



Für einen staatlichen elektronischen Identitätsnachweis in der Schweiz

Positionspapier der Swiss Data Alliance



Vorbemerkung

Dieses Positionspapier nimmt grundsätzlich Stellung zum Thema des staatlichen elektronische Identitätsnachweises (staatliche E-ID).

Das Positionspapier wurde in der ursprünglichen Fassung (Version 1.0) von Oktober 2016 bis Februar 2017 von den folgenden Personen erarbeitet:

André Golliez (Redaktion)
Prof. Dr. Abraham Bernstein
Dr. Alain Gut
Dr. Christian Laux
Prof. Dr. Alessia Neuron
Prof. Dr. Reinhard Riedl
Dr. Hans Rudolf Sprenger

Der Expertenausschuss der Swiss Data Alliance hat das Positionspapier am 27. Januar 2017 diskutiert.

Am 22. Februar 2017 hat der Bundesrat den Vorentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) mit Vernehmlassungsbericht publiziert. Die Swiss Data Alliance hat auf der Grundlage dieses Positionspapiers eine Stellungnahme zum Entwurf des E-ID-Gesetzes erarbeitet und am 29. Mai 2017 eingereicht.

Die vorliegende überarbeitete und leicht gekürzte Fassung des Positionspapiers (Version 1.1) wurde für eine Publikation im Online-Magazin SocietyBytes.swiss erstellt

Juli 2017

Inhaltsverzeichnis

1.	Einleitung	4
2.	Lösungsskizze	7
3.	Rechtliche Grundlagen	9
4.	Die ökonomische Sicht	11
5.	Die Aufgaben des Staates	13
6.	Anforderungen an eine staatliche E-ID	15

1. Einleitung

Zum Nachweis ihrer Identität stehen allen Einwohnerinnen und Einwohnern der Schweiz sowie den im Ausland lebenden Schweizer Bürgerinnen und Bürgern in der analogen Welt staatliche Ausweispapiere wie der Pass, die Identitätskarte oder der Ausländerausweis zur Verfügung. Die Erstellung, Abgabe und Verwaltung dieser Papiere ist eine hoheitliche Aufgabe und wird auf Basis der amtlichen Personenregister wahrgenommen. Diese staatlichen Identitätsdokumente geniessen ein hohes Vertrauen. Fälschungen und Missbrauch werden in der Regel rasch entdeckt und geahndet.

In der digitalen Welt fehlt in der Schweiz bis anhin eine vergleichbare einfache und breit abgestützte Lösung. Wenn wir in der globalen digitalen Wirtschaft mithalten möchten, muss sich dies bald ändern. Die 2010 eingeführte Swiss-ID, der Schweizer Standard für sichere Authentifikation und elektronische Signatur, fand bis anhin keine breite Akzeptanz und fristet ein Nischendasein. Mangels einer staatlich anerkannten und verbreiteten elektronischen Identität in der Schweiz ist die Entwicklung digitaler Dienstleistungen der öffentlichen Hand und im privaten Sektor eingeschränkt. Silolösungen einzelner Unternehmen und Organisationen für die Identifikation ihrer Kunden sind aus diesem Grund bis heute die Regel.

Worin besteht der staatliche elektronische Identitätsnachweis?

Der staatliche elektronische Identitätsnachweis (staatliche E-ID) ist keine Nummer. Die E-ID ist eine Sammlung von verschiedenen geprüften Angaben über eine Person. Die Gesamtheit von verschiedenen, geprüften Angaben über eine Person (d.h. die „gesamte E-ID“) sowie nicht selten bereits Teile der E-ID (also Untermengen dieser Angaben) ermöglichen, eine Person zu authentisieren. Die E-ID wirkt damit wie ein Ausweis.

Eine eindeutige Identifikationsnummer (Personennummer) *kann* zu den Attributen des elektronischen Identitätsnachweises zählen und die technische Verwendung der E-ID erleichtern. Die E-ID darf aber nicht auf eine technische Nummer reduziert werden. Das vom Staat betriebene System für die E-ID kann vielmehr auch so aufgesetzt sein, dass der Staat im Zusammenhang mit einer Autorisierungsanfrage einen transaktionsbezogenen Token ausgibt (der Token könnte eine ad-hoc generierte Nummer sein, die nur einmal eingesetzt werden kann). Dies würde es konzeptionell ermöglichen, die E-ID von nummernbasierten Identifikatoren zu befreien.

Bedürfnis nach einem staatlichen elektronischen Identitätsnachweis

Aus Sicht der Benutzer – alle Einwohnerinnen und Einwohner der Schweiz sowie die im Ausland lebenden Schweizer Bürgerinnen und Bürger - ist ein staatlich gewährleisteter elektronischer Identitätsnachweis analog zum Pass, zur ID oder zum Ausländerausweis wünschenswert und entspricht einem Grundrecht.¹ Genau wie in der analogen Welt benötigt der Benutzer nicht für jede digitale Transaktion einen staatlichen Identitätsnachweis. Aber für bestimmte Handlungen ist dieser Nachweis unerlässlich. Dazu zählen z.B. die elektronische Stimmabgabe, der Zugang zum elektronischen Patientendossier, Eintragungen in amtlichen Registern oder das Leisten einer amtlich beglaubigten Unterschrift. In Anbetracht zunehmender Internetkriminalität spielt ein staatlich gewährleisteter elektronischer Identitätsnachweis eine zentrale Rolle, um vertrauenswürdige Geschäftsbeziehungen aufzubauen und zu unterhalten.

