisseur d'identité. Mais pour plusieurs raisons, un certificat/identité pourrait être révoqué par le fournisseur. Un vérificateur devrait vérifier que le certificat/identité présenté par l'utilisateur n'a pas été révoqué. Il y a deux manières de le faire :

- le vérificateur demande au fournisseur si l'identité de l'utilisateur en question a été révoquée. Cette opération permettrait au fournisseur de savoir que l'utilisateur est en contact avec le service/vérificateur (ex. Jacques Panchaud a un compte Tinder), de le profiler, ou de vendre ces données à des tiers (comme pour l'IdP).

[3] Signature cryptographique: avec la PKI, le fournisseur d'identité (Etat, ou privé) est muni d'une clé publique accessible pour tout le monde, et d'une clé privée. Il en va de même pour les utilisateurs: chacun est muni de sa clé publique (accessible à tous), et d'une clé privée, secrète, accessible pour l'utilisateur seulement. Pour authentifier un utilisateur, un vérificateur se sert de la clé publique pour lui envoyer un défi. L'utilisateur se sert de sa clé privée pour répondre au défi. Ce mécanisme prouve que la personne a effectivement la clé privée qui correspond à la clé publique. Reste à vérifier que cette identité est validée par l'Etat. C'est ce qui se passe en vérifiant la signature du certificat de l'utilisateur par l'Etat.

L'Etat signe les certificats des utilisateurs en utilisant sa clé privée, secrète, accessible seulement pour l'Etat. Pour vérifier la validité d'un certificat/identité d'un utilisateur, un vérificateur se sert de la clé publique de l'Etat. De la même manière:
- une organisation, telle qu'une université, peut signer un diplôme en utilisant sa clé privée. Pour vérifier la signature (ex. par un employeur), le vérificateur se sert de la clé publique de l'université.
- une personne peut signer un contrat (ex. prêt hypothécaire) en se servant de sa clé privée. Pour vérifier la signature, le vérificateur se sert de la clé publique de cette personne.

- le fournisseur d'identité publie une liste des identités révoquées. Un vérificateur consulte cette liste pour vérifier si l'identité de l'utilisateur y est. De cette manière, le fournisseur d'identité n'a aucune information sur les interactions entre les utilisateurs et les services.

Depuis plusieurs années, les PKI sont utilisées dans les certificats d'adresses mail, les certificats de pages web, et aussi dans les signatures électroniques. Certaines signatures électroniques ont la même validité que les signatures physiques. La loi sur la signature électronique du 18 mars 2016 (SCSE; RS 943.03)[4] cadre leurs utilisations. Le temps a prouvé la robustesse des PKI contre les fraudes et la simplicité de leur utilisation.

Cependant, l'un des inconvénients de l'utilisation de PKI pour les identités numériques est le manque de flexibilité: si, par exemple, l'identité numérique inclut le nom, prénom, sexe, date de naissance, et le lieu d'origine de l'utilisateur, ce dernier doit **tout** présenter à chaque vérification. Dans certains cas, il n'y a besoin que de vérifier si la personne a plus de 18 ans, sans autre information. Mais la personne doit tout présenter au vérificateur, faute de quoi l'identité/certificat paraitrait invalide. L'option des SSI, décrite dans la section suivante, résout ce problème (entre autres).

SSI ("Self-Sovereign ID" en anglais, ou "Identités Auto-Souveraines")

Le SSI est un concept datant de 2016[5], établi sur la base d'un article de 2012 sur les Autorités Auto-Souveraines[6]. Il définit 12 principes destinés à être utilisés par tout écosystème d'identité numérique:

1. **Représentation**

   Un écosystème SSI doit permettre à toute entité – de nature humaine, légale, naturelle, physique ou numérique – de pouvoir être représentée par un nombre quelconque d'identités numériques.

2. **Interopérabilité**

   Un écosystème SSI doit permettre aux données d'identité numérique d'une entité qu'elles soient représentées, échangées, sécurisées, protégées et vérifiées d'une manière interopérable, en utilisant des standards open-source, publics et libres de droits.

3. **Décentralisation**

   Un écosystème SSI ne doit pas dépendre d'un système centralisé pour représenter, contrôler ou vérifier les données d'identité numérique d'une identité.

