Sachdokumentation:

Signatur: DS 3509

Permalink: www.sachdokumentation.ch/bestand/ds/3509

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

Diskussionspapier zum «Zielbild E-ID»

Diskussionsgrundlage für eine gemeinsame Vision einer staatlichen elektronischen Identität im Hinblick auf den vom Bundesrat zu fällenden Richtungsentscheid

Zusammenfassung

Dieses «Zielbild E-ID» dient als Grundlage für die öffentliche Diskussion. Damit wird kein Variantenentscheid für eine neue, staatliche elektronische Identität (E-ID) angestrebt. Im Vordergrund der öffentlichen Diskussion steht die Frage nach dem Nutzen der E-ID und nach deren Anwendungsfällen sowie nach den Anforderungen an eine staatliche E-ID. Das Ergebnis dieser öffentlichen Diskussion dient dann dem Bundesrat als Basis für seinen Richtungsentscheid, welcher bis Ende 2021 erfolgen soll.

Für die Schweiz startet die Suche nach einer Lösung für eine E-ID neu. Als erster Schritt soll die Vision für eine neue E-ID diskutiert werden. Folgende Fragen stehen dabei im Vordergrund:

- Ist die E-ID ein vom Staat ausgestellter digitaler Ausweis, um die eigene Identität nachweisen zu können, und kann sie in der analogen wie auch der digitalen Welt genutzt werden?
- Könnte ein grösseres Ökosystem mit digitalen Nachweisen jeglicher Art von unterschiedlichsten öffentlichen und privaten Herausgeberinnen einen grösseren Nutzen und damit auch eine breitere Verwendung durch die Inhaberinnen und Inhaber bringen? Und was wären die Risiken?

Der Nutzen einer E-ID für die Inhaberinnen und Inhaber muss in der Diskussion im Vordergrund sein. Einige beispielhafte Anwendungsfälle werden skizziert, im Wissen, dass es *den einen* Anwendungsfall nicht gibt, sondern die Gesamtsumme des Nutzens aller Anwendungsfälle einen Erfolg der E-ID ausmachen wird. Gleichzeitig muss aber auch anerkannt werden, dass heute das Bedürfnis der unterschiedlichsten öffentlichen und privaten Dienstleisterinnen und Dienstleister nach einem einfach integrierbaren, offen ausgestalteten E-ID-Ökosystem unmittelbar vermutlich grösser ist als bei den eigentlichen Inhaberinnen und Inhabern einer E-ID. Entsprechend ist es entscheidend, dass durch geeignete Anwendungsfälle der konkrete Nutzen auch für die Inhaberinnen und Inhaber aufgezeigt werden kann. Hierbei kommen auf den Staat die weitergehenden Rollen des Initianten, Ermöglichers (Enablers) und Garanten zu.

Die Ausgangslage hat sich seit dem Start zum abgelehnten E-ID-Gesetz u.a. in folgenden Bereichen verändert:

- Datenschutz und im speziellen der Schutz der Privatsphäre wurden zu einem noch wichtigeren Thema in der Öffentlichkeit.
- Zukünftige Identitätssysteme basieren auf benutzerzentrierten Ansätzen.

Als technologische Umsetzungs-Varianten werden verschiedene Lösungsansätze ausgebreitet und zur Diskussion gestellt:

- Self-Sovereign Identity
- Public Key Infrastruktur
- Zentraler staatlicher Identitätsprovider

Bei allen Ansätzen gibt es offene Fragen; nicht jeder Ansatz deckt alle Anforderungen gleich gut ab. Die Bewertung der Lösungsansätze erfolgt jedoch nicht mit diesem «Zielbild E-ID», sondern soll im Rahmen einer öffentlichen Diskussion geschehen. Dabei sollen die Grundzüge einer gemeinsamen Vision zur E-ID, deren Nutzung und die Anforderungen an das Ökosystem herauskristallisiert werden. Die öffentliche Diskussion wird massgebend zum Richtungsentscheid durch den Bundesrat beitragen, welcher Ende 2021 vorgesehen ist. Anschliessend können die gesetzlichen Grundlagen erarbeitet werden, welche vom Parlament zu beschliessen sind.

Glossar

Ambitions-Niveau	Begriff aus der Überarbeitung der eIDAS-Verordnung (Ambition-Level) zur Klarstellung des Umfangs der Nutzung einer E-ID-Infrastruktur.
Attribut	Einzelner Datenpunkt, z. B. Vorname oder Geburtsdatum
Credentials	Begriff im SSI-Kontext: Daten-Set aus einem oder mehreren Attributen Begriff im IdP-Kontext: Login-Credentials: Eigenschaften der Identität, welche eine Authentifizierung des Subjekts ermöglichen, Synonym für Authentifizierungsfaktoren, z. B. Benutzername, Passwort oder PIN
Datensparsamkeit	Unter dem Begriff Datensparsamkeit sind zwei Aspekte zusammengefasst: Reduktion auf die minimal notwendigen Attribute bei der Daten-Übermittlung an Dritte und Vermeidung unnötiger Datenflüsse und der damit verbundenen Randdaten.
Dezentrale Datenspeicherung	Daten werden nicht in einem einzigen, zentralen Speicher gehalten sondern in einem Netzwerk von Speichersystemen verteilt oder auf Endbenutzer-Geräte ausgelagert.
Dezentrale Identität	Elektronische Identität, welche nicht durch ein zentrales System verwaltet wird und nur mittels dessen genutzt werden kann, sondern z. B. auf dem Smartphone des Users gespeichert ist und direkt mittels diesem Gerät genutzt werden kann.
Digitale Vertrauensinfrastruktur	Ein Set von Regularien, Prozessen, Konzepten und Infrastrukturelementen, welche das Vertrauen in digitale Prozesse und deren Prozesstreue sicherstellen und von einer breiten Öffentlichkeit akzeptiert und genutzt wird.
E-ID	E-ID steht für staatliche, elektronische Identität – eine Art digitaler Nachweis, welcher vom User zum Zweck des Nachweises der eigenen Identität genutzt werden kann.
E-ID-Ökosystem	Zusammenspiel aus verschiedensten Akteuren (staatlich und privat) mit unterschiedlichen Nutzungs- und Angebotsmöglichkeiten, welches mit der und um die E-ID sowie auf Basis einer gemeinsam genutzten digitalen Vertrauens-Infrastruktur erfolgt.
eIDAS-Verordnung	eIDAS steht für «electronic Identification, Authentication and trust Services» und ist eine Verordnung der Europäischen Union, welche in den Bereichen elektronische Identifizierung und elektronische Vertrauensdienste einheitliche Regelungen definiert.
Holder	Im Kontext von SSI und PKI steht der Holder für die Besitzerin oder den Besitzer einer Wallet mit digitalen Nachweisen.
Identitätsprovider (IdP)	Identitätsprovider bezeichnet die technische Systemkomponente, bei welcher ein Login durchgeführt wird, um anschliessend die Identität einer Benutzerin oder eines Benutzers «zu garantieren». Im erweiterten Sinn kann z. B. auch ein Ausweisdokument oder ein Wallet als Identitätsprovider verstanden werden.
Identity Hub “Backup”	Elektronische Sicherungsmöglichkeit von Identitätsnachweisen, welche die Daten zur Widerherstellung bereitstellt und deren Übertragung auf andere Geräte ermöglicht. Dies kann durch den Benutzer auf eigener Hardware selbst verwaltet oder durch einen Anbieter mit Cloudfunktionalität bereitgestellt werden.
Identity Management	Identity und Access Management werden oft zusammen genannt unter dem Kürzel IAM. Das Identity Management ist dabei für die Verwaltung der Identitäten und die Zuweisungen von Eigenschaften (technischen Attributen) zuständig – unabhängig damit einhergehenden Rollen und Berechtigungen. Unter einer Identität kann in diesem Kontext vereinfacht gesprochen auch ein Login oder Konto verstanden werden.
Institutional Agent	Begriff aus dem SSI-Kontext, eingeführt vom deutschen SSI-Pilotprojekt IDunion: Software-Applikation zur Ausstellung und Überprüfung von Verified Credentials.
Issuer	Synonym von Ausstellerin oder Aussteller. Institutionen, Organisationen und auch Privatpersonen, welche einen digitalen Nachweis ausstellen und dem User übergeben.
Node	Speicher-Knoten in einem verteilten Speichernetzwerk (Distributed Ledger, DLT)
Peer-to-Peer-Kommunikation	Direkte Kommunikation ohne Intermediär. Beschreibt im Kontext von SSI den Datenfluss zwischen Issuer und Holder resp. Holder und Verifier.
Privacy by design	Konstruktionsprinzip, nach welchem der Datenschutz und insbesondere die Datensparsamkeit aufgrund der konzeptionellen Ausgestaltung gegeben ist. Damit kann Vertrauen geschaffen werden, ohne durch rechtliche Grundlagen und den damit verbundenen Kontrollen eine Sicherheit herstellen zu müssen.
Public Key Directory (PKD)	Zentrales Register, in welchem die öffentlichen Schlüssel (Public Key) von Nachweis-Ausstellerinnen und -Ausstellern abgelegt sind. In hierarchischen PKI mit genau einem Vertrauensanker wird keine PKD benötigt.
Public Key Infrastruktur (PKI)	Gesamtsystem eines auf Basis von asymmetrischer Verschlüsselungstechnik aufgebautem Vertrauensnetzwerks.
Public Key Kryptografie	Asymmetrische Verschlüsselungstechnik, bei der ein Schlüssel öffentlich gemacht wird und der andere Schlüssel privat bleiben muss
Registry	Begriff aus dem SSI-Kontext: öffentlich lesbarer Speicher mit den nötigen kryptografischen Beweisen zur Gültigkeits-Überprüfung von Verified Credentials.

Relying Party (RP)	Analog Verifier, Begriff aus dem IdP-Kontext: Systemteilnehmerin, welche sich das E-ID-Ökosystem für die Prüfung von Identitätsnachweisen und Nutzung der durch die E-ID repräsentierten Personendaten zunutze machen.
Revokations-Liste	Öffentlich lesbare Liste von Kennnummern ausgestellter, aber zurückgezogener Nachweise und Zertifikate.
Selbstverwaltete Identität	Alternative Übersetzung von Self-Sovereign Identity. Im Kontext von SSI ist der User selbst für die Verwaltung seiner, durch Issuer ausgestellten und damit glaubwürdigen, digitalen Nachweise zuständig.
Self-Sovereign Identity (SSI)	Ein Set an datenschutz- und benutzerzentrierten Prinzipien, welches in den letzten Jahren zu einem davon abgeleiteten Technologieansatz für elektronische Identitäten geführt hat.
Trust over IP (ToIP) Framework	Richtlinien zur Definition von Entscheidungs-Ebenen zu Governance- und Technologie-Umsetzungsfragen, welche von Arbeitsgruppen der Trust over IP Fundation ausgearbeitet wurden.
Verified Credentials (VC)	Daten-Set aus einem oder mehreren Attributen, welches von der Ausstellerin oder vom Aussteller als «überprüft» signiert wird und dann dem User übergeben wird. Ausstellerin oder Aussteller, Ausstellungsdatum sowie die kryptografischen Beweise sind nebst den eigentlichen Daten Teil eines Verified Credentials.
Verifier	Analog Relying Party, Begriff aus dem SSI-Kontext: Systemteilnehmerinnen, welche sich das E-ID-Ökosystem für die Prüfung von Nachweisen und Nutzung der durch die User präsentierten Daten zunutze machen.
Wallet	Software-Applikation, oft als Smartphone-App konzipiert, welche digitale Nachweise speichert und die Kommunikation mit den Issuern und Verifiern sicherstellt.

Inhaltsverzeichnis

1 Zweck des Dokumentes

Dieses Dokument «Zielbild E-ID» bildet die Grundlage, um die gemeinsame Vision einer staatlichen, elektronischen Identität (E-ID), deren Ausgestaltung, den Umfang eines E-ID-Ökosystems und viele weitere Aspekte zu diskutieren. Das «Zielbild E-ID» verzichtet bewusst auf die Beschreibung und Bewertung einer endgültigen Lösung. Mit einer breiten Diskussion soll die Stossrichtung für die E-ID präzisiert werden können. Das Ergebnis dieser Diskussion dient der Vorbereitung eines Richtungsentscheids durch den Bundesrat für eine neue, staatliche E-ID-Lösung.

2 Ausgangslage

2.1 Volksabstimmung zum E-ID-Gesetz

Das Parlament hatte am 27. September 2019 mit deutlichem Mehr das Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID) verabschiedet. Dagegen wurde erfolgreich das Referendum ergriffen. Das E-ID-Gesetz wurde in der Volksabstimmung vom 7. März 2021 deutlich abgelehnt.

