/SSS information security society switzerland

Bundesamt für Justiz
Direktionsbereich Zentrale Dienste
Fachbereich Rechtsinformatik
3003 Bern

Bern, den 20.10.2022

Vernehmlassung ISSS zum neuen E-ID Gesetz BGEID

Sehr geehrte Damen und Herren

Gerne nehmen wir Stellung zum zweiten Vorschlag der Bundesverwaltung (Bundesamt für Justiz) über das E-ID Gesetz (BGEID).

Vorstellung Taskforce E-ID ISSS

Die Information Security Society Switzerland (ISSS) http://www.isss.ch ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1'100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander.

ISSS wurde 1993 als Verein gegründet und ist Mitglied von Digitalswitzerland sowie offizieller Security Fachpartner von SwissICT und ASUT. Mit unseren Mitgliedern arbeiten wir in Taskforces, um Fachexpertise gezielt abzuholen und der Öffentlichkeit zur Verfügung zu stellen. Auch vorliegende Stellungnahme wurde in einer Taskforce erarbeitet:

Taskforce Lead ISSS
Walder, Dario – Team Leader Redguard, Vizepräsident ISSS
Beranek Zanon, Nicole – Juristin HÄRTING Rechtsanwälte AG, ISSS-Vorstand
Juristen
Lehmann, Beat – Jurist, ISSS-Vorstand
Talleri, Rocco – Jurist Spezialgebiet Cyber Security, Talleri Law Studio legale
Zbinden, Reto – Jurist, Swiss Infosec
Organisationen & Fachexperten
Laube, Annett – Dozentin, Berner Fachhochschule
Monika Stucki – Senior Consultant, Redguard AG
Rickenbacher, Fridel – Senior Consultant / Investor, Swiss IT Security AG

Nachdem das Volk den ersten Gesetzesentwurf zur E-ID am 07.03.2021 deutlich abgelehnt hat, sind wir grundsätzlich erfreut zu hören, dass sich mit dem neuen Entwurf zum Bundesgesetz zur E-ID einiges zum Positiven hinbewegt hat. So nehmen wir beispielsweise mit Freude zur Kenntnis, dass die Infrastruktur neu durch das Bundesamt für Justiz (staatliche Vertrauensinfrastruktur) sichergestellt wird. Ausserdem bekennt sich der Bundesrat mit dem neuen BGEID zu drei wichtigen Grundsätzen zum Schutz der Persönlichkeit und der Grundrechte von Personen (Schutzes der Privatsphäre durch Technik «privacy by design», der Datensparsamkeit und der dezentralen Datenspeicherung). Auch freuen wir uns,

dass bei der Erstellung des neuen Gesetzesentwurfs ein partizipativer Ansatz verfolgt wird, durch den die Mitarbeit durch regelmässige Informationssitzungen[1] und auch ein entsprechendes Gitlab-Projekt[2] sichergestellt werden.

Trotzdem möchten wir auf weitere wichtige Security- und Privacy-Aspekte hinweisen, die aus unserer Sicht bei der Umsetzung der E-ID mitberücksichtigt werden sollen.[3] Dabei möchten wir an dieser Stelle insbesondere auf die Arbeiten im Rahmen der EU verweisen.[4] Aus unserer Sicht ist anzustreben, dass das BGEID heute oder in Zukunft dem harmonisierten Recht der digitalen Identität im EWR so weit als möglich entspricht: Es sollte die auch im Kommissionsvorschlag erwähnte ”Aequivalenz” mit dem harmonisierten europäischen Recht der Digitalen Identität angestrebt werden - wie das im bisherigen und neuen Datenschutzrecht, oder der Übernahme der Regelung der EU über Produktehaftung erreicht wurde.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz in unserem Lande leisten können und danken Ihnen für die Berücksichtigung unserer Anregungen.