4. **Contrôle et transfert**

   Un écosystème SSI doit permettre aux entités qui possèdent des droits d'identité naturels, humains ou légaux (détenteurs de droits d'identité, en anglais « Identity Rights Holders ») de contrôler l'usage de leurs données d'identité numérique, et d'exercer ce contrôle en mandatant et/ou en les transférant aux vecteurs et gardiens de leur choix, y compris tout individu, toute organisation, tout dispositif et logiciel.

5. **Participation**

   Un écosystème SSI ne doit pas obliger un détenteur de droits d'identité d'y adhérer.

6. **Egalité et inclusion**

   Dans son champ de gouvernance, un écosystème SSI ne doit pas exclure ou désavantager des détenteurs de droits d'identité.

7. **Fonctionnalité, accessibilité et cohérence**

   Un écosystème SSI doit maximiser la fonctionnalité et l'accessibilité aux vecteurs et à d'autres éléments du système SSI pour les détenteurs de droits d'identité, y compris la cohérence de l'expérience utilisateur.

8. **Portabilité**

   Un écosystème SSI ne doit pas limiter la possibilité des détenteurs de droits d'identité de remettre ou de transférer une copie de leurs données numériques à un autre vecteur ou système de leur choix.

[4] https://www.fedlex.admin.ch/eli/cc/2016/752/fr, consulté le 13 septembre 2022.
[5] https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-French-v01.pdf, consulté le 13 septembre 2022.
[6] https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html, consulté le 13 septembre 2022.

9. **Sécurité**

   Un écosystème SSI doit assurer aux détenteurs de droits d'identité la maîtrise de leurs données d'identité, soit durant leur transfert ou à l'état inactif, de contrôler leurs attributs identifiants et les clés de chiffrement, et d'utiliser un chiffrement de bout en bout pour toutes les interactions.

10. **Validation et authentification**

    Un écosystème SSI doit permettre aux détenteurs de droits d'identité de fournir une preuve vérifiable d'authenticité de leurs données d'identité numérique.

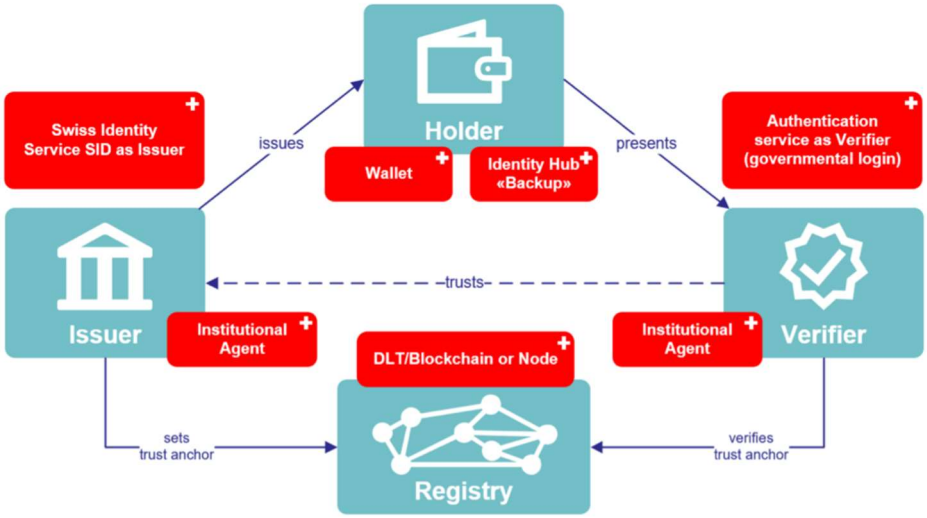
11. **Confidentialité et divulgation minimale**

    Un écosystème SSI doit permettre aux détenteurs de droits d'identité de protéger la confidentialité de leurs données d'identité numérique et de n'en divulguer que le strict nécessaire pour toute interaction spécifique.

12. **Transparence**

    Un écosystème SSI doit permettre aux détenteurs de droits d'identité et à toute autre partie intéressée d'accéder à et de vérifier facilement les informations nécessaires pour comprendre les motivations, les règles, les processus et les algorithmes selon lesquels les vecteurs et autres composants des écosystèmes SSI fonctionnent.

