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

Die Grundsätze des Vorentwurfs des neuen E-ID Gesetzes, wie Privacy by Design, Datensicherheit und Datensparsamkeit, sind sehr zu begrüssen. Die Beachtung dieser Grundsätze erlaubt eine Minimierung der Datenflüsse und gewährt den Inhaber*innen zusätzliche Kontrolle über ihre Daten.

Wir werden auf folgende Punkte eingehen, die wir bezüglich der Informationssicherheit und der technologieneutralen Formulierung des E-ID Gesetzes als wichtig erachten:

- Das Gesetz sollte die Funktionalität und Sicherheit der E-ID, anderer elektronischer Nachweise und deren Infrastruktur beschreiben und nicht die Architektur für die Implementierung dieser Infrastruktur.
- Sicherheitsbeweise, formale Spezifikationen und formale Sicherheitsanforderungen sind notwendig, um einen hohen Sicherheitsstandard zu gewährleisten.
- Wir beleuchten Aspekte, die bei der Ausstellung der E-ID abzuwägen sind und schlagen die Einführung einer Opt-Out-Funktion vor.
- Wir weisen auf weitere Punkte hin, die im Zusammenhang mit dem Schutz der Privatsphäre zu beachten sind.

Definieren der Funktionalität und Sicherheit anstatt der Implementierungsarchitektur

Im Vorentwurf wird definiert, dass die Vertrauensinfrastruktur aus fünf Komponenten[1] besteht. Dabei wird der Funktions- und Sicherheitsspezifikationen des Systems zu wenig Aufmerksamkeit geschenkt und stattdessen eine Architektur vorgeschrieben, die die technischen Realisierungsmöglichkeiten unnötig einschränkt. Eine grösstenteils funktionale und sicherheitsbezogene Spezifikation hingegen würde sowohl zu besseren Sicherheitsgarantien als auch zu mehr Flexibilität führen.

Funktions- und Sicherheitsspezifikationen sind notwendig, um eine Implementierung zu evaluieren. Wird ein System nur mit einer Spezifikation ihrer Architektur verglichen, kann zwar evaluiert werden, ob das System die vorgegebene Struktur hat, nicht aber ob es korrekt funktioniert. Ohne Funktions- und Sicherheitsspezifikationen ist es nicht klar, welche Verhaltensweisen von einer Implementierung erwartet werden und welche nicht erlaubt sind. Wird eine potenzielle Sicherheitslücke oder ein möglicher Bug gefunden, ist nicht klar, ob das gefundene Verhalten unerwünscht ist oder nicht. Bei der Entwicklung eines Systems sollten also die Architektur und die Technologien aufgrund von zuvor verfassten Funktions- und Sicherheitsspezifikationen gewählt werden. Da das E-ID-Gesetz die Grundlage für die Entwicklung eines solchen Systems sein soll, sollte es als Grundlage für die Funktions- und Sicherheitsspezifikationen dienen und nicht eine Architektur beschreiben.

1 Nämlich: das Basisregister (Art. 17), das System zur Bestätigung von Identifikatoren (Art. 18), eine Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen (Art. 19), eine Anwendung zur Prüfung von elektronischen Nachweisen (Art. 20) und ein System für Sicherungskopien (Art. 21).

Im Vorentwurf wird zum Beispiel das Basisregister als architektonische Komponente beschrieben. Es beinhaltet Daten über die Austellerinnen, Verifikatorinnen und zu widerrufenen Nachweisen. Diese Daten müssen jedoch nicht notwendigerweise in derselben Komponente enthalten sein. Es könnte sich auch um mehrere Komponenten handeln, je nachdem, welche Technologien und Architektur gewählt werden.

Somit ist der Vorentwurf zu konkret und zu strikt. Die Wahl der Technologie und der Architektur des Systems würde bereits von vorgeschriebenen Architekturkomponenten abhängen. Dies könnte gute Lösungen verhindern oder verkomplizieren und widerspricht der vom Vorentwurf angestrebten Technologieneutralität.

Insbesondere sollte das Gesetz die Anforderungen an die Vertrauensinfrastruktur regeln und nicht deren Architektur. Diese Anforderungen sollen die Funktionen und die Sicherheitseigenschaften des Systems beschreiben, etwa: Wem werden welche Daten zur Verfügung gestellt, welche Daten sollen zum Schutz der Privatsphäre geheim bleiben oder fälschungssicher sein.

