SGMI SSIM SSMI

Schweizerische Gesellschaft für Medizinische Informatik
Société Suisse d'Informatique Médicale
Società Svizzera d'Informatica Medica
Swiss Society for Medical Informatics

eMpfEhlung-RecommaNdaTion-RaccomandaziOne-Recommendation

Die Schweizerische Gesellschaft für Medizinische Informatik publiziert zu aktuellen Themen Empfehlungen für Ihre Mitglieder und die Öffentlichkeit

La Société Suisse d'Informatique Médicale publie des recommandations sur des sujets d'actualité à l'intention de ses membres et du public

Elektronische Identifikation (e-ID)

Identité électronique (e-ID)

La Società Svizzera d'Informatica Medica pubblica raccomandazioni su temi di attualità per i suoi membri e per il pubblico

The Swiss Society for Medical Informatics publishes recommendations on current topics for its members and the public

Septembre 2025

SGMI-MENTOR – Identité électronique (e-ID)

Introduction

Contexte

Depuis toujours, l'identification unique et infalsifiable de ses citoyens fait partie des tâches fondamentales d'un État. Depuis toujours également, elle est associée à un risque important d'abus de pouvoir, d'oppression et de surveillance. Les acquis de la démocratie moderne ont permis la création de lois et de réglementations qui réduisent ces risques et renforcent la protection des individus.

Malgré la numérisation croissante de la vie quotidienne, ce processus fondamental d'identification est toutefois resté largement analogique en Suisse jusqu'à présent. Sur le plan technologique, différentes variantes d'identité numérique juridiquement valables ont été testées, mais aucune n'a réussi à s'imposer jusqu'à présent.

La Suisse est l'un des rares pays européens à ne pas encore proposer d'identité électronique publique.

Situation initiale

La Confédération suisse a également reconnu la nécessité d'une identité électronique fiable et a soumis un premier projet de loi au vote populaire en 2021. Celui-ci a été clairement rejeté avec 64,4 % de voix contre. Il s'est avéré par la suite que les votants n'avaient pas dit « non » à l'identité électronique, mais à la manière dont elle était envisagée à l'époque (délivrance par des prestataires privés) [1].

La Confédération et le Parlement ont donc pris un nouveau départ et élaboré un nouveau projet de loi qui tient compte des critiques formulées lors du premier vote, notamment en matière de gouvernance et de protection des données. Ce projet a été adopté à une très large majorité par tous les partis lors de la session d'hiver 2024 du Parlement (Conseil national : près de 90 %, Conseil des États : 97 %).

Un conglomérat de différents groupes d'intérêt a lancé un référendum contre ce projet, qui sera donc soumis à un vote populaire le 28 septembre 2025.

L'e-ID

Principes techniques [2]

L'e-ID fonctionne comme une carte d'identité numérique. Elle est délivrée par l'État et permet une identification numérique incontestable et juridiquement valable.
L'e-ID est conçue de manière à répondre aux exigences les plus élevées en matière de sécurité, de protection des données, de minimisation des données et de fiabilité. Son utilisation est facultative. [1]

Sur le plan technique, une approche décentralisée et ouverte est adoptée. À cette fin, l'Office fédéral de l'informatique (OFIT) met à disposition un « portefeuille » pour téléphone mobile. Afin d'éviter toute utilisation abusive, l'identité électronique contenue dans ce portefeuille est cryptographiquement liée à un téléphone mobile spécifique et ne peut donc pas être copiée.

La délivrance initiale d'une e-ID ou d'un autre justificatif d'identité électronique (*credential*) est certes effectuée par une autorité centrale (*issuing authority*), mais le processus d'identification se déroule ensuite de manière décentralisée, directement entre le titulaire (*holder*) et un organisme de contrôle (*verifier*). Le titulaire garde ainsi le contrôle de ses données.

Le stockage et l'évaluation centralisés des données ne sont pas prévus sur le plan technique (*privacy by design).* La Confédération met toutefois à la disposition des acteurs une infrastructure de confiance composée d'un registre de base (*base registry*) et d'un registre de confiance (*trust registry*).

Le registre de base contient les identifiants décentralisés (*DID*) et leurs clés cryptographiques *sans données à caractère personnel*. C'est là que la validité est gérée, entre autres.
Le registre de confiance permet l'attribution officiellement certifiée d'émetteurs ou d'organismes de contrôle fiables aux DID.
Les données personnelles des utilisateurs *ne* sont *jamais* stockées de manière centralisée.

Ces deux registres permettent de vérifier la validité cryptographique des certificats délivrés et de les attribuer aux autorités ou organismes de contrôle officiellement agréés. Cela garantit que tous les acteurs peuvent se faire mutuellement confiance à tout moment pendant l'ensemble du processus d'identification.

La figure 1 présente un aperçu schématique des composants décrits.