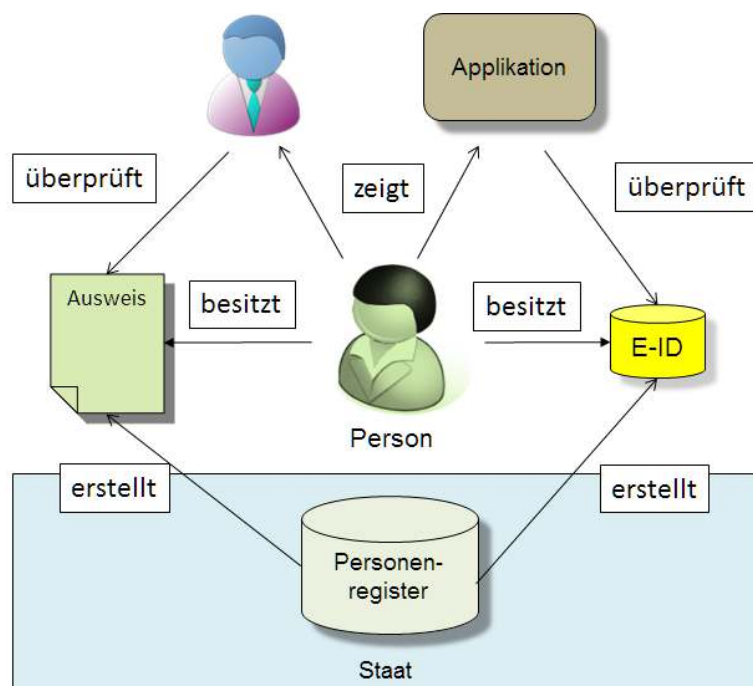
¹ Siehe unten, Abschnitt 2.

Der staatliche elektronische Identitätsnachweis (staatliche E-ID) muss so vertrauenswürdig und einfach handhabbar sein wie die analogen staatlichen Identitätsdokumente. Dies impliziert, dass die Ausgabe der staatlichen E-ID als hoheitliche Aufgabe vom Staat selber wahrgenommen werden muss. Dass ein Dritter im Rahmen einer verwaltungsrechtlichen Delegation die Erstellung und Verwaltung der staatlichen E-ID umsetzt, ist kein Widerspruch.

Der staatliche elektronische Identitätsnachweis löst nicht alle Probleme der elektronischen Identität. Wie ihr Pendant in der analogen Welt (Pass, ID etc.) sollte die staatliche E-ID nur, aber immerhin den staatlichen Identitätsnachweis für jene hoheitlichen Anwendungen ermöglichen, für welche der Staat einen solchen Nachweis voraussetzt ist (z.B. beim Grenzübertritt oder beim Wohnortwechsel). Daneben bestehen für einen Ausweis zahllose weitere Anwendungsbereiche. Für diese weiteren (nicht-hoheitlichen) Anwendungsbereiche im digitalen Raum, welche eine elektronische Identifizierung verlangen, ist die staatliche E-ID nur eine von zahlreichen Möglichkeiten des digitalen Identitätsnachweises (z.B. Nummer und Codes einer Kreditkarte). In diesem nicht-hoheitlichen Bereich ist es keine hoheitliche Aufgabe des Staates, die Identifikationsmöglichkeit zur Verfügung zu stellen. Darüber hinaus können in Zukunft Eigenschaftszertifikate (z.B. Hochschulabschlüsse, Fachausweise, Schiffsführerausweise) von den dazu berechtigten Institutionen mit Bezug auf die E-ID des Inhabers auch digital ausgegeben und im digitalen Geschäftsverkehr genutzt werden. Dies reduziert insbesondere in jenen Bereichen, in denen bisher Qualifikationen per Fotokopie belegt werden die Betrugsgefahr und erspart aufwendige Überprüfungsverfahren.

Einsatzbereiche des staatlichen elektronischen Identitätsnachweises

Basis für den staatlichen Identitätsnachweis sind sowohl in der analogen als auch in der digitalen Welt die amtlichen Personenregister. Die Eintragungen in diese Register - bei Geburt oder Niederlassung - sind eine zentrale hoheitliche Aufgabe des Staates.



Der analoge Identitätsausweis (Pass, ID, Ausländerausweis etc.) dient der staatlich beglaubigten Identifikation einer Person gegenüber anderen Menschen (z.B. Zollbeamter) und in gewissen Fällen auch

gegenüber Maschinen (z.B. Check-in Automaten). Der (andere) Mensch oder die Maschine überprüft anhand des Ausweises die Identität der Person, welche ihn vorzeigt. Der Staat gewährleistet bei der Ausstellung des Ausweises, dass die darauf ersichtlichen Angaben mit den Daten im amtlichen Personenregister übereinstimmen (Name, Vorname, Geburtsdatum etc.). Je nach Ausweisart werden die amtlich beglaubigten Daten aus dem Personenregister durch weitere Attribute ergänzt, um eine eindeutige Identifikation der sich ausweisenden Person zu unterstützen (z.B. Bild, Unterschrift, biometrische Daten). Der Staat händigt den erstellten Ausweis der Person aus, welche sich fortan für eine festgelegte Zeitdauer damit ausweisen (identifizieren) kann. Der Nachweis der Identität beruht primär auf dem physischen Besitz des Ausweises.