Stellungnahme zum neuen BGEID

- Art. 1 Abs. 2c beschreibt den Zweck des BGEID, dass die E-ID und die Vertrauensinfrastruktur dem aktuellen Stand der Technik entsprechen. Wir verstehen darunter auch, dass die Vertrauensinfrastruktur regelmässigen Sicherheitsprüfungen (Audit und/oder Pentest, inkl. allenfalls auch Second und Third Opinion) unterzogen werden muss zugunsten einer maximierten Angriffs- und Betriebs-Sicherheit in der immer dynamischer werdenden Bedrohungslage. Dies sollte bereits hier im Gesetz stehen (z.B. security & privacy by design, zero trust principle, need to know) und nicht erst nachträglich und zu einem späteren Zeitpunkt adressiert werden.
- Auch sehen wir es als notwendig, dass neben regelmässigen Sicherheitsprüfung die Vertrauensinfrastruktur Sicherheitszertifiziert wird (z.B. ISO 27001, NIST, COBIT, ITIL, ISACA). Mit auch entsprechendem Business Continuity Planning, Incident Response Planning zur Optimierung der Resilienz.
- Im Rahmen von nationalen Kampagnen und auch den Tätigkeiten im Zentrum NCSC wäre die weitere bzw. weitergehende Cybersecurity Sensibilisierung der Bevölkerung bzw. der Anwender der E-ID eine flankierend sinnvolle Massnahme im Umgang mit der digitalen Identität.
- Alle an der E-ID involvierten Akteure sollen entsprechend der Verordnung über die Datenschutzzertifizierungen (VDSZ[5]) zertifiziert sein. Als Beispiel dient hier Art. 59a 832.102, Verordnung über die Krankenversicherung (KVV): "Jeder Versicherer muss über eine Datenannahmestelle verfügen. Diese muss nach Artikel 11 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz zertifiziert sein."

- Art. 18 Abs. 2,3 stellt die Rolle des Bundes und Bundesrates betreffend Zurverfügungstellung von Systemen, Bestätigungen und Abfragen im System dar. Wir beurteilen es als notwendig, dass hier keine "kann-Formulierungen" sondern eine "muss-Formulierung" verwendet wird:
-
    - [2] Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund auch die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bestätigt.

[1] Swiss E-ID Ecosystem - https://github.com/e-id-admin (Stand 03.09.2022)
[2] Website des Bundesamts für Justiz – Partizipationsmöglichkeiten rund um die E-ID - https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/partizipationsmoeglichkeiten.html (Stand 03.09.2022)
[3] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-85476.html
[4] E-IDAs Verordnung (EU) Nr. 910/2014) https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX%3A32014R0910&from=BG sowie COM(2021)281 final vom 3.6.2021 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0281&from=DE
[5] der Verordnung über die Datenschutzzertifizierungen (VDSZ) https://www.fedlex.admin.ch/eli/cc/2007/701/de (Stand 23.09.2022)

- [3] Alle Behörden und Privaten ~~können~~ müssen die Zuordnungen durch Abfragen im System überprüfen.

-
- Gleiches gilt auch für Art., 20
  - Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund eine Anwendung zur Verfügung stellt, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können.

-
- Gleiches gilt auch für Art. 21 Abs. 1
  - Der Bundesrat ~~kann~~ muss vorsehen, dass der Bund ein System zur Verfügung stellt, dem die Inhaberinnen und Inhaber Sicherheitskopien ihrer elektronischen Nachweise zur Aufbewahrung übergeben können.

- Art. 25. Abs. 2 E-ID-Gesetz verursacht einerseits eine Normenkollision mit der Datenschutzgesetzgebung (im Rahmen von Bst. c), indem bis zum „Inkrafttreten der gesetzlichen Grundlage" eine rein materiellrechtliche Grundlage auch bei Bearbeitung besonders schützenswerter Personendaten ohne Weiteres genügen soll (ohne dass somit bis dann die für eine materielle Rechtsgrundlage geltenden Einschränkungen gelten, nämlich dass die Bearbeitung für eine in einem Gesetz im formellen Sinn festgelegte Aufgabe unentbehrlich zu sein hat oder der Bearbeitungszweck für die Grundrechte der betroffenen Person keine besonderen Risiken zu bergen hat (Art. 34 Abs. 3 nDSG)). Ein Widerspruch mit der Datenschutzgesetzgebung und eine Aufweichung der Grundrechte der betroffenen Personen ist zu vermeiden und verträgt sich ausserdem schlecht mit dem programmatischen Bekenntnis im E-ID-Gesetz selbst zur Datensparsamkeit (Art. 1 Abs. 2 E-ID-Gesetz).

- Weiter ist Art. 25. Abs. 2 E-ID-Gesetz potenziell verfassungswidrig: Nach Art. 36 Abs. 1 BV müssen schwerwiegende Einschränkungen von Grundrechten im (formellen) Gesetz selbst vorgesehen sein. Ausgenommen sind nur Fälle ernster, unmittelbarer und nicht anders abwendbarer Gefahr.

- Art. 25. Abs. 2 E-ID-Gesetz schafft ausserdem mehrfach unnötige Rechtsunsicherheit: Die Bestimmung enthält lediglich eine Aussage dazu, wann zusätzliche Vorgaben des Bundesrates zur Anpassung der Vertrauensinfrastruktur ausser Kraft treten sollen, nämlich dann, wenn eine rechtstaatlich solidere Rechtsgrundlage erreicht ist. Ihrem Wortlaut nach kann der Bestimmung aber nicht entnommen werden, dass entsprechende Vorgaben des Bundesrates Vorrang haben sollen gegenüber Art. 34 nDSG. Art. 25 Abs. 2 Bst. c E-ID-Gesetz lässt mit der Erwähnung der „gesetzlichen Grundlage" ausserdem offen, ob damit wirklich eine formellrechtliche (von der Legislative verabschiedete Vorgaben) verlangt wird oder eine materiellrechtliche Grundlage letztlich genügend könnte, was wiederum aus grundrechtlicher Perspektive äusserst bedenklich wäre und noch dazu im diametralen Widerspruch zur Datenschutzgebung.

