



Bern, Datum der digitalen Signatur

An die Mitglieder des Bundesrates

Aussprachepapier

Technologie-Entscheid für die initiale Umsetzung der E-ID-Vertrauensinfrastruktur

1. Ausgangslage

Am 26. Mai 2021 (EXE 2021.0983) beauftragte der Bundesrat das EJPD, in Zusammenarbeit mit dem EFD und der BK, eine Lösung für eine sichere staatliche elektronische Identifizierung zu erarbeiten. Auch sechs gleichlautende Motionen (21.3124, 21.3125, 21.3126, 21.3127, 21.3128, 21.3129) aus allen Fraktionen verlangen ein staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität (E-ID).

Bei der Umsetzung sollen insbesondere die Grundsätze «Datenschutz durch Technik» (Privacy by Design), Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Benutzerinnen und Benutzer) eingehalten werden. In der Vernehmlassung zum Vorentwurf des Gesetzes wurde nebst hohen Anforderungen an den Datenschutz auch die internationale Interoperabilität deutlich gefordert. Zudem wurde gewünscht, auf einen «Swiss Finish» zu verzichten.

Wegen des innovativen Charakters des Unterfangens wurden vom Projektteam von Beginn an verschiedenste Stakeholder und die breite Fachöffentlichkeit eingebunden. Am 22. November 2023 (EXE 2023.1280) hat der Bundesrat die Botschaft zum E-ID-Gesetz verabschiedet.

Der Nationalrat hat dem Entwurf zum E-ID-Gesetz am 14. März 2024 in der Gesamtabstimmung mit 175 zu 12 Stimmen bei 2 Enthaltungen zugestimmt. Der Ständerat hat dem Entwurf zum E-ID-Gesetz am 10. September 2024 mit 43 zu 1 (ohne Enthaltung) zugestimmt. Die RK-N hat am 17. Oktober 2024 die Differenzbereinigung durchgeführt. Die Schlussabstimmung beider Räte wird voraussichtlich in der Winter-session 2024 erfolgen.

Das EJPD hat dem Bundesrat am 14. Juni 2024 eine erste Informationsnotiz zum Technologie-Entscheid zur Kenntnis gebracht (EXE 2024.1378). Darin wurde festgehalten, dass zusätzliche Abklärungen für einen Entscheid erforderlich sind. Insbeson-



dere ging es darum, die Optionen «technische Interoperabilität mit der EU», «zusätzlicher Schutz der Privatsphäre» und «Unterstützung beider Optionen» genauer zu evaluieren, und zwar mit Blick auf technische Fragen und die finanziellen Auswirkungen.

2. Ergebnisse der zusätzlichen Abklärungen

Die zusätzlichen Abklärungen haben ergeben, dass die Option «zusätzlicher Schutz der Privatsphäre» mit unterschiedlichen Ansätzen umgesetzt werden kann. Dabei geht es insbesondere um die Frage der Unverknüpfbarkeit (unlinkability) von elektronischen Nachweisen. Diese Eigenschaft hat beispielsweise dann eine Bedeutung, wenn mit der E-ID ein Altersnachweis erbracht wird, ohne im Klartext Daten wie Name und genaues Geburtsdatum offenzulegen. Ist eine E-ID verknüpfbar, ist es technisch möglich, diesen Altersnachweis anderen Transaktionen mit der gleichen E-ID zuzuordnen.

Die überarbeitete eIDAS Verordnung, welche derzeit in der EU umgesetzt wird, sieht «Unverknüpfbarkeit» als Anforderung vor. Informelle Abklärungen haben ergeben, dass derzeit eine Verzögerung bei der Bereitstellung von Durchführungsrechtsakten und technischen Spezifikationen seitens der EU zu erwarten ist. Aufgrund von informellen Kontakten mit Deutschland ist allerdings davon auszugehen, dass Deutschland voraussichtlich bereits Ende 2025 eine unverknüpfbare E-ID anbieten wird. Dabei wird anstelle von nur einer E-ID gleich eine Reihe von E-ID ausgestellt (batch-issuance). Mit Blick auf den Klartext (Name, Geburtsdatum etc.) sind diese E-ID natürlich identisch; sie unterscheiden sich aber kryptographisch. Jede E-ID wird nur einmal verwendet. Damit sind die einzelnen Transaktionen, die eine Person vornimmt, nicht verknüpfbar. Für eine entsprechende Umsetzung in der Schweiz ist voraussichtlich ein halbes Jahr zusätzliche Entwicklungszeit notwendig.