Avant de détailler certains de ces principes qui sont pertinents en termes de protection de la vie privée, décrivons brièvement qui sont les "acteurs" et leurs fonctions, en se basant sur cette figure :



Le fournisseur d'identité (Issuer) génère l'identité et la passe à l'utilisateur (Holder). L'utilisateur est authentifié auprès de fournisseurs de services (Verifier) sans que ceux-ci interagissent avec le fournisseur d'identité (comme dans la PKI). Diverses preuves d'interactions sont stockées sur une chaine de blocs (blockchain / Registry).

Retour aux principes du SSI :

Le principe 1 "Représentation" permet à l'utilisateur d'avoir plusieurs identités numériques distinctes. Comme certains de nous préfèrent avoir des adresses email séparées pour le travail / personnel / autres, l'utilisateur va pouvoir avoir plusieurs identités numériques. En pratique, ceci complique la gestion des identités auprès de l'utilisateur, ainsi qu'auprès des autorités (une personne, différentes identités selon le domaine), mais servirait à compliquer le croisement non désiré des données auprès de différents fournisseurs de services. Il serait même possible, en principe, de signer divers documents auprès du même fournisseur de services, sans que ce dernier puisse les lier à la même personne. Il en va de même auprès de fournisseurs distincts.

Le principe 3 "Décentralisation" est pris en compte par l'utilisation d'une blockchain[7] où certaines preuves d'interactions et certaines données publiques sont gardées. Ainsi, la fiabilité et la confiance dans le système distribué sont élevées. A noter que la blockchain ne contient pas les données personnelles (lisibles pour tous), mais des versions codées (ex. Hash).

Le principe 11 va dans les détails de divulgation des données par l'utilisateur à un fournisseur de services. Les données doivent être le « minimum nécéssaire pour une interaction spécifique ». Cette minimisation est d'ailleurs l'un des principes de la loi suisse sur la protection des données et du RGPD. Elle peut être interprétée de deux manières :

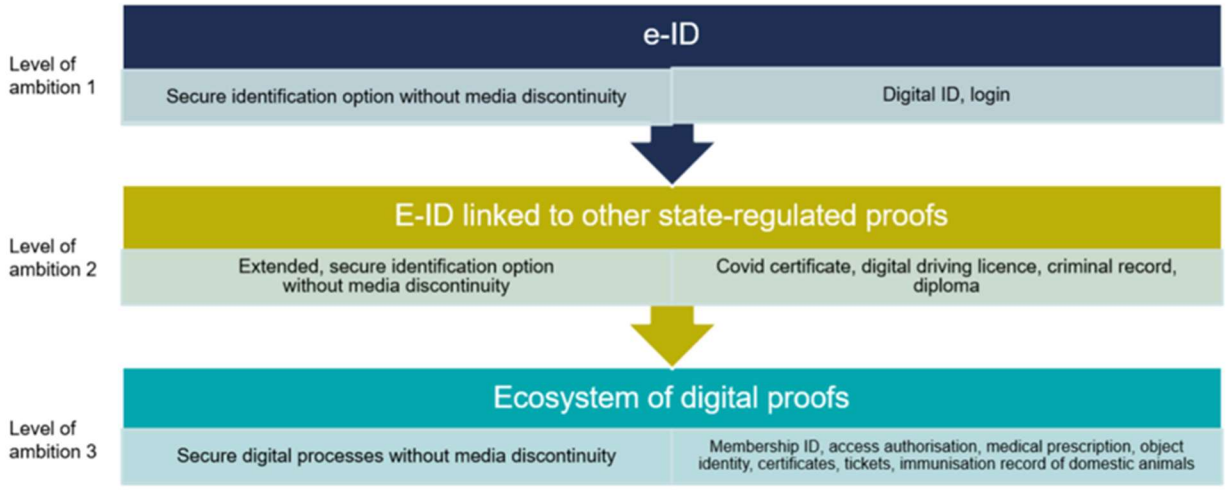
- l'utilisateur ne divulgue que les attributs nécessaires (ex. seulement la date de naissance, pour prouver qu'il est adulte et ainsi acheter du vin)
- même l'information contenue dans les attributs nécessaires est minimisée (ex. au lieu de la date de naissance, une preuve que l'utilisateur a plus de 18 ans, sans partager la date ni l'année de naissance)