2.2 Motionen

Nach der Ablehnung des E-ID-Gesetzes wurden am 10. März 2021 sechs Motionen mit identischem Wortlaut eingereicht:[1]

Der Bundesrat wird damit beauftragt, ein staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität (Authentifizierung) in der virtuellen Welt, vergleichbar mit Identitätskarte oder Pass in der physischen Welt, zu schaffen. Dabei sollen insbesondere die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Benutzerinnen und Benutzer) eingehalten werden. Diese E-ID darf auf privatwirtschaftlich entwickelten Produkten und Diensten beruhen. Der Ausstellungsprozess und den Gesamtbetrieb der Lösung muss aber durch staatliche, spezialisierte Behörden in der Verantwortung erfolgen.

Die zentralen Forderungen der sechs Motionen:

- Staatliches elektronisches Identifikationsmittel vergleichbar mit Pass
- Datensparsamkeit und «privacy by design»
- Dezentrale Datenspeicherung
- Verantwortung für den Ausstellungsprozess und den Gesamtbetrieb bei staatlichen Behörden

2.3 Klärung der Vision einer E-ID

Die Vorstellungen zur E-ID sind derzeit diffus, jede und jeder hat seine eigenen. Dieses Dokument soll zu einer Festigung und einer Weiterentwicklung der zu Grunde liegenden Vision anregen. So soll geklärt werden, ob eine E-ID auch in der physischen Welt genutzt werden

[1] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213129

können soll (analog digitaler Impfzertifikate), ob der E-ID die gleiche Beweiskraft wie physischen Ausweisdokumenten zugesprochen werden könnte und ob eine E-ID als Authentisierungsfaktor Teil eines nationalen, staatlichen Logins sein soll.

Der Nachweis einer Identität auf digitalem Weg ist die Kernaufgabe einer E-ID. Die E-ID kann somit als «Ausweis» verstanden werden und ein Login als *eine* mögliche Anwendung einer E-ID. Zusätzlich nimmt der Staat die Rolle des Ausstellers und Betreibers ein. Das ergäbe folgende Definition:

«Eine E-ID ist ein vom Staat ausgestellter digitaler Ausweis, um die eigene Identität nachweisen zu können.»

Um den Blickwinkel der Vision nicht zu eng zu fassen, wird in diesem Grobkonzept die Vorstellung einer E-ID direkt mit der Vision einer digitalen Vertrauensinfrastruktur der Schweiz verknüpft, die z. B. lauten könnte:

«Die Schweiz hat eine staatlich betriebene digitale Vertrauensinfrastruktur, welche sichere, medienbruchfreie Prozesse ermöglicht und fördert.»

Für eine solche digitale Vertrauensinfrastruktur könnte eine staatliche E-ID einen wichtigen Beitrag leisten, zu deren Realisierung bräuchte es aber noch mehr (vgl. Kapitel 2.4). Als anspruchsberechtigte Personen für eine E-ID werden – wie bereits im E-ID-Gesetz – Schweizerinnen und Schweizer sowie Ausländerinnen und Ausländer mit einem in der Schweiz anerkannten Ausweispapier oder einer gültigen Legitimationskarte verstanden; in der Fortsetzung des Dokuments «User» genannt. Juristische Personen handeln immer durch ihre Organe, also natürliche Personen und können deshalb nicht Inhaberin einer eigenen E-ID sein. Sie werden durch eine einheitliche Unternehmens-Identifikationsnummer (UID)[2] identifiziert.

2.4 Ansprüche an die Digitalisierung

Bei Digitalisierungsbemühungen bestehen oft hohe Ansprüche bei gleichzeitig unterschiedlichsten Erwartungen und Vorstellungen. Die Technik wird heute im Bereich von Daten- und Medienübermittlung nicht mehr als limitierender Faktor empfunden: «Technisch ist beinahe alles möglich». Eine fehlende physische Greifbarkeit erschwert aber manchmal ein gemeinsames, einheitliches Verständnis von Sachverhalten, Funktionen und Rollen.

Digitalisierung ist immer mit der Aufforderung verbunden, Prozesse und Rollen neu zu denken. Wenn bestehende Prozesse ungeprüft in digitale Kanäle überführt werden, entsteht in der Regel keine gute Digitalisierung mit effizienten digitalen Prozessen. Idealerweise lassen sich zuvor nötige, analoge Prozessschritte aufheben. Automatisierung verbunden mit der Digitalisierung der Prozesse (in dem Sinne, dass die Prozesse auch neu nach digitalen Prinzipien gestaltet werden), wird zu Ressourceneinsparungen führen und ermöglicht eine hohe Skalierfähigkeit des Systems, das mit nahezu identischen Ressourcen viel grössere Massen in einer höheren Qualität und Geschwindigkeit abwickeln kann.

Die User müssen in der Entwicklung in den Mittelpunkt gesetzt werden. Unter Usern sollen dabei nicht nur Privatpersonen gesehen werden, sondern auch Anwenderinnen und Anwender aus der Wirtschaft (handelnd für ihr Unternehmen), welche von digitalisierten Prozessen ungleich stärker profitieren können. Gute Digitalisierung verbessert also direkt die wirtschaftli-

[2] vgl. dazu https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer.html

chen Rahmenbedingungen, Abläufe können vereinfacht werden und die Wirtschaft kann wiederum den Usern neue Möglichkeiten bieten. So kann die gesamte Volkswirtschaft der Schweiz profitieren.

Mit dem Ruf nach einer staatlichen E-ID kann eine Aufgabenzuweisung an den Bund verstanden werden. Die genauen Kompetenzen des Bundes und damit die Möglichkeiten, die Digitalisierung mittels staatlicher digitaler Infrastruktur vorwärts zu bringen, müssen jedoch noch näher untersucht werden. Die E-ID ist dabei aber nicht das Wundermittel, auf das viele warten und dabei hoffen, alle Digitalisierungsprobleme würden damit gelöst. Die E-ID wird die Schweiz nicht digitalisieren, aber sie wird die weitere Digitalisierung unterstützen, weil sie eine wichtige Infrastrukturkomponente der Schweiz darstellt.

Abschliessend bleibt zu erwähnen, dass viele Ansprüche sich in einem Spannungsfeld gegenüberstehen und es dadurch nicht das *eine Richtige* gibt, sondern in der Diskussion ein konsensfähiger Weg gefunden werden muss, z. B. im Spannungsfeld zwischen:

- Benutzerfreundlichkeit ↔ Datenschutz ↔ Datensicherheit
- Selbstverantwortung ↔ Unterstützungsmöglichkeit
- Benutzerzentrierung ↔ Vertrauen
- Kontrollierte Umgebung mit schwerem Zugang ↔ Offenes System mit leichtem Zugang
- Wenige, kontrollierte Anwendungsfälle ↔ viele, unkontrollierte Anwendungsfälle
- Umsetzungsgeschwindigkeit ↔ Perfektion
- Flexibilität ↔ Schutz der User

3 Entwicklung im Bereich digitaler Identitäten

3.1 Technische Entwicklungen

Aufgrund von Forderungen nach hohem Datenschutz und dezentraler Datenspeicherung, welche auch in den in Kapitel 2.2 erwähnten Motionen gestellt werden, hat sich in den letzten Jahren eine weltweite Diskussion zum Thema «Dezentrale Identität» entwickelt. Dies wiederum führte zu einer ganzen Sammlung an Technologien, neuen kryptografischen Verfahren und Standards, welche für die Zwecke von Vertrauens-Systemen genutzt werden können. Self-Sovereign Identity (SSI) ist dabei aktuell der wohl meist diskutierte Ansatz, bestehend aus benutzerzentrischen Prinzipien und technologischen Mitteln. Gründe dafür sind insbesondere die Einfachheit des Konzepts, die Nähe der Technologie zur physischen Realität und die universelle Anwendbarkeit.

Ein technischer Grundstein von SSI-Technologie ist die Public-Key-Kryptografie, welche bereits seit Jahrzehnten für dezentrale, technische Herkunftsnachweise in Form von Zertifikaten (z. B. X.509) sorgt. Diese finden u.a. Anwendung zur Signatur von Daten im biometrischen Pass, zur Ausstellung des Covid-Zertifikats, im Bereich der elektronischen Signatur oder für den Aufbau geschützter Kommunikation mit einer Webseite.

International ist der Trend zur E-ID auf dem Smartphone zu sehen, da die Smartphone-Durchdringung heute sehr hoch ist. Ehemals mit Chip-Karten entwickelte Lösungen werden abgelöst von Smartphone-basierten Lösungen. Digitale «Wallets» als Aufbewahrungsort von dezentral geführten digitalen Nachweisen stehen auch in der Europäischen Union zuoberst

auf der digitalen Agenda. Tatsache ist aber, dass in Europa derzeit weiterhin viele E-ID-Lösungen «klassische IdP»-Lösungen sind, allerdings in vielen verschiedenen Ausprägungen (staatliche, private und föderierte Identitätsprovider).

Der E-ID-Neustart eröffnet für die Schweiz die Chance, von den neusten Erkenntnissen und Entwicklungen zu profitieren. Weil die technologische Entwicklung rasant ist, braucht es ein Konzept, das technisch flexibel umgesetzt werden kann. International liegen die Erneuerungszyklen von Lösungen für digitale Identitäten bei 5 bis 10 Jahren. Eine ultimativ perfekte Lösung wird es nicht geben und soll deshalb auch nicht angestrebt werden. Es sollte aber das Ziel sein, einen Weg zu wählen, welche Basis vieler Wertschöpfungsprozesse werden kann und die Digitalisierung der Schweiz fördert. Der zu schaffende Rechtsrahmen für eine staatliche E-ID-Lösung sollte so weit wie möglich technologieneutral ausgestaltet sein und damit eine Weiterentwicklung explizit zulassen.

3.2 Entwicklung im EU-Recht

Die Europäische Kommission hat am 3. Juni 2021 einen Vorschlag[3] zur Änderung der eIDAS-Verordnung[4] und zur Schaffung eines rechtlichen Rahmens für eine europäische digitale Identität (EUid) vorgelegt. Sollte die neue Verordnung gemäss Entwurf verabschiedet werden, würden die Mitgliedstaaten verpflichtet, den Bürgerinnen und Bürgern sowie Unternehmen digitale Brieftaschen zur Verfügung zu stellen, in denen sie ihre nationale digitale Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerschein, Abschlusszeugnisse, Bankkonto usw.) verknüpfen können. Von der nationalen digitalen Identität wird eine EUid abgeleitet. Die Brieftaschen können von Behörden oder privaten Einrichtungen bereitgestellt werden, sofern sie von einem Mitgliedstaat anerkannt sind.

Damit der Vorschlag so bald wie möglich umgesetzt werden kann, wird er durch eine Empfehlung ergänzt. Darin fordert die Kommission die Mitgliedstaaten auf, bis September 2022 ein gemeinsames Instrumentarium zu schaffen und unverzüglich mit den erforderlichen Vorarbeiten zu beginnen. Dieses Instrumentarium muss die technische Architektur, Normen, Leitlinien und bewährte Verfahren umfassen.

Der von der Kommission vorgegebene Rahmen ist technologisch neutral, basiert aber auf den Prinzipien von «Self-Sovereign Identity» (SSI). Die Mitgliedstaaten werden die technischen Standards ab September 2021 selbst verhandeln. Damit die künftige Schweizer E-ID nach der eIDAS Verordnung notifiziert werden kann, ist es vorteilhaft sich an dem von der Kommission gesetzten Rahmen zu orientieren.

[3] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

[4] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

4 E-ID-Ökosystem

4.1 Teil des Alltags werden

Alle Initiativen, eine nationale elektronische Identität erfolgreich einzuführen, kämpfen stets mit dem Huhn-Ei-Problem: Ohne E-ID werden keine Anwendungsfälle geschaffen und ohne Anwendungsfälle wird keine E-ID benötigt. Nebst der Verwendung einer E-ID für E-Government-Dienste wird deshalb im europäischen Umfeld oft auf Sekundärnutzungen wie E-Signatur-Fähigkeit oder E-Banking-Zugang gesetzt, um eine Verbreitung und eine häufige Nutzung zu fördern. Der Wert häufiger Nutzung liegt im besseren Beherrschen der Bedienung, erhöhtem Sachverständnis und der Chance, in der breiten Masse zur Gewohnheit zu werden.

Will man eine möglichst hohe Anzahl an Verwendungszwecken erlauben, ist ein funktionierendes Ökosystem nötig: Eine gemeinsam genutzte Infrastruktur, mit gemeinsam definierten Regeln und vielen Möglichkeiten für die verschiedensten Akteure des Systems. Im Idealfall funktioniert die E-ID deshalb in einem Ökosystem, welches über offene und standardisierte Schnittstellen verfügt, eine abgestimmte Governance hat, keine bürokratischen, hemmenden Regelungen pflegt und eine praktische, automatisierbare Aktualisierung der E-ID-Daten ermöglicht. Damit würde auch die Grundlage geschaffen, dass sich Unternehmen aus der Privatwirtschaft anschliessen und darauf neue Prozesse und Geschäfte entwickeln – womit zusätzliche Verwendungszwecke ermöglicht würden. Sind praktische Verwendungszwecke da und wird ein individueller Nutzen gesehen, wird auch das Interesse der potenziellen User geweckt.