Der staatliche elektronische Identitätsnachweis (E-ID) dient der staatlich beglaubigten Identifikation einer Person gegenüber Applikationen. Die Applikation überprüft anhand verschiedener Attribute, wie z.B. Namen, Vornamen und Geburtsdatum die Identität der Person, welche diese der nachfragenden Applikation auf elektronischem Weg als digitalen Datensatz zur Verfügung stellt («zeigt»). Der Staat gewährleistet, dass die der Applikation zur Identifikation übermittelten Daten mit den Daten im amtlichen Personenregister übereinstimmen. Je nach dem werden diese Daten durch weitere Attribute ergänzt, welche eine eindeutige Identifikation der sich ausweisenden Person unterstützen (z.B. digitale Signatur). Der Staat ermöglicht der Person, die zu ihrer Identifikation notwendigen Daten aus dem Personenregister sowie weitere Attribute an nachfragende Applikationen zu übermitteln. Die Befähigung zu dieser Übermittlung, z.B. durch sichere Identifikationsmethoden (Passwort mit weiteren Faktoren), entspricht dem Besitz eines physischen Ausweises in der analogen Welt.

Jede Behörde, die den Ausweis sieht, hat die Pflicht zu prüfen, wer der Berechtigte ist (Authentifizierung). Ausserdem hat sie im konkreten Anwendungsfall zu entscheiden, ob der Berechtigte im konkreten Fall berechtigt ist, gewisse Leistungen zu beziehen, oder gewisse Pflichten nicht hat.

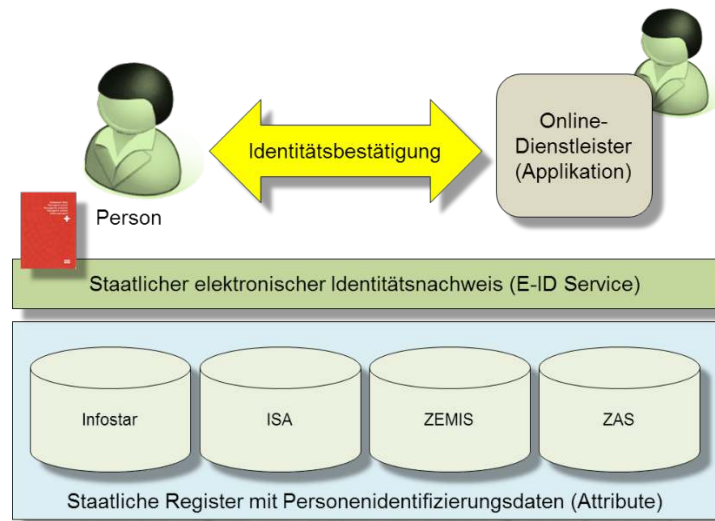
Sicherheitstechnische und ethische Herausforderungen

Wie in der physischen Welt können staatliche elektronische Identitätsnachweise gefälscht, gestohlen oder missbraucht werden. Die Technologien, um dies so weit wie möglich zu verhindern, stehen zur Verfügung und müssen zusammen mit der Einführung der E-ID zum Einsatz gelangen. Zudem ist die Verwendung der E-ID so einzuschränken, z.B. auf die Bekanntgabe einzelner Attribute, dass das Risiko von Missbrauch oder Entwendung minimiert wird.

Eine besondere ethische Herausforderung stellt die Verwendung der mit der E-ID verknüpften technischen Personen-Identifikationsnummer innerhalb der Verwaltung dar. Diese Nummer kann zu Verknüpfungen von Datenbeständen über Organisations- und Zuständigkeitsbereiche hinweg verwendet werden, welche vielleicht im Interesse einer effizienten Aufgabenbewältigung in der Verwaltung, nicht aber im Interesse der betroffenen Person liegen. Die flächendeckende Einführung eines staatlichen elektronischen Identitätsnachweises muss daher gewährleisten, dass diese Nummer und andere Attribute der E-ID auch innerhalb der Verwaltung nur mit der expliziten Zustimmung der betroffenen Person benutzt werden können. Auch die Verwendung von weiteren Attributen der E-ID muss der Kontrolle und expliziten Zustimmung der betroffenen Person unterstehen.

