ELCASecurity
AN ELCA COMPANY

Frau Bundesrätin Karin Keller-Sutter
Vorsteherin des Eidgenössischen
Justiz- und Polizeidepartementes EJPD
Bundeshaus West
3003 Bern

Direkt per E-Mail an:
rechtsinformatik@bj.admin.ch

Lausanne, 20. Oktober 2022
CGR / SUTC

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Stellungnahme zur Vernehmlassung V1.3

Sehr geehrte Frau Bundesrätin Keller-Sutter
Sehr geehrte Damen und Herren

Zusammenfassung

Wir danken Ihnen für die Möglichkeit, an dieser Vernehmlassung zur eID teilzunehmen. Als ELCA Security - eine Tochterfirma des privaten Schweizer Informatikunternehmens ELCA Informatik - sehen wir unsere Verantwortung weniger in der Bereitstellung von politischer Expertise, sondern wir konzentrieren uns voll und ganz auf unsere Cybersecurity- und Business-Fachwissen. Wir sind stolz, einige der talentiertesten Entwickler, Ingenieure, Analysten und IT-Berater der Schweiz als Teil unseres Teams zu nennen, denn es ist unsere Mission unseren Kunden die bestmöglichen Lösungen auf dem Markt zu bieten. Deshalb ist es uns eine Ehre, unser Fachwissen mit Ihnen zu teilen.
Neben unserer reinen Cybersecurity-Expertise sind wir auch als anerkannter Identity Provider in der Schweiz tätig. Seit mehr als drei Jahren betreuen wir

öffentliche Verwaltungen, alle Stammgemeinschaften sowie private Unternehmen. Wir sind daher überzeugt, dass unsere eID Marktexpertise und -erfahrung einen zusätzlichen wertvollen Input für diese Vernehmlassung bietet.

Wir möchten uns zu den folgenden acht Punkten, ohne Prioritätsreihenfolge, positionieren:

1. Sicherung und Speicherung kritischer Daten

Gemäss Artikel 21 muss ein Sicherungssystem entweder vom Bund selbst und/oder von zertifizierten und von der Regierung ernannten Anbietern bereitgestellt werden. Die Speicherung dieser kritischen Daten muss den höchsten Sicherheitsstandards entsprechen: Strenge - zertifizierte und geprüfte - Vorschriften sind erforderlich, um Sicherheitsverletzungen und Missbrauch zu verhindern.

2. Sicherheit und Kontrollen

Der Bund hat die Zuständigkeit und muss die Einhaltung und Authentizität, sowie die Sicherheit der künftigen Wallets zu garantieren. Gemäss Artikel 14 würde das Gesetz jedoch grundsätzlich jeder Applikation erlauben, kritische Daten zu speichern. Unserer Meinung nach muss das Gesetz die Zertifizierung von Applikationen und/oder Wallets klar definieren. Das bedeutet, dass Applikationen bestimmten Sicherheitsmassnahmen unterzogen werden müssen, um verwendet und installiert werden zu dürfen. Dies kann entweder durch die Regierung oder durch private Anbieter erfolgen, die bestimmte Sicherheits-, Authentifizierungs- und Akkreditierungsstandards einhalten.
Darüber hinaus würde die Regierung ein öffentliches Register mit akkreditierten Anbietern führen. Darüber hinaus müssten technische Massnahmen entwickelt werden, um die Nutzung unsicherer und nicht akkreditierter Anwendungen zu verhindern.
In einem Bericht der Agentur der Europäischen Union für Cybersicherheit (ENISA) über die digitale Identität wird folgende Erklärung abgegeben: "*Ein Wallet ist die Hauptkomponente der Lösung und muss den Anforderungen der Verordnung entsprechend zertifiziert sein. Eine Wallet wird vom Nutzer gehalten und betrieben. Der Nutzer sollte sich der Downloads bewusst sein und nur legitime Wallet-Anwendungen verwenden, die Schlüssel, Identität und Identifizierungsprozesse sichern. Ein nicht-autorisiertes Wallet kann für den Nutzer einen tatsächlichen Sicherheitsverlust bedeuten, was zu Risiken wie mangelnder Vertraulichkeit seiner Daten und einer möglichen Komprimierung seines Sicherheitsschlüssel führt.* "

3. Prüfbarkeit

Aufgrund des dezentralen Charakters des Systems wird es schwierig sein, im Streitfall Ermittlungen durchzuführen. Folglich müssen die Strafverfolgungsbehörden in der Lage sein, festzustellen, wo und wann eine bestimmte SSI verwendet wurde (z. B. zum Zwecke der Ermittlung bei Identitätsdiebstahl). Dies ist besonders wichtig für Aussteller und Prüfer von Attributen.

