ELCASecurity
AN ELCA COMPANY

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

Directly per email to:
rechtsinformatik@bj.admin.ch

Lausanne, October 20, 2022
CGR / SUTC

Federal Law on Electronic Proof of Identity and Other Electronic Proofs of Identity (E-ID-Gesetz, BGEID)

Response to the Consultation V1.3

Dear President Keller-Sutter
Ladies and Gentlemen

Management Summary

We thank you for the opportunity given to us to participate in this eID consultation. As ELCA Security – a daughter company of the privately owned information technology firm in Switzerland ELCA Informatique - we see our responsibility less in providing political expertise and to focus full heartedly on our cybersecurity and business expertise. We are proud to call some of the most talented developers, engineers, analysts and IT consultants of Switzerland as part of our team and it is our mission to provide our clients with the best solutions possible in the market. Hence, why we are honored to share our expertise with you.

Besides our pure cybersecurity expertise, we are also active as a recognized identity provider in Switzerland. Since more than three years we are serving public administrations, all health communities as well as private companies. Thus, we strongly believe that our eID market expertise and experience offers additionally valuable input for this consultation.

We would like to position ourselves on following eight points, in no order of priorities:

1. Backup and Critical Data Storage

Referring to article 21, a system of backup must be provided either by the Confederation itself and/or certified providers, appointed by the government. The storage of such critical data must comply with the highest level of security standards: strict regulations – certified and audited - are required to prevent security breaches and abuse.

2. Security and Controls

The Confederation is responsible and must guarantee compliance and authenticity as well as security of future wallets. Yet, as per article 14, the law would basically allow any application to store critical data. In our opinion, the law needs to clearly define the certification of applications and/or wallets. Meaning: applications must undergo specific security measures to be allowed to be used and installed. This can either be done by the government or by private providers complying with defined security, authentication and accreditation standards.
In addition, the government would operate a public register with accredited providers. In addition, technical measure would have to be developed, to prevent the usage of unsecure and not accredited applications.
Following statement, as issued in a report by the European Union Agency for Cybersecurity (ENISA) on digital identity, outlines:
"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. Auditability

Due to the decentralized nature of the system, it will be hard to perform investigation in case of dispute. Consequently, law enforcement must have the capability to see where and when a given SSI was used (e.g. for the purpose of an identity theft investigation). This is especially important for issuers and verifiers of attributes.

4. Information and Citizen Awareness

Past shows that the recent initiatives around eID and Electronic Patient Record (EPR) failed partially because of lack of targeted information to the citizen. The Confederation needs put in place regular and – even more importantly - efficient communication campaigns to enhance adoption by the citizens.
In addition, as we are moving to a more decentralized approach, the responsibility will linearly move to the citizen itself. Hence, the Swiss population must be made aware of the risks and responsibilities implicated through this move! This should occur via effective communication and national sensibilization campaigns.

5. SSI Maturity

As a technology provider and cybersecurity expert, we are encouraging decentralization and data minimization. However, our experience shows that these technologies are at a very early stage and not yet mature. Therefore we support following two actions:

a. Avoid any technology statements within the legal text as well as the ordonnance (e.g., mentioning of SSI infrastructure).
b. Continuous research projects to verify the feasibility of mentioned SII approach.

Furthermore, we would like to highlight the requirement, to take security impact of this decentralization into account from the very beginning.

6. Monetization

We agree, as outlined in article 26, that the eID must be free for all citizen and issuers. A fee should be applied wherever an attribute is issued or in return is consumed.
Yet, there should be a clear distinction between regulated and non-regulated attributes as it is also described in the "Regulation for European Digital Identity": *"With a free distributed service and a free and liberal market, the risk is that the citizen becomes a hostage of international tech providers that would monetize their data and breach data privacy."* Basically, if it's free then the user becomes the product. The Confederation must put in place control measures to avoid this kind of developments.

7. Offline Mode

The use of the eID and its identification verification process must operate equally offline as well as in online mode: In a country like ours, with extensive and rough nature (Alps), the system must be fully operational in offline mode and must in no case dependent on network access and availability! This is especially important because the foreseen usage of an eID will be more and more linked to physical real life use cases, where we cannot expect the citizen to have internet/network access.

8. Backwards Compatibility and Interoperability

As an IdP provider with extensive experience as issuer of ID e.g., for Electronic Patient Record (EPR) access, we ask that the new eID law will foresee and ensure continuous access for such existing verified identities, at least for a certain period of time: we recommend a minimum of 5 years.
Today, many actors - such as cantons - are already active identity providers. Therefore, this requirement is especially important, not to interrupt or risk continuous digitalization efforts. Also, because there are and will not be any alternative solutions available meanwhile and for the coming few years! These identity providers need to be certain that the new system will be interoperable. A complete migration of existing eID will not be acceptable for them.
Even more important: a backward compatibility with already certified identities in use within the health domain, specifically speaking the Electronic Patient Record (EPD), must be ensured and new registration of these citizens must be avoided.

Conclusion

We are very pleased to see that this subject has gained in importance and are hoping that we will have soon clarification on the way ahead.
We are part of the actors in the market, who have invested a lot in this topic in recent years → eID and EPD. Our expectation is that these efforts will be recognized and that companies, such as ours, will be considered and involved in the development of the new system as soon as possible. We believe a private-public partnership to be a good solution in this case! Thank you for your time and consideration.