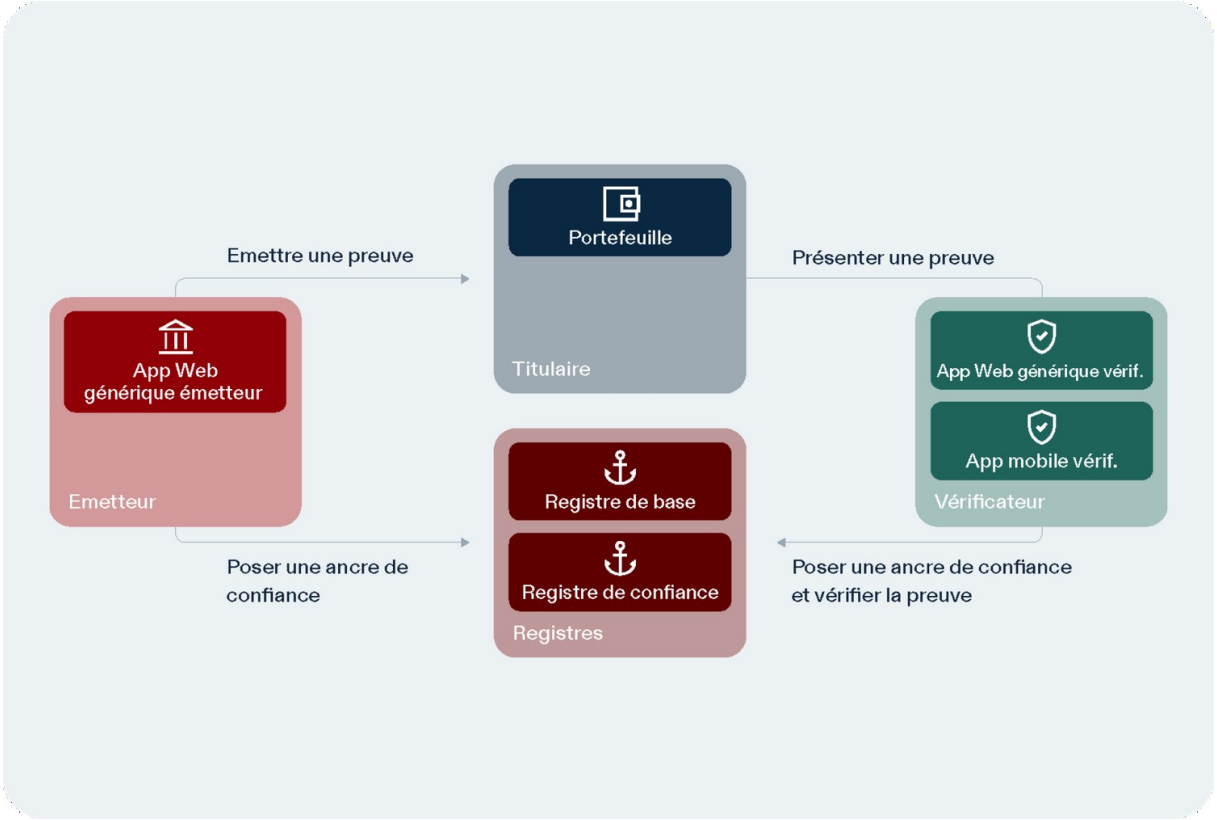

Fig. 1 : Aperçu simplifié des composants de l'e-ID (d'après [1], avec l'aimable autorisation)

Dans le cas de l'identification décentralisée, l'utilisateur ne peut échanger que les données nécessaires au processus d'identification concerné. Par exemple, dans le cas d'une vérification de l'âge, seule l'information selon laquelle la personne est âgée de plus de 18 ans (*vrai* ou *faux*) est échangée, sans aucune autre donnée personnelle, pas même la date de naissance.

Outre l'application Wallet/Portefeuille, l'Office fédéral de la technologie (OFIT) met également à disposition une application de vérification et d'autres composants techniques. Toutes les applications et tous les composants sont *open source.*

Points forts

L'approche « privacy by design » est certainement l'un des principaux atouts de la solution présentée, car elle permet de répondre de manière fondamentale aux exigences élevées en matière de confidentialité et de protection des données. De plus, la mise à disposition ouverte des codes sources des applications nécessaires renforce la confiance. Enfin, la base technologique est conçue de manière à pouvoir être utilisée par un grand nombre d'acteurs, qui peuvent ainsi bénéficier du haut niveau de confiance dans l'identification officielle des personnes.

Contrairement à l'identité physique, qui n'est pas infalsifiable, l'e-ID est sécurisée par des procédés cryptographiques de pointe et peut donc être utilisée en toute sécurité dans la vie numérique. Elle permet de poser un élément fondamental, jusqu'ici manquant, pour une numérisation cohérente et durable.

Problèmes

En raison de l'approche décentralisée cohérente et des considérations relatives à la protection des données, l'utilisation quotidienne peut s'avérer difficile pour les citoyens moins familiarisés avec la technologie. Il est impératif de disposer de son propre téléphone portable. De plus, le processus de vérification décentralisée, qui consiste à scanner un code QR et à confirmer la divulgation des données, prend un certain temps, ce qui peut entraîner des retards dans la vie quotidienne (par exemple, contrôle d'accès). Enfin, la vérification centralisée de la validité d'un certificat nécessite une connexion Internet permanente aux registres centraux, ce qui est également le cas pour d'autres applications numériques.