Beispielsweise könnten die Daten über den Widerruf von elektronischen Nachweisen im Basisregister folgendermassen als Funktionalität mit assoziierten Sicherheitseigenschaften beschrieben werden:

> Für das Verifizieren von Nachweisen stellt die Vertrauensinfrastruktur eine Funktion zur Verfügung, die bestätigt, dass ein bestimmter Nachweis nicht widerrufen wurde.
>
> - Dieser Prozess soll die Privatsphäre der Inhaber*in des Nachweises möglichst gut schützen.
> - Bei diesem Prozess dürfen die Verifikatorin, die den Nachweis verifiziert, die Inhaber*in dieses Nachweises, die Ausstellerin des Nachweises und die Vertrauensinfrastruktur involviert sein.
> - Die Ausstellerin darf die Identität der Verifikatorin und die vorgewiesenen Daten nicht erfahren.
> - Die Verifikatorin darf nur erfahren, ob der Nachweis widerrufen wurde, sowie auf die Daten Zugriff erhalten, die die Inhaber*in vorweisen will.
> - Auch darf die Betreiberin der Vertrauensinfrastruktur nichts über den Inhalt des Nachweises oder deren Inhaber*in lernen.
> - Falls nötig, darf die Vertrauensinfrastruktur Daten zu widerrufenen Nachweisen speichern, wie zum Beispiel Identifikatoren von widerrufenen Nachweisen.

Diese Beschreibung ist zwar länger als die Beschreibung der widerrufenen Nachweise im Vorentwurf, gleichzeitig aber viel flexibler formuliert. Beispielsweise wäre ein interaktiver Null-Wissen-Beweis (Zero-Knowledge-Proof) ähnlich wie bei E-Voting-Protokollen möglich, bei dem die Inhaber*in Nachrichten von der Verifikatorin an die Ausstellerin weiterleitet. Ein solcher Zero-Knowledge-Proof würde dann das Verknüpfen zweier Vorweisungen desselben Nachweises verhindern, was zum Datenschutz beiträgt. Eine solche interaktive Lösung ist im Vorentwurf nicht vorgesehen, da die Ausstellerin keine Kenntnis vom Vorweisen haben darf. Gleichzeitig erlaubt die obige Beschreibung eine Lösung mit einem Basisregister, wie im Vorentwurf definiert.

Das Beschreiben funktionaler Anforderungen und Sicherheitseigenschaften anstelle der Architektur ermöglicht also mehr Flexibilität bei der Wahl der Technologien und dem Design des Systems. So kann die Vertrauensinfrastruktur ohne Gesetzesänderungen an zukünftige technologische Entwicklungen angepasst werden. Ausserdem ist mit solchen Anforderungen viel klarer geregelt, wie sich ein System verhalten soll.

Anmerkung: Dies betrifft nur die Komponenten der Vertrauensinfrastruktur, nicht aber die Unterscheidung zwischen der Vertrauensinfrastruktur und dem Informationssystem des Fedpol. Da diese beiden Systeme von unterschiedlichen Stellen betrieben werden, ist eine Trennung sinnvoll. Somit bleiben die Daten für die Ausstellung der E-ID beim Fedpol und die Daten, die zur Betreibung der Vertrauensinfrastruktur benötigt werden, bei der Betreiber*in der Vertrauensinfrastruktur.

Notwendigkeit von Sicherheitsbeweisen

Die Sicherheit der E-ID ist zentral. So ging aus der öffentlichen Konsultation hervor: «Um Vertrauen in die E-ID zu entwickeln, fordert die Mehrheit (35) eine hohe Sicherheit der E-ID und des damit genutzten Systems.» Um die Sicherheit eines Systems zu gewährleisten, müssen Sicherheitseigenschaften definiert und bewiesen werden. Im Vorentwurf werden solche Sicherheitsbeweise jedoch nicht erwähnt.

Sicherheitsbeweise oder Konformitätsbeweise werden gemäss VEleS für das E-Voting verlangt. Sicherheitsbeweise sind auch für die E-ID und deren Infrastruktur sinnvoll. E-Voting und E-ID verlangen beide, dass ein grosses Vertrauen in die jeweiligen Systeme besteht. Selbstverständlich unterscheiden sich E-Voting und E-ID in ihren Sicherheitsanforderungen. Jedoch spricht nichts dafür, dass bei der E-ID die Einhaltung niedrigerer Sicherheitsstandards ein ausreichendes Vertrauensniveau gewährleisten würde. Sowohl beim E-Voting als auch der E-ID sollen koordinierte, grossflächige Angriffe verhindert werden. Zusätzlich können bei der E-ID einzelne Identitätsdiebstähle für die Geschädigten verheerend sein; dies betrifft sowohl die Personen, deren Identität gestohlen oder gefälscht wurde, als auch die getäuschten Verifikatorinnen. Somit müssen eine E-ID und deren Infrastruktur mindestens ähnliche Sicherheitsstandards wie ein E-Voting-System erfüllen.