4. Information und Sensibilisierung der Bürger

Die Vergangenheit hat gezeigt, dass die jüngsten Initiativen rund um die eID und das elektronische Patientendossier (EPD) zum Teil daran gescheitert sind, dass die Bürgerinnen und Bürger nicht gezielt informiert wurden. Der Bund muss regelmässige und - was noch wichtiger ist - effiziente Kommunikationskampagnen durchführen, um die Akzeptanz bei den Bürgern zu erhöhen.
Da wir zu einem dezentraleren Ansatz übergehen, wird sich die Verantwortung linear auf den Bürger selbst verlagern. Die Schweizer Bevölkerung muss sich also der Risiken und der Verantwortung bewusst werden, die mit diesem Schritt einhergehen! Dies sollte durch eine effektive Kommunikation und nationale Sensibilisierungskampagnen geschehen.

5. SSI Reifegrad

Als Technologieanbieter und Cybersicherheitsexperte fördern wir die Dezentralisierung und Datenminimierung. Unsere Erfahrung zeigt jedoch, dass sich diese Technologien noch in einem sehr frühen Stadium befinden und noch nicht ausgereift sind. Daher unterstützen wir die folgenden zwei Massnahmen:

a. Vermeiden Sie sowohl im Gesetzestext als auch in der Verordnung jegliche Technologieaussagen (z.B. Erwähnung der SSI-Infrastruktur).
b. Fortlaufende Forschungsprojekte zur Überprüfung der Durchführbarkeit des genannten SII-Konzepts.

Darüber hinaus möchten wir auf die Notwendigkeit hinweisen, die Sicherheitsauswirkungen dieser Dezentralisierung von Anfang an zu berücksichtigen.

6. Monetarisierung

Wir stimmen zu, dass die eID, wie in Artikel 26 dargelegt, für alle Bürger und Aussteller kostenlos sein muss. Eine Gebühr sollte überall dort erhoben werden, wo ein Attribut ausgegeben oder im Gegenzug erfragt wird.
Dennoch sollte es eine klare Unterscheidung zwischen regulierten und nicht regulierten Attributen geben, wie sie auch in der "Verordnung zur europäischen digitalen Identität" beschrieben wird:
"Bei einem frei verteilten Dienst und einem freien und liberalen Markt besteht die Gefahr, dass der Bürger zu einer Geisel internationaler Technologieanbieter wird, die seine Daten zu Geld machen und den Datenschutz verletzen würden."
Grundsätzlich gilt: Wenn es kostenlos ist, wird der Nutzer zum Produkt.
Der Bund muss Kontrollmassnahmen ergreifen, um solche Entwicklungen zu vermeiden.

7. Offline-Modus

Die Nutzung der eID und der Prozess der Identitätsüberprüfung müssen sowohl im Offline- als auch im Online-Modus funktionieren: In einem Land wie dem unseren, mit weitläufiger und rauer Natur (Alpen), muss das System im Offline-Modus voll funktionsfähig sein und darf auf keinen Fall vom Netzzugang und dessen Verfügbarkeit abhängig sein! Dies ist besonders wichtig, weil die vorgesehene Nutzung einer eID immer mehr mit realen Anwendungsfällen verbunden sein wird, bei denen wir nicht erwarten können, dass der Bürger Zugang zum Internet/Netzwerk hat.

8. Abwärtskompatibilität und Interoperabilität

Als IdP-Anbieter mit umfassender Erfahrung in der Ausstellung von Ausweisen, z. B. für den Zugang zum elektronischen Patientendossier (EPD), fordern wir, dass das neue eID-Gesetz einen kontinuierlichen Zugang für solche bestehenden verifizierten Identitäten vorsieht und sicherstellt; zumindest für einen bestimmten Zeitraum. Wir empfehlen mindestens 5 Jahre.
Viele Akteure - wie z.B. die Kantone - sind heute bereits aktive Identitätsanbieter. Deshalb ist diese Anforderung besonders wichtig, um die laufenden Digitalisierungsbemühungen nicht zu unterbrechen oder zu gefährden. Auch, weil es in der Zwischenzeit und in den nächsten Jahren keine alternativen Lösungen gibt und geben wird! Diesen Identitätsanbieter muss zugesichert sein, dass das neue System interoperabel sein wird. Eine vollständige Migration der bestehenden eID wird für sie nicht akzeptabel sein.
Noch wichtiger ist, dass eine Rückwärtskompatibilität mit bereits zertifizierten Identitäten, die im Gesundheitsbereich, insbesondere dem elektronischen

Patientendossier (EPD), verwendet werden, gewährleistet und eine Neuregistrierung dieser Bürger vermieden werden muss.

Schlussfolgerung

Wir freuen uns sehr, dass dieses Thema an Bedeutung gewonnen hat, und hoffen, dass wir bald Klarheit über das weitere Vorgehen haben werden.
Wir gehören zu den Akteuren auf dem Markt, die in den letzten Jahren viel in dieses Thema investiert haben → eID und EPD. Wir erwarten, dass diese Anstrengungen anerkannt werden und dass Unternehmen wie unseres so bald wie möglich in die Entwicklung des neuen Systems miteinbezogen werden. Wir glauben, dass eine privat-öffentliche Partnerschaft in diesem Fall eine gute Lösung ist! Wir danken Ihnen für Ihre Zeit und Ihre Bemühungen.