2. Lösungsskizze

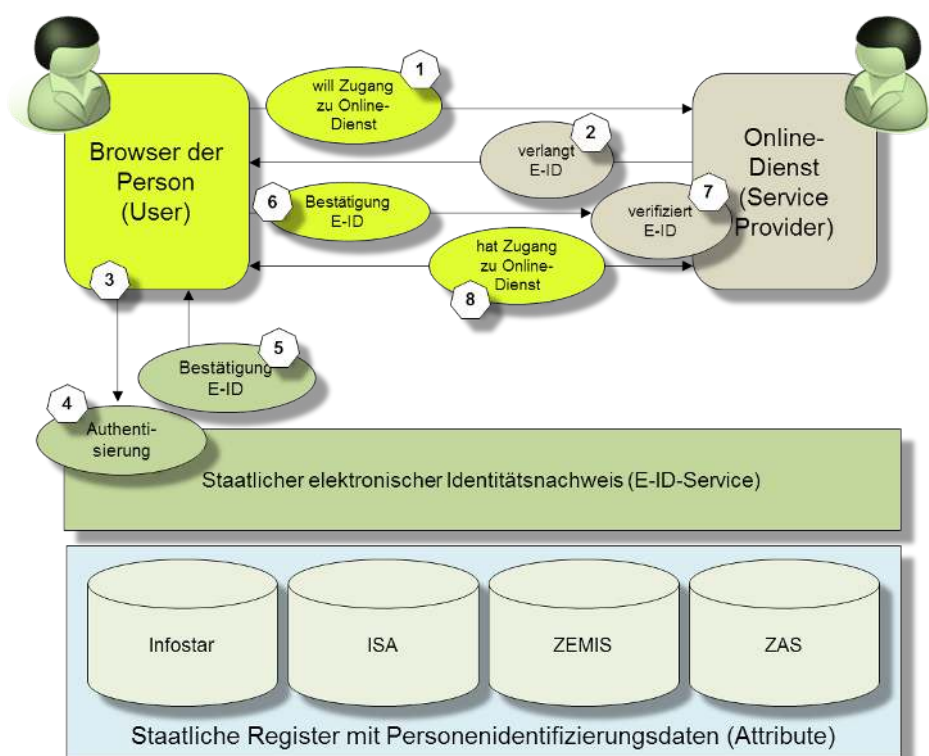
Voraussetzungen



Der staatliche elektronische Identitätsnachweis beruht auf den folgenden Voraussetzungen:

1. Der staatliche elektronische Identitätsnachweis einer Person gegenüber einem Online-Dienstleister («Identitätsbestätigung» oder «Authentisierung») beruht auf den staatlich beglaubigten Personenidentifizierungsdaten (Attribute), welche in den bestehenden staatlichen Registern geführt werden (Infostar, ISA, ZEMIS und ZAS).
2. Die Verwaltung dieser Attribute ist für diese Register rechtlich bereits geregelt. Zusätzlich zu den bestehenden Verwendungszwecken dieser Daten wird deren Nutzung für den staatlichen elektronischen Identitätsnachweis zugelassen.
3. Für den staatlichen elektronischen Identitätsnachweis stehen die Attribute aus diesen Registern im Rahmen eines gemeinsamen E-ID-Service zur Verfügung und können dort von der Person selbst sowie den nachfragenden Online-Dienstleistern, sofern dazu berechtigt, abgefragt werden (Ablauf der Identitätsbestätigung siehe unten).
4. Jede Person hat für ihre Attribute einen Lesezugriff und kann von ihnen eine Kopie zur freien Verwendung und Weitergabe anfertigen. Die Person wird für diesen Zugriff durch die für den staatlichen elektronischen Identitätsnachweis zuständige Stelle autorisiert. Zudem hat jede Person die Möglichkeit, die Abfrage ihrer Attribute durch Dritte nachzuvollziehen («Logfile»).
5. Jede Anbieterin eines den staatlichen E-ID-Service verwendenden Online-Dienstes ist grundsätzlich berechtigt, von einer Person einen staatlichen elektronischen Identitätsnachweis zu verlangen, als Voraussetzung für die Nutzung der betreffenden Applikation.
6. Jede Person ist grundsätzlich frei, ob und in welchem Umfang sie den staatlichen elektronischen Identitätsnachweis gegenüber einer bestimmten Applikation erbringen will oder ob sie lieber auf die Nutzung der Applikation verzichtet.
7. Der staatliche elektronische Identitätsnachweis ist in der Lage, jeder abfragenden Applikation gegenüber die Identität einer bestimmten Person nachzuweisen, welche dieser Identifizierung zugestimmt hat.

Möglicher Ablauf der staatlichen elektronischen Identitätsbestätigung²



Die staatliche elektronische Identitätsbestätigung auf Basis der vorhandenen Personenregister kann wie folgt ablaufen :

1. Eine Person (User) will den Online-Dienst eines Service Providers nutzen und macht die dazu notwendigen Angaben (z.B. Name, Vorname, Adresse bzw. ein beim E-ID-Service vom User hinterlegter eindeutiger Benutzername).
2. Der Online-Dienst verlangt vom User den staatlichen Nachweis seiner Identität (E-ID) und generiert dafür eine entsprechende Anfrage an den E-ID Service.
3. Der Browser des Users leitet die Anfrage an den staatlichen E-ID-Service weiter.
4. Der staatliche E-ID-Service überprüft die Anfrage und authentisiert die betreffende Person.
5. Der staatliche E-ID-Service generiert eine Bestätigung der E-ID und schickt diese an den Browser des Users.
6. Der Browser des Users leitet die Bestätigung der E-ID an den Online-Dienst weiter.
7. Der Online-Dienst verifiziert die Bestätigung der E-ID.
8. Der User wurde erfolgreich identifiziert und hat nun Zugang zum Online-Dienst.

² Dieser Ablauf des staatlichen elektronischen Identitätsbestätigung orientiert sich am internationalen Standard SAML (siehe für eine vereinfachte Erläuterung hierzu <https://blog.surf.nl/en/saml-for-dummies>). Für die Abfrage von spezifischen Attributen beim E-ID Service direkt durch den Online-Dienst (Service Provider) wäre zudem OAuth einsetzbar. Zudem ist der eCH-Standard eCH-0170 (Qualitätsmodell zur Authentifizierung von Subjekten) sowie das zugehörige IAM Glossar eCH-297 zu berücksichtigen.

3. Rechtliche Grundlagen

Die Schweizerische Bundesverfassung gibt dem Bund die Kompetenz zum Erlass von Regeln betreffend den Erwerb und den Verlust von Bürgerrechten (Art. 38 Bundesverfassung, **BV**) sowie die Kompetenz zur Regelung von Angelegenheiten betreffend die Ein- und Ausreise, den Aufenthalt und die Niederlassung von Ausländerinnen und Ausländern sowie über das Asylwesen (Art. 121 BV). Die Bundesversammlung genehmigt völkerrechtliche Verträge (Art. 166 BV), wie z.B. das Abkommen über die Rechtsstellung von Flüchtlingen. Dadurch ergibt sich für Schweizer Staatsangehörige³ sowie Ausländerinnen und Ausländer⁴, die keine Flüchtlinge⁵ sind, ein **Anspruch auf Ausstellung eines Ausweises**.

