Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Fachbereich Weiterentwicklung Ausweise

Staatlich anerkannte elektronische Identifizierungsmittel (E-ID)

Konzept 2016

Version vom 02.02.2017

Eine E-ID dient zum Nachweis der eigenen Identität in der digitalen Welt.

Übersicht

Mit der Verbreitung des Internets und der hohen Verfügbarkeit von leistungsfähigen Mobilgeräten können Geschäftsprozesse immer einfacher in die digitale Welt verlagert werden. Gemäss den Angaben des Bundesamtes für Statistik [1] haben 2015 durchschnittlich 88% der Bevölkerung das Internet genutzt: 56% für Online-Einkäufe, 49% für E-Banking, 48% für Dienstleistungen im Zusammenhang mit Reisen, 48% für das Ausfüllen von Online-Formularen von Behörden und 35 % für politische Tätigkeiten. Für den Kontakt mit Behörden nutzten 79% aller Internetnutzerinnen und -nutzer das Internet. Die E-Commerce-Ausgaben der Haushalte sind innerhalb eines Jahrzehntes im Jahr 2014 auf über sieben Milliarden Franken gestiegen.

Rechtssicherheit und Vertrauen sind wesentliche Voraussetzungen für die Abwicklung von Geschäften. Dazu gehören adäquate Kenntnisse über die Identität der Beteiligten. Für die physische Welt stellt der Bund dazu bereits heute konventionelle Identifizierungsmittel aus, nämlich Schweizer Pass, Identitätskarte und Ausländerausweis. Ergänzend dazu soll nun die Identität einer natürlichen Person auch elektronisch bewiesen werden können. Dazu hat der Bundesrat das EJPD beauftragt, ein Konzept für staatlich anerkannte elektronische Identifizierungsmittel (E-ID) auszuarbeiten. Staatlich anerkannte E-ID werden den Inhaberinnen und Inhabern ermöglichen, sich bei Online-Diensten sicher zu registrieren und später erneut sicher anzumelden. Weitere Vertrauensdienste, wie die elektronische Signatur, können von Identitätsdienstleistern angeboten werden, sind jedoch nicht Bestandteil der E-ID.

Das nun vorliegende E-ID-Konzept stützt sich auf die Vorarbeiten von fedpol aus den Jahren 2013-2015, im Rahmen derer auch wichtige Stakeholder des Marktes konsultiert wurden. Es berücksichtigt weiter die Erkenntnisse aus bisherigen Lösungen für E-ID-Systeme, die Vorgaben [2] [3] für die EU-Kompatibilität[1] sowie die internationalen Entwicklungen für praxisnahe starke Lösungen für E-ID-Systeme [4] [5] [6] [7] [8]. Ebenso erfolgte soweit möglich ein Abgleich mit den Anforderungen im Bereich des elektronischen Patientendossiers (EPDG) [9] und der elektronischen Signatur (ZertES) [10].

Das Konzept sieht vor, dass der Bund keine eigene E-ID herausgibt, sondern vielmehr geeignete E-ID-Systeme des Marktes auf drei verschiedenen Sicherheitsniveaus staatlich anerkennen und beaufsichtigen kann. Dazu schafft der Bund neu die *Anerkennungsstelle für Identitätsdienstleister (AID)*. Zudem tritt der Bund als Vertrauensanker für die Identität einer Inhaberin oder eines Inhabers einer E-ID auf, in dem er vorhandene Personenidentifizierungsdaten (Namen, Vornamen, Geburtsdatum, Foto usw.) an staatlich anerkannte Herausgeber von E-ID elektronisch übermittelt. Für diese zweite Aufgabe wird die neue *Schweizerische Stelle für elektronische Identität (SID)* beim Bund zuständig sein.

Um die Rechtssicherheit im E-ID-Bereich sicher zu stellen, schafft der Bund ein *Bundesgesetz über anerkannte elektronische Identifizierungseinheiten(E-ID-Gesetz),* einschliesslich der erforderlichen Ausführungsbestimmungen. Diese werden konkrete technische und organisatorische Vorgaben für staatlich anerkannte E-ID-Systeme enthalten, um den notwendigen soliden Vertrauensrahmen zu schaffen. U.a. soll so auch die Interoperabilität zwischen verschiedenen Betreibern von E-ID-Systemen sichergestellt werden. Das vorliegende Konzept diente als inhaltliche Basis für die Erarbeitung des E-ID-Gesetzes.

[1] Diese erlauben eine gegenseitige Anerkennung der E-ID-Systeme. Zur so genannten Notifizierung bedarf es aber in jedem Fall des Abschlusses eines bilateralen Übereinkommens mit der EU.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Begriffsverzeichnis

National und international haben sich im E-ID-Bereich verschiedene Begrifflichkeiten etabliert siehe dazu das Begriffsverzeichnis unten und das Glossar im Anhang.

eID-Konzept	E-ID-Gesetz	eIDAS Deutsch	English
Anerkennungsstelle für Identitätsdienstleister (AID)	Anerkennungsstelle für IdP (Anerkennungs-stelle)	-	Accreditation Authority
Antragsteller	antragstellende Person	Antragsteller	Applicant
Authentifizierung	Authentifizierung	Authentifizierung	Authentication
Eindeutiger Perso-nenidentifikator (EPID)	E-ID-Registrierungs-nummer	eindeutige Kennung	Unique Personal Identi-fication Number
staatlich anerkanntes Identifizierungsmittel (E-ID)	anerkannte elektroni-sche Identifizierungsein-heit (E-ID)	Elektronisches Identifi-zierungsmittel	Credential
elektronisches Identifi-zierungssystem (E-ID-System)	E-ID-System	Elektronisches Identifi-zierungssystem	Identity System
Elektronische Identifi-zierung	Elektronische Identifi-zierung	Elektronische Identifi-zierung	Identification
staatlich anerkannter Identitätsdienstleister (Identity Provider, IdP), Herausgeber, Aussteller	anerkannte Identity Pro-vider (IdP) oder Anbie-terinnen von Identitäts-dienstleistungen	Aussteller	Identity Provider (IdP), Credential Service Pro-vider (CSP)
Inhaber	Inhaber und Inhaberin	natürliche Person	Claimant/Subscriber
Interoperabilität	Interoperabilität	Interoperabilität	Interoperability
Online-Dienste	Online-Dienste	Online-Dienste	Online Services
Personenidentifizie-rungsdaten (PID)	Personenidentifizie-rungsdaten	Personenidentifizie-rungsdaten	Identity Attribute
Registrierung	Registrierung	Registrierung	Registration
Schweizerische Stelle für elektronische Identi-tät (SID)	Schweizerische Stelle für elektronische Identi-tät (Identitätsstelle)	verlässliche Quelle	Steering Group and At-tribute Authority, Root Attribute Authority
Vertrauende Beteiligte (vBt)	Betreiberin von E-ID-verwendenden Diens-ten	Vertrauender Beteiligter	Relying Party (RP)
vertrauender Dienst	E-ID-verwendender Dienst	-	Relying Service
Sicherheitsniveau	Sicherheitsniveau	Sicherheitsniveau	Level of Assurance / Assurance Level

1 Einführung

1.1 Aufbau und Inhalt

In diesem Dokument werden die grundlegenden Überlegungen beschrieben, die zum E-ID-Konzept und dem dazugehörigen Gesetzesentwurf für staatlich anerkannte elektronische Identifizierungsmittel geführt haben. Vorgestellt werden die Funktionen der Teilnehmer im E-ID-Ökosystem, die Abläufe für den Bezug und den Einsatz von staatlich anerkannten E-ID, die Überlegungen zur Sicherheit sowie die Rolle des Staates und die daraus entstehenden finanziellen Folgen. In einem gesonderten Kapitel werden Ausgestaltung, Funktionalität und Kosten der neuen **Schweizerischen Stelle für elektronische Identität (SID)** und der neuen **Anerkennungsstelle für Identitätsdienstleister (AID)** beim Bund vorgestellt. Ersterer operiert als elektronischer Dienst für die Übermittlung staatlich verwalteter Identitätsattribute an Identitätsdienstleister, während die zweitgenannte Stelle hauptsächlich als Kontrollorgan tätig ist. Im Anhang schliesslich gibt es eine Einführung in die Zusammenhänge und Begriffe des digitalen Identitätsmanagements, das Basis des vorliegenden Konzepts ist.

1.2 Elektronische Identifizierungsmittel

1.2.1 Um was geht es?

Damit Geschäftsprozesse online abgewickelt werden können, müssen die Geschäftspartner (fortan als **vertrauende Beteiligte (vBt)** bezeichnet) das Vertrauen in die angegebene Identität und in die online Authentifizierung des Gegenübers haben, sowohl national als international. Sind in der physischen Welt die hoheitlichen Ausweise wie Pass oder Identitätskarte die Mittel zum vertrauenswürdigen Nachweis der eigenen Identität, so sind es in der digitalen Welt die **elektronischen Identifizierungsmittel (E-ID)**. Eine E-ID erlaubt es vertrauenden Beteiligten, Personen vor der Erbringung eines Vertrauensdienstes zu identifizieren und zu authentifizieren. Vertrauenswürdige E-ID sind damit notwendige Komponenten für die Implementation von elektronischen Geschäftsprozessen.

Die E-ID wird von einem staatlichen oder privaten **Identitätsdienstleister (Identity Provider, IdP)** ausgestellt, welche die E-ID in einem Registrierungsprozess einer vertrauenswürdig identifizierten Person (fortan **Inhaberin oder Inhaber** genannt) zuordnet. Eine E-ID beinhaltet einen eindeutigen digitalen **Identifikator**[2] und eine Funktion, welche die E-ID sicher mit einer Person verbindet und die als **Authentifikator**[3] bezeichnet wird. Mit einer E-ID kann die Inhaberin oder der Inhaber einer vertrauenden Beteiligten, z.B. einem Internetportal eines E-Commerce-Shops, **Identitätsattribute** wie Name, Alter, Nationalität usw. übermitteln (**Identifizierung**) und nachweisen, dass sie oder er die Person ist, zu der die angegeben Identitätsattribute gehören (**Authentifizierung**). Sie oder er ist der vertrauenden Beteiligten dann unter dem eindeutigen digitalen Identifikator der E-ID oder einem zugeordneten Pseudonym bekannt[4].

---

[2] Der Identifikator ist ein digitaler Code der abgesichert mit der E-ID verbunden ist; er repräsentiert die Inhaberin oder den Inhaber einer E-ID in einer Online-Identifizierung.

[3] Der Authentifikator verifiziert beim Einsatz der E-ID die physische Präsenz der Inhaberin oder des Inhabers zum Beispiel indem er überprüft, dass der richtige PIN Code oder das zur Inhaberin oder zum Inhaber gehörende biometrische Merkmal eingegeben ist. Auch der physische Träger einer E-ID (Smartcard, Smartphone etc.), der fest im Besitz einer Inhaberin oder eines Inhabers ist, hat die Funktion eines Authentifikators.

[4] Der Identifikator der E-ID kann auch kryptographisch geschützt genutzt und sektoriell pro vertrauende Beteiligte oder sogar transient für einen kurzzeitigen Kontakt definiert werden.

Beim Einsatz identifiziert die E-ID mit dem digitalen Identifikator die Inhaberin oder den Inhaber und liefert einen digitalen Beweis[5] für die Präsenz der Person. Die E-ID ermöglicht dadurch den vertrauenden Beteiligten die Identifizierung und Authentifizierung der Inhaberin oder des Inhabers auf einem bestimmten **Sicherheitsniveau**. Dieses hängt davon ab, wie sicher der Registrierungsprozess[6] ist, wie sicher die E-ID im Feld funktioniert, wie sicher die Präsenz der Inhaberin oder des Inhabers beim Einsatz der E-ID überprüft wird und wie sicher das Resultat einer Identifizierung oder Authentifizierung dem vertrauenden Beteiligten kommuniziert wird[7]. Auch übermittelte Identitätsattribute sind dabei auf einer bestimmten Vertrauensstufe definiert, wobei man davon ausgehen kann, dass staatlich festgestellte Identitätsattribute, die so genannten **Personenidentifizierungsdaten (PID),** ein sehr hohes Vertrauen geniessen. Der Staat ist deshalb prädestiniert solche Daten zuhanden der staatlich anerkannten IdP bereit zu stellen, welche diese dann im Auftrag von Inhaberinnen und Inhabern an vertrauende Beteiligte übermitteln können.

Eine E-ID wird mit den unterlegten Personenidentifizierungsdaten zum digitalen Bindeglied zwischen der natürlichen Person und ihrer staatlich definierten Identität (fortan als **zivile Identität**[8] bezeichnet**)**, die von vertrauenden Beteiligten für die Organisation von Geschäftsprozessen gebraucht wird. Für die Vereinfachung dieser Geschäfte wird in der Schweiz im Kontext der E-ID zusätzlich ein **Eindeutiger Personenidentifikator (EPID**) als weiteres Attribut der zivilen Identität eingeführt.

Eine ausführlichere Einführung in Zusammenhänge und Begriffe im digitalen Identitätsmanagement ist im Anhang gegeben. An dieser Stelle werden nur die wichtigsten Begriffe und ihre Bedeutung eingeführt.

Die Gesamtheit aller natürlichen und juristischen Personen, vertrauenden Beteiligten, Identitätsdienstleister und öffentlichen Instanzen, die elektronische Identifizierungsmittel und darauf aufbauende Vertrauensdienste wie digitale Signaturen, Transaktionsabsicherungen usw. nutzen oder zu deren Betrieb beitragen, wird als **E-ID-Ökosystem** bezeichnet. Ebenfalls zum E-ID-Ökosystem gehören die staatlichen Stellen der Schweiz und der EU, die gesetzliche Regulierungen vollziehen und allenfalls weitere, den digitalen Markt unterstützende, Dienstleistungen erbringen, wie zum Beispiel einen **Attributdienst** oder die geplanten paneuropäischen Proxy Dienste für die internationale Nutzung von E-ID. Das **elektronische Identitätsmanagement (E-IdM)** und die dazugehörigen **E-ID-Systeme** die von den IdP betrieben werden, bilden das Rückgrat des E-ID-Ökosystems.

---

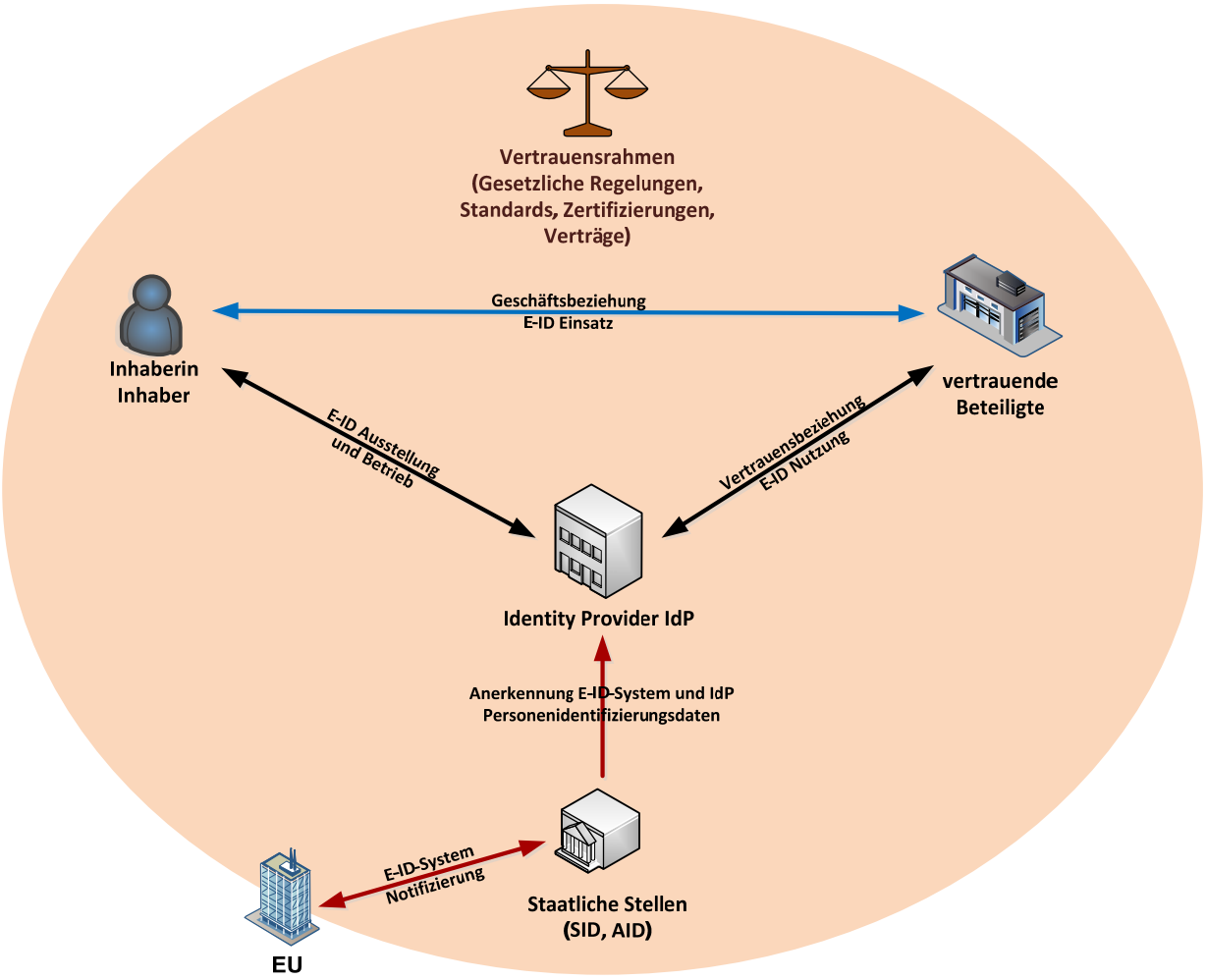
5 Im Normalfall ist die E-ID nur einsetzbar, wenn die berechtigte Person die E-ID durch eine geeignete Handlung aktiviert und damit implizit auch ihre physische Präsenz nachweist.

6 Im Registrierungsprozess bei der Ausstellung der E-ID wird einerseits die Person mit der E-ID verbunden (z.B. durch die Festlegung eines PIN-Codes der fortan beim Gebrauch der E-ID durch die Person einzugeben ist) und andererseits wird die Identität der Person verifiziert (z.B. durch Vorlage eines staatlichen Ausweises).

7 Die Sicherheitsniveaus werden durch gemeinsame Standards und Regeln definiert („Trust Framework“ [28] [8]) an die sich alle Beteiligten in einem E-ID Ökosystem zu halten haben. Die Gesamtvertrauen in die Sicherheit setzt sich aus den drei Teilbereichen Robustheit der initialen Registrierung und Identifizierung, Robustheit der Authentifizierung bei der Nutzung der E-ID und Robustheit der Vermittlung der Resultate einer Prüfung an vertrauende Beteiligte zusammen [6].

8 Die zivile Identität steht für die Gesamtheit der Personenidentifizierungsdaten, die für eine Person in den staatlichen Personenstandsregistern erfasst ist. Einige wenige dieser Attribute oder der neu eingeführte eindeutige Personenidentifikator genügen schon um eine zivile Identität eindeutig zu bestimmen.

Die für die schweizerisch staatlich anerkannten E-ID-Systeme wichtigsten Instanzen und Relationen eines E-ID-Ökosystems sind schematisch in Skizze 1 aufgeführt[9].



Skizze 1: Wichtigste Instanzen und Relationen im E-ID-Ökosystem

1.2.2 Vertrauenswürdigkeit

Einer E-ID kann man vertrauen, wenn die Prozesse und Abläufe bei der Ausstellung und dem Einsatz der E-ID sowie die Übermittlung der Resultate von Überprüfungen durch IdP an vertrauende Beteiligte sicher sind und das gesamte E-ID-System regelmässig auf Erfüllung von standardisierten und aktuellen Sicherheitskriterien überprüft wird.

Besonders wichtig sind dabei die Registrierung, die im E-ID-System verwendete Technologie und die Organisation des IdP, die Richtigkeit der erfassten Attribute, die Sicherheit der E-ID im Feld und die Protokolle für die interoperable Verwendung von E-ID:

- Bei der **Registrierung** einer Person im E-ID-System erfasst der IdP einerseits Attribute der zivilen Identität, welche die Inhaberin oder den Inhaber in der **Bevölkerung** identifizieren, und andererseits **persönliche Attribute** als **Authentifizierungsfaktoren** für die spätere Authentifizierung der Inhaberin oder des Inhabers mit der E-ID. Die Authentifizierungsfaktoren

[9] Ein vollständiges Referenzmodell für ein E-ID-Ökosystem findet man zum Beispiel in [29]. Für die Positionierung und einfach verständliche Darstellung der grundsätzlichen Interaktionen einer staatlichen E-ID ist das auf die relevanten Instanzen reduzierte Modell jedoch besser geeignet.

werden dabei meist nicht zentral sondern nur im Trägergerät der E-ID erfasst. Im **Bindungsprozess** werden diese fest mit dem Authentifikator der E-ID verbunden[10]. Beide Teilprozesse müssen in einem technisch und organisatorisch sicheren Protokoll abgewickelt werden, das durch die Anforderungen an das Sicherheitsniveau der E-ID bestimmt ist. Nach der Registrierung ist beim IdP der eindeutige Identifikator der E-ID den erfassten Identitätsdaten der Inhaberin oder des Inhabers zugeordnet.