Es stellt sich ausserdem die Frage, ob das Konzept der Sicherheitsbeweise auf eine E-ID und andere elektronische Nachweise überhaupt anwendbar ist. Im Gegensatz zu einem E-Voting-Protokoll handelt es sich bei der E-ID, den anderen elektronischen Nachweisen, der Vertrauensinfrastruktur und dem System des Fedpol nicht um ein *einzelnes* Protokoll. Daher wird es vermutlich nicht sinnvoll oder möglich sein, alle Komponenten in einem Beweis zu verifizieren. Es wäre jedoch möglich, für einzelne Komponenten, Protokolle und Zertifikate symbolische und/oder kryptographische Beweise durchzuführen. Die genauen Anforderungen an solche Beweise müssten wohl ähnlich wie für das E-Voting auf Verordnungsstufe geregelt werden.

Um Sicherheitsbeweise durchzuführen, müssen zuerst die Sicherheitsanforderungen formal definiert werden. Diese Anforderungen können Eigenschaften wie Unfälschbarkeit von Nachweisen, Untraceability oder die Geheimhaltung von privatem Schlüsselmaterial beinhalten. Weiterhin wird eine formale Spezifikation des Systems benötigt, zum einen, um die Sicherheitseigenschaften der Spezifikation zu beweisen, zum anderen, um zu überprüfen, dass sich die Implementierung an die Spezifikation hält. Zu diesem Zweck können Code-Reviews durchgeführt und Programmverifikationstechniken angewendet werden. Eine formale Spezifikation und formale Sicherheitsanforderungen sind also nicht nur mit Blick auf Sicherheitsbeweise, sondern für jede Art von Sicherheitsüberprüfung essenziell. Wenn ein potenzieller Bug oder eine mögliche Sicherheitslücke gefunden wird, ist ohne formale Spezifikation und ohne formale Sicherheitsanforderungen nicht klar, ob das gefundene Verhalten unerwünscht ist oder nicht.

Flexibilität und Sicherheit des Ausstellungsprozesses

Der Ausstellungsprozess der E-ID, insbesondere die Verifikation der Identität der antragstellenden Person, ist extrem sicherheitskritisch. Bisher wurde vorgeschlagen, den Ausstellungsprozess digital und mithilfe einer App umzusetzen. In den Partizipations-Meetings und auf GitHub gab dieses Thema Anlass zu intensiven Diskussionen. Es wurden Bedenken geäussert, dass eine rein digitale Lösung im Vergleich zu einer Lösung, bei der das physische Erscheinen vorausgesetzt wird, nicht gleich starke Sicherheitseigenschaften garantieren kann. Gegen das persönliche Erscheinen sprechen die benötigten Ressourcen und die verringerte Benutzerfreundlichkeit. Diese Aspekte müssen gegeneinander abgewogen werden. Dabei ist es wichtig, wie oben erwähnt, die Sicherheitseigenschaften der gewählten Lösung formal zu definieren. Alternativ könnte, wie beispielsweise von der europäischen eIDAS-Richtlinie[2] vorgesehen, zwischen verschiedenen Identitätssicherungsniveaus (*assurance levels*) mit unterschiedlichen Anforderungen an den Ausstellungsprozess unterschieden werden.

Art. 14 verlangt, dass die Inhaber*in das Mittel zur Aufbewahrung selbst wählen kann. Dies ermöglicht eine grössere Kontrolle der Inhaber*in über ihre Daten. Die bisherigen vorgeschlagenen Ausstellungsprozesse sind aber ausschliesslich an eine Smartphone-App gekoppelt. Wenn, wie vorgeschlagen, die E-ID an das Smartphone gekoppelt würde, könnten keine anderen technischen Mittel, wie z.B. Desktop-Applikationen, Hardware-Wallets oder USB-Sticks, gewählt werden. Wird also festgelegt, dass die E-ID an ein Smartphone gekoppelt wird, würde dies dem aktuellen Vorentwurf widersprechen. Hierbei gilt es erneut zwischen der Kontrolle der Inhaber*innen über ihre Daten, den Sicherheitsgarantien der einzelnen Lösungen und der Benutzerfreundlichkeit abzuwägen.