Dieser Anspruch wurde bislang durch Ausstellung von physischen Ausweisdokumenten erfüllt. Man muss davon ausgehen, nicht zuletzt mit Blick auf Art. 13 Abs. 2 BV⁶, dass die Schaffung der E-ID eine neu zu erlassende ausdrückliche gesetzliche Grundlage notwendig macht⁷.

Dass diese neue gesetzliche Grundlage für die E-ID geschaffen werden soll und der Bund dazu kompetent ist, ist derzeit unbestritten⁸, weswegen an dieser Stelle auf weitere Ausführungen zur inhaltlichen Notwendigkeit verzichtet wird. Es besteht insofern Konsens dazu, dass der Datenschutz der *Schaffung* der E-ID nicht im Weg stehen soll (wie z.B. in anderen Ländern wie etwa Deutschland⁹). Vielmehr ist die E-ID ein Element der digitalen Infrastrukturen der Schweiz.

Zur wirksamen und datenschutzkonformen Ausgestaltung der E-ID sollten von der Privatwirtschaft so rasch wie möglich Anwendungen geschaffen werden, die dem Nutzer erlauben, vielschichtige bzw. sektoriell differenzierte (abgeleitete) Identitäten anzunehmen. Beispielsweise sollte ein Nutzer z.B. für Social Media eine andere abgeleitete Identität einsetzen können als im Verkehr mit einem Ge-

³ Für alle **Schweizer Staatsangehörige** hält das Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG) fest: «Alle Schweizer Staatsangehörigen haben Anspruch auf einen Ausweis je Ausweisart.» (Art. 1 Abs. 1 AwG).

⁴ Für **Ausländerinnen und Ausländer** mit dem Recht auf Niederlassung hält das Bundesgesetz über die Ausländerinnen und Ausländer (Ausländergesetz, AuG) fest: «Ausländerinnen und Ausländer erhalten mit der Bewilligung in der Regel einen entsprechenden Ausweis.» (Art. 41 Abs. 1 AuG und Art. 71 Abs. 1 Satz 1 der Verordnung über Zulassung, Aufenthalt und Erwerbstätigkeit, VZAE).

⁵ Für **Flüchtlinge** gilt die Verordnung über die Ausstellung von Reisedokumenten für ausländische Personen (RDV). Gemäss RDV besteht kein Anspruch auf Ausstellung von Reisedokumenten, es gilt jedoch das Willkürverbot.

⁶ Das Datenschutzrecht setzt dem Verwaltungshandeln Grenzen. Art. 13 Abs. 2 BV schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (Recht auf informationelle Selbstbestimmung). Siehe auch Art. 17 Abs. 1 DSGVO: «Organe des Bundes dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht». Nach Art. 19 Abs. 3 DSGVO dürften Bundesorgane Personendaten nur durch ein Abrufverfahren zugänglich machen, wenn dies ein Rechtssatz ausdrücklich so vorsieht. Für besonders schützenswerte Personendaten sowie Persönlichkeitsprofile besteht die einschränkende Bedingung, dass das Abrufverfahren in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein muss.

⁷ Inwiefern diese Grundlagen bereits genügen, wird in den Fachkreisen derzeit nicht eindeutig beantwortet, siehe z.B. den Bericht über die Stellungnahmen im Rahmen der vom Bundesamt für Polizei informelle Konsultation zum "Konzept für schweizerische staatlich anerkannte E-ID-Systeme", <http://www.schweizerpass.admin.ch/pass/de/home/aktuell/konsultation.html>

⁸ Siehe das Konzept des FedPol "Staatlich anerkannte elektronische Identifizierungsmittel (E-ID) (Konzept 2016)" vom 13. Januar 2016, S. 2, <http://www.schweizerpass.admin.ch/pass/de/home/aktuell/konsultation.html>.

⁹ Siehe dazu Fn. 11.



sundheits- oder Verkehrsdienstleister. Datenschutzfragen (insbesondere Datensicherheit und Zweckbindung) sind somit im Zusammenhang mit der Umsetzung der E-ID zu berücksichtigen.

4. Die ökonomische Sicht

Das Internet eröffnet grosse Freiräume für geschäftliche und soziale Aktivitäten. Damit verbunden sind hohe Risiken für alle Involvierten. Aufgrund dieser Risiken wird das Internet für eben jene Aktivitäten tatsächlich viel weniger genutzt, als dies möglich wäre – dies sowohl innerhalb eines Landes als auch in vermehrten Mass länderüberschreitend. Hauptgrund ist, dass bislang breit nutzbare Vertrauensdienste wie digitale Authentifizierung, digitale Zeitstempel, digitale Individual- und Organisationssignaturen (Siegel), etc. fehlen. Digitale Authentifizierungsmittel sind dabei das Analogon von Personalausweisen in der Offline Welt. Sie fallen unter den Begriff der elektronischen Identitäten (E-IDs).

Gegen diese Beobachtung wird oft angeführt, dass es gar keinen Bedarf für eine weitergehende Nutzung gibt. Das ist richtig, aber auch nicht: Auch für andere heute viel genutzte digitale Kommunikationskanäle und Kommunikationswerkzeuge gab es ursprünglich keinen Bedarf – sogar für Computer selbst. Und für das Internet war der ursprüngliche Bedarf primär ein militärischer und sekundär ein akademischer, keinesfalls aber ein mit Geschäftsmodellen belegbarer, kommerzieller Bedarf. Es ist deshalb ahistorisch, über Dienste, die die Weiterentwicklung der Nutzung des Internets fördern, aus der Bedarfsperspektive nachzudenken.