Neben der batch-issuance gibt es eine Reihe von anderen technischen und organisatorischen Ansätzen, mit denen ebenfalls Unverknüpfbarkeit realisiert werden könnte. Für die Prüfung der Umsetzungsmöglichkeiten wurde inzwischen eigens ein Team im E-ID-Programm aufgestellt. Mit zusätzlichen Mitteln sollen auch Forschungsarbeiten finanziert werden.

Unabhängig von der Frage, ob beziehungsweise wann Unverknüpfbarkeit gewährleistet werden kann, wird bei der staatlichen E-ID des Bundes mit folgenden Elementen ein hoher Datenschutz erzeugt:

- Dezentrale Datenhaltung: Die E-ID wird ausschliesslich auf dem Smartphone der Inhaberin gespeichert und ist dort vor unerlaubtem Zugriff geschützt.
- Entscheidungsfreiheit der Inhaberin: Daten werden nur mit der Zustimmung der Inhaberin übermittelt. Diese weiss, mit wem sie welche Daten teilt, kann dies im Nachhinein nachvollziehen und allfälligen Missbrauch melden.
- Übermittlung von einzelnen Datenfeldern: Es ist möglich, anstelle aller Daten der E-ID – oder eines anderen elektronischen Nachweises – nur einzelne Datenfelder abzufragen. So kann zum Beispiel der Nachweis erbracht werden,



über 18 Jahre alt zu sein, ohne das genaue Geburtsdatum oder gar den Namen preiszugeben.

- Der Bund hat keine Einsicht in die Nutzung: Der Bund, der die E-ID ausstellt und die Vertrauensinfrastruktur betreibt, hat keine Kenntnisse über die Handlungen der einzelnen Inhaberinnen und Inhaber oder der Ausstellerinnen und Verifikatorinnen.
- Missbrauchsliste: Bei Missbrauch, zum Beispiel bei unverhältnismässigen Datenabfragen durch eine Verifikatorin, können entsprechende Akteure auf eine Missbrauchsliste gesetzt werden. Dies ermöglicht es dem Bund, Nutzerinnen und Nutzer vor diesen Akteuren zu warnen.

3. Mögliche Umsetzungsszenarien

Wie in der Informationsnotiz vom 14. Juni 2024 (EXE 2024.1378) vorgeschlagen, wird daran festgehalten, dass die Vertrauensinfrastruktur unterschiedliche Technologie unterstützen können soll (Multi-Stack). Folgende Überlegungen sprechen dafür:

- Nach dem erfolgreichen Referendum gegen das erste E-ID-Gesetz wurde in sechs gleichlautenden Motionen eine vertrauenswürdige, staatliche E-ID gefordert, die nach dem Grundsatz «Privacy by Design» konzipiert wird. Es ist möglich, dass in Zukunft neue Technologien mit einem noch besseren Schutz der Privatsphäre zur Verfügung stehen werden. Gemäss dem Gesetz würde der Bund verpflichtet sein, diese neuen Technologien zu übernehmen. Mit einem Multi-Stack-Ansatz wäre diese einfacher zu bewerkstelligen.
- Der Nutzen einer E-ID, die mit der EU – und Drittstaaten – interoperabel ist, ist unbestritten. Von niemandem wird eine helvetische Insellösung gefordert. Das EJPD anerkennt, dass für die Wirtschaft der Nutzen der Vertrauensinfrastruktur durch eine allfällige EU-Interoperabilität erhöht wird. Dabei ist allerdings zu beachten, dass eine funktionale Interoperabilität mit der EU voraussetzt, dass die Schweiz die technischen Durchführungsrechtsakte der EU übernimmt und einen Staatsvertrag abschliesst. Entsprechende Verhandlungen zwischen der Schweiz und der EU zur gegenseitigen Anerkennung der Systeme wurden noch nicht aufgenommen. Die allfällige Interoperabilität mit Drittstaaten ist von der jeweiligen Technologie abhängig und muss im Einzelfall geprüft werden.
- Die Unterstützung mehrerer Technologien bietet auch einen Investitionsschutz. Die technologischen Entwicklungen in der Domäne elektronischer Nachweise gehen rasant voran. Eine Vertrauensinfrastruktur, welche von Beginn an die Unterstützung mehrerer Technologien ermöglicht, zeichnet sich durch Flexibilität aus. Sollte sich eine Technologie in Zukunft als obsolet erweisen, können Alternativen eingeführt werden, ohne dass das ganze System neu entwickelt werden muss.