Cette minimisation est un bon moyen de respect de la vie privée, mais elle présente certains défis :

- Techniques : à la base, une modification des informations de l'identité numérique devrait invalider sa signature numérique (et de la vérification). Rendre possible la minimisation par exclusion de certains attributs ou même en les manipulant (ex. date de naissance -> preuve d'âge adulte) tout en gardant les signatures valides implique des connaissances techniques avancées et l'utilisation de nouvelles techniques cryptographiques (tels que les "Zero Knowledge Proofs"). Ceci risque de retarder l'implémentation des minimisations pour les identités numériques.
- Pratiques : il est relativement difficile pour l'utilisateur moyen de comprendre et gérer seul tout type de minimisation. Il va falloir de bonnes campagnes de sensibilisation et/ou des lignes directrices pour les fournisseurs de services, et que ces dernières soient suivies. C'est pour cela que le principe de minimisation risque de prendre du temps pour entrer en pratique.

LE NOUVEAU PROJET DE LOI EN SUISSE[8]

Après le rejet en votation populaire le 7 mars 2021 de l'ancienne loi sur les services d'identification numérique, le Conseil fédéral a lancé une consultation publique, pour une solution d'identification numérique étatique, du 2 septembre au 14 octobre 2021: IdP, PKI, ou SSI. Pour le SSI, un choix supplémentaire était imposé, entre 3 "niveaux d'ambition" :



[7] Blockchain: sans entrer dans les détails des blockchains, il suffit de le considérer comme un registre de données, robuste contre les attaques et infalsifiable. Le système consiste en un grand nombre de nœuds (ordinateurs), gérés par différentes entités/personnes/organisation, qui gardent des copies des données (ou preuves). Pour pouvoir falsifier les preuves, il faudrait compromettre une majorité des nœuds de la blockchain (ce qui est rendu très difficile, vu qu'ils sont contrôlés par différentes entités) ainsi qu'un temps de calcul énorme. Il existe deux types de blockchains: privés et publics, où les nœuds sont respectivement contrôlés par un groupe fermé d'organisations, ou par un groupe ouvert à tous.

[8] https://www.ejpd.admin.ch/ejpd/fr/home/themes/abstimmungen/bgeid.html, consulté le 13 septembre 2022.

1. l'eID tout simple, incluant les informations des cartes d'identités physiques.
2. l'eID lié à d'autres preuves issues par l'Etat, telles que certificats Covid, permis de conduire, diplômes, extraits judiciaires, etc.
3. un écosystème de preuves numériques (pas exclusivement étatiques) tel que les cartes de membres, titres de transport, tickets de concerts etc. Cette solution est couramment appelée "eWallet", ou portefeuille numérique.

En se basant sur les résultats de cette consultation publique, le Conseil fédéral a publié sa décision le 17 décembre 2021[9], en faveur des SSI :

"Les utilisateurs de l'e-ID devront, dans toute la mesure du possible, avoir la maîtrise de leurs données (principe de l'identité auto-souveraine). La protection des données sera assurée notamment par le système lui-même (principe de la protection de la vie privée dès la conception), mais aussi par la limitation des flux de données nécessaires (principe de l'économie des données) et une sauvegarde décentralisée des données".

Et le niveau d'ambition 3 :

"L'e-ID fonctionnera dans une infrastructure gérée par l'État, qui pourrait être mise à la disposition des services publics et des entreprises pour créer les preuves numériques les plus diverses".

Le nouveau projet de loi est actuellement mis en consultation publique[10] jusqu'au 20 octobre 2022.

En Suisse, une identité numérique devrait être acceptée à tous les niveaux : fédéral, cantonal, et communal. Au niveau international, le système suisse d'identification électronique respectera les normes internationales afin que l'eID puisse être reconnue et utilisée à l'étranger (ex. eIDAS[11] dans l'UE).