Als wichtiges Kriterium sollte zudem die Benutzerfreundlichkeit und -zufriedenheit beigezogen werden. Interaktionen im Ökosystem mit der E-ID müssen bequem, transparent und dennoch verständlich sein. Gleichzeitig muss ein Grundvertrauen in das System, die Teilnehmerinnen und Teilnehmer sowie die Beweiskraft der E-ID entstehen. Die Verwendung sollte keine zusätzlichen technischen Geräte erfordern. Und die Nutzung einer E-ID müsste für deren User vermutlich kostenlos sein, da selbst kleine Beträge abschreckend wirken können. Die Eintrittshürden sollten bewusst tief gehalten werden. Die E-ID muss schliesslich auch die Schutz- und Sicherheitserwartungen der Beteiligten erfüllen.

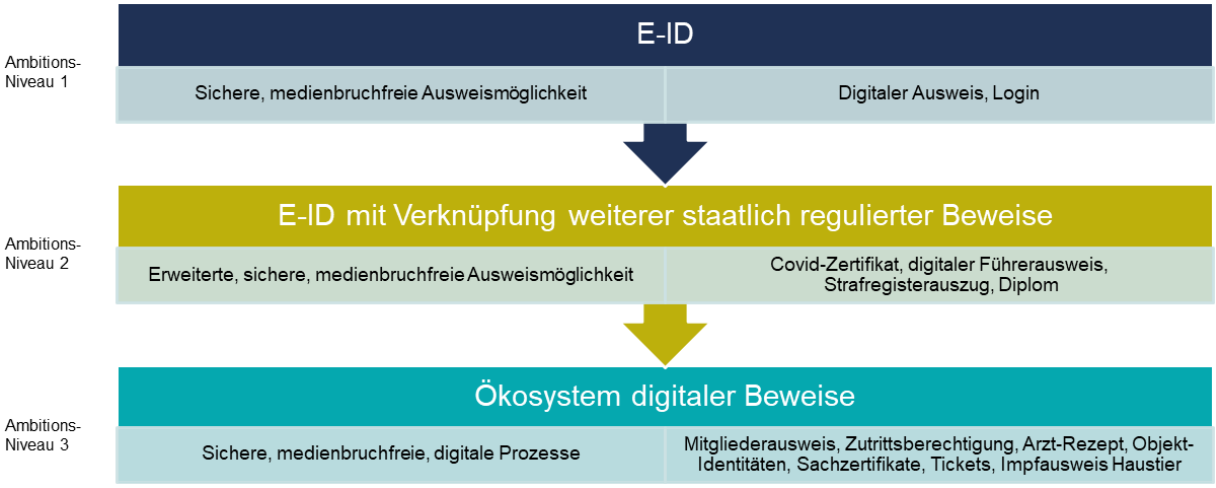
Reicht dies, um Teil des Alltags zu werden? Genügt es, das E-ID-Ökosystem rund um eine E-ID aufzubauen, oder sollte der Umfang des Ökosystems grösser sein, in dem die E-ID nur noch *einen digitalen Nachweis* unter vielen darstellen würde? Im folgenden Abschnitt wird dieser Aspekt behandelt.

4.2 Umfang des Ökosystems

Bevor man in die Technologieüberlegungen einsteigt, macht es Sinn, sich auch zur Frage des Umfangs der künftigen E-ID-Nutzung (den sog. Ambitions-Niveaus) und damit zum Umfang des Ökosystems Gedanken zu machen. Es bestehen Wechselwirkungen zwischen Ambitions-Niveau, dem Aufbau und der Gestaltung des Ökosystems und den einsetzbaren Technologien. Die Wahl der Technologie sollte grundsätzlich vom gewünschten Resultat abhängig sein, gleichzeitig ist aber wichtig zu wissen, dass verschiedene technische Umsetzungen von ähnlicher Komplexität unterschiedliche Resultate ermöglichen.

Als Diskussionsgrundlage werden – in Anlehnung an die Diskussion in der EU[5] – folgende drei Ambitions-Niveaus definiert:

[5] Auch die EU definiert für die EUid drei Niveaus als «Level of Ambition»



Ambitions-Niveau 1: E-ID

Ambitions-Niveau 1 stellt den Minimalzweck einer E-ID dar: Die E-ID ist ein Ausweis, der in der digitalen Welt genutzt werden kann, um die eigene Identität nachzuweisen. Als Aussteller tritt dabei ausschliesslich der Bund auf. Die E-ID könnte dabei *durch ein* Login ergänzt oder *für ein* Login genutzt werden. Der direkte Nutzen einer E-ID als digitale Ausweismöglichkeit besteht grundsätzlich in folgenden Anwendungsfällen:

- Bestätigung der Identität (z. B. Bankkonto, Mobiltelefon-Abonnement, Bestellung Strafregisterauszug, Post-Schalter, Personenkontrolle)
- Bestätigung des Alters (mit abgeleiteten Attributen)

Aus Erfahrung mit der Abstimmung zum E-ID-Gesetz besteht der Eindruck, dass der Nutzen dieser Anwendungsfälle nicht restlos überzeugen konnte.

Ambitions-Niveau 2: E-ID mit Verknüpfung weiterer staatlich regulierter Nachweise

Das Ambitions-Niveau 2 zielt auf ein E-ID-Ökosystem, in welchem die staatliche E-ID eine Basis-Identität darstellt, auf welcher viele weitere staatlich regulierte Nachweise aufbauen, wie z. B. der digitale Führerausweis. Dabei liefert die Basis-Identität die Personeninformationen wie Name, Geburtsdatum und Gesichtsbild. Der Führerausweis-Zusatz bräuchte nur noch die zusätzlichen Attribute wie Fahrzeugkategorie und Gültigkeitsdatum zu ergänzen.

Durch kryptografische Verknüpfungen würde eine Abhängigkeit zur Basis-Identität entstehen. Bei logischen Verknüpfungen könnte ein weiterer staatlicher Nachweis auch alleinstehend funktionieren und wäre nicht betroffen, wenn z. B. die Basis-Identität revoziert werden müsste.

Der Umfang des Ökosystems wäre damit im Vergleich zu Level 1 deutlich grösser bei einer viel höheren Anzahl an Nutzungsmöglichkeiten. Als Ausstellerinnen wären verschiedenste staatliche Akteure zugelassen, welche auch die Richtigkeit von Verknüpfungen garantieren würden.

Ambitions-Niveau 3: Ökosystem digitaler Nachweise

Das Ambitions-Niveau 3 bietet das grösste Potential, das Huhn-Ei-Problem zu lösen. Im vollen Umfang des Ökosystems wird die E-ID nur noch einen von vielen digitalen Nachweisen darstellen. Eine Verknüpfung zur E-ID ist dabei möglich, ein digitaler Nachweis kann jedoch auch unabhängig der E-ID sein, z. B. ein Event- oder ÖV-Ticket, ein Mitgliederausweis, ein Impfausweis eines Haustieres, ein Fahrzeugausweis oder die Bescheinigung einer erfolgreichen Motorfahrzeugkontrolle für ein Auto.

Beim Ambitions-Niveau 3 können staatliche und private Stellen digitale Nachweise ausstellen. Die Ausstell-Fähigkeit von Privaten ist denn auch entscheidend, machen doch im Alltag von Privat zu Privat ausgestellte Nachweise eine gewichtige Anzahl aus. Somit lassen sich mit standardisierten Mitteln viele Prozesse medienbruchfrei umsetzen, z. B. im Kunden-, Lieferanten- und Angestellten-Management und überall dort, wo Ausweise, Belege und Zertifizierungen im Spiel sind. Für den User hat dies den Vorteil, dass die Anwendung (empfangen, speichern, präsentieren) immer identisch ist und sich damit ein kollektives Verständnis von digitalen Nachweisen etablieren kann. Im Ökosystem steht nicht mehr die E-ID im Vordergrund, sondern ein staatlich regulierter und gesicherter, dezentraler Aufbewahrungsort, «das staatliche Wallet», aus dem Informationen mit hohem Vertrauen bezogen werden können.

Die EU spricht sich bei der EUid für die Voll-Variante von Level 3 aus, einem «Highly Secure Personal Digital Identity Wallet».

Die E-ID stellt unumstritten ein Kernelement eines solchen Ökosystems dar; die E-ID könnte darin den Aufbau einer offenen, nationalen, digitalen Vertrauensinfrastruktur unterstützen. Dabei ist eine etappierte Entwicklung grundsätzlich möglich, wobei das finale Ambitions-Niveau von Anfang an definiert werden sollte, da sich nicht jeder Technologieansatz für ein offenes Ökosystem digitaler Nachweise (Ambitions-Niveau 3) eignet. Jedes Ambitions-Niveau ist mit einer oder mehreren Technologien möglich. Jede Implementation bringt bestimmte Konsequenzen mit sich. Bevor aber mögliche Lösungsansätze beschrieben werden, macht es Sinn, im folgenden Abschnitt einige Beispiel-Anwendungsfälle zu beschreiben.

4.3 Anwendungsfälle

Um Lösungsansätze zu vergleichen, werden in diesem Abschnitt unterschiedliche, exemplarische Anwendungsfälle beschrieben. Für jeden Anwendungsfall sind der Ist- und ein möglicher Soll-Zustand skizziert. Jeder Anwendungsfall steht beispielhaft für einen bestimmten Typ von Anwendung und stellt deshalb spezifische Aspekte in den Fokus, welche helfen sollen, weitere Fragen zur Diskussion zu stellen.

Diese Auflistung von Anwendungsfällen erhebt nicht den Anspruch komplett zu sein. Für die geforderte Bürgernutzenbetrachtung ist die Suche nach relevanten Anwendungsfällen (Use-Cases) und deren Bewertung nach dem optimalen Nutzen aus User Sicht zentral. Wie schon vorgängig dargelegt wird dies nicht zu einem Zeitpunkt abschliessend möglich sein, sondern es muss evolutionär gelernt werden. Entsprechend sind, je nach Ambitionsniveau, gesteuerte agile Prozesse zu etablieren, die dies ermöglichen. Hierbei kommt dem Staat – wie auch in einigen Motionen gefordert – die Rolle eines proaktiven Ermöglichers (Enablers) zu.

Die Anwendungsfälle sollen beispielhaft den direkten, konkreten Nutzen für E-ID-User aufzeigen und hinterfragen. Implizit steht im Hintergrund dazu immer die Möglichkeit zur Prozessvereinfachung, wodurch den Usern ein indirekter Nutzen entsteht, sei es durch die Beschleunigung von Verfahren, Vergünstigung von Leistungen oder neuen Dienstleistungen. Dienst-

leisterinnen selbst (auch als Relying Parties bezeichnet) können sich je nach Ambitions-Niveau nicht nur als Nachweis-Empfängerinnen und -Überprüferinnen sehen, sondern auch als Ausstellerinnen.

Viele Diskussionen zum Thema machen deutlich, dass es *den einen Anwendungsfall* nicht gibt; die Summe und die Vielfalt der Anwendungsfälle macht's! Je höher das Ambitions-Niveau gesetzt wird, desto höher wird diese Summe und Vielfalt sein. Die in der Schweiz vorhandene innovative Wirtschaft könnte bei einem offenen «Ökosystem der digitalen Nachweise» diese Summe und Vielfalt deutlich erhöhen – und damit wären die Chancen reell, im Alltag der Menschen anzukommen.

4.3.1 Altersüberprüfung in der analogen und digitalen Welt

Bei der Altersüberprüfung geht es um die Feststellung, ob eine Person ein bestimmtes Alter überschritten hat. Das genaue Alter wie auch das Geburtsdatum sind dabei irrelevant. Der E-ID-Nutzen für den User liegt dabei in der einfachen, datensparsamen Anwendung, welche sowohl in der analogen wie auch in der digitalen Welt möglich ist.

Ist-Zustand analoge Welt, z. B. am Disco-Eingang:

- Das Sicherheitspersonal überprüft am Eingang der Disco die physischen Ausweispapiere um festzustellen, ob jemand beispielsweise schon 18 Jahre alt und damit zum Eintritt berechtigt ist.
- Auf dem Ausweis verzeichnet sind u.a. das Gesichtsbild, das genaue Geburtsdatum, der volle Name und die Nationalität.

Ist-Zustand digitale Welt, z. B. E-Commerce-Shop:

- In einer Vielzahl von Fällen wird auf die Überprüfung des Alters verzichtet und auf eine Selbstdeklaration durch die User abgestellt. Solche Massnahmen halten Minderjährige nicht vom Kauf von für ihr Alter nicht zugelassenen Artikeln ab.
- Eine Überprüfung durch einen Foto- oder Video-Beweis eines Ausweisdokuments ist verhältnismässig aufwändig und wird daher nur selten verlangt.