Personen, die keine E-ID beantragen, könnten befürchten, dass jemand sich in ihrem Namen eine E-ID ausstellt. Diese Sorge könnte deutlich gemindert werden, wenn eine Opt-Out-Funktion eingeführt würde: Personen, die keine E-ID möchten, könnten sich auf eine Liste setzen lassen, die die Ausstellung von E-IDs im Namen dieser Person verhindert. Somit könnten diese Personen auch beweisen, dass eine E-ID in ihrem Namen gefälscht wurde.

Privatsphäre

Der Schutz der Privatsphäre ist ein wichtiges Recht (Art. 13 BV), das mit dem Grundsatz Privacy by Design im Vorentwurf des E-ID Gesetzes verankert ist. Dabei sollte zwischen Situationen unterschieden werden, in denen die Identität der Inhaber*in entscheidend ist, zum Beispiel beim Eröffnen eines Bankkontos, und Situationen, in denen nur einzelne Attribute relevant sind, zum Beispiel bei einer Alterskontrolle. Im ersten Fall wird die Identität übermittelt. Im zweiten Fall kann die Anonymität der Inhaber*in entscheidend sein.

Zu beachten ist, dass auch aus anonymisierten Daten Informationen gewonnen werden können. Zum Beispiel: Würde der Identifier der E-ID immer mitgesendet, um zu überprüfen, dass sie nicht widerrufen wurde, könnten zwei unabhängige Verifikationsinteraktionen mit derselben E-ID verknüpft werden. Eine Methode zur Überprüfung der Gültigkeit einer E-ID sollte also keine solchen Identifikatoren preisgeben.

2 Siehe eIDAS, insb. Art. 8 „Sicherheitsniveaus elektronischer Identifizierungssysteme".

Die Daten in einem elektronischen Nachweis werden von der Ausstellerin authentifiziert. Im Fall der E-ID bestätigt also das Fedpol die Validität der Daten. Damit sind diese Daten viel wertvoller, als beispielsweise Daten aus einem Freitextfeld. Zwecks der Datenminimierung sollte deshalb verhindert werden, dass bei jeder digitalen Interaktion ein elektronischer Nachweis verlangt wird. Dies sollte durch das Datenschutzgesetz gegeben sein. Sowohl die Inhaber*innen der Daten, also auch die Verifikatorinnen und Ausstellerinnen sollten darauf sensibilisiert werden.

Art. 16 enthält einen wichtigen Punkt zum Schutz der Privatsphäre: Inhaber*innen sollen entscheiden, welche Bestandteile des Nachweises übermittelt werden. In bisherigen proof-of-concept Wallets gibt die Verifikatorin vor, was übermittelt werden soll. Dies ist benutzerfreundlicher, da die Inhaber*in die zu übermittelnden Daten nicht einzeln auswählen muss. Es ist jedoch problematisch, wenn der Inhaber*in keine Möglichkeit gegeben wird, diese Auswahl explizit zu bestätigen oder zu ändern. Zur Wahrung der Privatsphäre muss ein einheitlicher Prozess festgelegt werden, in dem die Inhaber*in die Auswahl der zu übermittelnden Daten im Voraus bestätigen bzw. ändern kann.

Erklärung: Diese Antwort stellt ausschliesslich die Auffassung der Unterzeichnenden dar und ist nicht als Stellungnahme der ETH Zürich zu verstehen.

Xenia Hofmeier

Xenia Hofmeier ist Doktorandin am Institut für Informationssicherheit der ETH Zürich. Ihre Forschungsinteressen beinhalten das Analysieren von Sicherheitsprotokollen mit formalen Methoden und automatisierten Tools.

François Hublet

François Hublet ist Doktorand am Institut für Informationssicherheit der ETH Zürich. Seine Forschungsinteressen umfassen Privacy by Design, Datenschutzregelungen und formale Methoden.

Dr. Christoph Sprenger

Christoph Sprenger ist leitender wissenschaftlicher Mitarbeiter und Dozent am ETH Institut für Informationssicherheit. Er forscht im Bereich von formalen Methoden zur Spezifikation und Verifikation der Korrektheit und Sicherheit von verteilten Systemen im Allgemeinen und von Sicherheitsprotokollen im Speziellen.