- Die verwendete **Technologie** und die **Organisation** des IdP müssen den Anforderungen für das definierte Sicherheitsniveau des E-ID-Systems[11] genügen. Der IdP ist zuständig für die korrekte Registrierung, die korrekte Funktion der E-ID im Feld und die korrekte Übermittlung von Identitätsdaten und Authentifizierungsresultaten an vertrauende Beteiligte im gesamten E-ID Ökosystem. Der IdP muss dazu sichere, standardisierte, transparente und zertifizierte[12] Systeme und Prozesse implementieren. Dies wird im Rahmen des Anerkennungsprozesses des E-ID-Systems und des ausstellenden IdP sichergestellt und durch Audits periodisch überprüft. Staatlich anerkannte IdP müssen einen Rechtssitz in der Schweiz haben und garantieren, dass sie allfällige Haftungsansprüche, die sich aus den gesetzlichen Regelungen ergeben, erfüllen können. Sie müssen zudem nachweisen, dass sie alle Personenidentifizierungsdaten ausschliesslich in der Schweiz aufbewahren.
- Der IdP ist verantwortlich für die **richtige Zuordnung der Identitätsattribute zur E-ID**. Er braucht sichere und verlässliche Attributquellen[13], die wenn immer möglich vom Staat garantiert sind. Er erhält mit dem Einverständnis der Inhaberin oder des Inhabers die staatlich garantierten Personenidentifizierungsdaten vom SID. Er darf diese Daten nur mit der ausdrücklichen Erlaubnis der Inhaberin oder des Inhabers an vertrauende Beteiligte übermitteln.
- Die ***Schweizerische Stelle für elektronische Identität (SID)*** ist verantwortlich für die richtige Zuordnung der Personenidentifizierungsdaten zum **eindeutigen Personenidentifikator (EPID)** im Moment der Übermittlung an den anerkannten IdP[14]. Auch diese Daten dürfen nur mit der ausdrücklichen Erlaubnis der Inhaberin oder des Inhabers vom SID an den IdP übermittelt werden. Die Personenidentifizierungsdaten werden vom SID direkt aus den Registern beim Bund (Infostar, ISA, ZEMIS, ZAS-UPI) abgefragt. Das Sicherheitsniveau der E-ID bestimmt, welche staatlichen Personenidentifizierungsdaten dem IdP übermittelt werden (siehe 2.6.3)[15].
- Die **Sicherheit der E-ID** im Feld wird wesentlich durch die Anzahl respektive Qualität der unabhängigen Authentifizierungsfaktoren bestimmt, die vom Authentifikator beim Einsatz der E-ID verifiziert werden. Solche Faktoren sind ‚Besitz eines personalisierten Objektes', Kennt-

---

10 Bei der Registrierung erfasst der Authentifikator der E-ID die Authentifizierungsfaktoren als Referenzdaten. Bei einer späteren Authentifizierung beim Einsatz erfasst die E-ID die Authentifizierungsfaktoren neu und vergleicht diese mit den Referenzdaten und akzeptiert oder verwirft die erfasste Person als authentifiziert oder nicht.

11 Schweizerische E-ID-Systeme können auf drei Sicherheitsniveaus anerkannt werden. Die drei Sicherheitsniveaus entsprechen denjenigen, die in der eIDAS-Verordnung der EU und auch in den Richtlinien für die digitale Authentifizierung der USA definiert sind.

12 Für E-ID-Systeme werden pro Vertrauensstufe geeignete Schutzprofile nach ISO/IEC 15408 definiert. Für die Anerkennung müssen Zertifizierungen gemäss diesen Schutzprofilen durchgeführt werden.

13 Nicht alle ausländische Staaten, deren Bürger als E-ID berechtigte Ausländer in der Schweiz leben, führen Personenregister auf derselben Qualitätsstufe, wie sie für die schweizerischen Register üblich sind. Sobald aber Daten in ZEMIS erfasst sind, gelten diese Daten per definitionem als gültige Quelle für die Attribute der zivilen Identität.

14 Bei der Registrierung erfasst der IdP die Nummer eines staatlichen Ausweises oder den eindeutigen Personenidentifikator der Person und beantragt mit dieser Information die Übermittlung der Personenidentifizierungsdaten zur E-ID beim SID.

15 Attribute, die auch im normalen Geschäftsleben nicht ohne weiteres mitgeteilt werden, sind für höhere Sicherheitsniveaus der E-ID reserviert; so wird zum Beispiel das Unterschriftsbild nur auf dem höchsten Sicherheitsniveau mitgeliefert.

nis eines Geheimnisses‘ oder eine ‚inhärente Eigenschaft der Person‘, die biometrisch gemessen werden kann. Die E-ID muss technisch so abgesichert sein, dass sie vom E-ID-System eindeutig durch ihren Identifikator identifiziert werden kann, dass die Authentifizierung der Person gemäss den Anforderungen des E-ID Sicherheitsniveaus abläuft und dass allfällige Meldungen an die Anzeige des Trägergeräts der E-ID und Rückmeldungen der Inhaber oder des Inhabers authentisch sind.

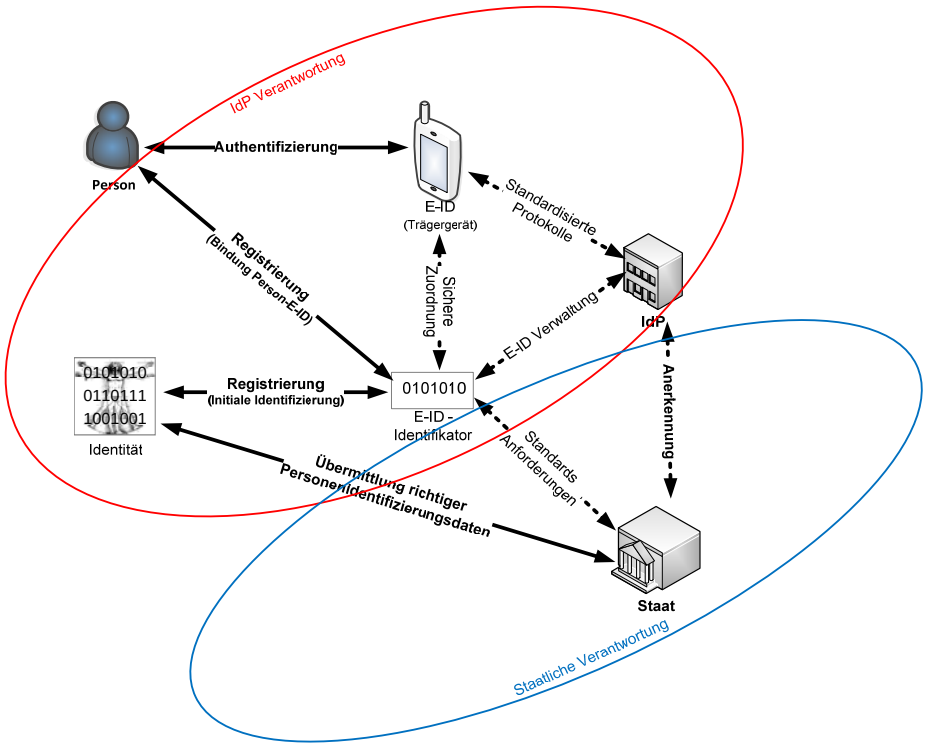
- Alle E-ID sollen unabhängig vom Aussteller bei allen vertrauenden Beteiligten eingesetzt werden können, die eine Identifizierung oder Authentifizierung auf dem Sicherheitsniveau der E-ID akzeptieren. Diese **Interoperabilität** ist eine wichtige Voraussetzung für die Akzeptanz einer E-ID im digitalen Geschäftsleben. Dies wird durch die Festlegung von Protokollen, Nachrichtenformaten und Zusammenarbeitsverpflichtungen zwischen den IdP erreicht. Sowohl für vertrauende Beteiligte als auch für Inhaberinnen und Inhaber einer E-ID soll der Einsatz und die Nutzung einer anerkannten E-ID überall gleich und transparent erfolgen.

Die Nutzung einer E-ID wird eine vertrauende Beteiligte immer unter diesen Sicherheitsaspekten in Relation zu ihren Geschäftsbedürfnissen setzen. Denn das für einen spezifischen Geschäftsprozess nötige Sicherheitsniveau wird in der Praxis durch die vertrauende Beteiligte bestimmt. Diese akzeptiert nur die E-ID-Systeme, die ihren Anforderungen an die Identifizierung und Authentifizierung der Geschäftspartner genügen. Sie bezieht die gewünschten Identitätsdienstleistungen von dem oder den IdP, die geeignete staatlich anerkannte E-ID-Systeme im Markt etabliert haben. Dank der Anforderung, dass staatlich anerkannte E-ID-Systeme interoperabel und standardisiert sein müssen, ist die vertrauende Beteiligte in ihrer Wahl kaum durch technische Hürden behindert und der Markt kann sich frei entfalten. Es sind verschiedene Geschäftsmodelle zwischen den vertrauenden Beteiligten, den Inhaberinnen und Inhabern sowie den IdP möglich. Der Markt entscheidet welche erfolgreich sind.

Inhaberinnen und Inhaber sowie die vertrauenden Beteiligten müssen sich darauf verlassen können, dass staatlich anerkannte E-ID-Systeme den deklarierten Sicherheitsniveaus genügen. Sie haften jedoch für die Sicherheitsaspekte, für die sie zuständig sind:

- die Inhaberin oder der Inhaber haftet für die korrekte Handhabung der E-ID und darf diese insbesondere nicht Dritten überlassen;
- die vertrauende Beteiligte muss durch Einhaltung der vom IdP vorgegebenen technischen und organisatorischen Prozesse bei der Nutzung von E-ID die korrekte Identifizierung und Authentifizierung durch das E-ID System der IdP ermöglichen.

Die Zuständigkeiten und die Aufteilung der Verantwortung zwischen Staat und IdP sind in der nachstehenden Abbildung dargestellt. Die grundsätzlichen Regelungen sind im Gesetz festgehalten; die Details werden in der Verordnung geregelt.



Skizze 2: Aufteilung der Verantwortung zwischen Staat und IdP.

1.2.3 Nutzerfreundlichkeit

Das Nutzerverhalten in den digitalen Märkten ist eng mit Innovationen und internationalen Technologieentwicklungen im globalen IT-Markt verbunden. Der Markt unterliegt schnellen Änderungen und lässt sich kaum durch starre Regulierungen oder staatliche Zwänge nachhaltig beeinflussen. Auf einen einfachen Nenner gebracht ist ein System nutzerfreundlich, wenn es vom Markt akzeptiert wird und umgekehrt. Gerade im Bereich von sicherheitsrelevanten Systemen, wozu ein E-ID-System gehört, werden oft die höchst möglichen Anforderungen an die Sicherheit und den Schutz der Privatsphäre gestellt. Es gibt aber eine wesentliche Diskrepanz zwischen solch idealistischen Anforderungen und konkretem Nutzerverhalten in der Praxis. Sehr oft führen theoretisch optimale aber oft etwas umständliche Sicherheitsmassnahmen zu einem Umgehungsverhalten der Nutzer und damit zu substanziellen Sicherheitslücken, die mit einfacheren und nutzerfreundlichen Sicherheitsmassnahmen vermeidbar wären.

Wichtige Eigenschaften für eine hohe Nutzerfreundlichkeit von E-ID-Systemen sind:

- **Zahlreiche Online Angebote** von bekannten und vertrauenswürdigen Organisationen mit hoher Marktpräsenz, bei denen die E-ID eingesetzt werden kann. Eine E-ID soll bei allen vertrauenden Beteiligten eingesetzt werden können, unabhängig davon, welcher IdP die E-ID ausgestellt hat. Einzig das für das Angebot verlangte Sicherheitsniveau muss durch die E-ID erfüllt sein.

- **Einfache Ausstellung und simple Inbetriebnahme**, wobei möglichst alle Schritte in einem durchgehenden Prozess online durchführbar sein sollten; allenfalls verlangte persönliche Vorsprachen müssen flexibel und ortsnah möglich sein oder noch besser durch sichere Alternativen wie zum Beispiel Videokonferenzen ersetzt werden.
- **Überall gleicher Ablauf** beim Einsatz der E-ID auf einem bestimmten Sicherheitsniveau. Es ist sehr wichtig, dass die Inhaberinnen und Inhaber ihre E-ID kennen und diese gerne möglichst häufig einsetzen. Dies kann nur mit einem einfachen, einheitlichen und verständlichen Nutzererlebnis über alle Einsatzorte hinweg erzielt werden. Die Standardisierung anerkannter E-ID-Systeme wird deshalb auch Anforderungen an die Nutzerschnittstelle und das Einsatzprotokoll beinhalten.
- **Universeller Einsatz der E-ID** wenn immer möglich jederzeit vom persönlichen Endgerät (PC, Smartphone) aus. Jedoch gleichzeitig weitgehende Unabhängigkeit von aktuellen Technologien und Geräten mit kurzer Lebensdauer, so dass die E-ID problemlos von einem Trägergerät zum nächsten transferiert werden kann.
- **Verständliche Sicherheitsmassnahmen,** so dass die Inhaberinnen und Inhaber den Sinn eines Sicherheitsprotokollschrittes verstehen und nicht in Versuchung kommen diesen zu umgehen.
- **Akzeptable Kosten und lange Gültigkeitsdauer**. Eine E-ID soll mehrere Jahre gültig und einsatzfähig sein. Falls beim Einsatz der E-ID für die Inhaberin oder den Inhaber eine Kostenbeteiligung vorgesehen ist, sollte diese nach einem ‚pay-per-use' Modell gestaltet werden mit einem Preis für die gesamte Online-Dienstleistung. Die mit einer E-ID verbunden Gesamtkosten sollten dabei so bemessen sein, dass der Besitz einer staatlich anerkannten E-ID als vorteilhaft und preiswert empfunden wird. Die initiale Ausstellung einer E-ID sollte wenn möglich kostenlos sein.

Nicht nur für die Inhaberinnen und Inhaber muss das E-ID-System einfach zu nutzen sein, sondern insbesondere auch für die vertrauenden Beteiligten, die eine E-ID akzeptieren und damit vielfältige Einsatzmöglichkeiten für E-ID schaffen. Wichtige Kriterien bei der Implementation eines E-ID-Systems in einen Anmeldeprozess eines **vertrauenden Dienstes** sind:

- Die **Integration der Protokolle des E-ID-Systems** in möglichst alle Geschäftsprozesse eines vBt, die eine Identifizierung und Authentifizierung erfordern, muss einfach sein. Dabei installiert die vertrauende Beteiligte in ihrem Portal (als **vertrauender Dienst** bezeichnet) eine standardmässig integrierbare Schnittstellen Anwendung für die Nutzung der Identitätsdienstleistungen des E-ID-Systems (als **E-ID-Schnittstelle** bezeichnet**)**. Diese E-ID-Schnittstelle wird vom IdP, mit dem die vertrauende Beteiligte zusammenarbeitet, definiert und enthält insbesondere auch die standardisierte Nutzeroberfläche für den Online Einsatz der E-ID. Die Ausführung der Identifizierung und Authentifizierung wird dann vom vertrauenden Dienst via E-ID-Schnittstelle an das E-ID-System delegiert. Das Resultat der Identitätsdienstleistung wird von diesem in Form eines abgesicherten Tickets via die E-ID-Schnittstelle dem vertrauenden Dienst zurückgeliefert. Die meisten heute marktgängigen E-ID-Systeme funktionieren nach diesem Schema und erlauben eine minimal invasive Integration eines E-ID-Systems in eine bestehende E-Commerce Anwendung. Durch Standardisierung z.B. die Authentifizierung nach den FIDO Spezifikationen [4] und das Attributmanagement nach den einschlägigen eCH-Standards [11], wird die Integration, aber auch der Wechsel von einem E-ID-System zu einem anderen, einfach realisierbar.
- Dank der verlangten **Interoperabilität** unter den staatlich anerkannten E-ID-Systemen ist es möglich, jede E-ID unabhängig vom ausstellenden IdP, bei jeder vertrauenden Beteiligten einzusetzen, sofern die E-ID das geforderte Sicherheitsniveau erfüllt. Dazu leitet der IdP, bei dem die vertrauende Beteiligte die Identitätsdienstleistung bezieht, den Identifizierungs- oder Authentifizierungsauftrag der vBt an den IdP weiter, der die spezifische E-ID ausgestellt hat.

Dies ist immer möglich, da die IdP untereinander interoperable Schnittstellen bereitstellen müssen. Der zuständige IdP führt den Auftrag aus und sendet das Antwort-Ticket über den gleichen Weg zurück zur vertrauenden Beteiligten. Somit sind weder die vertrauenden Beteiligten noch die Inhaberinnen und Inhaber in der Akzeptanz und dem Einsatz einer E-ID eingeschränkt.

- Der Einsatz der E-ID bedingt nur **geringe Anpassung der Geschäftsabläufe,** so dass das Online-Geschäft nicht beeinträchtigt wird. Vertrauende Beteiligte werden dank der verlangten Standardisierung die E-ID-Systeme ohne grosse Anpassungen ihrer IT-Infrastruktur oder ihrer Geschäftsmodell einsetzen können. Die Identifizierung und Authentifizierung mittels der E-ID soll nur zu simplen Protokollzusätzen in bestehenden Geschäftsprozessen führen. Die IdP werden gefordert sein, ihre Angebote an diesem Marktbedürfnis auszurichten. Mit Standardisierungsvorgaben und einem einfachen Gebührenmodell für die Übermittlung von Personenidentifizierungsdaten hilft der Staat den IdP diese Anforderung zu erfüllen.
- Der **Schutz von Geschäftsdaten** muss gewährleistet sein. Durch die Integration einer überall nutzbaren E-ID dürfen keine geschäftsrelevanten und vertraulichen Daten der vertrauenden Beteiligten, aber auch keine des IdP oder der Inhaberin oder des Inhabers preisgegeben werden. Durch geeignete Auflagen bezüglich Datenschutz und Aufsicht sorgt der Staat dafür, dass staatlich anerkannte E-ID-Systeme und die betreibenden IdP dieser Anforderung genügen.
- Der Einsatz einer staatlich anerkannten E-ID soll einen **ökonomischen Vorteil** bieten und unter dem Strich wirtschaftlicher sein, als das Ausrollen und der Betrieb einer eigenen Authentifizierungslösung (Silosystem) oder gar der Verzicht auf eine sichere Online-Identifizierung. Die Geschäftsmodelle der IdP, die staatlich anerkannte E-ID-Systeme anbieten, müssen diese ökonomische Zwangsbedingung berücksichtigen. Andererseits wird der Staat durch eine geeignete Haftungsregulierung vertrauende Beteiligte dazu ermutigen, vertrauenswürdige E-ID-Systeme für ihre Online-Dienstleistungen einzusetzen.

Gemäss eIDAS-Verordnung (Art. 7) können nur E-ID-Systeme notifiziert werden, die auch von öffentlichen Diensten für die Online-Identifizierung verwendet werden. Aus diesem Grund verpflichtet das E-ID Gesetz Online-Portale des Bundes, anerkannte E-ID-Systeme zu nutzen, sofern diese das für den Dienst nötige Sicherheitsniveau erreichen. Im Gegenzug soll die Nutzung einer E-ID durch öffentliche Stellen seitens IdP zu einem Einheitstarif nach einem ‚pay-per-use' Modell angeboten werden.

1.3 Umfeld

1.3.1 Sozioökonomische Entwicklung

Mit der Verbreitung des Internets und der hohen Verfügbarkeit von leistungsfähigen Mobilgeräten können Geschäftsprozesse immer einfacher in die digitale Welt verlagert werden. Die gut ausgebildeten und technologieaffinen jüngeren Generationen, welche sehr gut vernetzt und ständig online sind, begünstigen diesen sozioökonomischen Wandel.

Gemäss den Angaben des Bundesamtes für Statistik [1] haben 2015 88% der Bevölkerung über 14 Jahren das Internet in den vergangenen sechs Monaten mindestens einmal benutzt, wobei 99% der 14-19 Jährigen und immerhin 43% der über 70 Jährigen das Internet mindestens einmal pro Woche oder täglich nutzten. Im europäischen Vergleich liegt die Schweiz über dem Durchschnitt von 76%, aber noch hinter den führenden Ländern Island (97%) und Dänemark (93%) zurück. 42% der Internetnutzerinnen und –nutzer sind täglich 1-5 Stunden und 15% bereits über 15 Stunden online.

Die mobile Nutzung des Internets hat in den letzten Jahren stark zugenommen und lag 2015 bei

42% der Gesamtbevölkerung. Genutzt wurden dazu zu 95% das Mobiltelefon und zu 23% das Tablet. Dagegen hat sich die Nutzung des Laptops mit 42% seit 2010 beinahe halbiert.

56% der Bevölkerung nutzten 2015 das Internet für Online-Einkäufe, 49% für E-Banking, 48% für Dienstleistungen im Zusammenhang mit Reisen, 48% für das Ausfüllen von Online-Formularen von Behörden und 35 % für politische Tätigkeiten. Für den Kontakt mit Behörden nutzten 79% aller Internetnutzerinnen und –nutzer das Internet. Die E-Commerce-Ausgaben der Haushalte sind innerhalb eines Jahrzehntes im Jahr 2014 auf über sieben Milliarden Franken gestiegen.

1.3.2 Internationales Umfeld

Die Schweiz befindet sich mit der Einführung eines staatlich anerkannten elektronischen Identifizierungsmittels nicht allein. Das Thema ist seit gut 15 Jahren auf der Agenda der meisten entwickelten Staaten.

Es gibt mehrere gute Gründe, die Situation in andern Ländern wie auch auf internationaler Ebene zu studieren und bei der eigenen Konzeption zu berücksichtigen. Die Problemstellung bezüglich E-ID ist in vergleichbaren Ländern weitgehend die gleiche wie in der Schweiz; man kann daher von den Erfahrungen anderer Länder profitieren. In Anbetracht der globalen Natur von Online-Diensten im Internet, ist es wichtig, ein vom Staat anerkanntes elektronisches Identifizierungsmittel in konzeptioneller, technischer und rechtlicher Hinsicht so zu gestalten, dass es international, insbesondere im europäischen Raum eingesetzt werde kann. Schliesslich ist es in stark technisch beeinflussten Gebieten wichtig, auf die herrschenden Trends zu setzen. Ein einzelnes Land, und erst recht die Schweiz, ist zu klein, um technische Trends massgeblich beeinflussen zu können.

In mehreren europäischen Staaten und in einer beträchtlichen Zahl von Schwellenländern sind heute bereits staatliche E-ID, meist integriert in kontaktbehaftete Smartcards, eingeführt worden. Die Akzeptanz bei der Bevölkerung und der Wirtschaft ist noch bescheiden; insbesondere in den europäischen Staaten, die keinen Zwang zur Nutzung der E-ID eingeführt haben, konnten sich die zum Teil mit hohem Aufwand ausgerollten Systeme noch nicht bewähren. Beispielhaft zu erwähnen ist hier der neue deutsche Personalausweis (nPA), der bereits vor einigen Jahren eingeführt wurde und eine sehr sicher konzipierte E-ID enthält. Es zeigte sich aber, dass die E-ID im nPA wenig Akzeptanz findet, weil sie zwar bezüglich Sicherheit hervorragend, aber in der täglichen Handhabung kompliziert und für den betreibenden Staat sehr teuer ist [12]. In Deutschland wird nun versucht die E-ID auch auf mobilen Trägern, wie Smartphones, verfügbar zu machen. Auch andere Lösungen für E-ID-Systeme, die zusätzliche Infrastrukturkomponenten bei den Endnutzern verlangen, haben Akzeptanzprobleme; so wird zum Beispiel die belgische E-ID [13] meist nur für das Ausfüllen der Steuererklärung verwendet, weil die Bürger dazu verpflichtet werden und die E-ID der österreichischen Bürgerkarte wird nur von einer kleinen Minderheit verwendet [14] (im Gegensatz zu der ebenfalls angebotenen Lösung auf dem Smartphone).

