

Eine sichere elektronische Identität für die digitale und physische Welt

Position der Post zum E-ID-Gesetz

Die elektronische Identität ist ein Schlüsselement für eine erfolgreiche digitale Transformation, denn sie ist eine Voraussetzung für sichere und vertrauenswürdige digitale Dienstleistungen. Der Schweiz fehlt bis heute die Rechtsgrundlage für eine elektronische Identität. Die Post befürwortet deshalb das neue E-ID-Gesetz. Die E-ID schafft die nötige Rechtssicherheit und Vertrauen für Interaktionen in der virtuellen Welt.

Der Alltag und die Bedürfnisse der Menschen und Unternehmen in der Schweiz verändern sich. Prozesse der Unternehmen und der öffentlichen Hand werden vermehrt digitalisiert. Viele Besorgungen und Dienstleistungen des täglichen Lebens lassen sich inzwischen auch oder sogar nur noch online abwickeln. Mit einer vertrauenswürdigen elektronischen Identität können medienbruchfreie digitale Geschäftsprozesse effektiv vorangetrieben sowie Online-Geschäfte und E-Government-Anwendungen weiterentwickelt werden. Vor diesem Hintergrund ist die Möglichkeit, sich mit einer elektronischen Identität in der digitalen Welt eindeutig ausweisen zu können grundlegend für die weiter fortschreitende und sichere Digitalisierung in der Schweiz. Das neue E-ID-Gesetz schafft die rechtlichen Grundlagen für eine staatliche elektronische Identität und andere elektronische Nachweise.

Sichere digitale Systeme sind seit Langem Teil des Postalltags: sie schaffen die Voraussetzung dafür, dass die Post ihre Kernkompetenz umsetzen kann: sensible Informationen sicher und vertrauensvoll transportieren – im physischen Kerngeschäft wie auch in der virtuellen Welt. Die Post hat in den letzten Jahren ihre Kompetenzen und Ressourcen in der Informations- und Verschlüsselungstechnologie ausgebaut und bietet heute digitale Lösungen für Behörden sowie Geschäfts- und Privatkunden an. SwissSign, eine 100%-ige Konzerngesellschaft der Schweizerischen Post und damit vollständig in öffentlicher Hand, bietet u.a. zertifizierte Identifikations- und Authentifizierungslösungen unter der Marke SwissID an. SwissID wird nicht nur in der Privatwirtschaft, sondern auch von 13 Kantonen, mehreren Gemeinden sowie Städten und weiteren staatlichen Stellen genutzt. Sie zählt bereits über 4.3 Millionen Nutzerinnen und Nutzer.

Inhalt der Vorlage

Mit der neuen E-ID können sich Nutzerinnen und Nutzer sicher, schnell und unkompliziert digital ausweisen. Alle Personen, die über eine Schweizer Identitätskarte, einen Schweizer Pass oder einen von der Schweiz ausgestellten Ausländerausweis verfügen, können eine E-ID beantragen. Der Bezug und die Verwendung der E-ID sind kostenlos und freiwillig. Der Bund bietet eine App für das Smartphone an, in der die E-ID sicher verwaltet werden kann. Die E-ID kann sowohl im Internet – zum Beispiel bei der elektronischen Bestellung eines Strafregisterauszugs – als auch im analogen Kontext – beispielsweise als Altersnachweis beim Kauf von Alkohol – zum Einsatz kommen.

Im Gegensatz zum ersten Konzept des E-ID-Gesetzes, welches das Volk am 7. März 2021 klar abgelehnt hat, sieht der jetzige Gesetzesentwurf eine starke Rolle des Staates vor. Die E-ID beruht auf einer staatlich betriebenen Infrastruktur. Diese soll aber nicht ausschliesslich zur Ausstellung der staatlichen E-ID verwendet werden. Sie steht auch staatlichen und privaten Stellen zur Verfügung, damit diese Akteure andere elektronische Nachweise, wie Strafregisterauszüge, Führerausweise, Hochschuldiplome oder ärztliche Rezepte ausstellen können. Die staatliche Vertrauensinfrastruktur schafft damit die Voraussetzung für ein offenes Ökosystem, das es ermöglicht, auf gesicherte Weise verschiedene elektronische Nachweise auszustellen, einzusetzen und vorzuweisen. Der Ausbau dieses Ökosystems der elektronischen Nachweise soll schrittweise erfolgen.

Die Vorlage verfolgt einen Ansatz, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung beruht.



Die Post vertritt folgende Standpunkte

1. Aufbau des Ökosystems

Dass der vorliegende Gesetzesentwurf bzw. die vorgesehene Infrastruktur unterschiedliche elektronische Nachweise vorsieht und damit Richtung offenes Ökosystem abzielt, begrüßen wir.

→ *Wir fordern ein rasches und zielstrebiges Vorgehen zum Aufbau dieses offenen Ökosystems.*

2. Gleich lange Spiesse zwischen staatlicher E-ID und privaten Identitäts Providern

Die E-ID ist kein Login im Sinne einer Zugriffsberechtigung (Authentifikation) zu einem digitalen Dienst, sie ist ein digitaler Identitätsnachweis und damit ein digitales Pendant zum Pass oder zur Identitätskarte. Diese Unterscheidung wird aus unserer Sicht im E-ID-Gesetz zu wenig deutlich gemacht. Insbesondere weil der Bund inzwischen mit dem Authentifizierungsdienst AGOV eine eigene Login-Lösung für staatliche Anwendungen aufgebaut hat.