Aspekte im Fokus:

- Datensparsamkeit bei einer Altersüberprüfung mit einem Ausweisdokument ist nicht gegeben.
- Randdaten, welche bei Überprüfungsabläufen anfallen können.
- Unzureichender Jugendschutz aufgrund hoher technischer Aufwände.

Soll-Zustand analoge Welt, z. B. am Disco-Eingang:

- Eine E-ID kann in der physischen Welt gleich wie bestehende Ausweisdokumente verwendet werden.
- Zur Altersüberprüfung einer Person sind für die Überprüfung nur zwei Informationen nötig: «Bestätigung, dass älter als gefordert» und das Gesichtsbild. Diese Informationen müssen von der staatlichen E-ID abgeleitet und zur Überprüfung übergeben werden können, ohne weitere Daten offenzulegen. Der Schutz vor einer unerlaubten Weiterverwendung des Gesichtsbildes ist im Datenschutzgesetz geregelt.

Soll-Zustand digitale Welt, z. B. E-Commerce-Shop:

- Herausgeber der E-ID erfährt nicht, wann die E-ID eingesetzt wird.
- Für verlässliche Altersangaben wird die Abfrage der E-ID-Information «Bestätigung, dass älter als gefordert» als Prozessschritt integriert, ähnlich einem Zahlungsvorgang.

Konkreter Nutzen für den E-ID-User:

- Name und Geburtsdatum müssen nicht offengelegt werden, was letztendlich zur Gesamtsicherheit beiträgt.
- Beim Disco-Besuch muss kein physisches Ausweisdokument mitgeführt werden.
- Der Jugendschutz bei Online-Einkäufen wird gestärkt.

4.3.2 Bankkonto-Eröffnung

Kaum ein Bereich ist so stark reguliert wie der Finanzsektor. Eine Bankkonto-Eröffnung unterliegt dadurch vielen Gesetzen und Bestimmungen. Eine hohe Gewissheit zu haben über die Person, welche ein Konto eröffnen möchte, ist deshalb nötig (Know Your Customer). Der E-ID-Nutzen für den User liegt in der einfachen Übermittlung der Identitätsbestätigung. Zudem wäre die Einreichung weiterer Nachweise ohne Scannen und datenschutzkritisches Versenden per E-Mail möglich.

Ist-Zustand:

- Überprüfung der Identität vor Ort: Vorweisen einer Identitätskarte oder eines Passes; von den Ausweisdokumenten wird eine Kopie erstellt und zu den Akten genommen.
- Überprüfung der Identität bei Online-Prozessen z. B. mittels Foto-Aufnahmen von Ausweisen und anschliessender Video-Identifikation in z.T. automatisierten Online-Prozessen.
- Überprüfung der Identität mittels Überweisung eines Betrages von einem bestehenden Bankkonto, welches auf den gleichen Namen lautet.

Aspekte im Fokus:

- Hohe Aufwände (personell, finanziell, technisch) für die Durchführung der Identifikation.
- Sehr hohe Verlässlichkeit bei der Zuordnung von Identität zu Inhaber, um Handlungen der Identität zweifelsfrei dem Inhaber zurechnen zu können (Gerichtsverwertbarkeit).

Soll-Zustand:

- Die E-ID erlaubt eine einfache, medienbruchfreie und sichere Identifikation.
- Weitere Abgleich-Vorgänge bleiben unter Umständen aufgrund von branchenabhängigen Vorgaben weiterhin nötig auf Seiten der Bank, z. B. Verifikation der Person vor dem Bildschirm mittels Gesichtsbild des bei der Identifikation übermittelten, digitalen Ausweises.

4.3.3 Betreibungsregisterauszug

Bei Bewerbungen auf Wohnungen und Arbeitsstellen wird oft standardmässig ein Betreibungsregisterauszug verlangt. Die Bescheinigung muss dabei beim zuständigen Betreibungsamt eingeholt werden. Der E-ID-Nutzen für den User liegt sowohl im einfachen Identitätsnachweis bei der Bestellung bei einem der rund 400 Betreibungsämter wie auch im Erhalt eines digitalen Betreibungsregisterauszugs (Nachweis), welcher anschliessend beliebig oft präsentiert werden kann.

Ist-Zustand:

- Zuerst muss das zuständige Betreibungsamt gefunden werden. Eine entsprechende Suchfunktion bietet z. B. die Plattform des Bundes «EasyGov», welche auch beim Ausfüllen eines korrekten Auskunftsbegehrens unterstützt.
- Als nächstes wird in der Regel das Auskunftsbegehren ausgedruckt, unterschrieben und per Post – zusammen mit einer Ausweiskopie – eingeschickt. Je nach Betreibungsamt ist auch eine Vorauszahlung der fälligen Gebühr erforderlich.
- Das Amt retourniert einen Papierauszug.
- Der User sendet das Dokument (Original oder Kopie) weiter an die gewünschten Empfängerinnen und Empfänger.
- Angeboten werden auch digitale Prozesse, falls die Person, welche eine Eigenauskunft verlangt, über eine qualifizierte Signatur verfügt, oder einer Drittperson den Auftrag erteilt, mit Interessensnachweis die Auskunft einzuholen.
- In diesen Fällen sendet das zuständige Betreibungsamt ein signiertes PDF zurück. Die Empfängerin oder der Empfänger kann dieses PDF mittels Validator-Applikation auf Echtheit überprüfen.

Aspekte im Fokus:

- Weiterreichen des Auszugs: Oft ist ein Original-Dokument gefordert.
- Prozesse bei der Empfängerin oder beim Empfänger sind aufwändig, da ein Medienbruch stattfindet resp. ein PDF mittels Validator-Applikation auf seine gültige Signatur überprüft werden muss.
- Manipulierte Papierauszüge funktionieren bei Empfängerinnen oder Empfängern, welche nicht ein erkennbares Original verlangen.

Soll-Zustand:

- Identifikation der Bestellerin oder des Bestellers kann mittels E-ID überprüft werden.
- Digitaler Auszug als Nachweis wird über einen gesicherten Kanal an den User gesendet.
- Digitaler Auszug kann vom User direkt an eine Empfängerin oder einen Empfänger weitergeleitet werden.
- Empfänger-System kann Prozesse zur Überprüfung automatisieren.

Konkreter Nutzen für den E-ID-Nutzer:

- Der Gang auf ein Amt oder an den Post-Schalter entfällt.
- Original-Bestätigung kann beliebig oft präsentiert werden. Dadurch fallen keine zusätzlichen Kosten an, wenn das gleiche Dokument bei verschiedenen Stellen eingereicht werden muss.

4.3.4 Staatliches Login

Die Nutzung vieler E-Government-Services setzt ein Login voraus, um Zugang zur entsprechenden Plattform zu erhalten. Zur Authentisierung könnte ein staatlicher Authentifizierungsdienst genutzt werden, wobei die E-ID als Authentisierungsfaktor funktionieren könnte. Der E-ID-Nutzen für den User wäre in der Verwendung der gleichen Login-Daten für unterschiedliche E-Government-Plattformen.

Ist-Zustand:

- Unterschiedliche IdP oder Identity-Management-Systeme bei unterschiedlichen Portalen führen zu einer Vielzahl von Login-Credentials.
- Viele Kantone haben noch kein Identity-Management für mögliche E-Government-Services.
- Es existiert kein staatliches, landesweit genutztes Login.

Aspekte im Fokus:

- Parallel-Betrieb mit existierenden, produktiven Lösungen ermöglichen.
- Sichere Authentisierung mittels zusätzlicher Authentisierungsfaktoren.

Soll-Zustand:

- E-ID stellt ein (Multi-)Authentisierungsfaktor dar (besitzendes Element, ggf. auch geheimes Wissen und biometrisches Element).
- Ein staatlicher Authentifizierungsdienst stellt einen sicheren Authentisierungsmechanismus für alle staatlichen E-Government-Portale bereit.
- Identität und Zugriffsrechte können getrennt werden. Dies führt zu erheblichen Vereinfachungen in Bau und Unterhalt von Anwendungen.

Konkreter Nutzen für E-ID-User:

- Verwendung gleicher Login-Daten für unterschiedliche E-Government-Plattformen
- Sicherer Login-Prozess und dadurch hoher Zugangsschutz

4.3.5 Elektronische Signaturen

Elektronische Signaturen sind seit 2005 im Bundesgesetz über die elektronische Signatur geregelt, wurden aber von der breiten Bevölkerung bis heute nur wenig genutzt. Der E-ID-Nutzen für den User liegt im vereinfachten Zugang zu einer qualifizierten elektronischen Signatur.

Ist-Zustand:

- Für elektronische Signaturen stellen anerkannte Dienstleisterinnen die nötigen Services bereit.
- Initial wird von den Dienstleisterinnen eine Identifikation des Users durchgeführt, bei qualifizierten Signaturen erfordert es ein persönliches Erscheinen. Anschliessend wird ihm ein qualifiziertes Zertifikat ausgestellt.
- Durch Anwendung eines qualifizierten Zertifikats können Dokumente rechtsgültig digital signiert werden.
- Die Überprüfung von digital signierten Dokumenten kann mittels Validator-Applikationen gemacht werden.

Aspekte im Fokus:

- Schwerfälliger Zugang zur qualifizierten Signatur durch Pflicht zu persönlichem Erscheinen.

Soll-Zustand:

- Einfacher Zugang zur Möglichkeit, qualifizierte elektronische Signaturen zu erstellen.
- Förderung des digitalen Austausches von Vertragsdokumenten.

Konkreter Nutzen für den E-ID-User:

- Rechtssichere, digitale Vertragsabschlüsse werden zum Standard dank qualifizierten elektronischen Signaturen und sparen so Zeit und Kosten.

4.4 Rechtliche Grundlagen

Die Analyse der rechtlichen Grundlagen des zukünftigen Gesetzes sowie die Ausarbeitung des Gesetzesentwurfs sind nicht Gegenstand des «Zielbilds E-ID». Um die rechtlichen Grundlagen der staatlichen E-ID ausarbeiten zu können, muss zuerst das angestrebte Ambitions-Niveau und eine E-ID-Lösung bestimmt werden.

4.5 Kommunikation

Der Weg zu einer staatlichen E-ID benötigt von Anfang an eine gute Kommunikation mit allen: Potenzielle User, Kantone, Privatwirtschaft, Organisationen sowie die Bundesverwaltung sollen gleichermassen abgeholt werden, um die Vision mitzugestalten und diese letztendlich mitzutragen. Möglicher gesellschaftlicher Nutzen soll dabei stets ins Zentrum gerückt werden, gefolgt von möglichen Anwendungsfällen und -formen. Die Diskussion um die einzusetzende Technologie erfolgt nachgelagert.

Nebst den üblichen Mitwirkungsverfahren werden – wo möglich – über interaktive Diskussionsplattformen und öffentliche Intrusionstests weitere Stimmen miteinbezogen.

5 Verschiedene E-ID-Lösungsansätze

5.1 E-ID-Lösung mittels Self-Sovereign Identity

5.1.1 Ansatz

Self-Sovereign Identity (SSI) ist der jüngste der in diesem «Zielbild E-ID» vorgeschlagenen Lösungsansätze für ein E-ID-Ökosystem. 2016 formulierte Christopher Allen 10 benutzer- und datenschutzzentrierte Prinzipien, nach welchen «selbstverwaltete Identitäten»[6] konzipiert werden sollen – Identitäten, über welche der User die grösstmögliche Kontrolle hat. Dies entspricht dem «Zeitgeist», in welchem vermehrt Themen wie Datenschutz- und Datensicherheitsbedenken sowie Abhängigkeiten zu zentralen Identitäts-Systemen in den Fokus rücken, was sich auch in den in Kapitel 2.2 erwähnten Motionen widerspiegelt. Gleichzeitig werden auch Antworten gesucht, wie Systeme auf einem universelleren Weg digital miteinander verbunden werden können, anstatt immer wieder neue Schnittstellen definieren zu müssen.

Innert weniger Jahren entwickelten sich offene Standards, technische Frameworks und eine eindeutige Architektur, wie SSI umgesetzt werden kann. Dabei wurde das Rad nicht neu erfunden, sondern setzte auf Wissen von Public-Key-Infrastrukturen und fortgeschrittenen kryptografischen Verfahren auf. Dadurch wurde es möglich, dass heute bereits produktive SSI-Ökosysteme in Betrieb sind, auch wenn noch kein Staat eine E-ID auf SSI-Basis herausgibt. Die neusten Entwicklungen in der EU gehen ebenfalls in diese Richtung.

Der SSI-Ansatz ist prinzipiell auf das Ambitions-Niveau 3 ausgerichtet: ein Ökosystem digitaler Nachweise. Er eignet sich jedoch für alle Ambitions-Niveaus, die Unterschiede liegen dabei in der Governance, da die technisch eingesetzten Mittel identisch bleiben.