QUI DIT eID DIT AML ET KYC AUSSI

Le passage des cartes d'identité traditionnelles aux identités numériques est souvent considéré comme une amélioration contre les fraudes (ex. falsification de documents ou de signatures). En même temps, l'eID à la base des SSI donne aux utilisateurs divers moyens de préservation de leur vie privée (ex. principes de la représentation et de la divulgation minimale). Ceci a des implications sur diverses lois et pratiques contre le blanchiment d'argent que certains établissements, tels que les banques, sont tenus d'appliquer. Par exemple, la loi contre le blanchiment d'argent et de financement du terrorisme (AML/CFT, pour "Anti-Money Laundring / Countering the Financing of Terrorism" en Anglais) et le KYC ("Know Your Customer" en anglais, ou "connaitre son client"). Un rapport du Groupe d'Action Financière[12] (en anglais) aborde le sujet plus en détails.

AVANTAGES ET RISQUES

L'identité numérique promet une multitude d'**avantages** à tous les niveaux :

Pour l'utilisateur : l'eID réduit le nombre d'identifiants (et de mots de passe correspondants) pour différents services en ligne, simplifiant ainsi leur gestion. D'autre part, elle permet à l'utilisateur d'effectuer toute démarche administrative (ex. interactions avec l'Etat, les banques, etc.) en ligne, évitant ainsi les déplacements et les présentations aux guichets, accélérant ainsi toutes ces procédures tout en réduisant leurs coûts.

Pour l'Etat : l'eID permet la simplification des processus traditionnellement longs, manuels, et/ou exigeant une présence aux guichets. D'autre part, elle permet d'éviter diverses fraudes (ex. falsification des documents physiques/papiers) et les vols d'identité. L'eID présente aussi des avantages économiques.

Pour l'industrie / économie : l'eID simplifie, accélère et réduit les coûts des démarches administratives, favorisant l'utilisation des services et, par la suite, l'économie.

[9] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-86465.html, consulté le 13 septembre 2022.
[10] https://www.bj.admin.ch/bj/fr/home/aktuell/mm.msg-id-89515.html, consulté le 13 septembre 2022.
[11] https://en.wikipedia.org/wiki/EIDAS, consulté le 13 septembre 2022.
[12] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html, consulté le 13 septembre 2022.

Quant aux **risques** liés à l'eID :

Pour l'utilisateur : une solution eID basée sur les SSI met le contrôle entier dans les mains de l'utilisateur. Les échanges se passeront entre le fournisseur de services et l'utilisateur, sans aucun intermédiaire (Etat ou fournisseur d'identité). Il en découle qu'il est difficile d'alerter l'utilisateur d'une fraude qu'il subit, et de le maintenir vigilant sur ce qu'il partage avec qui. L'utilisateur doit gérer aussi des "backups" (sauvegardes), sans lesquels la perte de l'eID entraînerait une démarche pour la révoquer et d'en créer une nouvelle. D'autre part, les escrocs en ligne accompagnent chaque nouvelle technologie par de nouvelles arnaques, se basant souvent sur la confiance des utilisateurs habitués au monde physique ou sur leur manque de connaissance des systèmes souvent complexes. Le déploiement de l'eID, surtout basé sur les SSI, devrait être accompagné par des campagnes d'information et de sensibilisation des utilisateurs afin de réduire ces risques.

Pour l'Etat et l'industrie : avec l'eID, il serait plus difficile de tricher avec les données (photo, nom, etc.) qu'avec les cartes d'identité physiques. Cependant, les fraudes des cartes physiques ont une portée limitée (en nombre ou géographiquement). Dans un système eID+SSI assez complexe, ouvert et nouveau, l'exploitation de failles potentielles aurait une portée nationale voire même globale. L'utilisation de systèmes internationaux, "open source", ouverts pour les chercheurs en sécurité, va dans la bonne direction pour contrer ces risques.

QUELQUES LECTURES SUPPLEMENTAIRES

- Building a Swiss Digital Trust Ecosystem (https://digitalswitzerland.com/building-a-swiss-digital-trust-ecosystem/)
- World Bank, ID4D Practitioner's guide (https://id4d.worldbank.org/guide)

AUTEUR

Dr. Imad Aad, Centre pour la Confiance Numérique (C4DT - https://www.c4dt.org/), EPFL, septembre 2022

PPDT – 19.09.2022