In der ersten Phase der Beschäftigung der Staaten mit dem Thema der E-ID ging es primär um die Frage, ab wann, mit welcher Technologie und mit welchen Funktionen ein Staat seine Identitätskarte um die E-ID erweitern würde. Die wesentlichen Fragen waren, welche Chip-Technologie verwendet würde, welches Chip-Betriebssystem und ob der Chip kontaktbasiert oder per Funk (NFC) mit der Umwelt kommunizierte. Ein wichtiges juristisches und politisches Thema war, ob sich die E-ID auf einen bestehenden Personenidentifikator bezog und welcher Art dieser war. In funktioneller Hinsicht war zu entscheiden, ob der Chip gleichzeitig einen Schlüssel für die elektronische Signatur enthielt, und später, ob auch die inzwischen von der ICAO standardisierte elektronische Pass-Funktion (E-Pass-Funktion) [15] mit Funktechnologie enthalten sei.

Mit solchen Überlegungen haben in den letzten ca. 15 Jahren nach und nach viele europäische Staaten eine mit der Identitätskarte verbundene E-ID als Kernstück eines nationalen E-ID-Sys-

tems eingeführt. Pionier war Finnland, welches im Jahr 1999 eine Identitätskarte mit E-ID einführte. Es folgten Estland, Belgien, Spanien und Portugal. Deutschland hat im Jahr 2010 seinen elektronischen Personalausweis (ePA / nPA) [16] eingeführt. In den letzten Jahren haben insbesondere Länder im Nahen Osten und in Asien neue staatliche Identitätskarten mit E-ID Funktion eingeführt. Nicht selten vielleicht auch darum, weil man auf keinen Fall in Rückstand geraten wollte in Anbetracht der langen Produktezyklen von Identitätskarten im Vergleich zur raschen Entwicklung in der Technik (Mainstream). Hingegen haben weder die USA noch das Vereinigte Königreich eine staatliche E-ID eingeführt, was sich mit der generellen Skepsis gegenüber Identitätskarten in diesen Ländern deckt. Zumindest in den USA wird aber oft der Führerausweis ersatzweise als „Identitätsausweis“ eingesetzt. Einige Staaten der USA haben begonnen, einen E-Führerausweis einzuführen oder darüber nachzudenken [17] [18].

Eine erste typische Konstellation waren Smartcards mit X.509-Zertifikaten auf kontaktbasierten Chips, aufbauend im Wesentlichen auf der Technologie der Signaturkarten. Beispiele dieser Art waren die finnische, die estnische und die belgische E-ID Karte, sowie übrigens im Kern auch die SuisseID. Diese Karten sind inzwischen oft schon durch eine zweite Generation abgelöst.

Eine weitere verbreitete Konstellation ergab sich aus den Bemühungen der europäischen Chip-Industrie, ein Set von Standards mit Optionen für eine European Citizen Card (ECC) zu definieren. Diese Karten enthalten die E-Pass-Funktion gemäss ICAO, sowie eine an die E-Pass-Funktion angelehnte Funktion für die elektronische Online-Identifikation. Schweden, Monaco, Lettland, Finnland (2. Auflage) und die Niederlande haben solche Identitätskarten. Der ECC-Standard hat sich nie ganz stabilisieren können. Eine Ausprägung davon hat sich aber insbesondere EU-weit bei den Ausländerausweisen (Aufenthaltspapiere für Drittstaatenangehörige) durchgesetzt. Grund dafür ist, dass die EU in diesem Bereich – im Unterschied zu den Identitätskarten – legiferieren darf. Auch der Schweizer Ausweis für Drittstaatenangehörige folgt diesem Standard.

Eine Art Kulminationspunkt dieser Phase der E-ID Entwicklung ist der 2010 von Deutschland eingeführte elektronische Personalausweis (ePA). Er enthält im Wesentlichen die vorstehend erwähnten Komponenten, wurde aber an einigen Punkten verbessert und insbesondere um mehrere technisch anspruchsvolle Verfahren zur Verstärkung des Persönlichkeitsschutzes erweitert. So müssen sich Dienstanbieter (Service Provider) für den Bezug bestimmter Attribute vom Staat registrieren lassen und sich beim Einsatz gegenüber der E-ID ebenfalls authentifizieren. Eine Pseudonymisierungsfunktion (‘Restricted Identity’) sorgt dafür, dass sich der Personalausweis jedem Dienstanbieter gegenüber mit einem unterschiedlichen Identifikator meldet, damit die Erstellung von Benutzerprofilen erschwert wird. Mit einer übergreifenden Strategie hat Deutschland dafür gesorgt, dass die Aufenthaltstitel für Ausländerinnen und Ausländer mit kompatiblen «Online-Ausweisfunktionen» ausgestattet sind. In den letzten Jahren ist der deutsche ePA ein Stück weit die Messlatte für neue staatliche E-ID weltweit geworden. In Deutschland ist inzwischen etwa die Hälfte der Bevölkerung mit dem ePA ausgerüstet und noch ist nicht klar, ob die E-ID auf dem nPA tatsächlich einmal breit eingesetzt werden wird.

Ein wesentlicher Faktor, ob die E-ID von der Inhaberin oder dem Inhaber genutzt wird, ist ein breites Angebot an Dienstleistungen, bei welchen die E-ID eingesetzt werden kann. So zeigt sich, dass in grossen deutschen Agglomerationen, welche aktiv Online-Angebote bereitstellen, die Aktivierungsrate der E-ID des ePA deutlich höher liegt. Oder umgekehrt formuliert überwiegt in Regionen mit einem spärlichen Online-Angebot die Skepsis gegenüber der E-ID beim deutschen Personalausweis.

Am weitesten entwickelt ist das E-ID System in Estland, das seit über zehn Jahren im Einsatz ist und heute die meisten Dienste von E-Banking bis Vote électronique für die ganze Bevölkerung online erschliesst. Ebenfalls sehr erfolgreich ist das schwedische Modell mit der BankID, das auf der Zusammenarbeit der Banken mit dem Staat beruht und konzeptionell sehr nahe dem hier für die Schweiz vorgeschlagenen Modell ist. Die in diesen Ländern als entscheidend für den Erfolg der E-ID festgestellten Kriterien sind [19]

- die durchgehende Akzeptanz der E-ID bei allen öffentlichen online Diensten,
- Kooperation zwischen öffentlichem und privatem Sektor,
- Ein funktionierendes Geschäftsmodell für alle Beteiligten,
- Beim E-ID-Einsatz in allen Anwendungen ein durchgehend gleiches Nutzererlebnis,
- Ein generell verfügbarer Eindeutiger Personenidentifikator und
- Verbindliche Regeln als Vertrauensbasis sowie einheitliche Standards für die Infrastruktur.

1.3.3 Aktuelle Entwicklungen

Die punktuelle Optimierung der Sicherheit einer einzelnen Komponente in der Abwicklung von elektronischen Geschäftsprozessen kann die Gesamtsicherheit nicht erhöhen; dies gilt auch für E-ID [20]. Dass Sicherheit allein als bestimmendes Designkriterium nicht zielführend ist, zeigt auch die SuisseID. Trotz grosser Erwartungen hat sie sich in der Schweiz bisher nur als Nischenprodukt etablieren können. Als Schwächen bzw. Gründe für die eingeschränkte Verbreitung der SuisseID werden insbesondere die wenig komfortable Installation, die auf drei Jahre limitierte Gültigkeitsdauer der Zertifikate, der Mangel an Anwendungen und internationaler Interoperabilität sowie die aufwendige und teure Beschaffung genannt [21] [22]. Dagegen fallen z.B. bei der neueren Mobile ID keine direkten Kosten für den Nutzer an – diese werden über einen Nutzungsvertrag den vertrauenden Beteiligten belastet – und Ausstellung und Einsatz sind nutzerfreundlicher. Auch ausserhalb der Schweiz haben fast alle E-ID-Systeme, die unabhängig von konkreten Geschäftsfällen einseitig nur die Sicherheit priorisieren und die Benutzerfreundlichkeit vernachlässigen, Akzeptanzprobleme [23] [24] [25].

Das geplante E-ID Lösungskonzept für die Schweiz soll dagegen die wichtigsten Kriterien für die Marktakzeptanz möglichst gut und gleichgewichtet erfüllen. Dazu wurden bereits im Rahmen der Vorbereitungen für das vorliegende E-ID Konzept auf verschiedenen Ebenen umfangreiche Abklärungen durchgeführt. Es wurden private und öffentliche Aussteller von E-ID, potenzielle vertrauende Beteiligte und Trendsetter für zukünftige technologische Entwicklungen im Bereich des elektronischen Identitätsmanagements konsultiert. Im aktuellen E-ID Konzept konnten zusätzliche Vereinfachungen und Verbesserungen für anerkannte E-ID-Systeme realisiert werden, die alle zu einer weiteren Erhöhung der Marktakzeptanz führen sollten. So sind die entscheidenden Kriterien für eine akzeptierte und brauchbare E-ID, nebst der Vertrauensbasis in die rechtliche, technische und organisatorische Sicherheit, Benutzerfreundlichkeit, Wirtschaftlichkeit, standardisierte Anwendung und vielfältige Einsetzbarkeit [19] [26]. Die am Häufigsten gebrauchten Funktionen der E-ID ist Registrierung bei einer vertrauenden Beteiligten und später die Anmeldung beim vertrauenden Dienst, wenn man schon als Nutzer registriert ist. Diese Abläufe müssen deshalb besonders nutzerfreundlich und technologisch aktuell sein [27].

In den letzten Jahren hat sich deshalb der Fokus der Überlegungen zur staatlichen Förderung der E-ID weg von der Frage „welche E-ID auf der Identitätskarte?“ in eine neue Richtung entwickelt. Die wichtigsten Gründe dürften sein, dass der Produktezyklus einer staatlichen Identitätskarte im Vergleich zur Geschwindigkeit der Entwicklung in der elektronischen Welt viel zu lang ist und dass E-ID auf Karten immer auch eine teure und zuverlässige Lesegeräteinfrastruktur benötigen. Diese Lesegeräteinfrastruktur ist zwar nicht so aufwendig in der Anschaffung, jedoch meist kompliziert und teuer in der Anwendung und im Unterhalt. Zudem stehen nicht auf allen aktuellen Geräteplattformen, insbesondere den heute dominierenden mobilen Geräten, entsprechende Lesegeräte oder Anschlüsse dazu zur Verfügung.

Parallel zum US-amerikanischen Projekt der gemeinsamen Entwicklung eines Identity Ecosystems [28] begann man sich in vielen Ländern grundsätzlicher zu überlegen, wie eine gute Architektur für das gesamte nationale und internationale Ökosystem rund um die E-ID, unter Einbezug

aller Akteure, auszusehen hätte, und welches der Beitrag des Staates für ein solches E-ID-Ökosystem sein könnte. Die einzelnen Länder kamen dabei zu unterschiedlichen Schlüssen.

In den USA beschränkt sich die Rolle des Staates auf die eines Organisators und Förderers des E-ID-Ökosystems; er stellt selbst keine Dienste zur Verfügung, hat jedoch einen grossen Einfluss auf den Markt als Bezüger von E-ID für seine Mitarbeitenden und als Betreiber von vertrauenden Diensten im Rahmen der E-Government-Angebote. In Schweden, Norwegen und Dänemark wurden die Banken zu den wichtigsten Anbietern von E-ID für alle Branchen erkoren, bieten sie doch für ihre eigenen Dienstleistungen schon länger solche Produkte an. Staatliche Minimalanforderungen sorgen für eine definierte Qualität und für die Interoperabilität.

Die vorstehend schon erwähnte eIDAS-Verordnung der EU musste diese Entwicklung schliesslich akzeptieren und für die gegenseitige Anerkennung neben den vom Staat ausgestellten E-ID auch staatlich anerkannte E-ID-Systeme als gleichwertig akzeptieren. Diese Konzeption drückt sich im Artikel 7 wie folgt aus:

> **Voraussetzungen für die Notifizierung elektronischer Identifizierungssysteme**
>
> Ein elektronisches Identifizierungssystem kann nach Artikel 9 Absatz 1 notifiziert werden, wenn sämtliche folgenden Bedingungen erfüllt sind:
>
> a) Die elektronischen Identifizierungsmittel im Rahmen des betreffenden Systems werden
>
> i) vom notifizierenden Mitgliedstaat ausgestellt,
>
> ii) im Auftrag des notifizierenden Mitgliedstaats ausgestellt oder
>
> iii) unabhängig vom notifizierenden Mitgliedstaat ausgestellt und von diesem anerkannt.

Im gleichen Artikel wird anschliessend bestimmt, welche Haftung den Aussteller einer E-ID trifft und welchen Pflichten sich der Staat auf keinen Fall, also auch nicht in der Konstellation von Artikel 7 Buchstabe a) iii) entziehen kann.

1.3.4 Folgerungen für die Schweiz

Bereits heute agieren im schweizerischen E-ID-Ökosystem zahlreiche Identitätsdienstleister, die eine E-ID anbieten, wie z.B. die SuisseID, Mobile ID, Google ID, AppleID, Open ID und so weiter. Es existieren auch verwaltungsinterne Lösungen mit einer persönlichen Smartcard, wie zum Beispiel diejenige für die Authentifizierung beim SSO-Portal des EJPD. Im Rahmen des Projektes IAM-Bund soll sogar eine einheitliche Lösung für die ganze Bundesverwaltung realisiert werden. Zudem geben Unternehmen, wie zum Beispiel Banken oder Versicherungen, dedizierte Identifizierungsmittel für ihre Kunden heraus, die ausschliesslich für die eigenen Geschäfte gebraucht werden. Solche auf eine Anwendung beschränkte Identifizierungsmittel werden als „Silolösungen“ bezeichnet, im Gegensatz zu den obgenannten Lösungen, die in multiplen Kontakten eingesetzt werden können („föderierte bzw. interoperable Lösungen“). All diese Systeme haben eine unterschiedliche Verbreitung, Benutzerfreundlichkeit, Funktionalität und Sicherheit und sie sind untereinander meist nicht kompatibel. International geht jedoch der Trend klar in Richtung einer nutzerzentrierten, sicheren und interoperablen Authentifizierung und Identifizierung als Basis für alle darauf aufbauenden Vertrauensdienste.

Vergleicht man das hier vorgestellte und im Gesetzesentwurf umgesetzte Konzept für die staatliche Anerkennung elektronischer Identifizierungsmittel mit den Entwicklungen, Erfahrungen und aktuellen Überlegungen im nationalen und internationalen Umfeld, so sieht das wie folgt aus:

- Die Schweiz liegt mit ihrem Konzept einer staatlich anerkannten E-ID im Trend, bzw. hat die Lehren aus den Erfahrungen in anderen Ländern der letzten 15 Jahre gezogen.
- Das Schweizerische Konzept ist grundsätzlich EU-, bzw. eIDAS-konform.

- Das Schweizerische Konzept ist sehr flexibel und sollte auch bei einschneidenden technischen und ökonomischen Entwicklungen bestehen können.

Das vorgestellte Konzept ist auch gut vereinbar mit dem in der Schweiz entwickelten Referenzmodell für ein E-ID-Ökosystem [29].

1.3.5 EU-Kompatibilität

Ist schon für den klassischen Ausweis mit sichtbaren Daten die internationale Verwendbarkeit wichtig, trifft dies erst recht für die E-ID zu. Als Online-Ausweis wird diese auf dem von Natur aus grenzenlosen Internet eingesetzt. Für die EU, die sich der Realisierung eines schrankenlosen einheitlichen europäischen Binnenmarktes verpflichtet hat, ist dieses Anliegen besonders wichtig.

Am 23.Juli 2014 hat die EU daher die Verordnung (EU) Nr.910/2014 [2] des europäischen Parlaments vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) erlassen. Nebst der Regelung und Zertifizierung der Anbieter der elektronischen Signatur und weiterer Vertrauensdienste enthält die Verordnung als neues Thema die Notifikation und damit verbunden die gegenseitige Anerkennung von nationalen Systemen für die elektronische Identifizierung. Alle Mitgliedstaaten werden verpflichtet, überall dort, wo sie für den Zugang zu Behördendiensten eine E-ID verlangen, auch jede ausländische E-ID aus jedem notifizierten System zuzulassen (Artikel 6). Diese Verpflichtung gilt sogar für einen Mitgliedstaat, der selbst kein notifiziertes E-ID-System besitzt.

Das geplante E-ID-Gesetz und die staatlich anerkannten E-ID-Systeme der Schweiz sollen kompatibel zu den E-ID-Systemen der EU sein (vgl. auch Übersicht).

1.4 Strategien und Auftrag

1.4.1 Strategie des Bundesrates für eine digitale Schweiz

Die Strategie „Digitale Schweiz“ des Bundesrates vom April 2016 [30] beinhaltet das Ziel „Ein System für ein sicheres und benutzerfreundliches Identitätsmanagement steht schweizweit zur Verfügung“. Dabei gilt es, auf der Basis von internationalen Standards eine sichere, barrierefreie und benutzerfreundliche digitale Lösung für den schweizweiten Nachweis von Identitäten zu erarbeiten.

1.4.2 E-Government-Strategie Schweiz

Die „**E-Government-Strategie Schweiz**“ [31] [32] hat zum Ziel, dass sowohl die Wirtschaft als auch die Bevölkerung wichtige Geschäfte mit den Behörden elektronisch abwickeln können. Das priorisierte Vorhaben „B2.15 National und im EU-Raum barrierefrei anerkannte elektronische Identität“ [33] ist einer der Bausteine zur Umsetzung dieser Strategie des Bundesrates, der mit diesem E-ID Konzept bereitgestellt werden soll.

1.4.3 Bundesratsauftrag für staatlich anerkannte Identifizierungsmittel

Gestützt auf das Aussprachepapiers des EJPD vom 23. Dezember 2015 hat der Bundesrat am 13. Januar 2016 u.a. folgende Eckpunkte für die weitere Entwicklung staatlich anerkannter E-ID zur Kenntnis genommen und das EJPD beauftragt, ihm bis Ende 2016 eine Vernehmlassungsvorlage zu unterbreiten:

- Der Bund soll einen Rechts- und Standardisierungsrahmen sowie die Organisationsstruktur

für die staatliche Anerkennung von E-ID-Systemen und der E-ID ausstellenden Identitätsdienstleister schaffen. Dieser ist so auszugestalten, dass eine spätere gegenseitige Anerkennung der staatlich anerkannten E-ID-Systeme zwischen der Schweiz und der EU möglich bleibt.

- Staatlich anerkennbare E-ID-Systeme sollen durch private und öffentliche Identitätsdienstleister (IdP) bereitgestellt werden. Der Bund verzichtet auf die Herausgabe einer eigenen staatlichen E-ID.
- Geeignete E-ID-Systeme sollen auf einer von drei Vertrauensstufen staatlich anerkannt werden können.
- Staatlich anerkannte E-ID-Systeme sollen im Grundsatz allen Personen mit Schweizer Bürgerrecht sowie den ausländischen Personen in der Schweiz zugänglich sein.
- In Registern beim Bund geführte Personenidentifizierungsdaten sollen für staatlich anerkannte E-ID-Systeme über eine elektronische Schnittstelle an IdP übermittelt werden.
- Zur Identifikation einer Person soll ein eindeutiger Personenidentifikator (EPID) geschaffen werden.
- Die AHVN13 soll als Identitätsattribut geführt werden, wobei die Übermittlung an nicht für eine systematische Nutzung zugelassene Dritte technisch unterbunden wird.
- Eine weitere Vereinfachung der Abläufe im Zusammenhang mit der Übermittlung von Personenidentifizierungsdaten soll im Rahmen der weiteren Konzeptarbeiten geprüft werden.
- Als Investitionsschutzmassnahme sollen alle Bundesstellen grundsätzlich verpflichtet werden, staatlich anerkannte E-ID-Systeme bei ihren E-Government-Anwendungen, welche eine Authentifizierung des Benutzers erfordern, auf dem jeweils geeigneten Sicherheitsniveau zu verwenden.

1.5 Abgrenzungen

Nicht Inhalt dieses Konzepts sind weitere Vertrauensdienste wie die Verwaltung von Rollen und Rechten im digitalen Raum, digitale Signaturen oder Siegel oder Funktionsnachweise für auszuführende online Transaktionen. E-ID-Systeme sind ausschliesslich Werkzeuge für das elektronische Identitätsmanagement (E-IdM) und damit nur ein zentraler Baustein für umfassende Identitäts- und Zugangsverwaltungssysteme. Im Unterschied zu den Zugangsverwaltungen, die von allen vertrauenden Beteiligten entsprechend ihrem Dienstangebot individuell konzipiert werden müssen, kann das E-IdM institutionsübergreifend und damit sehr effizient realisiert werden.

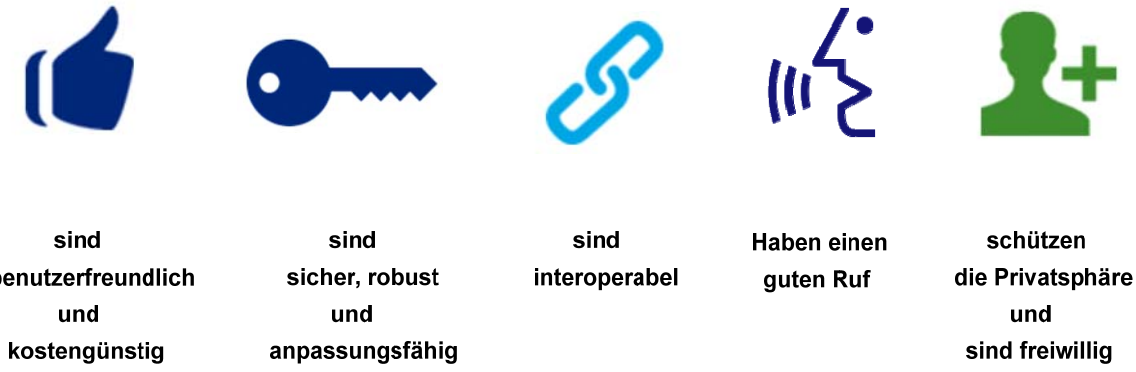
2 Konzept der staatlich anerkannten E-ID

2.1 Einleitung

Die direkten Nutzniesser von benutzerfreundlichen und vielfältig einsetzbaren staatlich anerkannten E-ID-Systemen sind die vertrauenden Beteiligten aus der Privatwirtschaft und der Behörden [34]. Aber auch die Inhaberinnen und Inhaber profitieren von einem dank der E-ID breiter aufgestellten Online-Angebot.