[6] Self-Sovereign Identity wird häufig mit «Selbstbestimmte Identitäten» übersetzt, was jedoch oft zu Missverständnissen führt, weil z. B. ein staatlicher Identitätsnachweis vom Staat ausgestellt wird und den Usern zur Nutzung und Verwaltung übergeben wird und nicht, entgegen dem Term «selbstbestimmt», von diesen selber definiert wird.

5.1.2 Funktionserklärung

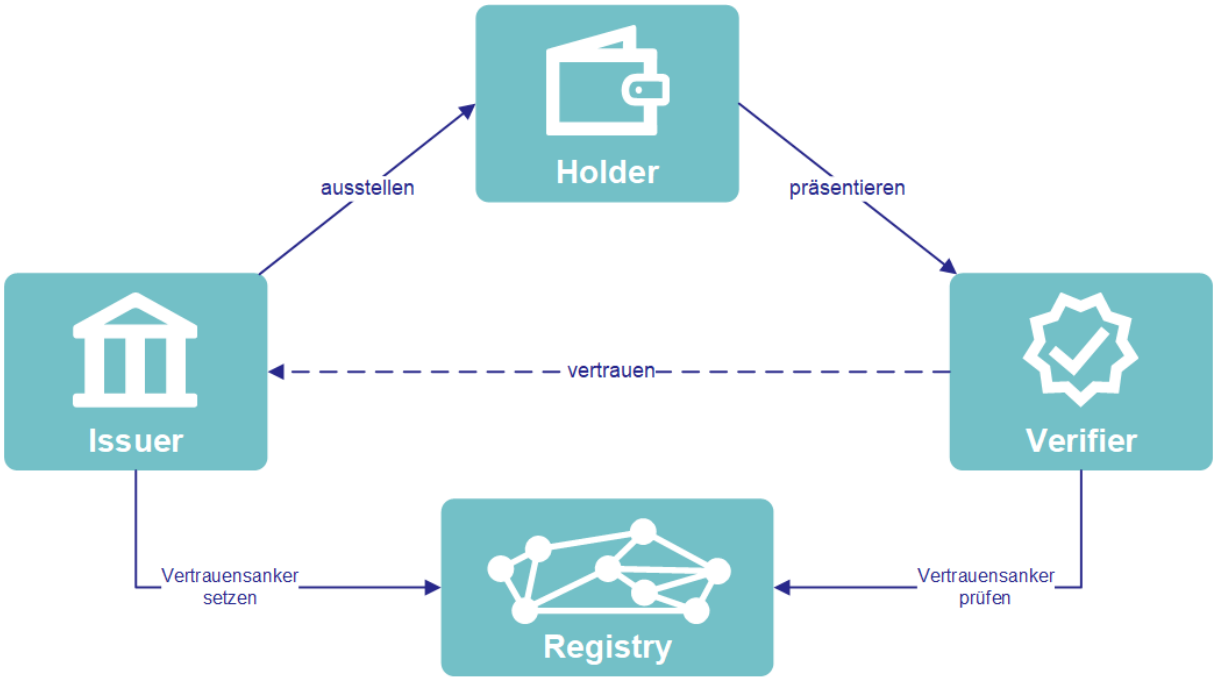


Abbildung 1: Basis-Architektur von SSI

Das Vertrauensdreieck «Ausstellerin/Aussteller (Issuer) – User (Holder) – Prüferin/Prüfer (Verifier, Relying Party)» ist in vielen Vertrauens-Architekturen vorhanden. Bei SSI ist entscheidend, dass die gezeichneten Verbindungen auch direkt die Kommunikationsflüsse darstellen – ohne weitere, dazwischenliegende Instanzen. Der Datenfluss zwischen Issuer und Holder resp. Holder und Verifier läuft als verschlüsselte Peer-to-Peer-Kommunikation ab. Der Kommunikationskanal wird in der Regel mit Hilfe eines QR-Code-Mechanismus erstellt.

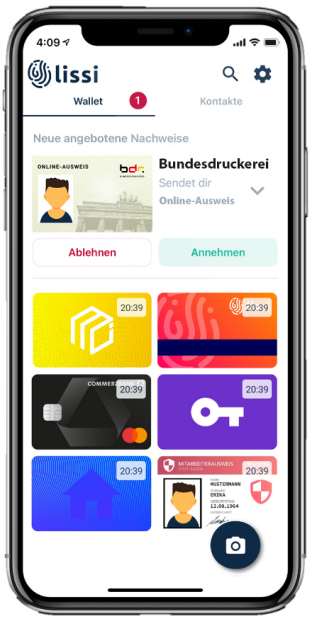


Abbildung 2: Beispiel einer Wallet-App, welche der Holder für das Empfangen, Verwalten und Präsentieren von Verified Credentials verwendet (Quelle: IDunion, lissi)

Vom Issuer werden «Verified Credentials», also bestätigte digitale Daten, an den Holder übermittelt. Dieser speichert sie in einer Wallet-App auf dem Smartphone. Der Verifier kann über den gesicherten Kommunikationskanal Daten vom Holder verlangen. Der Holder kann als Antwort bestimmen, welche Daten effektiv an den Verifier übermittelt werden. Diese Daten können Verified Credentials, Teile davon oder auch vom Holder selbst erfasste Daten sein.

Um die Echtheit von Verified Credentials zu überprüfen, stehen die kryptografischen Beweise – nicht die Daten selbst – in einem Register mit elektronischen Vertrauensankern (eine sog. Registry) zur Verfügung. Eine Registry ist ein in der Regel dezentraler Speicher (z. B. DLT, Blockchain). Jeder Issuer hat darin seine Identität wie auch seine öffentlichen Schlüssel abgelegt. Ein Verifier kann damit ohne Kontakt zum Issuer und ohne Dritt-Instanz die vom Holder präsentierten Daten überprüfen. Die Vertrauensbeziehung zwischen Verifier und Issuer basiert entweder auf einem persönlichen Kontakt oder auf einer öffentlichen Referenz (z. B. Information auf einer Webseite).

Verified Credentials können als «stornierbar/revozierbar» definiert werden. Dem Issuer bleibt damit die Möglichkeit, ein ausgestelltes Credential jederzeit und ohne Kontakt zum Holder für ungültig zu erklären. Die Information dazu wird in der Registry in einer Revokations-Liste geführt.

Der minimale Anwendungsfall für die E-ID ist folgendermassen angedacht:

- Der Staat (Issuer) stellt in einem vollautomatisierten Prozess dem User (Holder) die E-ID als Verified Credential aus.
- Der User verwaltet dieses Verified Credential in einer Wallet-App.
- Beliebige Dritte (Verifier) können die E-ID oder Teile davon erfragen und nach der kontrollierten und durch den User freigegebenen Übermittlung auf Echtheit prüfen.

5.1.3 Vom Staat betriebene Komponenten

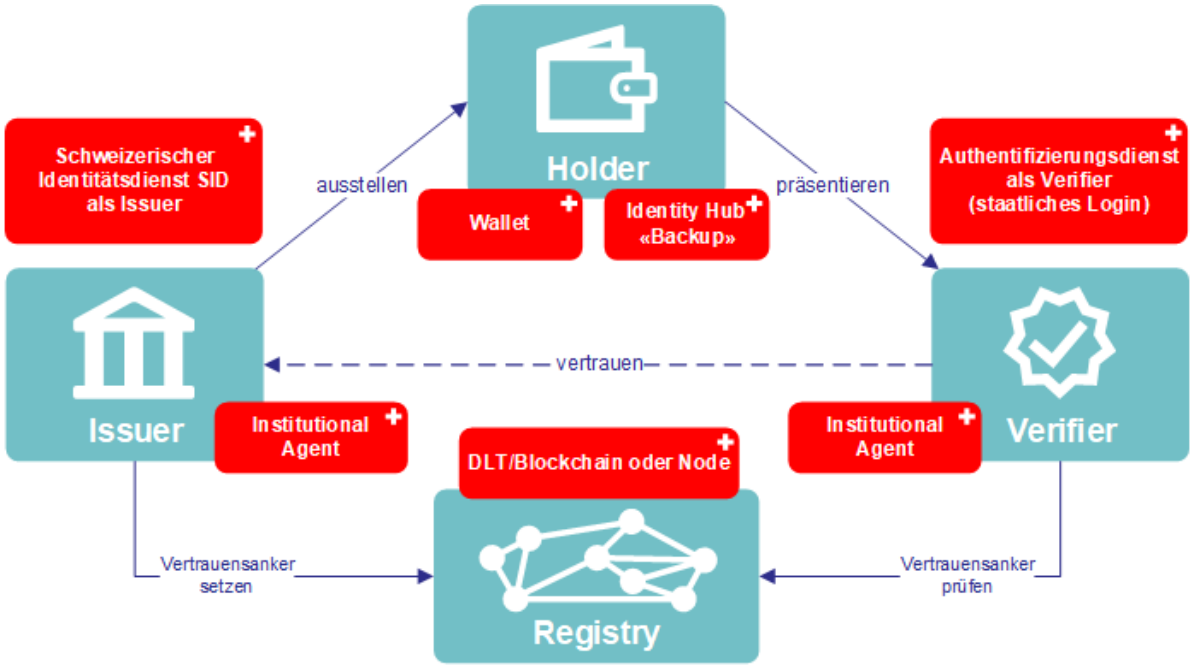


Abbildung 3: Übersicht der staatlich betriebenen oder zur Verfügung gestellten Komponenten (rot) in einer SSI-Architektur

In der Abbildung 3**Fehler! Verweisquelle konnte nicht gefunden werden.** sind in Rot die folgenden technischen Einzel-Komponenten aufgeführt, welche nach der Forderung der Motionen unter der Verantwortung des Staates zu betreiben respektive als freizugängliche Software vom Staat zur Verfügung zu stellen wären:

- **Schweizerischer Identitätsdienst SID:** Digitaler, vollautomatisierter Prozess zur Validation, Resolution und Verifikation einer Person. Resultat des Prozesses (unter Zuhilfenahme eines Institutional Agent) ist die Ausstellung und Übermittlung eines Verified Credentials. Dieses Verified Credential ist die E-ID.
- **Institutional Agent:** Software zum Ausstellen und Verifizieren von Verified Credentials, welche eine API (technische Schnittstelle) für den kompletten Funktionsumfang bereitstellt.

- **Wallet:** Smartphone-Applikation zur sicheren Verwaltung von Credentials.
- **Registry:** Datenspeicher mit elektronischen Vertrauensankern, welcher von allen Teilnehmerinnen und Teilnehmern des E-ID-Ökosystems genutzt und in der Regel als Distributed Ledger (DLT), z. B. mittels einer Blockchain, umgesetzt wird. In der Registry werden kryptografische Beweise, Identitäten und öffentliche Schlüssel von Issuern, Credential Definitionen und Schema von Credentials, aber nie Personen- oder Sachdaten gespeichert.
- **Identity Hub «Backup»:** Komponente zur Vereinfachung von Portabilität und Backup der eigenen Credentials. Ein Identity Hub ist für die Minimalfunktonalität mit E-ID nicht nötig, wäre aber für eine langwährende Benutzerfreundlichkeit und -zufriedenheit in einem Ökosystem mit vielen Credentials empfehlenswert.
- **Authentifizierungsdienst:** Login-Dienst für staatliche und allenfalls auch private Plattformen. Das E-ID-Credential wird dabei als (Multi-)Authentisierungsfaktor genutzt.

Nach der Forderung der in Kapitel 2.2 erwähnten Motionen muss der Betrieb der E-ID-Lösung in Verantwortung einer staatlichen Behörde geschehen. Der minimale Anwendungsfall sollte demzufolge mit ausschliesslich staatlich erstellten resp. betriebenen Komponenten möglich sein. Die technische Offenheit, welche dem Ökosystem zu Grunde liegt, liesse es jedoch zu, dass Komponenten auch von privaten Anbieterinnen bereitgestellt würden (v.a. Institutional Agent, Wallet, Identity Hub). Bei der Registry ist es möglich, dass der Staat davon einen Teil (Node) oder das komplette System – z. B. unter Einbezug der Kantone – zur Verfügung stellt.

Die Komponenten SID, IdP und Identity Hub sind SSI-Externe Systeme, welche sich das SSI-Ökosystem zunutze macht für die Ausstellung, Übermittlung und Echtheits-Überprüfung der E-ID.

Standards für das Zusammenspiel sind heute in Entwicklung. Dadurch können die verschiedenen Komponenten unabhängig voneinander und im Auftrag des Staates entwickelt werden. Die technischen Abhängigkeiten der einzelnen Elemente sind auf die Definition der Standards beschränkt.

