ELCASecurity
AN ELCA COMPANY

Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössisches
Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Berne

Par email à :
rechtsinformatik@bj.admin.ch

Lausanne, 20 octobre 2022
CGR / SUTC

Loi Fédérale sur l'Identité Electronique et les Autres Identités Electroniques (E-ID-Gesetz, BGEID)

Prise de Position sur la Consultation V1.3

Madame la Conseillère fédérale Keller-Sutter
Mesdames et Messieurs

Résumé

Nous vous remercions de l'opportunité qui nous a été donnée de participer à cette consultation sur l'eID. En tant qu'ELCA Security - une filiale de l'entreprise privée de technologie de l'information ELCA Informatique en Suisse - nous considérons que notre responsabilité consiste moins à fournir une expertise politique qu'à nous concentrer pleinement sur notre expertise en matière de cybersécurité et de commerce. Nous sommes fiers de compter dans notre équipe certains des développeurs, ingénieurs, analystes et consultants en informatique les plus talentueux de Suisse et notre mission est de fournir à nos clients les meilleures solutions possibles sur le marché. C'est pourquoi nous sommes honorés de partager notre expertise avec vous.

Outre notre expertise pure en matière de cybersécurité, nous sommes également actifs en tant que fournisseur d'identité reconnu en Suisse. Depuis plus de trois

ans, nous sommes au service d'administrations publiques, de toutes les communautés de santé ainsi que d'entreprises privées. Ainsi, nous sommes convaincus que notre expertise et notre expérience du marché de l'identité électronique constituent un apport précieux pour cette consultation.

Nous souhaitons nous positionner sur les huit points suivants, sans ordre de priorité :

1. Sauvegarde et stockage des données critiques

En référence à l'article 21, un système de sauvegarde doit être fourni soit par la Confédération elle-même, soit par des prestataires certifiés, désignés par le gouvernement. Le stockage de ces données critiques doit être conforme aux normes de sécurité les plus élevées : des règles strictes - certifiées et contrôlées - sont nécessaires pour prévenir les violations de sécurité et les abus.

2. Sécurité et contrôles

La Confédération est responsable et doit garantir la conformité et l'authenticité ainsi que la sécurité des futurs wallets. Pourtant, selon l'article 14, la loi autoriserait en principe n'importe quelle application à stocker des données critiques. A notre avis, la loi doit définir clairement imposer une certification des applications et/ou des wallets. Autrement dit, les applications doivent être soumises à des mesures de sécurité spécifiques pour pouvoir être utilisées et installées. Cela peut être fait soit par le gouvernement, soit par des fournisseurs privés se conformant à des normes de sécurité, d'authentification et d'accréditation définies.
De plus, le gouvernement gèrera un registre public des fournisseurs accrédités. En outre, des mesures techniques devront être développées pour empêcher l'utilisation d'applications non sécurisées et non accréditées.
La déclaration suivante, telle que publiée dans un rapport de l'Agence de l'Union européenne pour la cybersécurité (ENISA) sur l'identité numérique, souligne :
"*A wallet is the main component of the solution and is required to be certified as meeting the requirements of the regulation. A wallet is held and operated by the user. The user should be aware of downloads and use legitimate wallet applications that secure keys, identity, and identification processes. An unauthorized wallet can cause an actual security loss for the user, leading to risks that include a lack of confidentiality of their data and a possible key compromise.*"

3. Auditabilité

En raison de la nature décentralisée du système, il sera difficile de mener une enquête en cas de litige. Par conséquent, les services de police doivent être en mesure de savoir où et quand une SSI donnée a été utilisée (par exemple, dans le cadre d'une enquête sur un vol d'identité). Ceci est particulièrement important pour les émetteurs et les vérificateurs d'attributs.

4. Information et sensibilisation des citoyens

Le passé montre que les récentes initiatives concernant l'eID et le dossier électronique du patient (DEP) ont échoué en partie à cause d'un manque d'information pour les citoyens. La Confédération doit mettre en place des campagnes de communication régulières et - plus important encore - efficaces pour favoriser l'adoption par les citoyens.
En outre, comme nous passons à une approche plus décentralisée, la responsabilité se déplacera progressivement vers le citoyen lui-même. La population suisse doit donc être sensibilisée aux risques et aux responsabilités qu'implique cette évolution ! Cela doit se faire par le biais d'une communication efficace et de campagnes nationales de sensibilisation.