Der in diesem Konzept verfolgte Ansatz für die Bedienung des E-ID-Ökosystems mit einer geeigneten Lösung für die E-ID unterscheidet sich von den bisher staatlich ausgerollten Systemen in anderen europäischen Ländern (vgl. 1.3.2.). Da bisherige E-ID-Systeme mit wenigen Ausnahmen mit Akzeptanzproblemen kämpfen, erscheint ein neuer Ansatz für die Umsetzung nicht nur sinnvoll, sondern zwingend. Die Innovationskraft des Marktes im Bereich der elektronischen Dienstleistungen im Allgemeinen und der elektronischen Identifizierungsmittel im Speziellen soll durch keine starren staatlichen Lösungen eingeschränkt werden. Insbesondere soll die Bereitstellung von staatlich anerkannten E-ID-Systemen nicht als Monopol durch den Staat erfolgen. Die Geschäftsmodelle müssen im Markt entwickelt und validiert werden, so dass sie Akzeptanz erhalten. Die Aussteller und Betreiber von E-ID-Systemen erbringen Vertrauensdienste, die für einen funktionierenden elektronischen Markt notwendig sind.

Erfolgreiche E-ID-Systeme [35] …



Skizze 3: Leitgedanken für erfolgreiche E-ID-Systeme

Im vorliegenden Konzept unterstellen sich die IdP mit ihren E-ID-Systemen den Vorgaben für die staatliche Anerkennung freiwillig und erhalten dafür das vertrauensfördernde staatliche Gütesiegel der Anerkennung und direkt vom Staat Personenidentifizierungsdaten der Inhaberinnen und Inhaber ihrer staatlich anerkannten E-ID.

2.2 Zielsetzung

Der zentrale Beitrag des Staates zum schweizerischen E-ID-Ökosystem ist die Bereitstellung eines Rechts- und Standardisierungsrahmens („Trust Framework“) für staatlich anerkannte E-ID-Systeme. Dieser Rahmen liefert die notwendige Basis für ein wachsendes Vertrauen in Online-Dienstleistungen und reguliert den Markt so, dass Interoperabilität, internationale Anerkennung,

Nutzerfreundlichkeit, breite Anwendbarkeit, Sicherheit und Schutz der Privatsphäre gefördert wird.

Eine staatlich anerkannte E-ID kann ausgestellt werden für

- alle Schweizerinnen und Schweizer, die zum Zeitpunkt der Ausstellung einen gültigen Schweizer Ausweis gemäss Ausweisgesetz (AwG) haben, und
- Ausländerinnen und Ausländer, die zum Zeitpunkt der Ausstellung über einen gültigen Ausländerausweis gemäss Ausländergesetz (AuG) verfügen.

Die unterschiedlichen Bedürfnisse bezüglich Sicherheit der Identifizierung und Authentifizierung von Inhaberinnen und Inhabern durch die vBt werden durch abgestufte Sicherheitsniveaus der staatlich anerkannten E-ID-Systeme abgedeckt. Die Sicherheitsniveaus werden auf drei Stufen definiert, die der Abstufung der europäischen und auch der amerikanischen E-ID entsprechen.

Staatlich anerkannte E-ID sollen, unabhängig vom ausstellenden IdP, möglichst vielfältig bei vertrauenden Beteiligten eingesetzt werden können. Das Anwendungsprotokoll wird deshalb überall gleich und einfach in die Geschäftsprozesse der vBt integrierbar sein. Dabei soll es genügen, wenn vertrauende Beteiligte nur mit einem IdP eine Nutzungsvereinbarung für ein E-ID-System abschliessen. Die Interoperabilität für systemfremde E-ID, die bei einer vertrauenden Beteiligten eingesetzt werden, wird durch die anerkannten IdP realisiert, die ihre Systeme gegenseitig interoperabel vernetzen. Staatlich anerkannte E-ID auf ausreichendem Sicherheitsniveau sollen insbesondere bei Behörden ohne weitere Einschränkung bei der Registrierung oder Anmeldung zu einem vertrauenden Dienst eingesetzt werden können.

Zusätzlich betreibt der Staat als Dienstleistung einen Attributdienst für die Übermittlung von staatlich registrierten Personenidentifizierungsdaten an IdP, die staatlich anerkannte E-ID-Systeme betreiben. Inhaberinnen und Inhaber hinterlegen ihre staatlichen Personenidentifizierungsdaten beim IdP, der ihnen eine E-ID ausstellt. Nach der Registrierung können sie den IdP, bei dem ihre Personenidentifizierungsdaten hinterlegt sind, beauftragen, Attribute ihrer zivilen Identität auch an vertrauende Beteiligte ihrer Wahl zu liefern.

2.3 Grundsätze

Die wichtigsten Grundsätze der vorgeschlagenen Lösung sind in den folgenden Punkten zusammengefasst:

- Viele Vertrauensdienste sind Teil des Wirtschaftslebens und werden meist von privaten und öffentlich-rechtlichen Marktteilnehmern und nicht von Staates wegen erbracht. Dies gilt konsequenterweise auch für die Bereitstellung von E-ID-Systemen.
- Der Staat wirkt jedoch als Regulator für einen vertrauenswürdigen Markt, indem geeignete E-ID-Systeme und die anbietenden IdP staatlich anerkannt werden. Die IdP werden dabei auf einschlägige Standards und Regelungen bezüglich Sicherheit, Datenschutz und Interoperabilität verpflichtet. Der Staat verzichtet explizit auf die Ausstellung einer eigenen staatlichen E-ID (etwa auf der IDK), welche in Konkurrenz zu innovativen Lösungen des Marktes stehen würde.
- Eine E-ID ist, zumindest aus heutiger Sicht, kein Reisepass und wird deshalb nur dann beschafft, wenn die E-ID für wirtschaftliche, gesellschaftliche oder administrative Online-Tätigkeiten gebraucht wird. Die E-ID-Systeme müssen sich deshalb im Zusammenspiel von Angebot und Nachfrage in den digitalen Märkten bewähren. Dies bedeutet, dass die Geschäftsmodelle der IdP in der Praxis der elektronischen Märkte entwickelt und validiert werden müssen, so dass sie Akzeptanz erhalten.

- Der Markt der Identitätsdienstleister stellt E-ID in unterschiedlicher Qualität bezüglich Vertrauen (Sicherheit) und Nutzerfreundlichkeit (niedrige Eintrittsschwelle, einfacher Einsatz, verbreitete Anwendbarkeit) bereit. Der Staat anerkennt E-ID-Systeme auf drei Sicherheitsniveaus (niedrig auch mit „Silber“ bezeichnet, substanziell gleich „Gold“, hoch gleich „Platin“), die äquivalent zu den Sicherheitsniveaus von E-ID-Systemen der EU definiert sind [2].
- Grundsätzlich können alle berechtigten Personen in der Schweiz eine staatlich anerkannte E-ID von einem staatlich anerkannten IdP ihrer Wahl kostenlos beziehen. Sie wählen die E-ID entsprechend ihren Bedürfnissen bezüglich Sicherheitsniveau und Nutzerfreundlichkeit. Sie müssen dabei den vorgeschriebenen Registrierungsprozess durchlaufen und für die staatliche Anerkennung insbesondere ihre Personenidentifizierungsdaten durch die Schweizerische Stelle für elektronische Identität (SID) an den IdP übermitteln lassen.
- Der ausstellende IdP ist für alle Belange der E-ID der direkte Ansprechpartner, sowohl für die Inhaberinnen und Inhaber als auch für die vertrauenden Beteiligten, mit denen er eine Nutzungsvereinbarung hat. Der IdP stellt geeignete Support und Exception Handling Dienste zur Verfügung. Er haftet für Fehlfunktionen entsprechend den gesetzlichen Verpflichtungen, die für das Sicherheitsniveau seines E-ID-Systems gelten. Der IdP ist auch dafür verantwortlich, dass Identitätsattribute aktuell und richtig zugeordnet sind und nur mit Einverständnis der Inhaberin oder des Inhabers an berechtigte vertrauende Beteiligte geliefert werden.
- Die Integrität der mit staatlich anerkannten E-ID verwendeten Personenidentifizierungsdaten ist wichtig. Der Bund verfügt mit dem Informationssystem Ausweisschriften (ISA) und dem Zentralen Migrationssystem (ZEMIS) und dem Zivilstandsregister (Infostar) bereits über staatlich geführte Register von Personenidentifizierungsdaten, welche sich auf eine hoheitliche Identifikation der Person abstützen. Der Staat liefert den IdP für anerkannte E-ID-Systeme Personenidentifizierungsdaten, die bei der letzten offiziellen staatlichen Identifizierung in diese Register eingetragen wurden, in kryptografisch abgesicherter Form. Der Umfang der übermittelten Attribute ist für die drei Sicherheitsniveaus unterschiedlich definiert (siehe 2.6.3). Das Datum der zugrunde liegenden Identifizierung wird in jeder Übermittlung mitgeliefert. Der Staat ist verantwortlich für Fehler in diesen Daten.
- Der Staat definiert als Teil der zivilen Identität, die er verwaltet, einen eindeutigen Personenidentifikator (EPID), der auf jedem Sicherheitsniveau der E-ID mit den Personenidentifizierungsdaten, die an den IdP übermittelt werden, mitgeliefert wird.
- Die Betreiber von E-ID-Systemen entscheiden frei, ob sie eine staatliche Anerkennung ihrer E-ID-Systeme erreichen wollen und so einen Marktvorteil gewinnen können. Es besteht kein Zwang ein E-ID-System staatlich anerkennen zu lassen. Der Staat definiert die Regelungen so, dass anerkannte E-ID-Systeme auch auf europäischer Ebene anerkannt, das heisst entsprechend dem erreichten Sicherheitsniveau notifiziert werden können.
- Staatlich anerkannte E-ID-Systeme müssen interoperabel sein. Die Interoperabilität wird einerseits durch einfache standardisierte elektronische Schnittstellen Komponenten (E-ID-Schnittstelle) bei den vertrauenden Diensten der vBt und andererseits durch die Interoperabilität der E-ID-Systeme untereinander realisiert. Die IdP von anerkannten E-ID-Systemen müssen dazu für alle anderen IdP mit anerkannten E-ID-Systemen standardisierte Schnittstellen für die interoperable Nutzung ihrer E-ID zur Verfügung stellen. Interoperable E-ID, die bei allen vertrauenden Beteiligten entsprechend dem verlangten Sicherheitsniveau eingesetzt werden können, fördern die rasche Verbreitung anerkannter E-ID-Systeme im E-ID Ökosystem.
- Vertrauende Beteiligte, die im Markt angebotene staatlich anerkannte E-ID-Systeme für

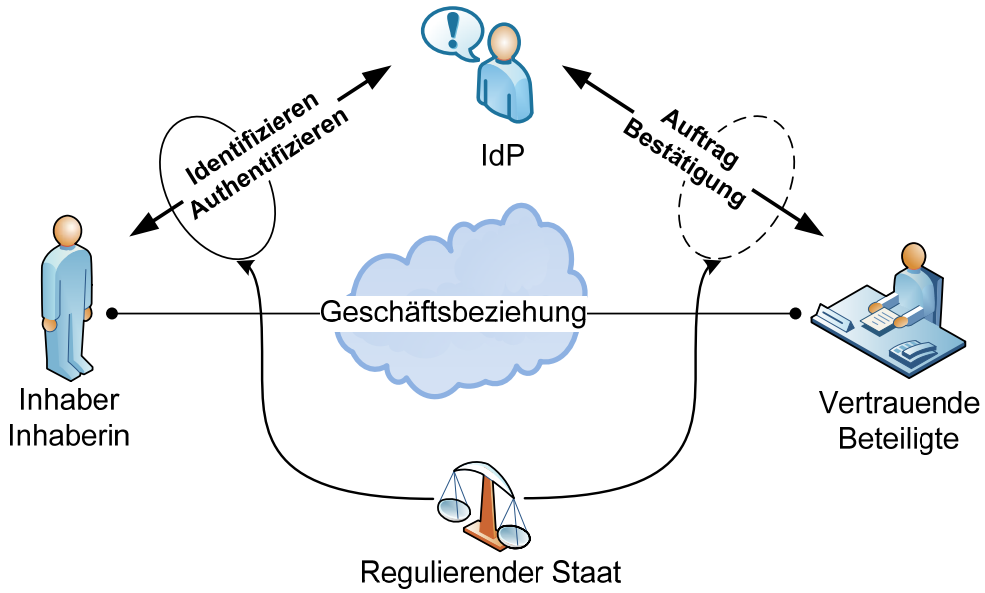
die Identifizierung und Authentifizierung ihrer Kunden entsprechend ihren Anforderungen nutzen (Vertrauen, Sicherheit, Regulierungen, Geschäftsfall, Haftung), können sich dabei auf die Einhaltung interoperabler Standards durch alle Betreiber von E-ID-Systemen verlassen. Sie haften jedoch für die konforme Nutzung der E-ID durch ihren vertrauenden Dienst bei der Identifizierung oder Authentifizierung der Inhaberinnen und Inhaber.

- Die berechtigten Personen entscheiden frei, ob sie eine staatlich anerkannte E-ID beziehen wollen. Für eine staatliche Anerkennung ihrer E-ID müssen sie jedoch dem ausstellenden IdP die explizite Erlaubnis geben, die dem Sicherheitsniveau entsprechenden Personenidentifizierungsdaten beim staatlichen Attributdienst zu beziehen. Als Inhaberin oder Inhaber können sie von Fall zu Fall entscheiden, ob und welche dieser Attribute der zivilen Identität vom IdP an vBt weiter übermittelt werden sollen.
- Inhaberinnen und Inhaber sind verpflichtet ihre E-ID sorgfältig und im Rahmen ihres Einflussbereiches sicher zu nutzen. Sie haften für Schäden, die aus unsachgemässem Gebrauch entstehen. Auch die vertrauen Beteiligten haften für Schäden, die durch fehlerhaften Einsatz der E-ID bei der Identifizierung oder Authentifizierung ihrer Kunden entstehen.

Der Bund stellt die nötige Infrastruktur für die Umsetzung der gesetzlichen Regulierung und für den Dienst zur Übermittlung von Personenidentifizierungsdaten zur Verfügung (siehe Kap 3). Er führt dazu unter der Bezeichnung **Anerkennungsstelle für Identitätsdienstleister (AID)** eine Verwaltungseinheit, die den Anerkennungsprozess für staatlich anerkannte IdP und E-ID-Systeme durchführt und die anerkannten IdP beaufsichtigt. Er führt zudem unter der Bezeichnung **Schweizerische Stelle für elektronische Identität (SID)** eine Verwaltungseinheit, die ein Informationssystem betreibt, das Personenidentifizierungsdaten bei den einschlägigen staatlichen Personenregistern des Bundes abfragen kann und diese mit dem Einverständnis der Inhaberinnen und Inhaber an staatlich anerkannte IdP übermittelt, die E-ID-Systeme betreiben.

2.4 Architektur und Prozesse

Ausgangslage ist die Aufnahme einer online Geschäftsbeziehung einer Inhaberin oder eines Inhabers mit einer vertrauenden Beteiligten. Im elektronischen Identitätsmanagement (E-IdM) kommen nebst der Rolle der Inhaberin oder des Inhabers und der Rolle der vertrauenden Beteiligten, die Inhaberinnen oder Inhaber identifizieren und authentifizieren will, zwei weitere Rollen dazu und zwar diejenige des Identitätsdienstleisters (IdP), der das E-ID-System betreibt, und diejenige des regulierenden Staates. Letzterer definiert die Zusammenarbeitsregeln zwischen den Beteiligten und die Anforderungen an staatlich anerkannte E-ID-Systeme, so dass ein gesicherter Vertrauensrahmen entsteht und er ist per se auch der Verwalter der zivilen Identität aller Personen im E-ID-Ökosystem. Im E-ID-Ökosystem delegieren die vertrauenden Beteiligten (vBt) die Prozesse der elektronischen Identifizierung und Authentifizierung von Inhaberinnen oder Inhabern einer E-ID an die IdP. Jede vBt betreibt dazu eine Informatikanwendung als vertrauender Dienst, der via einen E-ID-Schnittstelle mit einem E-ID-System eines IdP verbunden ist. Nach der Erledigung eines Auftrages für eine Identitätsdienstleistung liefert das E-ID-System dem vertrauenden Dienst, der den Auftrag erteilt hat, das Resultat der Identifizierung oder Authentifizierung zurück.



Skizze 4: Die Rollen im elektronischen Identitätsmanagement

2.4.1 Systeme des E-IdM

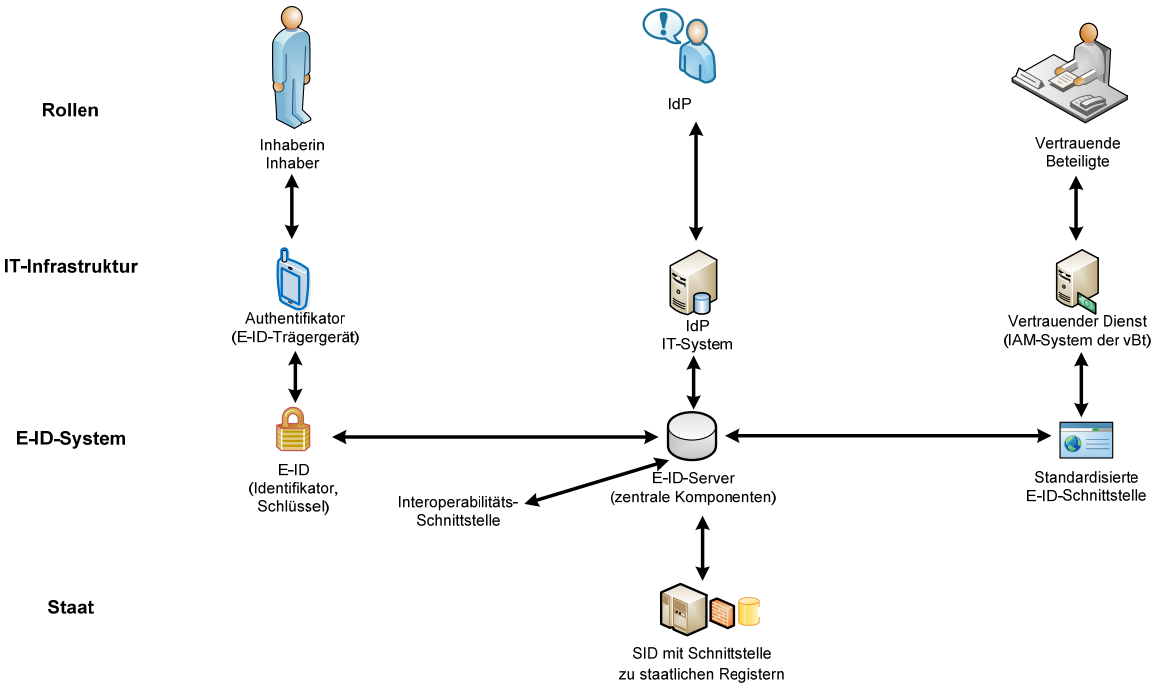
Die zu den Rollen gehörenden digitalen Systeme des E-IdM sind:

- Der Authentifikator meist in Form eines persönlichen Geräts[16] der Inhaberin oder des Inhabers mit der sicher und vertrauenswürdig integrierten E-ID-Anwendung. Die Anwendung hat einen Identifikator, eine Authentifizierungsfunktion mit den Referenzdaten für die Erkennung der Inhaberin oder des Inhabers, ein fest mit dem Identifikator verbundenes Geheimnis und eine abgesicherte Kommunikationsschnittstelle zum zentralen System des IdP. Optional kann beim Einsatz der E-ID auch die Anzeige des Trägergeräts abgesichert unter der Kontrolle der installierten E-ID Anwendung sein.
- Das Verwaltungs- und Dienstleistungssystem der vertrauenden Beteiligten für die online Geschäftsabwicklung als vertrauender Dienst mit einer integrierten und standardisierten Schnittstelle zum E-ID-System. Diese E-ID-Schnittstelle sind standardisierte Prozesse und Protokolle, die bei der Registrierung oder der Anmeldung einer Inhaberin oder eines Inhabers beim vertrauenden Dienst zum Einsatz kommen und den Auftrag für die Identitätsdienstleistung generieren. Sie erhält von der Inhaberin oder dem Inhaber und vom vertrauenden Dienst die notwendigen Angaben zum Auftrag und leitet diesen an das E-ID-System des IdP weiter. Zurück erhält sie das Antwortticket mit dem Resultat des durchgeführten Auftrages und leitet das Resultat an den vertrauenden Dienst weiter.
- Die E-ID-System Komponenten des IdP verwalten alle erfassten Identitätsattribute[17] der Inhaberinnen und Inhaber, erhalten die Aufträge der vertrauenden Dienste über die E-ID-Schnittstellen, führen mittels den E-ID im Feld die sicheren Identifizierungen und Authentifizierungen der Inhaberinnen und Inhaber durch und erstellen die Antworttickets für die vertrauenden Dienste. Jeder IdP hat eine abgesicherte Schnittstelle zum staatlichen Attributdienst und einen Service für die Realisierung der Interoperabilität mit anderen anerkannten

[16] Der Authentifikator ist ein weit zu fassender Begriff (engl. Authenticator oder ehemals Token), der sich nicht nur auf elektronische Geräte als Träger beziehen kann. Wichtig ist, dass er unter der persönlichen Kontrolle des Inhabers einen Nachweis für dessen Identität liefern kann.

[17] Die Gesamtheit der Identitätsattribute einer Inhaberinnen oder eines Inhabers, die der IdP aus unterschiedlichen Quellen erhalten kann, wird als partielle Identität bezeichnet (siehe dazu die Erläuterungen im Anhang).

IdP. Er führt zudem eine online abrufbare Liste der vorübergehend gesperrten und permanent inaktivierten E-ID.

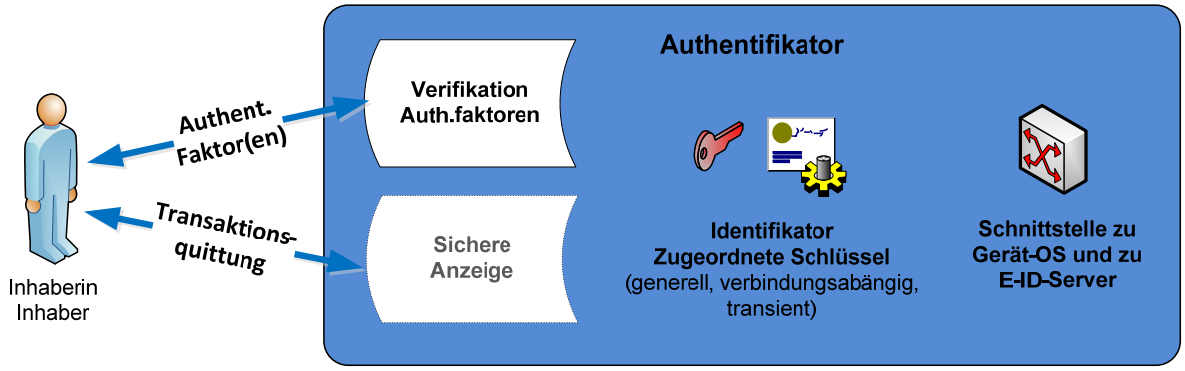


Skizze 5: Systemebenen und zugeordnete E-IdM Komponenten

2.4.2 Authentifikator und E-ID

Zentrales Element eines E-ID-Systems ist der Authentifikator, der die Verbindung zwischen der physischen Person und ihrer im E-ID-System erfassten Identität gewährleistet. Der Authentifikator kann in unterschiedlicher Form realisiert sein. Dies kann zum Beispiel ein in eine Plastikkarte integriertes Sicherheitselement (Chip), eine Applikation in einer SIM-Karte, ein USB-Key oder spezielles Gerät sein, aber auch Software Varianten wie Zertifikate verbunden mit einem Freischaltmechanismus oder andere Formen sind denkbar. Grundsätzlich kann auch die Kombination von UserID und Passwort als abstrahierte Form eines Authentifikators angesehen werden. Wichtig ist, dass der Authentifikator in einem Registrierungsprozess eindeutig mit einer Person verbunden wird, dass er durch einen integrierten Identifikator repräsentiert wird und dass er in sicherer Weise mit dem E-ID-Server in Verbindung treten kann. Der Identifikator kann dabei pro Sektor, vBt oder Zeitraum unterschiedlich definiert sein, muss jedoch im Kontext des E-ID-Systems immer eindeutig einem Authentifikator zugewiesen werden können.