Sur le plan formel, c'est à l'utilisateur de décider quelles données il souhaite partager, mais dans la pratique, il partagera peut-être plus de données que nécessaire si l'organisme de contrôle l'exige et qu'il ne peut pas bénéficier d'un service autrement. La loi actuelle ne prévoit aucune réglementation supplémentaire pour protéger les données des utilisateurs.

Le principal problème technique pour les utilisateurs devrait être le lien avec un téléphone portable spécifique. Cela est nécessaire d'un point de vue cryptographique, mais empêche le transfert des preuves d'identification vers un autre (nouvel) appareil. Par conséquent, de nouvelles preuves doivent être demandées avec le nouvel appareil.
La Confédération prévoit certes la création à moyen terme de sauvegardes centralisées et cryptées, mais cela relativise à nouveau l'approche décentralisée.

Le comité référendaire avance également des arguments relatifs à un État surveillant numérique, dans lequel chaque citoyen serait contraint d'utiliser l'e-ID et chaque action numérique serait authentifiée/identifiée et utilisée pour des systèmes de crédit social. Il semble s'agir ici davantage d'une méfiance générale envers l'État et la société que de préoccupations fondées concernant la mise en œuvre technique proposée.

Enfin, l'e-ID, dans sa forme actuelle, est pour l'instant un produit purement suisse. Elle n'est pas encore reconnue à l'étranger et devrait surmonter des obstacles diplomatiques mais aussi techniques (par exemple, l'absence d'infrastructure de contrôle décentralisée).

Dans l'ensemble, il faut toutefois garder à l'esprit que tous les problèmes mentionnés s'appliquent souvent de la même manière ou de manière similaire aux cartes d'identité physiques ou à d'autres produits numériques. En outre, il est toujours possible d'utiliser les cartes d'identité classiques lorsque cela s'avère plus judicieux. Il sera donc nécessaire d'optimiser la convivialité de l'e-ID afin qu'elle soit plus facile à utiliser au quotidien que les alternatives analogiques.

Avantages pour le secteur de la santé

L'identification électronique est également un élément fondamental indispensable à la numérisation du secteur de la santé, qui faisait jusqu'à présent défaut. Les domaines d'application possibles sont donc multiples.

Il convient bien sûr de mentionner en premier lieu l'identification numérique fiable des personnes. Une e-ID permettrait par exemple de proposer des admissions ou des prises de rendez-vous par voie numérique. Elle faciliterait également l'ouverture d'un DEP (dossier électronique du patient) et le rendrait plus accessible au grand public.

Du côté des professionnels de la santé, l'identité électronique offre également de nouvelles possibilités. Par exemple, l'authentification en tant que médecin agréé pourrait se faire au moyen de l''identité électronique, ce qui simplifierait considérablement l'interaction numérique avec les patients et les autres acteurs du secteur de la santé.

Enfin, la signature numérique de rapports, de certificats, d'ordonnances ou de documents d'information semble également présenter un grand potentiel.

Dans le secteur de la santé également, l'approche décentralisée et centrée sur le patient présente des avantages, car le patient conserve à tout moment la maîtrise de ses données les plus sensibles.

Conclusion

Avec la solution d'identité électronique proposée au vote, la Confédération suisse poursuit une approche innovante et moderne, unique au monde. Il ne s'agit pas seulement de créer une version numérique de la carte plastique, mais aussi de mettre en place un écosystème de confiance qui favorisera la digitalisation dans de nombreux domaines. Cette évolution est particulièrement bienvenue et urgente dans le secteur de la santé.

Elle parvient à concilier la confiance (qui nécessite une autorité centrale) et l'autodétermination (autonomie décentralisée).

Les abus ne peuvent en principe être exclus pour aucune forme d'identité. Une démocratie de base qui fonctionne bien et un système juridique intact sont nécessaires et importants pour assurer le contrôle. À notre avis, ces deux conditions sont réunies en Suisse.

La SGMI recommande donc d'accepter le projet et soutient l'e-ID en tant qu'élément fondamental du futur système de santé numérique.

Remerciements

Nous remercions chaleureusement le professeur Serge Bignens, *de la Haute école spécialisée bernoise*, pour sa collaboration au MENTOR et pour la traduction française. Nous remercions également les autres membres du comité directeur de la Société suisse d'informatique médicale (SSIM) pour leur relecture critique du manuscrit.

Correspondance

Deutsche Version

Dr. med. Lukas Dürst
Kantonsspital Graubünden
Loëstrasse 170
7000 Chur

lukas.duerst@ksgr.ch

Version française

Prof. Serge Bignens
Berner Fachhochschule
Technik und Informatik
Lehre
Höheweg 80
2502 Biel

serge.bignens@bfh.ch

Sources

[1] Confédération suisse, « Identification électronique ». Consulté le 27 août 2025. [En ligne]. Disponible à l'adresse : https://www.eid.admin.ch/de/

[2] Confédération suisse, « Technologie swiyu ». Consulté le 27 août 2025. [En ligne]. Disponible à l'adresse : https://swiyu-admin-ch.github.io/introduction/