5.1.4 Vor- und Nachteile des SSI-Ansatzes

Vorteile:

- Die Philosophie von SSI ist auf Datenschutz, Datensparsamkeit und «privacy by design» ausgerichtet und erfüllt die Forderungen der Motionäre.
- Der generische Ansatz bietet viele Anwendungsmöglichkeiten und Nutzungsszenarien und bleibt der physischen Realität einer «Brieftasche» dabei sehr nah.
- Komplette Übersicht aller empfangenen und gesendeten Transaktionen für den User.
- Internationale Entwicklung geht derzeit stark in diese Richtung, es sind viele Initiativen und Projekte mit diesem Lösungsansatz im Gang.
- Freie, standardisierte Schnittstellen ermöglichen die Anbindung von Drittsystemen.
- Bietet einen direkten, verschlüsselten Peer-to-Peer-Kommunikationskanal zwischen den Parteien. Nebst der Übermittlung von Credentials ist auch die Übermittlung anderer Nachrichten durch den geschützten Kanal möglich.

- Die Basis-Technologien stehen als Open Source Entwicklungen zur Verfügung.

Nachteile:

- Relativ junger Ansatz, einige Grundsatzfragen sind noch nicht abschliessend geklärt und Standards sind noch nicht komplett.
- Das breite Bewusstsein für die Möglichkeit dieses ganzheitlichen Ansatzes (im Vergleich zu einem Login) muss zuerst entstehen.
- Die Verantwortung zur Verwaltung von Verified Credentials wird vollständig dem User übergeben, was Hilfeleistungen durch den Issuer praktisch verunmöglicht.
- Forensische Auswertbarkeit ist schwierig, da das System dezentral und kryptografisch gut geschützt ist. Dies kann beim Missbrauchsfall der E-ID oder anderen Nachweisen dazu führen, dass es schwierig wird nachzuweisen, dass man etwas «nicht gewesen» ist.
- Hochsichere Wallets für spezielle Anwendungen müssten auf Secure Elements in Smartphones aufbauen. Derzeit sind aber noch nicht alle Smartphones damit ausgestattet und die dazu benötigten Entwicklerwerkzeuge sind noch nicht vollständig und einfach verfügbar.

5.1.5 Einbezug von bestehenden, kantonalen E-Government-Plattformen

Auf kantonalen E-Government-Plattformen könnten einerseits Identitätsnachweise durch die E-ID als Prozessschritt eingebaut werden, ähnlich einem Bezahlprozess. Andererseits wäre die Nutzung des staatlichen Authentifikationsdienstes möglich.

Weiter könnte sich ein Kanton das Ökosystem zunutze machen, um selbst als Issuer aufzutreten und eigene Nachweise auszustellen: z. B. Wohnsitzbescheinigung oder Motorfahrzeugausweis. Dies wäre auch für Gemeinden möglich.

In einem Ökosystem mit Ambitions-Niveau 3, bei welchem auch privatwirtschaftliche Akteure als Issuer agieren, wären noch viele weiteren Vereinfachungen seitens kantonaler E-Government-Plattform denkbar: Stellen Arbeitgeberinnen und Arbeitgeber die Lohnausweise und Banken die Zinsausweise als Credential aus, könnten diese z. B. bei der Online-Steuererklärung direkt eingereicht werden, was nachfolgende Prozesse vereinfachen würde.

5.1.6 Offene Fragen zum SSI-Ansatz

Der Kern von Self-Sovereign Identity ist in den aktuellen SSI-Community-internen Diskussionen kaum bestritten. Diskussionspunkte zum vorgeschlagenen Lösungsansatz finden sich vor allem zu Governance-Aspekten und SSI-externen Prozessen:

- Welche Governance-Ebenen gibt es und wer ist dafür zuständig (z. B. Governance-Ebenen nach Trust over IP Framework: Ökosystem, Credentials, Provider, Utility)?
- Muss der Staat auf gewissen Komponenten das Monopol haben? Müssen Wallets staatlich zertifiziert werden? Wird die Auswahl von Wallet und Institutional Agent dem User überlassen? Gibt es eine Regelung, welche Teile kooperativ, welche in Konkurrenz erstellt und betrieben werden?
- Wer betreibt die Registry? Ist eine eigene, nationale Registry nötig oder schliesst man sich einem bestehenden, internationalen Ökosystem an? Wollen oder sollen Kantone,

Städte oder private Unternehmen Speicher-Knoten (Nodes) betreiben dürfen? Welche Technologie wäre zu bevorzugen? Welche Rolle spielt die Datenmenge? Wie löst man Interoperabilitätsfragen zu anderen Registries? Besteht für den Issuer sogar die Wahlfreiheit der Registry?

- Wer darf Issuer sein? Bleibt das System völlig offen zum Gewinn zusätzlicher Anwendungsfälle oder werden die Issuer spezifisch ausgewählt oder berechtigt?
- Wie werden Backups und Transfers von Credentials ermöglicht? Wie können zentrale Backups und damit attraktive Hacker-Angriffsziele vermieden werden? Welche Rolle spielt eine mögliche kryptografische Verbindung zwischen Wallet und Verified Credentials?
- Welche Sicherheitsmechanismen sind für den Zugriff zur Wallet nötig?
- Wie können Verified Credentials auf mehreren Geräten benutzt werden? Wann wäre dies nötig? Reicht es, wenn mit dem einen Smartphone immer eine Verbindung zum Verifier aufgebaut werden kann, unabhängig davon, auf welchem anderen Gerät man gerade den nach der E-ID-fragenden Prozess initiiert hat?
- Wer definiert Credential-Schema, braucht es eine ausgewiesene Stelle zur Definition und Koordination (z. B. eCH) oder werden die Definitionen branchenabhängig entwickelt?
- Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll, um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?

5.2 E-ID Lösung mittels Public-Key-Infrastruktur

5.2.1 Ansatz

Eine Public-Key-Infrastruktur (PKI) ist bereits heute in staatlichem Einsatz zur Sicherung und Validierung von Daten in Ausweisdokumenten mit Chip (Pass, Ausländerausweis). Dabei signiert der Bund als Herausgeber die Daten digital, bevor sie auf dem Chip gespeichert werden und ermöglicht durch die öffentliche Publikation des öffentlichen Schlüssels allen Verifiern die Validierung. Die Technik ist seit über 30 Jahren standardisiert und wird weltweit in verschiedensten Technologien genutzt. Aktuellste Anwendung einer PKI-Lösung ist das Covid-Zertifikat.

Der PKI-Ansatz ist dem SSI-Ansatz ähnlich. Eine als Zertifikat (X.509) ausgestellte E-ID ist eine dezentrale Identität, welche in der vollständigen Kontrolle des Users liegt – und damit auch in dessen vollständiger Verantwortung. Die Privatsphäre des Users bei der Nutzung der E-ID ist gegenüber dem Issuer gegeben, da der Issuer keine Kenntnis des Einsatzes bekommt. Datensparsamkeit zu erreichen ist mit diesem Ansatz jedoch ungleich schwieriger, da die E-ID grundsätzlich als Ganzes signiert ist und damit auch nur als Ganzes an den Verifier zur Identitätsbestätigung übergeben werden kann.

Der Ansatz deckt die Ziele eines digitalen Nachweises in analoger und digitaler Anwendung ab. Die Online-Anwendung von dieser Art von Zertifikaten ist standardisiert (Mutual TLS Authentication). Für die Anwendung in der analogen Welt haben sich verschiedene QR-Code-basierte Verfahren durchgesetzt (z. B. Swiss Pass in der SBB-App, Covid-Zertifikat), wenngleich eine Standardisierung der Offline-Anwendung fehlt.

Der generische Ansatz von Zertifikat-Ausstellungen ermöglicht eine Realisierung aller Ambitions-Niveaus. Das logische oder mathematische Verknüpfen von Nachweisen ist möglich. Das Einbinden von privatwirtschaftlichen Issuern ist ebenfalls technisch möglich, der PKI-Ansatz wird aber in der Regel nur bei Issuern einer kontrollierten resp. kontrollierbaren Gruppe genutzt.

5.2.2 Funktionserklärung

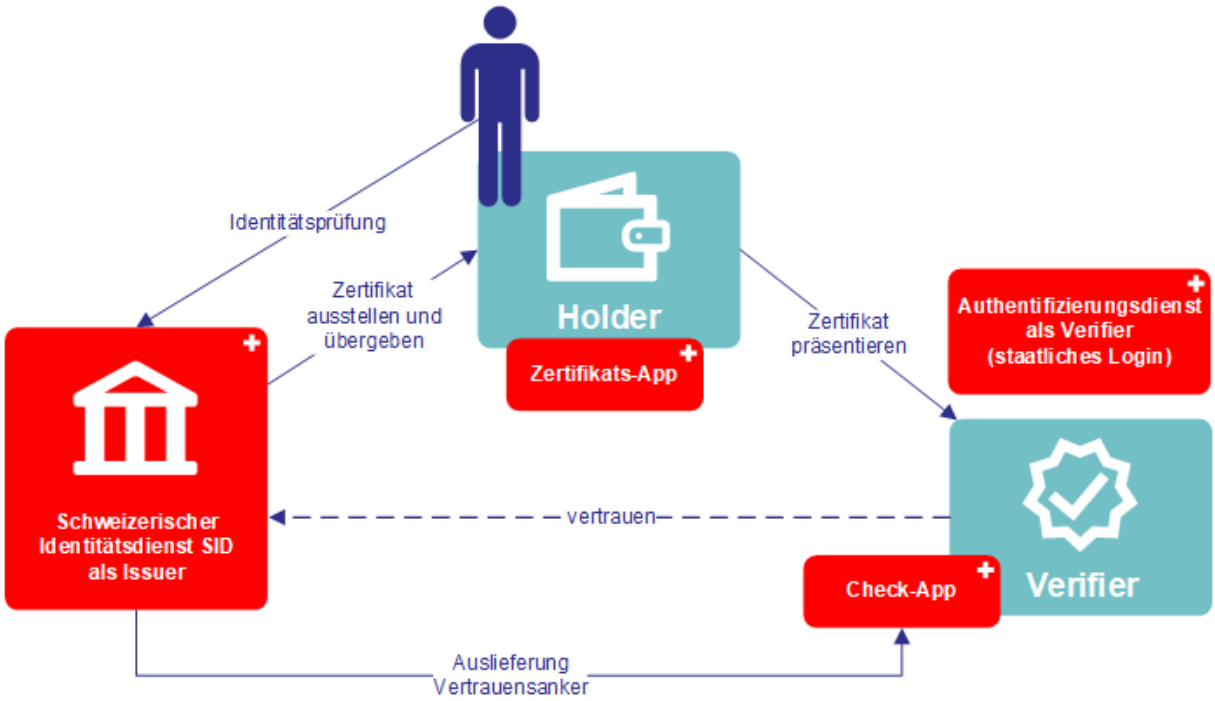


Abbildung 4: Architektur einer PKI-Lösung

Das Vertrauensdreieck «Ausstellerin/Aussteller (Issuer) – User (Holder) – Prüferin/Prüfer (Verifier, Relying Party) » ist auch hier vorhanden. Die Kommunikationsflüsse erfolgen wie dargestellt, jedoch sind im Vergleich zum SSI-Ansatz unterschiedliche Kommunikationskanäle möglich.

Vom Issuer wird nach der Identitätsüberprüfung das Zertifikat ausgestellt und an den User übergeben. Dieser speichert das Zertifikat in einer Zertifikat-App, welche das Zertifikat kopiersicher verwahrt. Bei Bedarf kann der User das Zertifikat über einen digitalen Kanal oder visuell via Barcode einem Verifier präsentieren. Dabei werden alle signierten Daten offengelegt. Der Verifier kann nach Erhalt des Zertifikats mittels Check-App die Gültigkeit des Zertifikats überprüfen. In der Check-App wird dabei der öffentliche Schlüssel des Issuers direkt ausgeliefert und erlaubt damit die Überprüfung auch an einem Ort ohne Internetverbindung.

Um bereits ausgestellte Zertifikate für ungültig zu erklären führt der Issuer eine Revokations-Liste mit allen zurückgezogenen Zertifikaten. Es existieren hierzu verschiedene datenschutzstärkende Verfahren und Protokolle zum Bezug der Revokations-Liste, damit der Verifier dem Issuer nicht zu offen darlegt, wann er denn eine Überprüfung macht. Der Bezug der Revokations-Liste kann online in Echtzeit, periodisch oder sogar dezentral im Selbstabruf gemacht werden.