Über AGOV soll die geplante staatliche E-ID u.a. für die Identifizierung im Kontext des elektronischen Patientendossiers EPD verwendet werden können. Aus Sicht Post muss die angedachte Regelung rund um AGOV und das elektronische Patientendossier nochmals überprüft werden, insbesondere weil: Gemäss den Vorgaben des geltenden EPDG dürfen nur die elektronischen Identifikationsmittel von zertifizierten Herausgebern für die Eröffnung und Nutzung des EPD verwendet werden. Aktuell gibt es drei private zertifizierte Identifikations- und Authentifizierungslösungen: SwisID, TrustID und HIN eID. Mit dem neuen E-ID-Gesetz soll über AGOV die staatliche E-ID für die Identifizierung zum EPD möglich sein können. Der Bund als zukünftiger Herausgeber der E-ID soll aber nicht der Zertifizierungspflicht unterliegen.

Dass ungleich zu den heute zertifizierten Herausgebern von digitalen Identitäten für den Bund keine Zertifizierungspflicht gilt, ist unserer Meinung nach nicht nachvollziehbar. Dadurch werden die bestehenden Identitätsprovider, die eigens für das EPD ein aufwändiges Zertifizierungsvorhaben absolviert haben, ungleich behandelt und ihre Lösungen vom Markt verdrängt.

→ *Wir fordern, dass der Bund bei der Herausgabe der staatlichen E-ID für den Zugang zum EPD den gleichen Anforderungen untersteht, wie sie mit dem Zertifizierungsverfahren für die bestehenden privaten Identitätsprovider gelten.*

3. Weitere Massnahmen zur Stärkung des Vertrauens

Zur weiteren Stärkung des Vertrauens in Interaktionen in der digitalen Welt sieht die Vorlage vor, dass der Bund auch die Identität von Verifikatoren (z.B. Unternehmungen) bestätigen kann, indem diese im entsprechenden Vertrauensregister eingetragen sind. Dadurch kann auch der Privatkunde bei der Abwicklung eines digitalen Geschäfts erkennen, ob sein Geschäftspartner derjenige ist, den er ausgibt zu sein.

Aus Sicht der Post ist dies ein weiterer zentraler Aspekt, der das gegenseitige Vertrauen zwischen den Akteuren in der

virtuellen Welt massgebend fördert.

→ *Die Post schlägt vor, die Verifikatoren im dafür vorgesehenen Register der Vertrauensinfrastruktur zu identifizieren. Entgegen dem Vorschlag des Bundesrates, schlagen wir vor, das Thema auf Gesetzesebene zu regeln und damit dessen Wichtigkeit zu unterstreichen.*

Es ist vorgesehen, dass der Staat eine staatliche elektronische Brieftasche (Wallet) anbietet, welche die E-ID und weitere elektronische Nachweise enthalten kann. Aus unserer Sicht ist positiv, dass Nutzerinnen und Nutzer auch andere (private) Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden können.

→ *Wir schlagen vor, aus Sicherheitsgründen die Nachweise nur auf Wallets zu übertragen, die von anerkannten Vertrauensdiensteanbietern ausgegeben werden.*

Weitere Massnahmen zur Stärkung des Vertrauens und der Sicherheit sind möglich: Die Europäische Union geht in ihrer Gesetzgebung zum Beispiel so weit, dass eine E-ID in eIDAS 2 nur mit einem Sicherheitsniveau "Hoch" im Rahmen der EUID-Wallet akzeptiert wird.

Ein höheres Sicherheitsniveau kann sich auf die rasche Verbreitung der E-ID auswirken.

Weiterführende Informationen

Identifikation: Die elektronische Identität ist eine digitale Form des Identitätsnachweises, die es einer Person erlaubt, sich online auszuweisen. Eine elektronische Identität besteht aus einem persönlichen Attribut, wie z.B. einem Namen oder einer E-Mail-Adresse, und einem geheimen Authentifizierungsmittel, wie z.B. einem Passwort oder einem biometrischen Merkmal. In der physischen Welt erfolgt die Identifikation mittels offiziellen Dokuments wie bspw. Reisepass oder Identitätskarte.

Authentifikation: Bei einem Login bzw. im Rahmen einer Authentifizierung wird überprüft, ob eine Person berechtigt ist, auf eine bestimmte Ressource oder einen bestimmten Dienst zuzugreifen – hierbei handelt es sich also um eine Zugangsbeechtigung. Im Rahmen des Login-Prozesses wird also in einem ersten Schritt entsprechend bestätigt, dass eine Person tatsächlich im Besitz der elektronischen Identität ist, die sie verwendet, und in einem zweiten Schritt berechtigt ist, auf einen entsprechenden Dienst zuzugreifen. Die Authentifizierung ist jeweils ein zu wiederholender Schritt und findet in der Regel vor jeder Nutzung eines Dienstes statt.

AGOV: Damit ist der Authentifizierungsdienst der Schweizer Behörden gemeint. AGOV ist zudem ein Identitätsprovider und Identitätsverbund von Bund und Kantonen. Er steht seit Anfang 2024 produktiv zur Verfügung. Er erlaubt, dass sich



Privatpersonen in einem einheitlichen Anmeldeverfahren zu Online-Diensten der Verwaltung anmelden können, wenn sie dafür eine digitale Identität verwenden, die zum Identitätsverbund AGOV gehört.

SwissID und staatliche E-ID – zwei unterschiedliche Dinge:

Die SwissID ist eine sichere digitale Identität, die als Zugang zu Onlinediensten genutzt werden kann, die einen Identitätsnachweis erfordern, wie zum Beispiel als Zugang zum elektronischen Patientendossier. Es ist aber kein staatlicher digitaler Identitätsausweis. Die E-ID ist ein digitaler Identitätsnachweis und damit ein digitales Pendant zum Pass oder zur Identitätskarte, sie ist kein Login im Sinne eines Zugangsmittels (Authentifikation) zu digitalen Diensten.