Derzeit werden in vielen Staaten Versuche unternommen, Vertrauensdienste aufzubauen. Einige Staaten waren damit spontan sehr erfolgreich (Beispiel Dänemark), andere Staaten waren nach jahrelangen Versuchen erfolgreich (Beispiel Österreich¹⁰) und wieder andere sind bislang gescheitert (Beispiel Deutschland¹¹). Mittlerweile sind aber die Erfolgsfaktoren gut verstanden. Es sind dies namentlich die Erkennbarkeit konkreter Vorteile (bzw. allenfalls verpflichtende Nutzung), eine einfache Verständlichkeit sowie eine gute Benutzerfreundlichkeit. Der dritte Punkt bezieht sich dabei nicht auf Geräte, sondern auf Nutzungskontexte. Die SuisseID scheiterte unter anderem daran, dass ein digitales Signieren im Geschäftskontext die meisten Entscheidungsträger überforderte. Auch die Misserfolgsfaktoren sind bekannt. Zu nennen sind übertriebener Datenschutz und ungenügende Kommunikation.

Zusätzlich zu den nationalen Aktivitäten hat die EU mit eIDAS die rechtlichen Rahmenbedingungen für eine grenzüberschreitende Nutzung von Vertrauensdiensten geschaffen, wie sie für einen digitalen Binnenmarkt zwingend notwendig ist. Sie hat die Standards zur Umsetzung von eIDAS definiert und sie fördert finanziell Projekte zur Schaffung der notwendigen Dienste für eine grenzüberschreitende Nutzung von Vertrauensdiensten.

Seit Juli 2016 ist eIDAS teilweise in Kraft. Im September 2018 tritt es vollständig in Kraft. Angesichts der laufenden Projekte zur Umsetzung von eIDAS ist davon auszugehen, dass es eine EU der zwei oder drei Geschwindigkeiten geben wird. Voraussichtlich wird eIDAS etwa fünf Jahre nach der ersten Inkraftsetzung beziehungsweise drei Jahre der vollständigen Inkraftsetzung in den ökonomisch führenden Staaten eine breitere Wirkung entfalten wird (d.h. im Jahr 2021). In den darauffolgenden fünf Jahren wird diese schrittweise eine beträchtliche ökonomische Bedeutung gewinnen (bis 2026). Das bedeutet, dass frühestens ab 2021 und spätestens ab 2026 Einwohner und Unternehmen in der

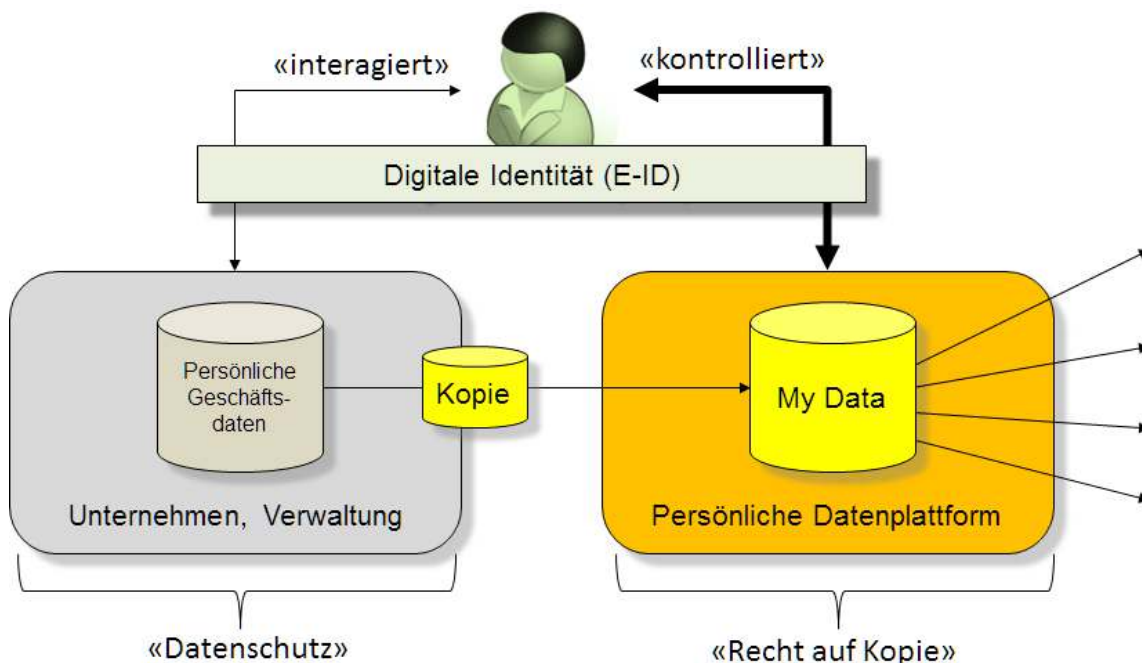
¹⁰ Durch Einführung der Handysignatur, deren Nutzung sehr einfach ist, siehe <https://www.handy-signatur.at/>.

¹¹ Gründe sind unter anderem der Ausgabeprozess (anders als in Belgien wurde nicht das nötige Personal bereitgestellt) und die besonders hohen Anforderungen in Bezug den Datenschutz, die es aufwendig, kompliziert und teuer machen, als Diensteanbieter eine deutsche E-ID zu akzeptieren.