5.2.3 Vom Staat betriebene Komponenten

In der Abbildung 4 sind in Rot die folgenden technischen Einzel-Komponenten aufgeführt, welche nach der Forderung der Motionen unter der Verantwortung des Staates zu betreiben respektive als Open Source Software zur Verfügung zu stellen wären:

- **Schweizerischer Identitätsdienst SID:** System für den digitalen, vollautomatisierten Prozess zur Validation, Resolution und Verifikation einer Person. Resultat des Prozesses ist die Ausstellung und Übermittlung des Zertifikats. Das Zertifikat ist die E-ID. Zusätzlich führt das System die Revokations-Liste und hält diese zum Abruf bereit.
- **Zertifikats-App:** Applikation zum Empfangen, Speichern und Präsentieren von Zertifikaten.
- **Check-App:** Applikation zum Empfangen, Anzeigen und Überprüfen von Zertifikaten.
- **Authentifizierungsdienst:** Login-Dienst für staatliche und allenfalls auch private Plattformen. Das E-ID-Credential wird dabei als (Multi-)Authentisierungsfaktor genutzt.

5.2.4 Vor- und Nachteile des PKI-Ansatzes

Vorteile:

- Einsatz langjährig erprobter und stark verbreiteter Techniken und Technologien.
- Unterschiedlichste Ausprägungen und Anforderungen an die Lösung sind mit diesem Ansatz adressierbar.
- Die Identitäten und deren Nutzung sind dezentralisiert. Bei der Nutzung entstehen keine zusätzlichen Randdaten. Der Anforderung «privacy by design» wird bei der Anwendung Rechnung getragen.
- Unterstützt das Credo «E-ID ist ein Ausweis, nicht nur ein Login»

Nachteile:

- Verwahrung der Identitäten wird vollständig an den User abgegeben und höhere Verlässlichkeit an die Verwahr- und Einsatzsicherheit sind fast immer an zusätzliche Hardware gebunden (z. B. für Kopierschutz oder starke Multi-Faktor-Authentifizierung).
- Grundsätzlich können Zertifikate nur als Ganzes präsentiert werden. Um Datensparsamkeit zu ermöglichen wären Teilzertifikate denkbar, der User müsste dann aber mehrere E-ID-Zertifikate beantragen und verwalten, eine situative Auswahl einzelner Attribute ist dadurch schwerfällig.
- Unterschiedliche mögliche Übermittlungskanäle zwischen Issuer, Holder und Verifier erschweren den «korrekten, sicheren Umgang» mit den Zertifikaten.

5.2.5 Einbezug von bestehenden, kantonalen E-Government-Plattformen

Auf kantonalen E-Government-Plattformen könnten einerseits Identitätsnachweise durch die E-ID als Prozessschritt eingebaut werden, ähnlich einem Bezahlprozess. Andererseits wäre die Nutzung des staatlichen Authentifikationsdienstes möglich.

Weiter könnte sich ein Kanton das Ökosystem zunutze machen, um selbst als Issuer aufzutreten und eigene Zertifikate auszustellen: z. B. Wohnsitzbescheinigung oder Motorfahrzeugausweis. Dies wäre auch für Gemeinden möglich.

5.2.6 Kartenbasierte PKI-Lösungen

Als Variante des PKI-Ansatzes wäre – anstelle der Zertifikats-App auf seinem Smartphone – auch die Verwendung einer Chip-Karte als sicherer Speicher für das Zertifikat möglich. Um das Zertifikat zu präsentieren, wird ein Kartenlesegerät benötigt – in der analogen Welt muss der Verifier damit ausgestattet sein, bei der Online-Anwendung der User. Viele heute verfügbaren Smartphone-Modelle eignen sich zum Auslesen von Chip-Karten. Ohne ein solches ist ein spezielles Kartenlesegerät nötig.

Die SuisseID und der Deutsche neue Personalausweis (nPA) bauen beide auf diesem Prinzip und bieten u.a. eine digitale Identifikation. Der durchschlagende Erfolg blieb bei beiden Umsetzungen aus, wobei die Kartennutzung an sich nur eines der Hindernisse war. International zeichnet sich derzeit eine Abkehr von E-ID-Systemen mit physischen Chip-Karten ab. Zukunftsträchtige Systeme setzen auf die Nutzung von Mobilgeräten/Smartphones mit speziellen Apps, was vor allem durch hohe Benutzerfreundlichkeit für eine bessere Adoption sorgt. Als Beispiel hat das E-Government-Pionier-Land Estland ursprünglich mit einer Chip-Karte begonnen, danach eine Mobile-ID mit Verknüpfung zu SIM-Karten eingeführt und bietet heute in erster Linie eine komplett dematerialisierte App-Lösung (Smart-ID) an. Auch in Deutschland wird derzeit nach der Lösung gesucht, die Daten des nPA sicher auf dem Smartphone hinterlegen zu können, damit die physische Karte für die Verwendung nicht mehr nötig ist. Die Schweiz sollte von diesen Erfahrungen profitieren.

Gegen eine konkrete Umsetzung mittels staatlicher Identitätskarte mit Chip, ähnlich dem nPA, sprechen nebst den oben genannten Gründen noch weitere:

- Zwar ist eine Einführung einer neuen Identitätskarte in den kommenden Jahren vorgesehen. Die E-ID-Funktionalität war jedoch nicht Teil der durchgeführten öffentlichen Ausschreibung und müsste nachträglich beschafft werden. Letzteres gilt auch für alle Ausländer- und Diplomatenausweise.
- Der Roll-Out eines physischen Ausweisdokuments in der Schweiz dauert aufgrund der Gültigkeitsdauer mindestens 10 Jahre (plus Vorlaufzeit). Die Adoption einer E-ID vom Erneuerungszyklus der Identitätskarte abhängig zu machen ist nicht zielführend.
- Der Einsatz eines physischen Trägers zur Übermittlung der Personeninformationsdaten schränkt die Auswahl und Möglichkeiten einer zukunftsfähigen E-ID-Lösung ein.

5.2.7 Offene Fragen zum PKI-Ansatz

- Sind anwendungsspezifische Zertifikate für die E-ID notwendig? Liessen sich diese auf eine kleine Anzahl beschränken?
- Welche Vorteile würde ein Public Key Directory, eine Verwaltungsinstanz der öffentlichen Schlüssel und Revokations-Listen bringen? Wie wären damit die Unterschiede zum SSI-Ansatz zu gewichten?
- Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll,

um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?

5.3 E-ID-Lösung mittels zentralem staatlichem Identitätsprovider

5.3.1 Ansatz

Das gescheiterte E-ID-Gesetz sah eine Lösung mit Einbezug von anerkannten Identitätsprovider-Betreiberinnen von Staat und Privatwirtschaft vor. Die Idee hinter dem Einbezug war, dass möglichst schnell eine möglichst breite Benutzerbasis mit einer E-ID ausgestattet ist und gleichzeitig bereits Anwendungsmöglichkeiten vorhanden sind. Der Einbezug von Privaten war dann aber einer der Gründe für das Scheitern des E-ID-Gesetzes in der Volksabstimmung.

Die Grundidee, den Usern eine staatlich verifizierte elektronische Identität auf Basis eines Logins zu ermöglichen, kann auch mit einem zentralen, staatlichen Identitätsprovider (IdP) erreicht werden. Mit diesem vereinfachten Ansatz würden sich im Vergleich zur Architektur gemäss abgelehntem E-ID-Gesetz bestimmte Interoperabilitäts- und Datenflussfragen erübrigen, eine rasche Verbreitung würde jedoch schwieriger. Verantwortlich für den Betrieb des Systems ist der Bund. Die Lösung ermöglicht primär ein staatliches, einheitliches E-Government-Login.

Die technologischen Grundlagen und Protokolle (z. B. OpenID Connect) für diesen Ansatz sind etabliert und für das Ambitions-Niveau 1 geeignet. Um höhere Ambitions-Niveaus abzudecken, sind Erweiterungen nötig, welche derzeit in Entwicklung sind.

5.3.2 Funktionserklärung

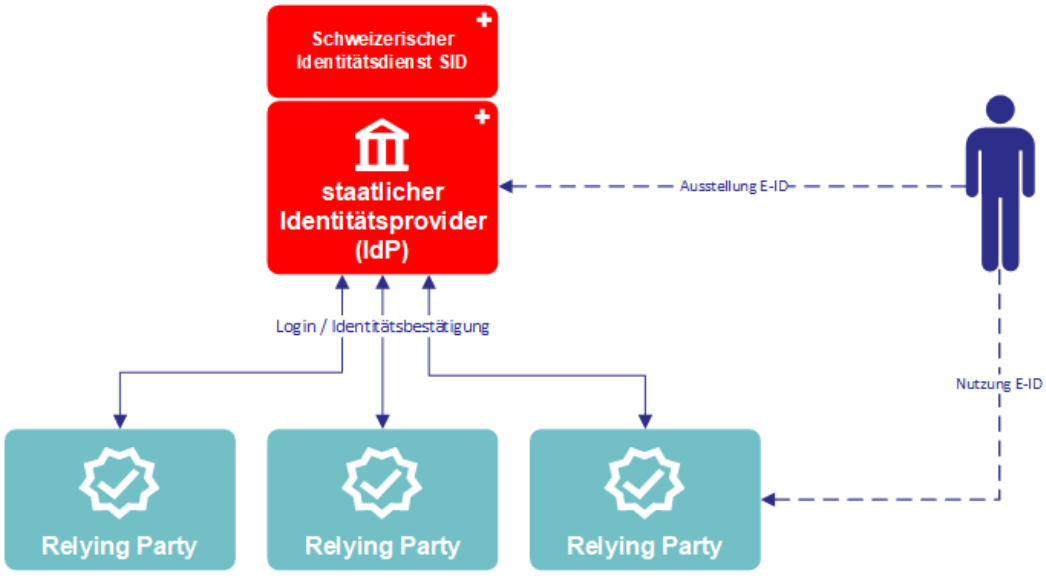


Abbildung 5: Architektur-Übersicht einer E-ID-Lösung auf Basis eines zentralen, staatlichen Identitätsproviders

Im Zentrum dieses Lösungsansatzes steht ein staatlicher Identitätsprovider. Dieser führt die E-ID des Users, welche durch einen Login-Prozess genutzt werden kann. Beliebige Relying Parties, z. B. kantonale E-Government-Plattformen, können sich an den staatlichen IdP anbinden. Dazu bestehen zwei Möglichkeiten:

- Die Relying Party nutzt den IdP-Dienst für aktives Identitäts-Management, so dass ein Konto-Login des Users mittels staatlichem IdP gemacht wird.
- Die Relying Party nutzt den IdP-Dienst nur als «Ausweis-Service», bei dem der User in einem Prozessschritt bestimmte Attribute der E-ID an die Relying Party freigeben kann, ohne dass der staatliche IdP die Funktion des Identitäts-Managements übernimmt.

Die Ausstellung einer E-ID initiiert der User direkt beim staatlichen IdP. Der IdP nutzt für die vollständige Verifizierung den schweizerischen Identitätsdienst SID (siehe 5.4 Ausstellungsprozess E-ID).

Relying Parties könnten auf Basis einer angebundenen E-ID grundsätzlich verknüpfte Nachweise (Ambitions-Niveau 2) anbieten. Dabei wäre ein vom IdP unabhängiger Technologieansatz möglich, z. B. ähnlich dem PKI-Ansatz (siehe 5.2 E-ID Lösung mittels Public-Key-Infrastruktur).

5.3.3 Vom Staat betriebene Komponenten

Der geringe Umfang eines Ökosystems mit einem zentralen IdP wirkt sich auf die Umsetzung aus. In der Abbildung 5 sind in Rot die folgenden technischen Einzel-Komponenten aufgeführt, welche nach der Forderung der Motionen unter der Verantwortung des Staates zu betreiben respektive als freizugängliche Software zur Verfügung zu stellen wären:

- **Schweizerischer Identitätsdienst SID:** Digitaler, vollautomatisierter Prozess zur Validation, Resolution und Verifikation einer Person. Resultat des Prozesses ist die Bestätigungs-Übermittlung der Verifikation an den IdP zum Anlegen der E-ID.
- **Identitätsprovider:** Staatlicher Identitätsprovider (IdP) welcher die E-ID verwaltet und durch einen Login-Prozess nutzbar macht für staatliche und allenfalls auch private Relying Parties.

5.3.4 Vor- und Nachteile des IdP-Ansatzes

Vorteile:

- Einfache Architektur, übersichtliche Lösung
- Breit genutzte Technologien und Protokolle
- Kopplung von Personen-Verifikation und E-ID-Login macht daraus eine sichere Login-Möglichkeit.

Nachteile:

- Lösung steht im Widerspruch gegenüber den in den Motionen geforderten Grundsätzen. Sie ist nicht dezentral und «privacy by design» ist nicht gegeben, da der Ansatz auf vollem Vertrauen gegenüber dem IdP basiert. Die Sorgen um Datensparsamkeit und Randdaten wären etwas entschärft durch die Tatsache, dass die Gesamt-Verantwortung des Systems beim Bund liegt und damit eine genaue Kontrolle möglich ist.
- Ungelöstes Huhn-Ei-Problem: Chancen einer schnellen Adaption durch User wie auch einer raschen und freiwilligen Anbindung vieler Dienstleistungsmöglichkeiten sind gemäss Erfahrungen im Ausland eher gering.