Bei der Registrierung wird der Authentifikator an einerseits eine Person und andererseits (serverseitig) an ihre Identitätsdaten gebunden und wird damit zu einer E-ID. Erst mit der so bereitgestellten E-ID kann sich die registrierte Person digital authentifizieren und identifizieren.



Skizze 6: Eine E-ID ist ein auf eine Person registrierter Authentifikator mit der Person zugeordneten Identitätsdaten.

2.5 Lebenszyklen im E-ID-System

Jedes E-ID-System wird einerseits als System einen Lebenszyklus durchlaufen und andererseits den Lebenszyklus der einzelnen E-ID und denjenigen der E-ID-Schnittstelle bei den vertrauenden Beteiligten verwalten. Dazu müssen für jeden der drei Lebenszyklen organisatorische Abläufe und IT-Prozesse implementiert werden. Zur Illustration sind diese Zyklen und Prozesse eines Mustersystems beschrieben. In der Praxis wird es sicher eine recht breite Variabilität dieser Lebenszyklen und Prozesse geben, die nur durch zwingende gesetzliche Anforderungen eingeschränkt ist.

Die Beschreibung des Mustersystems geht davon aus, dass die E-ID eine Smartphone Applikation (Authentifikator) ist, die in einem abgesicherten Bereich eines Smartphones (TEE oder SIM-App) installiert werden kann.

2.5.1 Aufbau und Betrieb eines E-ID-Systems

Ein IdP, der ein staatlich anerkanntes E-ID-System betreiben will, muss die Voraussetzungen für die staatliche Anerkennung erfüllen. Dazu muss er

- Einen Geschäftssitz in der Schweiz haben oder eröffnen und für den Betrieb des E-ID-Systems qualifizierte Personen beschäftigen, die einen unbescholtenen Leumund haben;
- Nachweisen, dass ausreichend finanzielle Mittel für die Deckung allfälliger Schäden vorhanden sind, die sich aus einer Verletzung seiner Verantwortung ergeben könnten;
- Eine nach einschlägigen Schutzprofilen zertifizierte IT-Infrastruktur für das E-ID-System mit Datenspeicherung ausschliesslich in der Schweiz aufbauen. Insbesondere gehören dazu
    - Zertifiziert sichere, organisatorische und technische Prozesse für die Registrierung von zukünftigen Inhaberinnen und Inhaber der E-ID und für die Abarbeitung von Authentifizierungs- und Identifizierungsaufträgen.
    - Die zertifiziert sichere E-ID Anwendung als Authentifikator für die Erkennung der Inhaberin oder des Inhabers. Je nach angestrebtem Sicherheitsniveau des E-ID-Systems muss die integrierte Authentifizierungsfunktion eine Person mit zwei unabhängigen Authentifizierungsfaktoren (Niveau: Gold) oder mit zwei Faktoren, wovon einer biometrisch sein muss (Niveau: Platin) erkennen können. Die Anwendung wird für die abgesicherten Bereiche[18] der verschiedenen Betriebssysteme der Smartphones erstellt, auf denen die E-ID installiert werden kann;

[18] Abgesicherte Bereiche in modernen Smartphones sind zum Beispiel durch sogenannte Trusted Execution Environment (TEE) oder einsetzbare Secure Elements (SE) realisiert [58] [47]

- Ein sicheres Verteilungssystem für die E-ID Anwendungen mit der Definition von E-ID Identifikatoren in einem standardisierten Format, die nach der Installation fest mit dem Träger-Smartphone verbunden sind. Die E-ID Identifikatoren müssen einen Kennungsteil haben, so dass sie von allen E-ID-Systemen dem ausstellenden IdP zugeordnet werden können[19];
- Die standardisierte E-ID-Schnittstelle zu den vertrauenden Diensten in den IAM-Systemen der vertrauenden Beteiligten, so dass bei allen vertrauenden Beteiligten immer die gleichen Nutzungsprotokolle beim Einsatz einer E-ID ablaufen;
- Die standardisierte Interoperabilitätsschnittstelle zu allen bestehenden staatlich anerkannten E-ID-Systemen, die auf dem gleichen oder höheren Sicherheitsniveau anerkannt sind;
- Die sichere standardisierte Schnittstelle mit geschütztem Kommunikationskanal zum SID für die Übermittlung und periodische Aktualisierung der Personenidentifizierungsdaten;
- Der Webservice für die Bereitstellung von abrufbaren Sperr- und Revokationslisten der E-ID im Feld;

- Ein online Unterstützungs- und Hilfeangebot bereitstellen, das zu jeder Aktion, die mit der E-ID ausgeführt werden kann, situationsabhängige Erklärungen und Hilfestellungen bietet.
- Einen Kundendienst als Meldestelle für Störungen, Missbrauch oder Verlust einer E-ID bereitstellen.

Mit diesen Voraussetzungen beantragt der IdP die staatliche Anerkennung bei der AID und liefert die Nachweise, hauptsächlich in Form von Zertifizierungen nach Schutzprofilen und Auditberichten, für die Erfüllung dieser Anerkennungsvoraussetzungen. Nach Prüfung der Nachweise anerkennt die AID den IdP und das oder die angemeldeten E-ID-Systeme auf dem erreichten Sicherheitsniveau. Die AID publiziert die anerkannten IdP und E-ID-Systeme sowie die zugeteilten Kennungen für die identifizierenden Teile der E-ID Identifikatoren.

Der staatlich anerkannte IdP muss für den Nachweis der permanenten Erfüllung der Anerkennungsvoraussetzungen seine E-ID-Systeme mindestens jedes dritte Jahr auditieren lassen und die Auditberichte der AID zustellen. Der AID verlängert die Anerkennung, wenn der Auditbericht die Erfüllung der Voraussetzungen bestätigt und wenn der IdP die fälligen Gebühren für die Übermittlung von Personenidentifizierungsdaten bezahlt hat.

Die staatliche Anerkennung kann entzogen werden, wenn der IdP gegen die gesetzlichen Bestimmungen verstösst, die Anerkennungsvoraussetzungen nicht mehr erfüllt oder die Geschäftstätigkeit aufgibt oder mit Konkurs aufgeben muss. In einem solchen Fall kann das E-ID-System von einem anderen staatlich anerkannten IdP übernommen werden.

Ein IdP kann seine staatlich anerkannten E-ID-Systeme den vertrauenden Beteiligten und den zum Bezug einer E-ID berechtigten Personen anbieten. Die Ausstellung einer E-ID sollte für die Person kostenlos sein. Der IdP kann jedoch ein beliebiges Geschäftsmodell für die Durchführung von Identifizierungen und Authentifizierungen anwenden. Der Bund wird jedoch Einschränkungen für Zusatzgebühren definieren, die bei der Nutzung von Interoperabilitätsdiensten berechnet werden dürfen. Alle Bundesstellen, die für ihre Online Dienste eine Identifizierung oder Authentifizierung verlangen, müssen die E-ID eines auf einem hinreichenden Sicherheitsniveau anerkannten

[19] In gleicher Weise wie der Herausgeber von Kreditkarten durch einen Teil der Kreditkartennummer identifiziert wird, soll der E-ID Identifikator einen Identifierteil enthalten, der den ausstellenden IdP und das E-ID-System identifizieren. Dieser Identifier hilft bei der Realisierung der Interoperabilität zwischen den E-ID-Systemen.

E-ID-Systems als Identifizierungsmittel akzeptieren. Jede betroffene Bundesstelle muss mit mindestens einem IdP eine entsprechende Vereinbarung treffen[20], so dass alle, vom Sicherheitsniveau her geeigneten, staatlich anerkannten E-ID eingesetzt werden können.

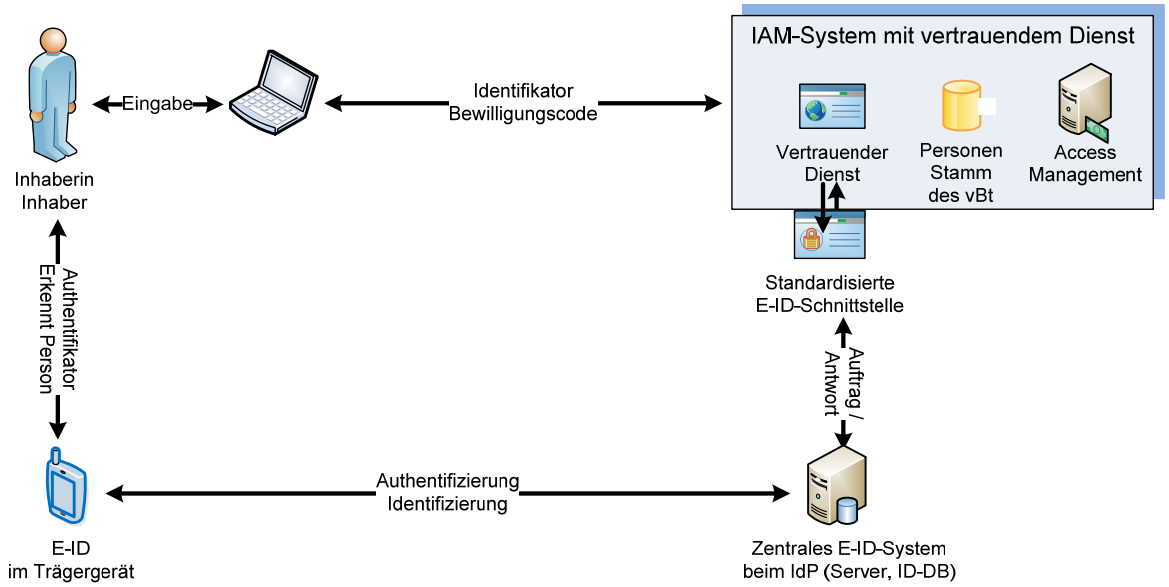
Sobald die Schweiz mit der EU einen entsprechenden Staatsvertrag abschliesst, kann ein IdP ein von ihm betriebenes staatlich anerkanntes E-ID-System, das im Markt mit einem hinreichenden Marktanteil etabliert ist, durch den Bund bei der EU notifizieren lassen. Die genauen Voraussetzungen dafür können erst mit dem Abschluss des Staatsabkommens definiert werden.

2.5.2 Lebenszyklus der Nutzung eines E-ID-Systems

Falls eine vertrauende Beteiligte für ihr IAM-System staatlich anerkannte E-ID für die Identifizierung und Authentifizierung der Mitglieder in ihrem Personenstamm nutzen will, muss sie mit mindestens einem IdP eine Nutzungsvereinbarung für ein E-ID-System auf dem verlangten Sicherheitsniveau eingehen. Sie ist dabei in ihrer Wahl des anbietenden IdP frei und entscheidet auf Grund von geschäftlichen Überlegungen. Die technischen und organisatorischen Schnittstellen hingegen sind für alle angebotenen E-ID-Systeme weitgehend standardisiert. Damit sie E-ID nutzen kann, muss sie eine E-ID-Schnittstelle in ihren vertrauenden Dienst integrieren, die folgende Funktionen bereitstellt

- Standardisiertes Registrierungs- und Anmeldeportal für E-ID Inhaber und Inhaberinnen für die Erfassung des E-ID Identifikators oder eines vom IdP dem Identifikator zugeordneten Pseudonyms. Bei der Neuaufnahme einer Inhaberin oder eines Inhabers in den Personenstamm der vBt (Registrierung) zeigt das Portal der Inhaberin oder dem Inhaber zusätzlich an, welche Identitätsattribute beim IdP zur Übermittlung angefordert werden.
- Standardisierte Schnittstelle zum vertrauenden Dienst, über die Registrierungs- oder Anmeldeaufträge des vertrauenden Dienstes entgegengenommen und die von den zentralen E-ID System Komponenten erstellten Antworttickets ausgeliefert werden. Jeder Auftrag und jede Antwort ist in einem standardisierten Format definiert und enthält immer den zugehörigen E-ID Identifikator bzw. den zum Auftrag gehörenden abgeleiteten Identifikator. Typischerweise ist die E-ID-Schnittstelle ein Webservice mit den nötigen Sicherheitselementen für die Auftragsübermittlung und den Empfang der Antworten.
- Empfang von Personenidentifizierungsdaten, die vom E-ID-System auf Antrag des Vertrauenden Dienstes und mit Einwilligung der Inhaberin oder des Inhabers in standardisierter und abgesicherter Form geliefert werden. Die Einwilligung erteilt die Inhaberin oder Inhaber mit einem One-Time-Code, der sie oder er vom IdP erhält und über das Registrierungsportal des vertrauenden Dienstes via E-ID-Schnittstelle an den IdP zurückschickt.

[20] Dazu wird es eine öffentliche Ausschreibung geben, für die sich alle IdP mit einem E-ID-System auf geeignetem Sicherheitsniveau bewerben können.



Skizze 7: Schnittstellen des E-ID-Systems

Der vertrauende Dienst wird von der vBt bei Bedarf an die Entwicklung des eigenen IAM Systems aber auch für die Akzeptanz von neueren Generationen von E-ID angepasst. Der vertrauende Dienst ist verpflichtet, alle E-ID die das verlangte Sicherheitsniveau einhalten, unabhängig vom herausgebenden IdP zu akzeptieren. Die E-ID-Schnittstelle ist so standardisiert, dass sie alle Formen von E-ID Identifikatoren, Tickets und Rückmeldungscodes verarbeiten kann.

Eine vBt kann die direkten Kosten des Einsatzes von E-ID bei ihrem vertrauenden Dienst den Inhaberinnen oder Inhabern verrechnen.

2.5.3 Lebenszyklus der E-ID

Für die Inbetriebnahme und Nutzung einer E-ID, die je nach E-ID System für eines der drei Sicherheitsniveaus konzipiert ist, werden folgende Schritte realisiert:

- **Ausstellung eines E-ID-Authentifikators.** Die Ausstellung des Authentifikators erfolgt integriert in einem Trägergerät bzw. als Anwendung für ein geeignetes Endgerät der zukünftigen Inhaberin oder des Inhabers oder sogar nur in Form einer Prozessinstruktion, die der Inhaber oder die Inhaberin wissen muss, wenn sie eine allgemein verfügbare Infrastruktur als Authentifikator verwenden kann. Der E-ID-Authentifikator hat gesicherte Schnittstellen zur Eingabe der Authentifizierungsfaktoren, zur Kommunikation mit den zentralen Komponenten des E-ID-Systems (E-ID-Server) beim IdP und zur Anzeige von One-Time-Codes. Wenn möglich kann der Authentifikator sogar eine komfortable Anzeige- und Eingabemöglichkeit gesichert ansteuern und damit gewisse Transaktionsabsicherungen ermöglichen. Der E-ID-Authentifikator generiert nach der sicheren Installation im Gerät einen eindeutigen Identifikator und Sicherheitselemente für die Kommunikation mit dem E-ID-Server des IdP. Alternativ kann der E-ID-Authentifikator in einem dedizierten sicheren Trägergerät mit vorinstalliertem Identifikator und Sicherheitselementen ausgeliefert werden. Der E-ID-Authentifikator ist bereit für die Registrierung der Inhaberin oder des Inhabers, wenn die sichere Kommunikation mit dem E-ID-Server etabliert und der Identifikator im zentralen E-ID-Server registriert ist.

- **Registrierung der Inhaberin oder des Inhabers beim IdP.** Die Registrierung der Inhaberin oder des Inhabers beinhaltet die Herstellung einer festen Bindung der Person an den E-ID-Authentifikator mittels der Authentifizierungsfunktion und die initiale Identifizierung der Person durch Erfassung ihrer Personenidentifizierungsdaten.
    - Die Bindung erfolgt durch die Erfassung von persönlichen Attributen als Referenzdaten für die Authentifizierungsfaktoren, d.h.
        - Festlegung eines Geheimnisses zum Beispiel durch Erfassung eines PIN-Codes durch die Inhaberin oder den Inhaber,
        - Erfassung von biometrischen Merkmalen der Inhaberin oder des Inhabers im E-ID-Authentifikator, wobei auch die permanente Messung von mehreren typischen Verhaltensweisen durch die Sensorik des Trägergeräts wie zum Beispiel die Messung der Bewegungsdynamik bei der Eingabe auf einem Touchscreen, als biometrische Merkmale zählen,
        - Inbesitznahme des E-ID-Authentifikators als persönliches Trägergerät. Zum Beispiel eine personalisierte Smartcard aber auch ein persönliches Smartphone mit registrierter SIM-Karte ist ein solch persönliches Trägergerät, das immer im Besitz der Inhaberin oder des Inhabers bleibt.
    - Die initiale Identifizierung erfolgt durch die Erfassung von Personenidentifizierungsdaten, die mit definierter Sicherheit der Person zugeordnet sind, die eine Bindung mit dem E-ID-Authentifikator hergestellt hat. Dies kann anlässlich einer persönlichen Vorsprache bei einer zur Identifizierung autorisierten Stelle des IdP oder auch im Rahmen einer Videoidentifizierung geschehen. Zwingend ist dabei, dass die Person aufzeigt, dass der E-ID-Authentifikator sie mit den festgelegten Authentifizierungsfaktoren erkennt, und gleichzeitig mit einem staatlichen Ausweis ihre zivile Identität nachweist. In diesem Schritt wird die richtige Zuordnung von persönlichen Authentifizierungsfaktoren, eingekapselt im E-ID-Authentifikator , zu den Attributen der zivilen Identität überprüft. Der zentrale E-ID-Server registriert die Personenidentifizierungsdaten zusammen mit dem E-ID-Identifikator, der für die persönlichen Attribute steht, die durch den Authentifikator geprüft werden. Im Normalfall werden im zentralen E-ID-Server keine weiteren persönlichen[21] Attribute erfasst.
- **Der Abruf von staatlichen Personenidentifizierungsdaten.** Im Fall der staatlich anerkannten E-ID wird die Zuordnung der zivilen Identität zur E-ID, die im Prinzip auch für nicht staatlich anerkannte E-ID gemacht werden muss, noch zusätzlich verstärkt. Im Rahmen der initialen Identifizierung der Person erfasst der IdP die Nummer des vorgezeigten Ausweises und Angaben für die Aufnahme einer Verbindung mit der Inhaberin oder dem Inhaber über einen unabhängigen Kommunikationskanal. Dies ist bevorzugt eine Telefonnummer, kann aber auch eine E-Mail-Adresse oder sogar eine Postadresse sein. Der IdP übermittelt die beiden Angaben an den SID und verlangt die Zustellung der staatlichen Personenidentifizierungsdaten, die zu der Ausweisnummer gehören und dem Sicherheitsniveau der E-ID entsprechen. Der SID erbittet dann via den unabhängigen Kommunikationskanal von der Inhaberin oder dem Inhaber die Erlaubnis, die verlangten Daten an den IdP zu übermitteln. Er sendet ihm dazu einen One-Time-Code für die Erlaubnisbestätigung zu, den die Inhaberin oder der Inhaber dem IdP mitteilen kann. Der IdP sendet die Erlaubnisbestätigung an den SID weiter und erhält von diesem die staatlichen Personenidentifizierungsdaten der Inhaberin oder des Inhabers inklusive dem staatlich zugeordneten eindeutigen Personenidentifikator (EPID). Der IdP aktiviert darauf die E-ID. Verweigert die Inhaberin oder der Inhaber die Erlaubnis, kann die E-ID, je nach Geschäftspolitik des IdP, trotzdem aktiviert

[21] Persönliche Attribute sind, im Unterschied zu den Personenidentifizierungsdaten, nicht öffentlich bekannte Attribute der Person, wie zum Beispiel biometrische Daten (siehe dazu die Erläuterungen im Anhang).

werden. Sie ist dann aber keine staatlich anerkannte E-ID, was bei jeder späteren Identifizierung oder Authentifizierung dem auftragenden vertrauenden Dienst mitgeteilt werden muss. Wird im Rahmen der Einführung von staatlich anerkannten E-ID ein bestehendes E-ID-System neu staatlich anerkannt, können die bereits aktivierten E-ID des Systems als staatlich anerkannte E-ID betrieben werden, falls für die staatliche Anerkennung nur der Abruf der Personenidentifizierungsdaten ausstehend ist. Der Abrufprozess muss dann innerhalb einer bestimmten Frist nachgeholt werden.