- Schliesslich halten wir die Regelung in Art. 25. Abs. 2 E-ID-Gesetz für verzichtbar, weil die Datenschutzgesetzgebung auf Bundesebene bereits Bestimmungen enthält zur automatisierten Datenbearbeitung mit besonders schützenswerten Personendaten im Rahmen von Pilotversuchen (Art. 35 nDSG)

- Aus all diesen Gründen regen wir die ersatzlose Streichung von Art. 25. Abs. 2 E-ID-Gesetz an. Dies nicht zuletzt auch deshalb, um damit nicht die gesamte Vorlage einem erhöhten Risiko auszusetzen, im Rahmen der parlamentarischen Beratungen Schiffbruch zu erleiden.

Datenschutz:

- Der Vorschlag, die AHV-Nummer als integrierten Bestandteil der Digitalen Identität aufzunehmen,

Information Security Society Switzerland (ISSS) - Kochergasse 6 - 3011 Bern - sekretariat(at)isss.ch - +41 31 311 53 00

kann einen Verstoss gegen elementare Grundsätze des Datenschutzes darstellen. Denn damit droht durch die Spur, die jeder Einsatz der E-ID durch den Benützer notwendigerweise hinterlässt, die Gefahr einer Kontrolle seines Verhaltens und bewirkt ein verpöntes Profiling im Sinne von Art. 5 Bst. f) und g) revDSG 2020.

- Die Verknüpfung der E-ID mit einem universellen Mitteln zur Identifikation von Personen ist im harmonisierten europäischen Recht verboten, denn es schafft die Grundlage für die umfassende Kontrolle des Verhaltens von Personen, wie dies heute in technologisch weit entwickelten autoritären Staaten (z.B. China) realisiert ist.
- Im Weiteren stellt die Beschränkung des BGEID auf bestimmte Kategorien amtlich registrierter natürlicher Personen, möglicherweise eine Verletzung von Art. 6 der Allgemeinen Erklärung der Menschenrechte der Vereinten Nationen dar und weicht ebenfalls vom harmonisierten europäischen Recht ab.

Inputs zum erläuternden Bericht zur Eröffnung des Vernehmlassungsverfahrens

- Art 14 - Hier wird erwähnt, dass man die E-ID nur auf einem einzigen Gerät installieren kann. Das wäre eine Einschränkung der Verwendung (was genau wären die Probleme damit?).
- Art. 15 Abs. 1 Hier soll geregelt werden, wie im Delegationsfall (z.B. bei Ausnahmefällen / Notfällen – siehe z.B. auch beim ePD-Notfall-Zugang) vorgegangen werden soll. Genau da muss man ja, die E-ID einer Drittperson überlassen.
- Art. 15 Abs. 2 Ein grundsätzliches Problem ist die Wiederherstellung von privaten Schlüsseln (Key Recovery), die es ja nur einmal geben darf und damit Sicherheitskopien und das Wiederherstellung eigentlich verunmöglichen. (siehe auch Art 21)
- Art. 17 und 18 es ist nicht klar, warum Aussteller und Verifikationen ihre Identifikatoren erst selbst in Basisregister eintragen können und dann ein System zur Bestätigung der Identifikatoren gebaut wird. Hier wird auch im Gegensatz zum Rest der Dokumente auf sehr tiefem technischen Niveau argumentiert
- Art. 17 Abs. 4: «Das Basisregister enthält keine Daten über die einzelnen elektronischen Nachweise mit Ausnahme über deren Widerruf.» Das könnte Auswirkungen auf die Privacy des Holders haben, in den Fällen, wenn allein der Besitz oder die Revokation eines Nachweises eine sensible Information darstellt, z.B. Mitgliedschaft in einer religiösen Gemeinschaft. Hier muss man sehr sorgfältig schauen, wie ein einzelner Nachweis referenziert wird.

Mit freundlichen Grüssen

ARIÉ MALZ
CO-PRÄSIDENT

DARIO WALDER
VIZE-PRÄSIDENT

Information Security Society Switzerland (ISSS)
Zentweg 13, 3006 Bern
E-Mail: president@isss.ch
E-Mail: vicepresident@isss.ch