3.1 Variante «zeitlich gestaffelte technische Einführung»

Aus heutiger Sicht kann bei der staatlichen E-ID bis zum Zeitpunkt des geplanten Einführungstermins (anfangs 2026) nur der Multi-Stack-Ansatz mit verknüpfbarer



E-ID umgesetzt werden. Deshalb wird vorgeschlagen, die Unverknüpfbarkeit der E-ID erst in einem zweiten Schritt zu implementieren. Dabei steht der Ansatz «batch-issuance» im Vordergrund. Parallel dazu sollen weitere Umsetzungsmöglichkeiten geprüft werden, mit welchen den höheren Anforderungen an den Schutz der Privatsphäre Rechnung getragen werden könnte.

Der Nachteil dieser Variante besteht darin, dass bereits nach voraussichtlich einem halben Jahr eine technische Erweiterung des Systems eingeführt würde. Die bis zu diesem Zeitpunkt herausgegebenen E-ID wären zwar weiterhin einsetzbar, würden aber keinen zusätzlichen Schutz der Privatsphäre bieten. Wer eine unverknüpfbare E-ID verwenden will, müsste sich entsprechend eine neue E-ID ausstellen lassen.

3.2 Variante «Verschiebung Einführungstermin»

Als Alternative zu einer zeitlich gestaffelten technischen Einführung der initialen Umsetzung der E-ID-Vertrauensinfrastruktur wäre eine Verschiebung des Einführungstermins um mindestens ein halbes Jahr denkbar. Dies würde erlauben, von Beginn an auch den zusätzlichen Schutz der Privatsphäre anzubieten. Damit würde nicht bereits innerhalb eines halben Jahr eine technische Erweiterung des Systems eingeführt.

Der Nachteil dieser Variante besteht darin, dass die Einführung der E-ID frühestens in der zweiten Hälfte des Jahres 2026 möglich wäre. Damit würden sich verschiedene Projekte ebenfalls verzögern, die die E-ID zur Identifizierung ihrer Nutzerinnen und Nutzer einzusetzen möchten. Innerhalb der Bundesverwaltung sind dabei insbesondere zu nennen:

- BAG: Einführung des neuen, elektronischen Organ- und Gewebespenderegisters ist an die Verfügbarkeit der E-ID gekoppelt.
- BSV: Altersüberprüfung im Kontext des Jugendschutzes in den Bereichen Film und Videospiele.
- DVS/BK: Erhöhung der Qualität der Identifikation der Nutzerinnen und Nutzer von AGOV, damit das Behörden-Login zum Beispiel auch für das elektronische Patientendossier EPD eingesetzt werden kann.

4. Finanzielle Auswirkungen

Beide Varianten können auf der Grundlage der bereits gesprochenen Mittel umgesetzt werden. Auch das Team und die entsprechenden Mittel, die für die Erforschung des zusätzlichen Schutzes der Privatsphäre erforderlich sind, können mit bereits im 2024 gesprochenen Mitteln finanziert werden. Vorbehalten sind die finanziellen Auswirkungen der Anpassungen am E-ID-Gesetz, die vom Parlament vorgenommen werden (Systeme zur Erhöhung des Schutzes der Privatsphäre resp. Sicherstellung einer Bindung der E-ID an die Inhaberin oder den Inhaber bei der Ausstellung). Für die Umsetzung der Massnahmen für einen zusätzlichen Schutz der Privatsphäre wird



mit Entwicklungskosten von rund 1.5 Mio Franken gerechnet. Auch diese Mehrkosten können mit den bereits gesprochenen Mitteln finanziert werden, wobei eine haushaltsneutrale Verschiebung der später anfallenden Betriebs- und Weiterentwicklungskosten – die anfangs 2023 erfolgte Planung ging noch von einem Einführungszeitpunkt von Mitte 2025 aus – in die Entwicklungskosten erfolgt.