- Eingeschränktes Nutzungsszenario, eher schwierige Nutzung in der analogen Welt.
- Das Ökosystem ist nur schwer auf höhere Ambitions-Niveaus ausbaubar.
- Keine Trennung von Ausstellung der E-ID und deren Nutzung. Dies widerspricht der heutigen Nutzung von Identitätsdokumenten und entspricht so nicht dem Pendant in der analogen Welt.
- Verknüpfungen der E-ID mit weiteren Nachweisen nur durch die verbundenen Services möglich, was die Anwendung dieser Nachweise erschwert.
- Folgt nicht dem Grundsatz «E-ID = digitaler Ausweis».
- System-Abhängigkeit von einem IdP.

5.3.5 Einbezug von bestehenden, kantonalen E-Government-Plattformen

Der zentrale IdP wird an die existierenden kantonalen E-Government-Plattformen angeschlossen. Das Zugriffs- und Rollenmanagement bleibt bei der jeweiligen Plattform, die Identität käme aber vom Bundes-IdP, welcher ein sicheres Login-Verfahren garantiert. Dies könnte eine Erleichterung für Kantone darstellen, welche noch keine eigene Login-Lösung haben und eine Entlastung für die Kantone, welche heute einen eigenen IdP betreiben. Kantone mit bestehenden IdP könnten den Bundes-IdP auch zusätzlich an ihre E-Government-Plattformen anbinden, was in der Praxis heisst, dass eine Verknüpfung einer bereits vorhandenen Identität beim eigenen IdP mit der vom Bundes-IdP gelieferten Identität gemacht wird und somit nicht ein paralleler Betrieb darunter zu verstehen ist. Dabei ist anzumerken, dass gerade für mobile Applikationen eine Architektur mit mehreren genutzten IdP nur schwer umzusetzen ist (Refresh-Token etc.). Beim Einsatz eines Bundes-IdP für eine kantonale Plattform müsste zudem dem Thema «Support» die entsprechende Beachtung geschenkt werden, damit User bei Problemen eine klare Ansprechstelle hätten.

Grundsätzlich wäre eine Föderation von bereits bestehenden kantonalen IdP möglich. Eine Föderation brächte aufgrund der Verteilung auf verschiedene Systeme eine Art Dezentralisierung (Regionalisierung). Föderative Systeme bedeuten aber im Vergleich zu einer zentralen IdP-Lösung nebst einem grösseren Aufwand auch einen grösseren Bedarf an Regulation und Kontrollmechanismen (Standards, Vertrauensniveau der Identität, Datenschutz etc.). Bei der Weiterentwicklung zusätzlicher Funktionen, wie z. B. der Ausstellung von Alterszertifikaten, müssten dann stets zuerst Standards festgelegt werden und anschliessend wäre jeder IdP gezwungen, diese Weiterentwicklung ebenfalls umzusetzen. Nur so könnten alle User, unabhängig des kantonalen IdP, die gleichen E-ID-Funktionen nützen. Trotz Wiederverwendung bestehender IdP einiger Kantone werden die Aufwände für den Staat wesentlich höher eingeschätzt als bei der Umsetzung eines staatlichen, zentralen IdP, welcher an kantonale Plattformen angebunden werden muss.

5.3.6 Offene Fragen zum IdP-Ansatz

- Wer darf den zentralen staatlichen IdP als Login-Lieferant und zur Bestätigung bestimmter Attribute nutzen? Ist die Anbindung staatlichen Plattformen vorenthalten oder steht diese auch privatwirtschaftlichen Systemen zur Verfügung?
- Welche E-Government-Plattformen würden einen staatlichen IdP anbinden? Wie viele Kantone benötigen zum Zeitpunkt der Umsetzung noch eine IdP-Lösung?

- Ist die Auslagerung des Logins für Kantone und weitere Relying Parties überhaupt sinnvoll?
- Wer wird Vertragspartner gegenüber den Relying Parties und wird für die Vertragserstellung zuständig? Welche Voraussetzungen müssten Relying Parties erfüllen? Wie wird die Kontrolle sichergestellt?

5.4 Ausstellungsprozess E-ID

Der Ausstellungsprozess einer E-ID ist unabhängig vom Lösungsansatz. Dabei sind folgende Schritte nötig:

- Die antragstellende Person legt einen bestehenden Identifikationsnachweis vor.
- Der Identifikationsnachweis wird mit der Person abgeglichen.
- Die E-ID wird vom Staat an die Person übergeben.

Ein vollautomatisierter Online-Prozess, wie z. B. in Italien, ist für eine schnelle und einfache Verbreitung anzustreben. Das schliesst Hilfestellungen an physischen Schaltern nicht aus. Der Staat betreibt das dafür nötige System und übermittelt den digitalen Nachweis über einen gesicherten Kanal an die antragsstellende Person.

Mit dem Grundsatz, dass Datensparsamkeit und abgeleitete Attribute möglich sein sollten, kann der Inhalt einer E-ID neu betrachtet werden. So muss nicht aus Datenschutzbedenken vorsorglich auf Attribute verzichtet werden, weil die Kontrolle zur Weitergabe jedes einzelnen Attributs beim User liegt. In der E-ID würden die Daten integriert, welche auch auf einem physischen Ausweisdokument vorhanden sind: Vorname, Name, Geburtsdatum, Gesichtsbild, Heimatort, Geburtsort, Nationalität, Ausstellungsdatum. Denkbar wäre zusätzlich eine Integration der AHV-Nummer, welche bei vielen Behördengeschäften erforderlich ist und deshalb für den User praktisch wäre.

Um International eine hohe Interoperabilität zu ermöglichen ist ein hohes Sicherheitsniveau bei der Ausstellung der E-ID (Identifikation und Verifikation) anzustreben. Das Sicherheitsniveau einer E-ID kann jedoch nicht isoliert auf die Ausstellung betrachtet werden. Beim Speichern und Präsentieren des Nachweises oder bei der Anwendung durch den digitalen Ausweis sind je nach Umsetzung unterschiedliche Sicherheitsniveaus möglich. Es macht deshalb keinen Sinn, sich in der Diskussion auf ein Sicherheitsniveau zu fixieren – die gesamte Vertrauenskette muss bei jedem Anwendungsfall angeschaut werden, idealerweise mit einem stark vertrauenswürdigen Anker: der E-ID.

Die Details der Umsetzung des Ausstellungsprozesses sind noch zu erarbeiten und sind deshalb nicht Gegenstand dieses Grobkonzepts.

6 Umsetzungsplanung

6.1 Zeitplan

Nach der öffentlichen Diskussion über die verschiedenen Fragestellungen des vorliegenden «Zielbilds E-ID» und deren Auswertung wird der Bundesrat voraussichtlich bis Ende 2021 einen Richtungsentscheid fällen. Aufgrund der daraus resultierenden Vorgaben wird der Vorentwurf zum neuen E-ID-Gesetz erarbeitet, damit Mitte 2022 die Vernehmlassung zum Gesetz eröffnet werden kann. Es folgen die Erarbeitung der Botschaft, die parlamentarische Beratung,

ein allfälliges Referendum sowie der Erlass der Ausführungsbestimmungen. Wann die Einführung einer staatlichen E-ID möglich ist, hängt von diesem Prozess ab.

Um Zeit zu gewinnen, ist es möglich, parallel zum Gesetzgebungsprozess mit der Umsetzungsplanung bzw. der effektiven Umsetzung zu beginnen. Dabei könnten bereits während der technischen Umsetzungsplanung erste Pilot-Anwendungen und Proof of Concept umgesetzt werden, um mögliche Fragen in der Praxis zu klären. Nach ersten richtungsweisenden Diskussionen im Parlament könnten dann Ausschreibungen und Entwicklungsarbeiten in die Wege geleitet werden.

6.2 Kostenschätzung der verschiedenen E-ID-Lösungsansätze

Genauso wie beim Zeitplan bestehen auch bezüglich Kostenschätzungen viele Unbekannte. Eine fundierte Schätzung ist aufgrund der noch völlig offenen Anforderungen nicht möglich. Man kann davon ausgehen, dass sich die Umsetzung aller aufgezeigten Lösungsansätze in einem ähnlichen Kostenrahmen bewegt. Deshalb wird zu diesem Zeitpunkt auf eine grobe Kostenschätzung verzichtet. Die Kosten lassen sich in drei Bereiche aufgliedern:

1) Kosten für den Aufbau, Betrieb und Weiterentwicklung der funktionalen und technischen Systeme.
2) Kosten für die Förderung des Nutzens und Einsatzes der E-ID durch User, Wirtschaft und Staat durch geeignete Kommunikation sowie Pilot- und Förderprogramme.
3) Kosten für die Sicherstellung der Kompatibilität zur Sicherstellung der Nutzenentwicklung (International, Föderal, Anforderungen aus der Wirtschaft).

Naturgemäss werden die Kosten mit steigendem Ambitions-Niveau höher ausfallen. Dies ist aber auch direkt mit einer höheren Nutzenerwartung verbunden.

6.3 Finanzierungsmöglichkeiten

Wenn ein Hauptziel lautet, eine «vielgenutzte Plattform» zu schaffen, wäre eine staatlich subventionierte Finanzierung zu prüfen: Der Staat kommt für die Aufwendungen auf und sieht es als Basis-Beitrag zur Digitalisierung der Schweiz an. Die Einwohnerinnen und Einwohner der Schweiz erwarten eine staatliche, digitale Identität als Grundleistung des Staates.

Dieser Ansatz erfüllt zwar nicht das Erfordernis, staatliche Leistungen mit kostendeckenden Gebühren zu erbringen, verhindert jedoch einen abschreckenden bürokratischen Aufwand. Wird eine staatlich subventionierte Finanzierung abgelehnt, so sollten aufwändige Gebührenmodelle vermieden werden, um die Verbreitung nicht unnötig zu behindern.

Internationale Erfahrungen haben gezeigt, dass User nicht bereit sind, für eine E-ID zu bezahlen. Für den User muss die E-ID respektive die Nutzung der damit verbundenen Vertrauensinfrastruktur kostenlos angeboten werden können.

Bei der Frage, welche Rollen ihren Teil an die Finanzierung beitragen könnten, fällt bei dezentralen Systemen durch die Datenschutzvorkehrungen in der Regel die «Verifier/Relying Party»-Seite weg. Bleiben die Issuer, die z. B. in SSI durch eine Gebühr für das Hinterlegen auf der Registry ihrer eigenen Identities, Schema, Credential- oder Revokations-Definitionen einen Teil der Infrastruktur mitfinanzieren könnten (das effektive Ausstellen eines Verified Credentials wäre kostenlos, da nichts in die Registry geschrieben werden muss). Bei einer

IdP-Lösung könnten im Rahmen der Nutzungsverträge zwischen IdP und Relying Parties Tarife festgelegt werden.

7 Öffentliche Diskussion des Zielbilds E-ID

Das «Zielbild E-ID» ist – auch wenn es drei Lösungsansätze enthält – in erster Linie eine Diskussionsgrundlage. Die Schweiz steht vor einem wichtigen Richtungsentscheid, zu dem in der Fachöffentlichkeit Meinungen eingeholt werden. Was will die Schweiz für eine E-ID, welches Ökosystem wünschen sich User, Gemeinden und Kantone sowie die Wirtschaft, welche Anwendungsfälle brennen den Usern und den Dienstleiterinnen unter den Fingernägeln?

Als Richtlinie für schriftliche Stellungnahmen zum «Zielbild E-ID» sollte mindestens zu folgenden Punkten Position bezogen werden:

- Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?
- Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?
- Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z. B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Selbstverständlich können in den Stellungnahmen wie auch in der Diskussion zu allen weiteren Aspekten rund um die E-ID zusätzliche Kommentare beigetragen werden. Ebenfalls sollen in der Diskussion Fragen gestellt und Ansätze hinterfragt werden. Die Diskussion ist der Moment, um das Blickfeld zu erweitern, um breiter zu denken. Soll die Schweiz es wagen, auf eine E-ID-Lösung mit Potenzial zu setzen, ohne die genauen Details zu kennen? Oder reicht eine rein staatlich genutzte Minimal-Variante? Die Diskussion soll Anhaltspunkte und Antworten zu diesen Fragen liefern.

Die öffentliche Diskussion läuft in verschiedenen Sounding-Boards ab mit diversen Vertreterinnen und Vertretern aus der Politik, Wirtschaft, Wissenschaft, Zivilgesellschaft, den Kantonen und der Verwaltung. Zudem wird eine öffentliche, konferenzielle Diskussion organisiert. Die Resultate der verschiedenen Diskussionen sowie die bereits bekannten Anforderungen werden zusammengetragen und dienen dem Bundesrat als Basis für einen grundsätzlichen Richtungsentscheid. Am Ende muss ein politisch mehrheitsfähiger Gesetzesentwurf entstehen, der vom Parlament und Volk akzeptiert werden kann.