5. Maturité de la SSI

En tant que fournisseur de technologies et expert en cybersécurité, nous encourageons la décentralisation et la minimisation des données. Cependant, notre expérience montre que ces technologies sont à un stade très précoce et ne sont pas encore matures. C'est pourquoi nous soutenons les deux actions suivantes :

a. Éviter tout détail lié à une technologie donnée dans le texte juridique ainsi que dans l'ordonnance (par exemple, mentionner une infrastructure SSI).
b. Continuer les projets de recherche ayant pour but de vérifier la faisabilité de l'approche SSI.

En outre, nous tenons à souligner l'obligation de prendre en compte, dès le départ, de l'impact de cette décentralisation sur la sécurité.

6. Monétisation

Nous sommes d'accord, comme le souligne l'article 26, que l'eID doit être gratuite pour tous les citoyens et émetteurs. Une redevance doit être appliquée chaque fois qu'un attribut est émis ou consommé en retour.

Toutefois, il convient d'établir une distinction claire entre les attributs réglementés et non réglementés, comme le décrit également le "Règlement sur l'identité numérique européenne" :
"Avec un service distribué gratuitement et un marché libre et libéral, le risque est que le citoyen devienne l'otage de fournisseurs de technologie internationaux qui monétiseraient leurs données et violeraient la confidentialité de ces données". En effet, si c'est gratuit, l'utilisateur devient le produit. La Confédération doit mettre en place des mesures de contrôle pour éviter ce genre de développements.

7. Mode hors ligne

L'utilisation de l'eID et son processus de vérification de l'identification doivent fonctionner aussi bien en mode hors ligne qu'en mode en ligne : Dans un pays comme le nôtre, à la nature étendue et rude (Alpes), le système doit être pleinement opérationnel en mode hors ligne et ne doit en aucun cas dépendre de l'accès et de la disponibilité du réseau ! Ce point est particulièrement important car l'utilisation d'une carte d'identité électronique sera de plus en plus liée à des cas d'utilisation dans la vie réelle, où l'on ne peut pas attendre du citoyen qu'il ait accès à l'internet/au réseau.

8. Rétro-compatibilité et interopérabilité

En tant qu'IDP ayant une grande expérience en tant qu'émetteur d'identités, par exemple pour l'accès au dossier électronique du patient (EPR), nous demandons que la nouvelle loi sur l'eID prévoie et garantisse un accès continu aux identités vérifiées existantes, au moins pendant une certaine période : nous recommandons un minimum de 5 ans.
Aujourd'hui, de nombreux acteurs - comme les cantons - sont déjà des fournisseurs d'identité actifs. C'est pourquoi cette exigence est particulièrement importante, pour ne pas interrompre ou mettre en danger les efforts continus de numérisation. En outre, il n'y a et n'y aura aucune solution alternative disponible entre-temps et dans les années à venir ! Ces fournisseurs d'identité doivent être certains que le nouveau système sera interopérable. Une migration complète des identités électroniques existantes ne sera pas acceptable pour eux.
Plus important encore : il faut assurer la rétrocompatibilité avec les identités déjà certifiées utilisées dans le domaine de la santé, notamment dans le dossier électronique du patient (DEP), et éviter un nouvel enregistrement de ces citoyens.

Conclusion

Nous sommes très heureux de constater que ce sujet a gagné en importance et nous espérons que nous aurons bientôt des éclaircissements sur la voie à suivre. Nous faisons partie des acteurs du marché qui ont beaucoup investi dans ce sujet ces dernières années → eID et DEP. Nous espérons que ces efforts seront reconnus et que des entreprises comme la nôtre seront prises en compte et impliquées dans le développement du nouveau système dès que possible. Nous pensons qu'un partenariat privé-public est une bonne solution dans ce cas ! Nous vous remercions de votre temps et de votre attention.