- **Die Registrierung der Inhaberin oder des Inhabers bei einer vBt**. Mit einer aktivierten staatlich anerkannten E-ID kann sich eine Inhaberin oder ein Inhaber bei allen vertrauenden Diensten von vBt, die staatlich anerkannte E-ID akzeptieren, online registrieren, vorausgesetzt das Sicherheitsniveau der E-ID ist ausreichend für den vertrauenden Dienst. Sie oder er beantragt auf dem Portal des vertrauenden Dienstes der vBt eine Neuregistrierung für den Personenstamm der vBt. Der vertrauende Dienst der vBt zeigt die Registrierungsseite mit den Angaben zu den verlangten Anmeldeinformationen an. Die Inhaberin oder der Inhaber gibt in diesem Anmeldeformular[22] den Identifikator der E-ID ein[23] und erbittet eine Registrierung. Sie oder er startet den E-ID-Authentifikator zu diesem Zeitpunkt, falls dieser nicht sowieso permanent aktiv ist. Allenfalls kann dann gleichzeitig mit dem Identifikator, je nach E-ID, bereits ein Authentifizierungsnachweis mitgeliefert werden. Der vertrauende Dienst erteilt einen **Registrierungsauftrag** für die mit dem Identifikator bezeichnete E-ID und sendet diesen via E-ID-Schnittstelle an seinen IdP. Dieser prüft, ob er diese E-ID verwaltet oder ob er den Auftrag via Interoperabilitätsschnittstelle an einen anderen zuständigen IdP weiterleiten muss. Der zuständige IdP authentifiziert die Inhaberin oder den Inhaber mit der E-ID. Hat sich die Inhaberin oder der Inhaber authentifiziert, wird der Inhaberin oder dem Inhaber eine Nachricht zugestellt mit der Bitte um Erlaubnis für die Übermittlung der vom vertrauenden Dienst verlangten Daten[24]. Die Nachricht enthält zum Beispiel einen One-Time-Code als Erlaubnisbestätigung. Je nach Kommunikationssituation erteilt die Inhaberin oder der Inhaber die Erlaubnis direkt über ihre E-ID oder durch Eingabe des One-Time-Codes im Anmeldeformular des vertrauenden Dienstes, der diesen als Ergänzung zum Registrierungsauftrag an den IdP weiterleitet. Falls die Erlaubnis erteilt wird, übermittelt der IdP ein Antwortticket an die E-ID-Schnittstelle beim vertrauenden Dienst mit der Identifizierungsbestätigung und den für den vBt freigegeben Daten. Falls die Freigabe nicht erfolgt, sendet der IdP nach einem Timeout lediglich ein Antwortticket mit der Authentifizierungsbestätigung. Der vBt muss dann entscheiden, ob er das neue Mitglied nur unter dem eingegeben Identifikator[25] in seinem Personenstamm registrieren will oder nicht. Er könnte dann jeweils nur feststellen, dass es sich bei einer späteren Anmeldung mit dieser E-ID immer um die gleiche Inhaberin oder den gleichen Inhaber handelt, hätte aber keine Daten der zivilen Identität der Person.
- **Wiederanmeldung bei einer vBt (Login).** Die Inhaberin oder der Inhaber meldet sich beim vertrauenden Dienst im Anmeldeportal mit dem E-ID Identifikator oder einem zugehörigen Pseudonym an und gibt, falls dies verlangt wird, weitere identifizierende Daten ein. Sie oder er startet dazu den E-ID-Authentifikator, falls die E-ID nicht sowieso permanent aktiv ist. Der vertrauende Dienst erstellt zuhanden seines IdP einen **Anmeldeauftrag**. Dieser prüft, ob er diese E-ID verwaltet oder ob er den Auftrag via Interoperabilitätsschnittstelle an den

[22] Die Anmeldeformulare der vBt werden gewisse Standardisierungsanforderungen erfüllen müssen, so dass das Grundschema in allen Portalen gleich ist.

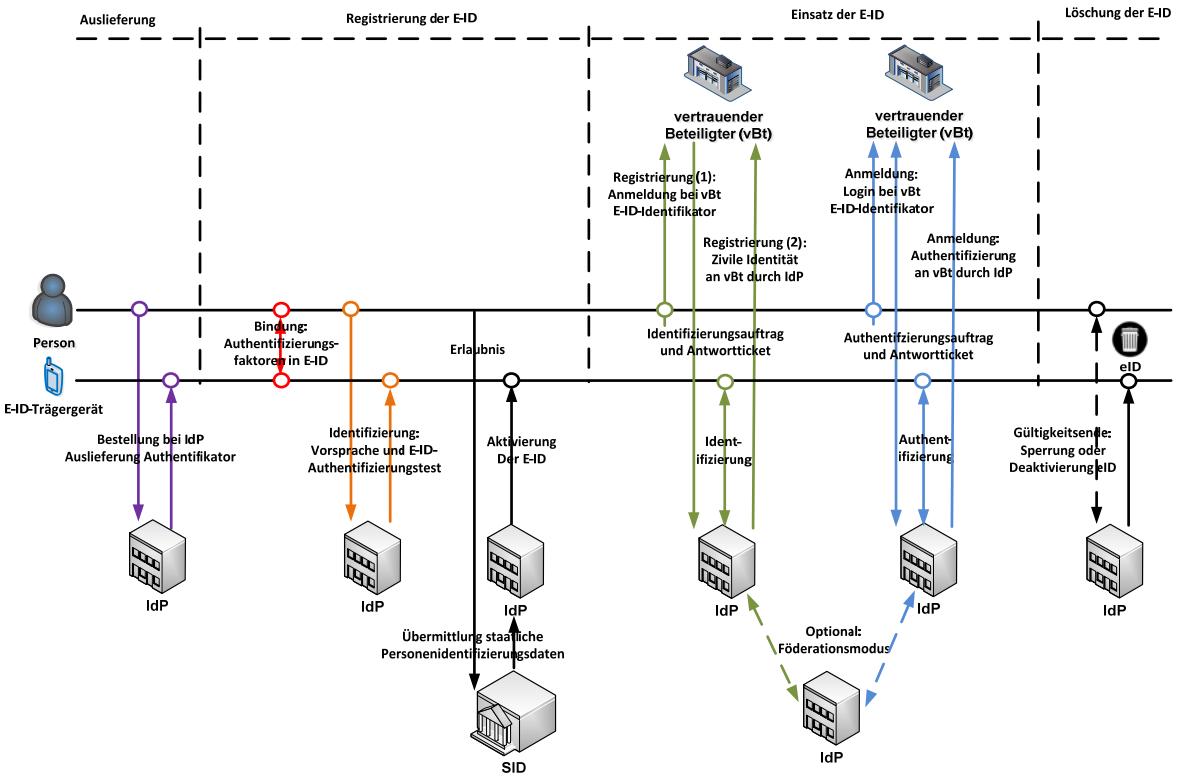
[23] Je nach Portal des vertrauenden Dienstes erfolgt die Eingabe über ein Keyboard oder auf elektronischem Weg, wenn die E-ID und das Portalgerät zum Beispiel eine NFC-Schnittstelle haben.

[24] Die vBt kann für die Verwaltung ihres Personenstamms, Attribute der staatlichen Personenidentifizierungsdaten aber auch weitere vom IdP verwaltete Attribute anfordern.

[25] Der Identifikator kann dabei in abgeleiteter Form sektoriell oder auch transient offengelegt werden. Er würde dann nur für die vBt und evtl. nur während einem bestimmten Zeitraum identifizierend sein.

zuständigen IdP weiterleiten muss. Der zuständige IdP authentifiziert die Inhaberin oder den Inhaber mit der E-ID. Bei erfolgreicher Authentifizierung, sendet der IdP ein Antwortticket an die E-ID-Schnittstelle beim vertrauenden Dienst mit der Authentifizierungsbestätigung.

- **Interoperabilität der E-ID.** Die interoperable Zustellung der Aufträge von vBt an IdP und der Antworttickets von IdP an vBt im E-ID-Ökosystem erfolgt in einem festen Format und geschützt via abgesicherte Webservices. Die Nachrichten enthalten den eindeutigen Identifier des zuständigen IdP. Bekommt ein IdP eine solche Nachricht, prüft er, ob er der richtige Adressat ist und sendet die Nachricht gegebenenfalls an den richtigen Empfänger IdP zur Bearbeitung. Es genügt daher, wenn die Interoperabilitätsinfrastruktur alle anerkannten IdP verbindet. Bei hinreichender Standardisierung erübrigen sich zusätzliche Schnittstellendienste. Ohne Einführung von gewissen Standards könnte die Interoperabilität durch einen zentralisierten Hub auch noch realisiert werden, was aber zusätzliche und im Prinzip vermeidbare Kosten erzeugt, die, zumindest mittelfristig, von den IdP getragen werden müssten.
- **Löschung einer E-ID durch die Inhaberin oder den Inhaber.** Die Inhaberin oder der Inhaber können beim IdP die Löschung ihrer E-ID beantragen. Dazu melden sie sich auf dem Online-Kundenservice des IdP an und verlangen die Löschung der E-ID. Der IdP verlangt eine Authentifizierung mit der E-ID und sendet nach erfolgter Authentifizierung einen One-Time-Code auf die Anzeige der E-ID. Mit diesem Code kann die Inhaberin oder der Inhaber die Löschung bestätigen. Der IdP stellt darauf die E-ID auf inaktiv und löscht den Dateneintrag zur Inhaberin oder Inhaber in seinem Personenstamm. Eine Löschung der E-ID kann auch bei festgestelltem Missbrauch oder Verlust beantragt werden. In diesem Fall muss sich der Inhaber oder die Inhaberin über einen anderen Weg als berechtigte Person authentifizieren.
- **Sperrung**. Eine vorübergehende oder permanente Sperrung der E-ID durch den Authentifikator oder durch den IdP kann durch drei unterschiedliche Ereignisse ausgelöst werden:
    - Die Inhaberin oder der Inhaber versucht mehrmals vergeblich sich gegenüber der Authentifizierungsfunktion der E-ID zu authentifizieren. Wird dabei die maximale Zahl der erlaubten Versuche überschritten, sperrt sich die E-ID lokal auf dem Trägergerät. Je nach Typ der E-ID und der Sicherheitspolitik des IdP kann eine solche Sperrung zurückgesetzt werden oder ist permanent.
    - Falls dem IdP über einen beliebigen Weg glaubhaft zugetragen wird, dass eine bestimmte E-ID korrumpiert oder in falschen Händen sei, wird er diese sperren und den E-ID-Identifikator auf eine Sperrliste setzen. Er benachrichtigt die Inhaberin oder den Inhaber über die Sperrung.
    - Der IdP stellt bei der periodischen Überprüfung der Gültigkeit der EPID fest, dass ein bestimmter EPID vom SID vorübergehend oder permanent als ungültig gekennzeichnet ist. Falls er für eine Person mit diesem EPID eine E-ID ausgestellt hat, muss er diese sperren oder Widerrufen und den entsprechenden E-ID-Identifikator auf die Sperrliste setzen.
- **Reaktivierung**. Der IdP kann eine Sperre aufheben und die E-ID reaktivieren, wenn die Inhaberin oder der Inhaber nachweisen kann, dass die E-ID normal funktioniert und in ihrem oder seinem Besitz ist. Für die lokale Entsperrung muss die E-ID gestartet sein.



Skizze 8: Lebenszyklusprozesse der E-ID mit Ausstellung (Auslieferung, Registrierung), Einsatz und Löschung

Sicherheitsniveau der E-ID	**Silber**	**Gold**	**Platin**
Schritt 1: E-ID- Authentifikator bestellen, erhalten und installieren	Zustellung des E-ID-Authentifikators per Post als physische Einheit oder online als Anwendung automatische Installation auf Trägergerät Funktionstest mit E-ID Identifikator an IdP		
Schritt 2: Registrierung bei IdP (1) Bindung Person an E-ID	Erfassung eines Authentifizierungsfaktors (evtl. nur Besitz)	Erfassung 2 Authentifizierungsfaktoren	Erfassung 2 Authentifizierungsfaktoren mit Biometrie
Schritt 3: Registrierung bei IdP (2) Prüfung der Identität der Person mit Validierung der Ausweisgültigkeit, Personenidentität und Bindung der Person an E-ID	Nummer Identitäts-ausweis	Persönliche Vorsprache oder Videoidentifizierung gestützt auf Identitätsausweis	
	-		Überprüfung Gesichtsbild
Schritt 4: Registrierung bei IdP (3) Personenidentifizierungsdaten übermitteln von SID an IdP	Erlaubnisanfrage über unabhängigen Kanal Erlaubniscode an IdP durch Inhaberin oder Inhaber Auslieferung der Personenidentifizierungsdaten an IdP		
Schritt 5 E-ID Aktivieren	IdP aktiviert E-ID für Nutzungseinsatz Mitteilung an Inhaberin oder Inhaber		

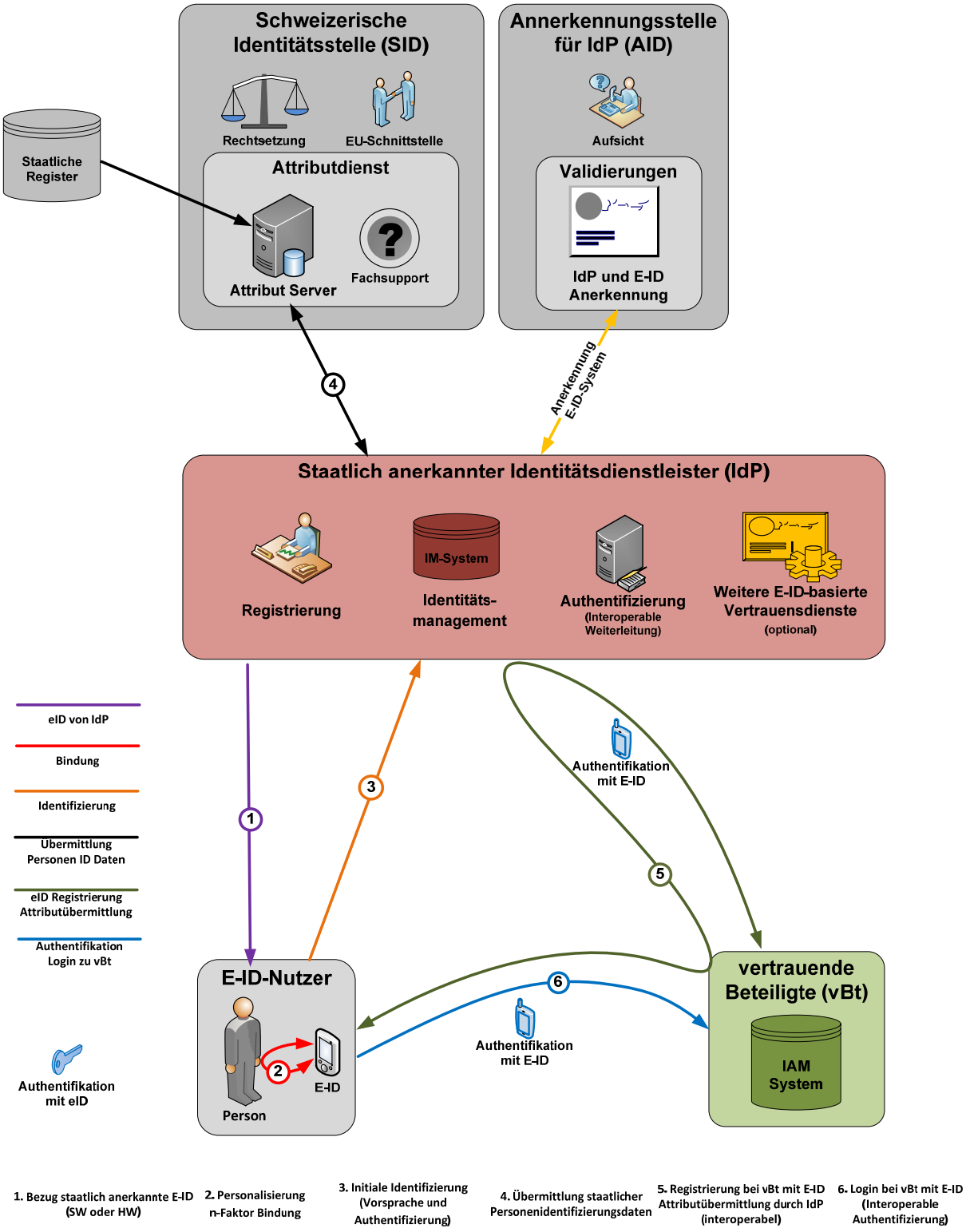
Tabelle 1: Ausstellung einer E-ID beim IdP

Sicherheitsniveau der E-ID	Silber	Gold	Platin
Erstanmeldung bei vBt mit Registrierung			
Schritt 1: Registrieren bei vBt	Anmeldung mit E-ID Identifikator oder Pseudonym beim vertrauenden Dienst der vBt (E-ID-Schnittstelle) Starten des E-ID-Authentifikators		
Identifizierungsauftrag vBt an IdP	E-ID Identifikator, Sicherheitsniveau und Attributsanfrage via E-ID-Schnittstelle		
Schritt 2: Authentifizierung durch IdP gemäss Sicherheitsniveau	Erfassung eines Authentifi-zierungsfaktors	Erfassung 2 Authentifizie-rungsfaktoren	Erfassung 2 Authentifizie-rungsfaktoren mit Biometrie
Schritt 3: Attribute der zivilen Identität über-mitteln von IdP an vBt	Anzeige Attributliste und One-Time-Code für Erlaubnis auf Anzeige des E-ID Trägergeräts Rückgabe Codes durch Inhaberin oder Inhaber an IdP		
Antwortticket IdP an vBt	E-ID Identifikator und Attribute der zivilen Identität		
Schritt 4: Abschluss Registrierung bei vBt	Inhaberin oder Inhaber erhält Zugang zu vBt Dienst		

Tabelle 2: Betriebsprozess Erstanmeldung bei vBt

Sicherheitsniveau der E-ID	Silber	Gold	Platin
Wiederanmeldung			
Schritt 1 Anmelden bei vBt	Anmeldung mit E-ID-Identifikator oder -Pseudonym beim vertrauenden Dienst der vBt (E-ID-Schnittstelle) Starten des E-ID-Authentifikators		
Authentifizierungsauftrag vBt an IdP	E-ID Identifikator und Sicherheitsniveau		
Schritt 2 Authentifizierung durch IdP gemäss Sicherheitsniveau	Erfassung eines Authentifi-zierungsfaktors	Erfassung 2 Authentifizie-rungsfaktoren	Erfassung 2 Authentifizie-rungsfaktoren mit Biometrie
Antwortticket IdP an vBt	E-ID Identifikator und Bestätigung Authentifizierung		
Schritt 3: Abschluss Anmeldung bei vBt	Inhaberin oder Inhaber erhält Zugang zu vBt Dienst		

Tabelle 3: Betriebsprozess Wiederanmeldung bei vBt (Login)



Skizze 9: E-ID Ausstellung und Einsatz

2.6 Wichtige Elemente der Umsetzung

Einige für die schweizerische Lösung wichtige Elemente wie das Konzept der Sicherheitsniveaus, der neue eindeutige Personenidentifikator und die pro Sicherheitsniveau verfügbaren staatlichen Personenidentifizierungsdaten, der Übermittlungsprozess von staatlichen Personenidentifizierungsdaten an den IdP und die Interoperabilität innerhalb des Netzwerks der staatlich anerkannten E-ID-Systeme werden nun noch etwas ausführlicher beschrieben.

2.6.1 Die drei E-ID Sicherheitsniveaus

Nicht für alle Geschäftsfälle ist eine E-ID des höchsten Sicherheitsniveaus notwendig. Ein hohes Sicherheitsniveau ist oftmals mit einer schlechteren Benutzerfreundlichkeit, insbesondere bei der initialen Registrierung, und höheren Kosten verbunden. Oft genügt für einfache Geschäftsfälle ein relativ niedriges Sicherheitsniveau, das mit einer einfachen Registrierung mit initialer Online-Identifizierung (wie z.B. für eine AppleID oder eine Google ID) und der Erfassung von einem Faktor für die Authentifizierung erreicht werden kann. Erst für kritischere Geschäftsprozesse muss die E-ID ein höheres Sicherheitsniveau garantieren, das bei der Registrierung eine persönliche Vorsprache für die initiale Identifizierung (wie z.B. für eine SuisseID oder eine Mobile ID) und im Einsatz mindestens eine 2-Faktor-Authentifizierung bedingt. Eine Einschränkung auf nur ein Sicherheitsniveau wäre also für die Verbreitung von staatlich anerkannten E-ID hinderlich. Deshalb werden geeignete E-ID-Systeme auf einem von drei Sicherheitsniveaus staatlich anerkannt. Die drei Sicherheitsniveaus für schweizerisch staatlich anerkannte E-ID-Systeme sind so definiert, dass sie bezüglich Sicherheit die gleichen Anforderungen erfüllen, die für die drei in der eIDAS-Verordnung der EU definierten E-ID-Sicherheitsniveaus verlangt werden (Art 8 der eIDAS-Verordnung [2] und dazugehörige Durchführungsrechtsakte [3]). Auch die Authentifizierungsanforderungen der NIST sehen gleiche drei Sicherheitsniveaus vor [6]. Jedes Sicherheitsniveau vermittelt ein unterschiedliches Mass an Vertrauen in die Identität und Authentizität der E-ID Inhaberin oder des Inhabers. Welches Sicherheitsniveau für welche Art der Anwendung in Frage kommt, wird in den jeweiligen Spezialerlassen für E-Government Anwendungen festgehalten bzw. durch die vertrauenden privaten Beteiligten definiert. So kann für E-Education ein anderes Sicherheitsniveau gewählt werden, als es für Vote électronique vorgeschrieben oder für E-Health-Anwendungen notwendig ist.

Neben der Vertrauenswürdigkeit der IdP und der Attributquellen, die von den IdP genutzt werden um die zivile Identität für die Inhaberin oder den Inhaber zu erstellen, haben die Registrierung (initiale Identifizierung der Person und die Bindung der E-ID an die Person), die Authentifizierung im Feld mittels der E-ID (1-Faktor, 2-Faktor, Biometrie) und die Übermittlung und Verarbeitung der Aufträge und Antworten im interoperablen Netzwerk der anerkannten E-ID-Systeme wesentlichen Einfluss auf das Sicherheitsniveau einer E-ID. Die drei Niveaus werden aus kommunikativen Überlegungen mit Silber, Gold und Platin bezeichnet. Die wichtigsten Eigenschaften der drei Niveaus sind in den folgenden Punkten und in der Tabelle 3 dargestellt (in Klammern die EU-Bezeichnungen für das entsprechende Sicherheitsniveau):

- SILBER (niedrig): Die E-ID hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung zu vermindern. Die Registrierung kann online gestützt auf einen staatlichen Ausweis erfolgen. Vom SID werden nur wenige Personenidentifizierungsdaten an den IdP übermittelt (Name, Vornamen, Geburtsdatum und EPID). Der Einsatz der E-ID verlangt mindestens eine Ein-Faktor-Authentifizierung. Die Handhabung einer solchen E-ID ist damit vergleichbar mit einem Zutrittsbadge, einer kontaktlosen Bezahllösungen für kleinere Beträge oder einem Login mit Identifikator und sicherem Passwort oder PIN. Das Sicherheitsniveau „SILBER“ bezieht sich auf ein elektronisches Identifizierungsmittel, das ein relativ niedriges aber immer noch höheres Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt, als eine simple Selbstdeklaration mit frei gewählter UserID und beliebigem Passwort.
- GOLD (substanziell): Die E-ID hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung erheblich zu vermindern. Die Registrierung erfolgt mit persönlicher Vorsprache beim IdP oder einer Videoidentifikation gestützt auf einen staatlichen Ausweis. Vom SID werden neben den Personenidentifizierungsdaten des unteren Niveaus noch weitere Attribute übermittelt (z.B. Geschlecht, Zivilstand, Gesichtsbild usw). Der Einsatz der E-ID verlangt mindestens eine 2-Faktor-Authentifizierung. Die Handhabung einer solchen E-ID ist somit zum Beispiel mit im Bankenbereich

üblichen Lösungen vergleichbar (Kontokarten, Kreditkarten, E Banking-Lösungen). Das Sicherheitsniveau „GOLD“ bezieht sich auf ein elektronisches Identifizierungsmittel, das ein substanzielles Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt.