Gestützt auf die Abklärungen durch Sachverständige der Deutschen Fraunhofer-Gesellschaft (Institutsteil Wirtschaftsinformatik) wird eine belastbare Kostenschätzung erarbeitet, welche insbesondere für die im Sommer 2025 vorzunehmende Bedarfserhebung 2027/2028 dient.

5. Variantenwahl

Das EJPD erachtet beide in Ziffer 3 beschriebenen Varianten als valide Optionen für die initiale Einführung der E-ID und der Vertrauensinfrastruktur. Der Gesetzesentwurf ist technologieneutral formuliert und lässt die nötige Flexibilität, um auf technologische Entwicklungen in der Umsetzung und dem Betrieb reagieren zu können. Beide Szenarien sind mit dem Gesetzesentwurf konform. Die ausgeglichenen Rückmeldungen der informellen Konsultation lassen keine klare Tendenz erkennen, welche als Herleitung für eine Entscheidung des Bundes dienen könnte. Beide Lager argumentieren mit guten Gründen.

Dabei ist wichtig zu erwähnen, dass es sich hier nicht um eine rein technische Fragestellung handelt, in der es gilt, Vor- und Nachteile von Technologien abzuwägen. Mit der anstehenden Entscheidung gilt es vor allem zu klären, welchem Kriterium der Vorzug gegeben werden soll: Einhaltung des Einführungstermin versus Unverknüpfbarkeit ab Einführung der E-ID.

Unabhängig von der Entscheidung ist zu bedenken, dass angesichts des technologischen Fortschritts und der internationalen Entwicklungen auch nach erfolgreicher Einführung des Systems eine konstante Weiterentwicklung notwendig sein wird, um den Zweck des Gesetzes dauerhaft zu erfüllen.

Aufgrund der grossen politischen Bedeutung der E-ID, erachtet das EJPD einen Richtungsentscheid des Bundesrates als angemessen.

5.1 Bevorzugte Variante: «zeitlich gestaffelte technische Einführung»

Das EJPD empfiehlt für die initiale Umsetzung auf die Variante «zeitlich gestaffelte technische Einführung» zu setzen. Die Frage der Unverknüpfbarkeit von elektronischen Nachweisen spielt nur in einem begrenzten Anwendungsbereich eine Rolle und hat insbesondere dann eine Bedeutung, wenn mit der E-ID ein Altersnachweis (zum Beispiel beim Alkohol- oder Tabakverkauf) erbracht wird, ohne Daten wie Name und genaues Geburtsdatum offenzulegen. In den meisten Anwendungsfällen – ins-



besondere im Bereich E-Government wie zum Beispiel die Bereitstellung des Strafregisterauszugs ohne Medienbruch durch das BJ oder die Ausstellung des elektronischen Führerausweises durch asa/ASTRA – muss die Inhaberin immer im Klartext eindeutig identifiziert werden.

Das EJPD sieht die Publikation einer Medienmitteilung vor, welche dieses Vorgehen zusammenfasst und dabei die Strategie des Bundes offenlegt. Dies ermöglicht gegenüber der Öffentlichkeit und verschiedenen Stakeholdern eine Aussage zu den weiteren Schritten im E-ID-Programm. In dieser Medienmitteilung wird auch darauf hingewiesen, dass der Bund ab dem ersten Quartal 2025 eine öffentliche Testumgebung zur Verfügung stellt, die bereits mit derjenigen Technologie betrieben wird, die in einem ersten Schritt für die E-ID genutzt werden soll. Parallel zur Publikation der Medienmitteilung werden auch erste Bestandteile der Testumgebung als Open Source veröffentlicht. Aufgrund technischer Abhängigkeiten werden damit Name und visuelle Gestaltung der elektronischen Brieftasche des Bundes sichtbar.

Wir bitten Sie, vom Aussprachepapier Kenntnis zu nehmen und über die vorgeschlagenen Varianten eine Aussprache zu führen.

Eidgenössisches Justiz- und Polizeidepartement EJPD

Beat Jans

Beilagen:

- Medienmitteilung (d)