Schweiz gegenüber Einwohnern und Unternehmen in der EU klar benachteiligt sein werden, wenn die Schweiz bis dahin über keine Vertrauensdienste verfügt, die grenzüberschreitend genutzt werden können.

Im möglichen aber eher unwahrscheinlich Fall, dass die EU mit der eIDAS Regulierung scheitert und auch 10 Jahre nach der ersten Einführung grenzüberschreitend nutzbaren Vertrauensdienste nicht breit genutzt werden, ist davon auszugehen, dass amerikanische Unternehmen die hoheitliche Aufgabe der Ausgabe von elektronischen Identitäten übernehmen werden und damit eine Kontrolle über die digitalen Personendaten erlangen werden, wie sie heute die öffentliche Verwaltung hat. Dass in dieser Situation staatliche Regulierung Bürgerrechte wie den Datenschutz nach wie vor gewährleisten können ist theoretisch denkbar, praktisch unwahrscheinlich.

Einwohner und Unternehmen in der Schweiz sowie Auslandschweizer sollen das Recht auf eine breit nutzbare E-ID zu vernünftigen Kosten haben. Dieses Recht ist aus zwei Gründen von zentraler Bedeutung: Erstens garantiert es das freie, unbeschränkte wirtschaftliche und soziale Agieren im Internet. Zweitens ist es die Grundvoraussetzung dafür, dass Berechtigte die Kontrolle über ihre Daten ausüben können. Nur wenn sie ihre Identität im Internet einfach nachweisen können, können sie einfach und ohne grösseren Aufwand die Rechte an ihren eigenen Daten gegenüber den Datenhaltern geltend machen. Eine digitale Selbstbestimmung ist ohne E-ID praktisch nicht möglich.



5. Die Aufgaben des Staates

Auch im elektronischen Bereich ist der staatliche Nachweis der Identität gleich wie die Ausgabe von physischen Identitätsausweisen eine hoheitliche Aufgabe. Diese umfasst die folgenden drei Punkte:

- Betrieb einer Datenbank, in welcher die zu einer Person gehörigen, staatlich beglaubigten Attribute gespeichert und auf dem aktuellen Stand gehalten werden (staatliches Personenregister).
- Verfahren, welches es der sich ausweisenden Person ermöglicht, einer abfragenden Stelle (in der Regel einer Applikation) einzelne oder mehrere über sie im staatlichen Personenregister gespeicherte Attribute einmalig zugänglich zu machen («zeigen»).
- Verfahren, welche es der abfragenden Stelle ermöglichen, die Korrektheit sowie die Zugehörigkeit der Attribute zu der sich ausweisenden Person zu verifizieren («überprüfen»).

Der Staat sollte explizit vertrauensstiftende Massnahmen treffen. Dazu gehört, dass er dafür haftet, dass die Daten der E-ID zum Ausstellungszeitpunkt ordnungsgemäss nachgeführt korrekt waren. Der Staat muss weiter dafür sorgen, dass die E-ID zumindest innerhalb der gesamten Verwaltung sowie in allen E-Government-Anwendungen, die eine Identifizierung verlangen, einsetzbar ist.

Nutzbarkeit im Ausland

Um die Einsetzbarkeit und damit den Nutzen weiter zu erhöhen, sollte der Staat zusätzlich anstreben, dass die Ausweise auch im Ausland staatlich anerkannt werden. In Bezug auf die EU bedeutet dies, dass die Schweiz Mitglied im eIDAS Verbund werden muss.

Die EU hat mit der eIDAS Verordnung einen einheitlichen Identitätsraum konzipiert, der ab 2018 unfänglich in Kraft tritt. Er basiert auf dem Prinzip der gegenseitigen Anerkennung und auf einer Interoperabilitätsinfrastruktur, dem Netzwerk der so genannten eIDAS-Knoten. In diesem einheitlichen Identitätsraum gibt es drei Qualitätsklassen mit unterschiedlichen Haftungsanforderungen. Staaten können E-IDs von Identitäts Providern (IDPs) gegenüber den Mitgliedstaaten notifizieren. Die Notifikation hat zur Folge, dass solche E-IDs im Ausland für E-Government-Anwendungen anerkannt sind. Vorausgesetzt ist, dass solche E-IDs im Inland uneingeschränkt für Authentifizierungen im E-Government einsetzbar sind und dass alle E-IDs von notifizierten ausländischen IDPs, die die gleiche oder eine höhere Qualitätsstufe besitzen, auch im Inland von allen E-Government Diensten als Authentifizierungsmittel anerkannt sind.

Diese scheinbar einfache Regelung hat zur Folge, dass ein Staat, der seine E-IDs gegenüber dem Ausland notifizieren will, sich für eine minimale Qualitätsstufe für alle seine E-Government Anwendungen entscheiden muss (ausgenommen sind solche innerhalb der Verwaltung). Die Schweiz könnte deshalb eine E-ID der mittleren Qualitätsstufe nicht notifizieren, wenn z.B. der Kanton Luzern eine hohe Qualitätsstufe verlangt. Und sie könnte theoretisch gar keine E-ID notifizieren, wenn eine Gemeinde E-IDs gar nicht akzeptiert. Dieses Konzept erzeugt einen Umsetzungsdruck, der zu begrüssen ist. Es muss sich allerdings noch zeigen, wie dieses Konzept in der Praxis gelebt werden wird.