- PLATIN (hoch): Die E-ID hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung zu verhindern. Die Registrierung erfolgt mit persönlicher Vorsprache beim IdP oder mit Videoidentifikation gestützt auf einen staatlichen Ausweis. Zusätzlich wird die Echtheit des Ausweises und mindestens ein biometrisches Merkmal gestützt auf eine unabhängige behördliche Quelle überprüft (Ausweisgültigkeit und Gesichtsbild oder anderes biometrisches Erkennungsmerkmal). Vom SID werden alle verfügbaren Personenidentifizierungsdaten übermittelt (z.B. auch das Unterschriftsbild). Der Einsatz der E-ID verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss («inhärenter Faktor» gemäss eIDAS-Durchführungsrechtsakte [3]).). Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung. Die biometrische Authentifizierung bewirkt eine noch engere Bindung zwischen der E-ID und der Inhaberin oder dem Inhaber. Das Sicherheitsniveau „PLATIN“ bezieht sich auf ein elektronisches Identifizierungsmittel, das ein Höchstmaß an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt.

Tabelle 3: Sicherheitsniveaus der E-ID

Stufe	Silber (niedrig)	Gold (substanziell)	Platin (hoch)
Authentifizierung	Mindestens 1-Faktor	2-Faktoren	2 oder 3-Faktoren mit Biometrie
Registrierung: Bindung Person an E-ID	Person führt Bindung an E-ID unbeaufsichtigt aus	Person führt Bindung an E-ID verifiziert von IdP aus	Person führt Bindung an E-ID mit biometrischem Faktor verifiziert von IdP aus
Registrierung: Initiale Identifizierung	Online durch Ausweisnummer und Gültigkeitsdatum	Bei Vorsprache oder Videokonferenz mit Ausweis; Test E-ID Authentifizierung	Bei Vorsprache oder Videokonferenz mit Ausweis; Test E-ID Authentifizierung
Personenidentifizierungs-daten	Minimaler Satz und EPID; jährlicher Abgleich mit SID	Alle, ausser gewisse biometrische Daten; pro Quartal Abgleich mit SID	Alle Personenidentifizierungsdaten; wöchentlicher Abgleich mit SID
Anforderung an IdP und E-ID-System gemäss eIDAS-Definitionen [3], Art. 2.4	Anerkennung des E-ID-Systems mit Sicherheitsaudits für Sicherheitsniveau ‚niedrig‘, substanziell‘ oder ‚hoch‘ gemäss Art 2.4.7 in [3]		

Mit diesem Modell ist es möglich, vorerst eine geeignete E-ID mit 2-Faktor-Authentifizierung (heutiger de facto Industriestandard) auf Niveau Silber zu registrieren und diese später bei Bedarf mittels einer persönlichen Vorsprache auf ein höheres Sicherheitsniveau anzuheben. Mit dem Sicherheitsniveau Silber wird der Zugang zu staatlich anerkannten E-ID einfach gehalten, was einen essentiellen Erfolgsfaktor für die Anbieter von staatlich anerkannten E-ID-Systemen im Markt darstellen kann. Zudem kann eine Person mehrere E-ID von verschiedenen IdP oder auf unterschiedlichen Sicherheitsniveaus besitzen.

2.6.2 Eindeutiger Personenidentifikator (EPID)

Das Konzept geht davon aus, dass die heutige Praxis der Nutzung der AHVN13 bestehen bleibt und führt deshalb zusätzlich einen neuen eindeutigen Personenidentifikator (EPID) ein, der für die E-ID aber auch für andere Anwendungen zur Verfügung stehen soll. Falls hingegen die rigide Praxis der Verwendung der AHVN13 gelockert würde, könnte die AHVN13 direkt als EPID auch für die E-ID eingesetzt werden. Ob dies möglich ist, ist derzeit Gegenstand von Abklärungen.

Der Staat definiert für alle in den einschlägigen Personenregistern des Bundes erfassten Personen mit einem staatlich ausgestellten Ausweis und Aufenthaltsrecht einen neuen Eindeutigen Personenidentifikator (EPID), der unabhängig von anderen Personenidentifizierungsdaten wie Name oder AHVN13 ist. Der EPID dient als Anker für alle zu einer Person gehörigen Personenidentifizierungsdaten, die der SID dem IdP übermittelt, und für alle weiteren Attribute, die ein IdP oder eine vBt einer Person zuordnet. Die staatlichen Personenidentifizierungsdaten, die der SID an die IdP übermittelt, sind kryptografisch an den EPID gekoppelt, so dass die Integrität und Authentizität eines übermittelten Attributs durch den IdP jederzeit überprüft werden kann. Der IdP ist verpflichtet die Personenidentifizierungsdaten zu einer ausgestellten E-ID regelmässig durch eine entsprechende Abfrage beim SID zu aktualisieren, wobei die Periodizität der Abfrage vom Sicherheitsniveau abhängig ist. Der IdP ordnet in seinem E-IdM insbesondere auch den Identifikator der E-ID dem EPID der Inhaberin oder des Inhabers zu. Dies gilt auch für allfällig abgeleitete Identifikatoren oder Identifikatoren einer zweiten E-ID, so dass eine vertrauende Beteiligte allfällige Mehrfachanmeldungen mit verschiedenen E-ID mit Hilfe des IdP immer eindeutig als zu einer Person gehörig auflösen kann. Vertrauende Beteiligte können dank dem EPID ihre administrativen Prozesse vereinfachen, verlässlicher machen und damit Kosten sparen. Anstelle des EPID kann, falls dies vom IdP so festgelegt wird, für jede vertrauende Beteiligte eine abgeleitete Personenidentifizierung angewendet werden, so dass keine Instanzen oder Sektor übergreifende Profilierung möglich ist.

2.6.3 Personenidentifizierungsdaten (PID)

Der SID bezieht für jede berechtige Person ihre Personenidentifizierungsdaten (PID) aus den einschlägigen Personenregistern des Bundes (siehe Kap 4). Die PID werden vom Staat verwaltet und die erfassten Attribute entsprechen denjenigen Werten, die anlässlich der letzten staatlichen Identifikation der Person bei der Ausstellung eines hoheitlichen Ausweises oder eines anderen staatlichen Aktes, der zu einem Eintrag in den Personenregistern des Bundes (ISA, ZEMIS, Infostar, ZAS-UPI) geführt hat, festgestellt wurden[26].

Weitere staatliche Identitätsattribute können später zusätzlich aufgenommen werden, sollte im E-ID-Ökosystem dafür ein Bedarf und eine Rechtsgrundlage bestehen. Wichtig für das Verständnis ist, dass weder ein IdP noch eine vertrauende Beteiligte ohne ausdrückliches Einverständnis der betroffenen Person Zugriff auf diese Attribute erhalten. Es ist immer die Person, welche die PID eines Sicherheitsniveaus explizit, bewusst und ausschliesslich an den anerkannten IdP übermitteln lässt, von dem sie eine staatlich anerkannte E-ID bezieht. Auch eine spätere Übermittlung von einzelnen Attributen der staatlichen PID durch den IdP an eine vertrauende Beteiligte, darf nur nach der explizit erfolgten Erlaubnis der Inhaberin oder des Inhabers erfolgen.

[26] Aus Konsistenzgründen werden auch für die E-ID immer die gleichen Attribute übermittelt, wie sie in den letztausgestellten hoheitlichen Ausweisen oder in Infostar eingetragen sind. Spezialfälle wie Ausweisentzug, Ableben oder Identitätsänderungen in Zeugenschutzprogrammen werden im Detailkonzept geregelt.

Tabelle 4: Verfügbare Personenidentifizierungsdaten

Attribut	Silber	Gold	Platin
EPID	X	X	X
Amtlicher Name	X	X	X
Vornamen	X	X	X
Geburtsdatum	X	X	X
AHVN13 (nur an Berechtigte)		X	X
Geschlecht		X	X
Geburtsort		X	X
Zivilstand		X	X
Nationalität		X	X
Aufenthaltsstatus		X	X
Gesichtsbild		X	X
Ausweisart und -nummer		X	X
Unterschriftsbild			X

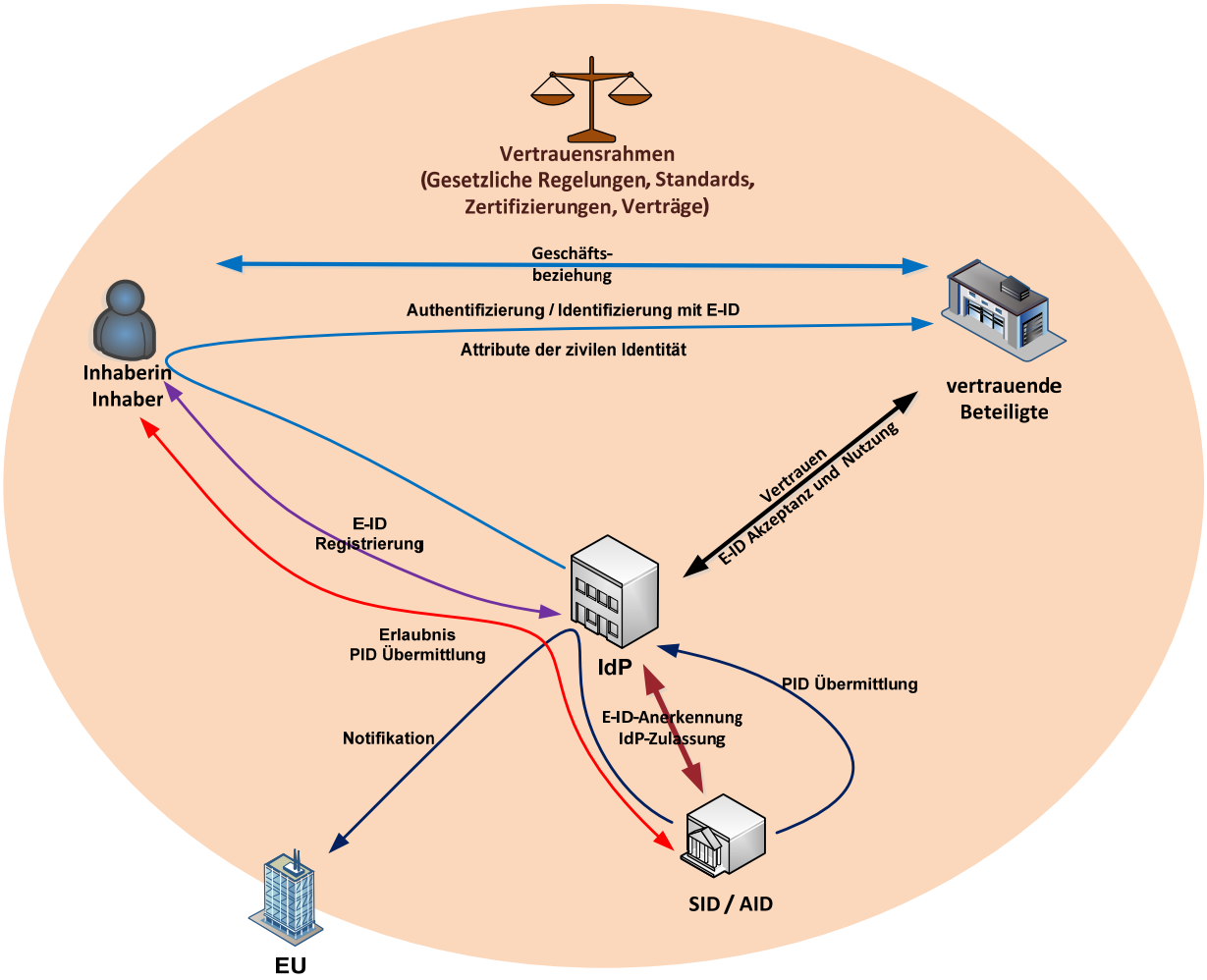
Datum jüngste Feststellung der Attribute für alle Attribute

2.6.4 Übermittlung von Personenidentifizierungsdaten

Die Übermittlung von Personenidentifizierungsdaten an einen IdP wird durch eine Anfrage des IdP ausgelöst. In der Anfrage teilt der IdP dem SID durch Angabe der Nummer eines gültigen von der Schweiz ausgestellten hoheitlichen Ausweises mit, für welche Person die Übermittlung der PID angefragt wird. Die Mitteilung des IdP an den SID enthält zusätzlich das Ausstellungsdatum des Ausweises, mit dem sich die Person bei der initialen Identifizierung ausgewiesen hat, das Sicherheitsniveau des E-ID-Systems, für das die PID angefordert werden, und die Angaben, wie die Inhaberin oder der Inhaber über einen unabhängigen Kanal kontaktiert werden kann.

Der SID teilt der Inhaberin oder dem Inhaber über den angegeben Kanal (z.B. Mobile Nummer, E-Mail-Adresse oder Postadresse) mit, dass der anfragende IdP für die staatliche Anerkennung der ausgestellten E-ID, die dem Sicherheitsniveau entsprechenden PID übermittelt haben möchte. Der SID gibt der Person einen Erlaubniscode bekannt, den diese dem IdP offenbaren muss, wenn sie mit der Übermittlung einverstanden ist.

Der IdP sendet diesen Erlaubniscode innerhalb einer definierten Zeitspanne zurück an den SID. Die Zeitspanne hängt dabei vom SID genutzten Kommunikationskanal zur Person ab. Sobald der SID den Erlaubniscode erhält, übermittelt er die dem Sicherheitsniveau entsprechenden PID an den IdP. Das ebenfalls immer übermittelte Datum der letzten Identifizierung braucht nicht identisch zu sein mit dem vom IdP übermittelten Datum des Ausweises. Eine Person kann mehrere gültige Ausweise haben und die PID entsprechen immer den Werten, die anlässlich der letzten staatlichen Identifizierung festgestellt wurden.



Skizze 10: Beziehungen und Prozesse bei der Ausstellung und im Einsatz einer E-ID

Der IdP muss die übermittelten Daten periodisch mit den aktuellsten Daten des SID aktualisieren. Die Periodizität hängt vom Sicherheitsniveau der zugehörigen E-ID ab. Der IdP muss auch täglich die von der SID publizierte Liste mit den Änderungen der PID abfragen, die für gewisse EPID erfasst wurden[27]. Für die Aktualisierung ist keine neue Erlaubnis der Inhaberin oder des Inhabers nötig.

2.6.5 Interoperabilität der E-ID-Systeme

Die Interoperabilität zwischen E-ID-Systemen auf gleichem Sicherheitsniveau ist ein wichtiger Faktor für die rasche Verbreitung und die Akzeptanz staatlich anerkannter E-ID-Systeme im EID Ökosystem. Es macht aber wenig Sinn, wenn jede vertrauende Beteiligte mit jedem staatlich anerkannten IdP für die nutzbaren E-ID-Systeme entsprechende Nutzungsvereinbarungen treffen muss. Deshalb wird im Konzept festgelegt, dass jede E-ID, die das notwendige Sicherheitsniveau erreicht oder übertrifft, bei allen vertrauenden Diensten von vBt unabhängig vom herausgebenden IdP eingesetzt werden kann.

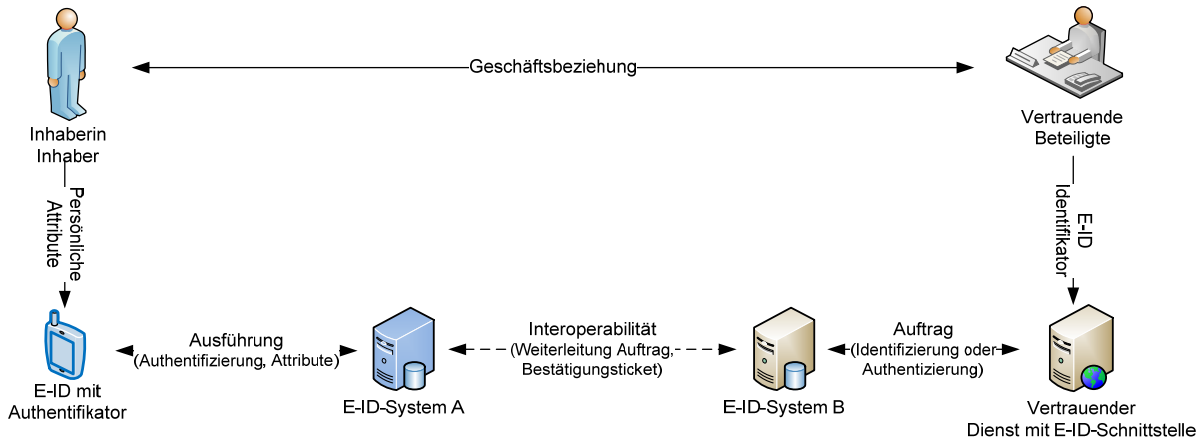
Das Protokoll für den Einsatz einer E-ID bei der Registrierung oder bei der Anmeldung an einen vertrauenden Dienst ist im Ablauf und in der Gestaltung pro Medium (mobile Geräte, PC, Internetkiosk etc.) immer gleich und vermittelt der Inhaberin und dem Inhaber ein vertrautes Nutzungserlebnis. Die vertrauenden Dienste integrieren in ihre Portale die entsprechenden Registrierungs-

[27] Attributänderungen können zum Beispiel bei Heirat erfolgen, wenn in der Zwischenzeit eine neue IDK oder ein neuer Pass ausgestellt wurde. Auch der Tod einer Person soll natürlich zu einem Widerruf der E-ID führen.

und Anmeldeseiten in Form einer weitgehend standardisierten E-ID-Schnittstelle. Der Einsatzdialog mit der Inhaberin oder dem Inhaber der E-ID soll unabhängig von E-ID-System und vBt immer gleichartig sein.

Auch für die vertrauenden Dienste ergibt sich durch die Interoperabilitätsanforderung kein zusätzlicher Aufwand. Sie erstellen die Identifizierungs- und Authentifizierungsaufträge für alle E-ID gleich und senden sie an den IdP, an dessen E-ID-System sie angeschlossen sind. Die Antworttickets erhalten sie auch immer über diesen IdP in einem Standardformat zurück.

Die Interoperabilität wird ausschliesslich durch die E-ID-Systeme der IdP realisiert. Jeder Auftrag enthält den Identifikator der E-ID. Ein Teil des Identifikators identifiziert das E-ID-System und den herausgebenden IdP (entspricht den Identifikatoren der staatlich anerkannten E-ID-Systeme die in der Liste der AID publiziert sind). Der IdP leitet einen Identifizierungs- oder Authentifizierungsauftrag an den zuständigen IdP weiter und erhält von ihm nach der Erledigung das Antwortticket, welches er an den vertrauenden Dienst zurückgibt.



Skizze 11: Realisierung der Interoperabilität auf Ebene IdPs und E-ID-Systeme

2.7 Notifizierbarkeit

Am 23.Juli 2014 hat die EU die Verordnung (EU) Nr.910/2014 [2] des europäischen Parlaments vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt erlassen. Ab September 2015 erfolgte dann die Verabschiedung der dazugehörigen Durchführungsrechtsakte [36] [37] [38] [39].

Nachstehend soll kurz erörtert werden, welche Anforderungen an ein schweizerisches E-ID-System zu stellen sind, wenn dieses konform zur E-ID-Verordnung sein soll, damit es später gegebenenfalls notifiziert werden könnte. Selbstverständlich gibt es für die Schweiz keine rechtliche Verbindlichkeit zur Übernahme der EU-Verordnung. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern wird aber davon ausgegangen, dass die Schweiz ein Interesse daran hat, früher oder später in das europäische System für die Interoperabilität von elektronischen Identitäten eingebunden zu sein. Auch wenn vorläufig völlig offen ist, ob, wann und wie die Schweiz sich staatsvertraglich in dieses System einbinden wird, soll das schweizerische E-ID-System von Beginn an so konzipiert werden, dass es grundsätzlich notifiziert werden könnte.

Damit ein nationales System notifiziert werden kann, muss es die in der eIDAS-Verordnung in

Artikel 7 genannten Bedingungen erfüllen. Buchstabe a) lässt in Ziffer iii) auch E-ID-Systeme wie das hier geregelte zu, wo der Staat von Privaten angebotene Systeme anerkennt. Die wesentlichen weiteren Anforderungen stehen in den Buchstaben c) bis f) und sind:

c) Sowohl das E-ID-System wie auch die E-ID erfüllen die technischen Anforderungen mindestens eines Sicherheitsniveaus gemäss Artikel 8 Absatz 3.

d) Der notifizierende Staat stellt sicher, dass – zum Zeitpunkt der Ausstellung – die richtigen Personenidentifizierungsdaten der E-ID zugeordnet sind und haftet dafür auch nach Artikel 11 Ziffer (1) zwingend selbst.

e) Der IdP, der die E-ID ausstellt, sorgt dafür, dass die E-ID gemäss den Spezifikationen entsprechend dem Sicherheitsniveau nur der richtigen Person zugewiesen wird.

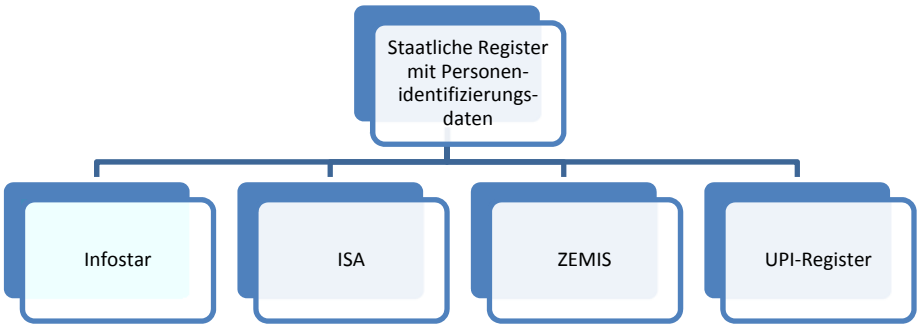
f) Der notifizierende Staat selbst stellt sicher, dass jedem vertrauenden Dienst EU-weit jederzeit eine Online-Authentifizierung zur Verfügung steht, wofür er im Schadensfall wiederum nach Artikel 11 Ziffer (1) haftet.

Diese Anforderungen wirken sich auf die schweizerische Regulierung aus. Mit dem geplanten E-ID-Gesetz wird u.a. ein Rechts- und Standardisierungsrahmen für die staatliche Anerkennung von E-lD-Systemen und die Anerkennung der IdP geschaffen. Dieser ist ausgestaltet, dass eine spätere gegenseitige Anerkennung der staatlich anerkannten E-lD-Systeme zwischen der Schweiz und der EU, oder einzelner Mitgliedstaaten, möglich bleibt. Die Kompatibilität des vorliegenden Konzepts mit den Durchführungsrechtsakten zur eIDAS-Verordnung wurde soweit möglich geprüft und für gegeben befunden.