Einbettung ins Schweizer E-Government

Die verwaltungsinterne organisationsübergreifende Zusammenarbeit im Schweizer E-Government basiert auf Standards, die von eCH herausgegeben werden. Im Rahmen von eCH arbeiten die Verwaltung, die Wirtschaft, die Hochschulen und die Zivilgesellschaft zusammen. Die Verwaltung hat sich

selbst verpflichtet, bei der Entwicklung neuer E-Government-Lösungen eCH Standards einzuhalten. Die Kantone halten sich weitgehend an diese selbstauferlegte Beschränkung, die Bundesverwaltung dagegen tendenziell weniger.

Es gibt zum Thema E-ID verabschiedete und gültige Standards von eCH, die unter anderem das zugrundeliegende Begriffssystem samt allen wesentlichen Konzepten sowie der Qualitätsbewertung (unter Einschluss von so genannten Identitätsbrokern) standardisieren. Wo diese noch nicht an eIDAS angepasst sind, werden derzeit neue Versionen erarbeitet. Da die Notifizierbarkeit gegenüber der EU den Einsatz im E-Government verlangt, sollten die eCH Standards von staatlich anerkannten IDPs unbedingt eingehalten werden.

Das Ökosystem

Die Erfahrung hat gezeigt, dass isolierte Massnahmen zur Herausgabe von E-IDs auf Nicht-Akzeptanz in der Bevölkerung treffen. Nur dort, wo das gesamte Ökosystem der Vertrauensdienste erstens als Ganzes und zweitens gezielt strategisch entwickelt wurde, fanden staatlich anerkannte E-IDs bisher breitere Nutzerkreise. Deshalb sollte auch die Schweiz dem guten Beispiel einer Gesamtentwicklung des Ökosystems folgen und die Herausforderung ganzheitlich angehen. Dies betrifft nicht nur alle Vertrauensdienste (d.h. weitere Dienste neben der Authentifizierung), sondern auch nichtstaatliche Authentifizierungsmittel (z.B. E-IDs für Social Media).

6. Anforderungen an eine staatliche E-ID

Abschliessend lassen sich die folgenden zentralen Anforderungen an eine staatliche E-ID formulieren:

1. Ziel muss sein, dass das ganze E-ID-Ökosystem inklusive der E-ID-basierten Vertrauensdienste und der Relying Parties, zum Fliegen kommt. Ein Referenzrahmen für das E-ID-Ökosystem findet sich im SECO-Bericht zum Schweizerischen [E-ID-Ökosystem-Modell](#).
2. Die E-ID muss die folgenden, konkreten und messbaren Ziele erreichen:
 - a. Sämtliche Vertrauensdienste des E-ID-Ökosystems in der Schweiz müssen in einer notifizierbaren Form – und nach Abschluss einer entsprechenden Vereinbarung mit der EU: in notifizierter Form – angeboten werden.
 - b. In der Schweiz muss ein Äquivalent zu einem eIDAS Node betrieben werden, der es Besitzern von notifizierten E-IDs aus der EU erlaubt, ihre E-IDs gegenüber eIDAS-kompatiblen Relying Parties in der Schweiz einzusetzen.
 - c. 10% der Einwohner der Schweiz sollen mindestens 10 Mal pro Jahr einen staatlich anerkannten (und notifizierbaren) Vertrauensdienst nutzen.
 - d. Es sollen mindestens 1'000 Onlinedienste in das E-ID-Ökosystem der Schweiz eingebunden sein.
 - e. Im E-ID-Ökosystem der Schweiz sollen für mindestens 100 Attribute (die über die Standardattribute des staatlichen Kerndienstes hinausgehen) Attributzertifikate angeboten werden.
 - f. Unternehmen sollen digitales Signieren institutionalisiert (aber nicht notwendigerweise ausschliesslich) einsetzen, so dass digitales Signieren für insgesamt mindestens 1'000'000 Mitarbeitende ein alltäglicher Vorgang ist (gemeint sind Mitarbeitende mit schweizerischem Arbeitsvertrag in leitender Stellung, wie z.B. Prokuristen).

Ziele a.) und b.) sollten spätestens zwei Jahre nach der EU-weiten Einführung von eIDAS erreicht sein (nämlich 2020). Ziele c.) bis f.) sollten spätestens fünf Jahre nach der EU-weiten Einführung von eIDAS erreicht werden (nämlich 2023).

3. Die Gesetzgebung soll die etablierten und genehmigten eCH Standards einsetzen und kompatibel sein mit der eIDAS Regulierung. Wo die eCH-Standards noch nicht kompatibel mit eIDAS sind, sollen diese so rasch wie möglich entsprechend angepasst werden.
4. Sobald dies grundsätzlich möglich ist, sollten Verhandlungen mit der EU starten, dass in der Schweiz anerkannte E-IDs in der EU eingesetzt werden können. Dabei soll bewusst nicht nur die Notifizierung angestrebt werden, sondern auch die Option ausgelotet werden, dass auch ohne Staatsvertrag die Schweiz am eIDAS Identitätsraum teilhaben kann.
5. Es soll die Entwicklung eines E-ID-Brokers gefördert werden, der staatlich anerkannte E-IDs mit sozialen E-IDs verknüpft und so die sozialen E-IDs in das auf staatlichen Regulierungen basierende E-ID-Ökosystem integriert.

Die staatlichen Massnahmen sollen sich daran orientieren, dass die hier genannten Ziele erreicht werden. Diese Ziele sind für die wirtschaftlichen Zukunftschancen der Schweiz von zentraler Bedeutung. Sie müssen Priorität haben gegenüber eher ideologisch geprägten Überlegungen zur Rolle des Staats.