3 Beitrag des Staates zur E-ID

3.1 Überblick

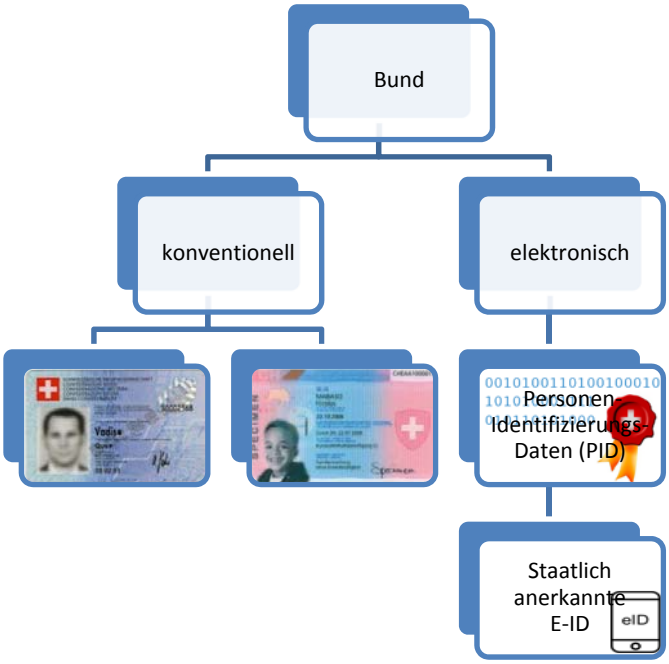
Die Schweizer Behörden führen bereits heute mehrere Personenregister, welche Personenidentifizierungsdaten enthalten. Stellvertretend seinen hier das elektronische Zivilstandsregister (Infostar), die Einwohnerregister und das Zentralregister der zentralen Ausgleichsstelle der AHV (ZAS) genannt. Im Ausweisbereich sind die Personenidentifizierungsdaten für Schweizerinnen und Schweizer im Informationssystem Ausweisschriften (ISA) und für ausländische Personen im Zentralen Migrationssystem (ZEMIS) enthalten. Auch das UPI-Register der zentralen Ausgleichsstelle dient der amtlichen Identifizierung von natürlichen Personen und der Zuweisung einer eindeutigen AHV-Nummer (UPI ist das Akronym für „Unique Person Identification“).



Skizze 12: Personenregister des Bundes

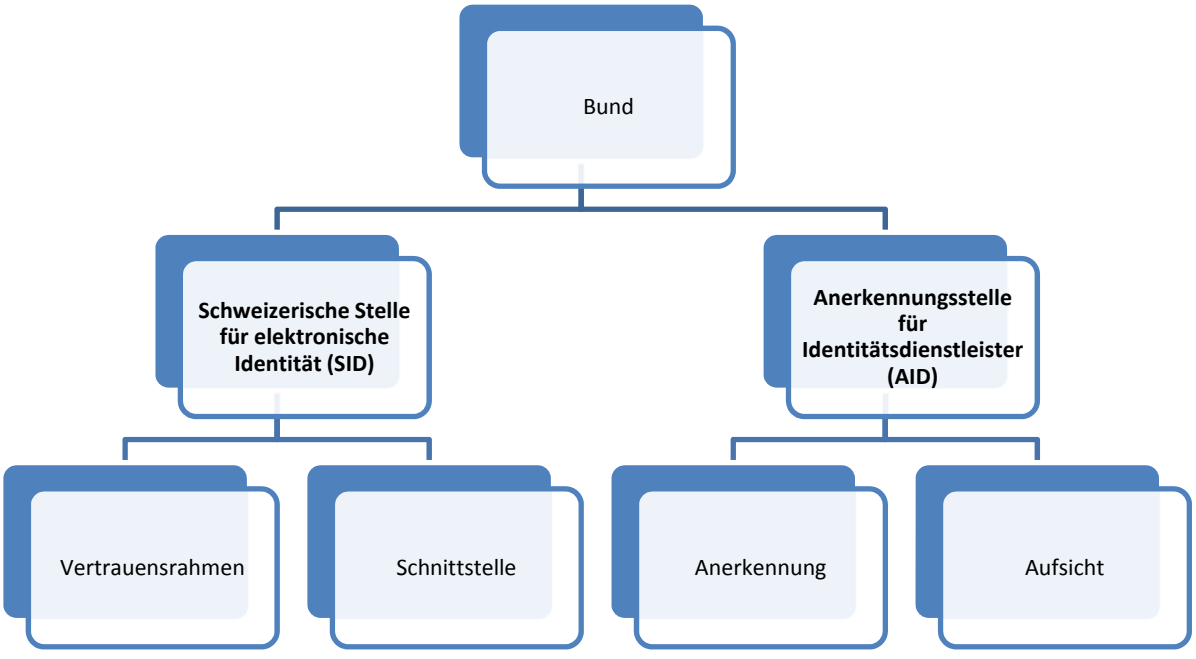
Im Rahmen des Gesetzes über die Registerharmonisierung (RHG) ist die neue AHV-Nummer (AHVN13) zum einzigen und eindeutigen Personenidentifikator in den von der Volkszählung betroffenen Registern bestimmt worden. Zu diesen Registern zählen die Personenregister des Bundes sowie die kantonalen und kommunalen Einwohnerregister. Auch die gemäss der Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV) von den Krankenversicherern ausgestellte Versichertenkarte enthält die AHV-Nummer als eindeutigen Personenidentifikator. Die AHVN13 ist nichtsprechend und besteht aus einer 13-stelligen Zahlenfolge (3 Stellen Ländercode nach ISO 3166, 9 Stellen Zufallszahl, 1 Stelle Prüfziffer).

Gestützt auf die Personenidentifizierungsdaten in ISA respektive ZEMIS stellt der Bund heute konventionelle Identifizierungsmittel aus, nämlich Schweizer Pass, Identitätskarte und Ausländerausweis. Der Bund tritt dabei als Vertrauensanker für die staatliche Identität einer Person auf. Mit der Einführung von staatlich anerkannten E-ID sollen gestützt auf die beim Bund vorhandenen Personenidentifizierungsdaten auch elektronische Identifizierungsmittel mit hinterlegten staatlich übermittelten Personenidentifizierungsdaten ausgestellt werden können.



Skizze 13: Staatliche Identifizierungsmittel

Der Bund übernimmt dazu vier Aufgaben: erstens schafft und pflegt er einen transparenten Rechts- und Vertrauensrahmen, zweitens betreibt er eine elektronische Schnittstelle, über welche anerkannte IdP staatlich geführte Personenidentifizierungsdaten beziehen können, drittens kann er IdP und ihre E-ID-Systeme staatlich anerkennen und viertens beaufsichtigt er staatlich anerkannte IdP und E-ID-Systeme. Diese Aufgaben sollen beim Bund von zwei Verwaltungseinheiten wahrgenommen werden: dem „Schweizerische Stelle für elektronische Identität (SID)“ und der „Anerkennungsstelle für Identitätsdienstleister (AID)“.



Skizze 14: Aufgaben SID und AID

3.2 Schweizerische Stelle für elektronische Identität (SID)

3.2.1 Rechtsrahmen

Der SID (auch Identitätsdienst genannt) pflegt im Betrieb in Zusammenarbeit mit der AID die rechtlichen, organisatorischen und technischen Vorgaben. Insbesondere definiert er die Standards der Schnittstellen für die Interoperabilität der E-ID-Systeme und passt die technischen und organisatorischen Anforderungen im Bereich der Anerkennung der IdP und E-ID-Systeme dem technischen und sozioökonomischen Fortschritt an.

Damit zu einem späteren Zeitpunkt ein E-ID-System der EU notifiziert werden kann, muss es die Vorgaben der eIDAS-Verordnung der EU einhalten. Deshalb ist darauf zu achten, dass die Vorgaben für staatlich anerkannte E-ID-Systeme der Schweiz die eIDAS-Verordnung abdecken, wie dies der Bundesrat mit seinem Auftrag stipuliert hat.

3.2.2 Schnittstelle

Der SID stellt für die anerkannten IdP beim Bund geführte Personenidentifizierungsdaten über eine elektronische Schnittstelle bereit. Durch die Etablierung und Übermittlung eines eindeutigen Personenidentifikators kann die Integrität der Zuweisung der Personenidentifizierungsdaten zur korrekten Person sichergestellt werden. Als B2B-Schnittstelle ist sie ausschliesslich den anerkannten IdP zugänglich.

Im Rahmen der Ausstellung einer staatlich anerkannten E-ID identifiziert sich die Person beim IdP mittels eines konventionellen Ausweises. Dieser übermittelt dem SID die Ausweisnummer. Der SID ermittelt durch Abfrage von ISA resp. ZEMIS den zugehörigen EPID und übermittelt diesen sowie die dem Sicherheitsniveau der E-ID entsprechenden Personenidentifizierungsdaten dem IdP.

Im Hinblick auf die Migration bestehender Datenbestände werden die bestehenden Identifikatorsysteme (z.B. AHVN13) für die Qualitätssicherung nutzbar sein.

Jede Übermittlung wird vom SID protokolliert und so gekennzeichnet, dass eine Aktualisierungsabfrage eines IdP eindeutig auf eine frühere Erstübermittlung zurückgeführt werden kann.

Der SID bezieht die Personenidentifizierungsdaten wie den Namen einer Person vorrangig aus Infostar und z.B. Ausweisnummern oder Foto subsidiär aus ISA resp. ZEMIS. Folgende Tabelle zeigt eine mögliche Auswahl von Personenidentifizierungsdaten mit der Angabe des Quellregisters.

Name des Attributs	**Quellenregister**
EPID	UPI, ZEMIS, ISA
amtlicher Name	Infostar
Vornamen	Infostar
Geburtsdatum	Infostar
Versichertennummer (AHVN13)	Infostar
Geschlecht	Infostar
Geburtsort	Infostar
Zivilstand	Infostar
Nationalität	Infostar
Aufenthaltsstatus	ZEMIS
Gesichtsbild	ISA, ZEMIS
Ausweisnummer(n) Pass	ISA
Ausweisnummer(n) IDK	ISA
Ausweisnummer(n) NAA	ZEMIS
Unterschriftenbild	ISA, ZEMIS

Tabelle 5: Staatliche Quellen für die Personenidentifizierungsdaten

Diese Register müssen vor der Einführung staatlich anerkannter E-ID mit der AHVN13 ergänzt und entsprechend migriert werden. Zur weiteren Erhöhung der Datenqualität empfiehlt sich zudem ein konsequenter Abgleich der Register mit den Daten von Infostar, wie dies bei ISA heute bereits der Fall ist.

Die Personenidentifizierungsdaten können mit zusätzlichen Metadaten, wie etwa eine Quellenangabe oder dem Datum der Erhebung, ergänzt werden. Sie sind zudem kryptographisch immer an den EPID gebunden. Die Erstübermittlung der Personenidentifizierungsdaten an den IdP soll nur mit dem ausdrücklichen und dokumentierten Einverständnis der betroffenen Person erfolgen.

Die IdP sind gehalten, die zu einem EPID bezogenen Personenidentifizierungsdaten periodisch zu aktualisieren. Auch dies geschieht über die Schnittstelle des SID, jedoch ist dazu aus Überlegungen der Benutzerfreundlichkeit keine erneute ausdrückliche Einwilligung der Person mehr erforderlich. Je nach Sicherheitsniveau müssen die IdP die Aktualisierungen jährlich (Silber), quartalsweise (Gold) oder wöchentlich (Platin) vornehmen. Die Aktualisierung kann vom IdP gestützt auf den EPID ausgelöst werden, wobei der SID prüft, ob für den EPID überhaupt eine Erstübermittlung an den konkreten IdP mit ausdrücklicher Bestätigung durch die Person stattgefunden hatte.

Um E-ID bei besonderen Umständen rasch sperren zu können, stellt der SID auf seiner Schnittstelle eine Liste mit gesperrten EPID bereit. Ein besonderer Umstand kann z.B. der Tod einer Person sein. Die IdP sind gehalten, alle E-ID umgehend zu sperren, welche zu einer gelisteten EPID ausgegeben wurden. Die Liste kann durch die IdP über die Schnittstelle kostenlos konsultiert werden. Er ist gehalten, dies regelmässig zu tun (täglich).

3.2.3 Organisation

Der SID hat rechtliche und insbesondere betriebliche Aufgaben. Für die Erarbeitung und an-

schliessenden Pflege der rechtlichen, organisatorischen und technischen Vorgaben für E-ID-Systeme sind beim SID entsprechende Ressourcen notwendig.

Der SID ist zudem für den Betrieb der Schnittstelle zur Übermittlung der Personenidentifizierungsdaten verantwortlich. Er ist Single Point Of Contact (SPOC) für alle fachlichen und technischen Fragen der angeschlossenen Register und IdP im Zusammenhang mit der Schnittstelle.

Abklärungen zu vermeintlich oder tatsächlich inkonsistenten resp. falschen Personenidentifizierungsdaten werden nicht vom SID selbst, sondern von der „Clearingstelle“ der ZAS-UPI vorgenommen, welche diese Aufgabe im Bereich der AHVN13 heute bereits innehat [40].

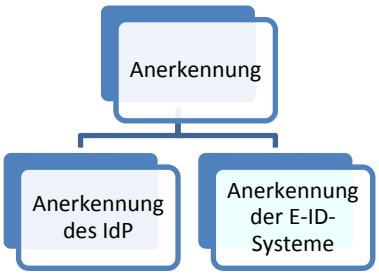
Zur Erfüllung dieser Aufgaben sind nach aktuellen Abschätzungen für den SID 300 unbefristete Stellenprozente notwendig (permanente Pflege und regelmässige Anpassung der technischen Vorschriften an aktuelle Entwicklungen, Betreuung des SPOC). Da die für die staatlich anerkannte E-ID relevanten Datenbanken (mit Ausnahme des UPI-Registers) in der Verantwortung des EJPD liegen, soll der SID sinnvollerweise im EJPD aufgebaut werden.

3.3 Anerkennungsstelle für Identitätsdienstleister (AID)

3.3.1 Anerkennung

Etablierte IdP (privatwirtschaftliche und solche der öffentlichen Hand) können sich und ihre E-ID-Systeme auf einem der vorgesehenen Sicherheitsniveaus vom AID staatlich anerkennen lassen. Ein IdP kann mehrere E-ID-Systeme auf unterschiedlichem Sicherheitsniveau anerkennen lassen.

Sowohl der IdP wie auch das konkrete E-ID-System müssen eine Anerkennung auf mindestens dem gewünschten Sicherheitsniveau erlangen. Dazu werden vom SID in Absprache mit dem AID rechtliche, organisatorische und technische Auflagen festgelegt, deren Erfüllung durch den IdP vom AID überprüft wird. Bestehende Zertifizierungen und Anerkennungen (z.B. Im Rahmen ZertES oder Zustellplattformen) werden dabei soweit als möglich in den Anerkennungsprozess integriert, so dass Doppelspurigkeiten vermieden werden.



Skizze 15: Anerkennung IdP und E-ID-System

Die Anerkennung soll sich grundsätzlich auf Konformitätsnachweise mit internationalen Normen und nationalen Schutzprofilen abstützen. Der IdP muss dazu die Konformität seiner Organisation und seiner E-ID-Systeme durch Zertifizierungen gegenüber der AID nachweisen. Die AID prüft die eingereichten Zertifizierungsunterlagen und entscheidet über die staatliche Anerkennung.

Ein Spezialfall der Anerkennung ist die allfällige Notifikation eines E-ID-Systems gegenüber der EU. Mit der Notifizierung wird ein E-ID-System in der EU anerkannt und kann dort auf dem entsprechenden Sicherheitsniveau verwendet werden. Reziprok müssen alle bereits notifizierten E-ID-Systeme der EU-Mitgliedstaaten auch in der Schweiz auf dem entsprechenden Sicherheitsniveau anerkannt werden. Die Schweiz muss für die Notifizierung einen bilateralen Vertrag mit der

EU abschliessen.

Weiter publiziert die AID eine Liste mit den anerkannten IdP und E-ID-Systemen, anhand derer die vertrauenden Beteiligten und natürlichen Personen den Status eines konkreten IdP resp. E-ID-Systems prüfen können.

3.3.2 Aufsicht

Die AID übt die Aufsicht über die anerkannten IdP und E-ID-Systeme aus und reagiert im Falle von Abweichungen von den Vorgaben oder Vorfällen im IKT-Sicherheitsbereich. Dazu beaufsichtigt die AID den Markt, sammelt und beurteilt Meldungen über die IKT-Sicherheit im E-ID-Bereich und leitet sie wenn notwendig an den SID weiter. Zudem fordert die AID von den anerkannten IdP in den festgelegten zeitlichen Abständen die notwendigen Konformitätsnachweise ein und prüft sie. Ultimo Ratio kann die AID einem IdP oder E-ID-System die staatliche Anerkennung entziehen.

3.3.3 Organisation

Die AID anerkennt und beaufsichtigt staatlich anerkannte E-ID-Systeme. Ihre Aufgaben weisen Synergien mit weiteren Aufgaben des Bundes im IKT-Bereich auf:

EFD: Das ISB ist für den Aufbau des IAM-Bund verantwortlich. In diesem Bereich ist wohl auch eine Aufsicht und Steuerung der eingebundenen IAM-Systeme notwendig.

Weiter könnte im Zusammenhang mit dem Informationssicherheitsgesetz eine Organisationseinheit geschaffen werden, welche solche Aufsichtsaufgaben wahrnimmt.

UVEK: Das BAKOM verfügt bereits über hohe Kompetenzen und Erfahrungen im Bereich der Marktüberwachung. Zudem ist das BAKOM bereits bei den elektronischen Signaturen (ZertES) engagiert.

WBF: Das SECO muss im Zusammenhang mit dem von ihm geförderten Identitätsverbund Schweiz (IDV-CH) wohl ebenfalls eine Aufsichtsfunktion wahrnehmen.

Gestützt auf eine erste Analyse scheint es sinnvoll, die AID beim EFD (ISB) aufzubauen, da IAM-Bund und IKT-Sicherheit thematisch stark mit den staatlich anerkannten E-ID-Systemen verbunden sind. Zur Erfüllung der genannten Aufgaben sind für die AID 100 unbefristete Stellenprozente notwendig.

3.4 Finanzielle Auswirkungen beim Bund

3.4.1 Modellannahmen

Analysiert man den im Markt durch E-ID entstehenden finanziellen Nutzen, fällt auf, dass dieser hauptsächlich bei den vertrauenden Beteiligten anfällt. Dies deshalb, weil diese ihre Prozesse durch den Einsatz von E-ID vereinfachen und vergünstigen können (z.B. weniger Schalter, Papier und Medienbrüche, rascherer Durchlauf, innovative Geschäftsmodelle, eindeutiger Personenidentifikator usw.). Das Finanzierungsmodell muss diese essentielle Erkenntnis berücksichtigen.

Deshalb qualifiziert sich das „pay-per-use"-Modell für die Verrechnung der staatlichen Leistungen an die Marktteilnehmer am besten. Das Modell sieht vor, dass alle beteiligten Stellen ihre Investitions- und Betriebskosten selbst tragen (also de facto eine Defizitgarantie übernehmen), die Auslagen jedoch mittelfristig mit Einnahmen egalisieren können. Damit ist gemeint, dass keine hohen Vorabgebühren, sondern Gebühren beim konkreten Einsatz der E-ID am erfolgversprechendsten sind. Der Bund sollte also dem IdP nur dann Gebühren in Rechnung stellen, wenn die IdP tatsächlich Attribute abrufen. Als zusätzlicher Anreiz könnte vorgesehen werden, dass der Bund auf die Erhebung der Gebühren für die Erstübermittlung der Personenidentifizierungsdaten verzichtet, falls ein IdP im Gegenzug die E-ID entgeltlos ausstellt.

Wie die IdP ihre Kosten dann dem Benutzer verrechnen, ist ihre Sache (z.B. „pay-per-use" oder „flat rate"). Die IdP können eine deutliche Kostenersparnis realisieren, wenn eine Vorsprache der Person bei der Ausstellung der E-ID vermieden werden kann. Dies könnte zum Beispiel dadurch realisiert werden, dass die IdP das vom Bund auf dem Sicherheitsniveau Gold und Platin übermittelte Gesichtsbild für eine biometrische Verifikation der Identität verwenden.

Im Rahmen der Arbeiten wurden noch andere Modelle geprüft, aber wieder verworfen. So etwa das Modell „prepaid", welches z.B. die SuisseID umgesetzt hat. In diesem Modell wird von den Nutzern vorab eine für den Herausgeber möglichst kostendeckende Gebühr verlangt. Die Prüfung dieses Modells hat aber ergeben, dass eine Gebühr, welche eine Person ohne offensichtliche und breite Einsatzmöglichkeit der E-ID zahlen muss, ein grosses Hindernis für die Akzeptanz der Lösung darstellt. Auch ein Modell „promotion", bei dem der Bund die Dienstleistungen des SID zeitlich unbeschränkt kostenlos anbietet, wurde geprüft und verworfen, da es die Kostenwahrheit gänzlich ignoriert. Immerhin hätte dieses Modell die Vorteile, dass die Eintrittshürde für die übrigen Beteiligten weiter gesenkt und der Aufwand für das Gebühreninkasso entfallen würde.

Für die Kostenabschätzungen beim Bund muss von einem Modell ausgegangen werden, dessen Parameter schwierig zu prognostizieren ist. Als grobe Abschätzung wird davon ausgegangen, dass rund die Hälfte der Bevölkerung der Schweiz mittelfristig über eine staatlich anerkannte E-ID verfügt und damit rund 10 Millionen Attributabfragen beim Bund einhergehen. Die mit diesen Abfragen verbundene Belastung wird aus heutiger Sicht keine Nachrüstung der Leistungsfähigkeit der bestehenden Datenbanken notwendig machen.

3.4.2 Investitions- und Betriebskosten SID und AID

Gestützt auf die Annahmen in Kapitel 3.4.1 wird für den Aufbau des SID mit Gesamtkosten von rund CHF 6.5 Mio. beim Bund gerechnet. Die jährlichen Betriebskosten einschliesslich der Personalkosten werden auf rund CHF 2.2 Mio. Franken veranschlagt.

Für den Betrieb des SID sind 300 unbefristete Stellenprozente und der AID 100 unbefristete Stellenprozente notwendig. Beim SID sind diese personellen Ressourcen für folgende Aufgaben vorgesehen: a) Fachsupport für die beteiligten bundesinternen Datenlieferanten, b) Fachsupport für die beteiligten staatlich anerkannten IdP, c) Anwendungsverantwortung und Pflege der beim SID notwendigen IKT-Infrastruktur (B2B-Schnittstelle und Anbindung Datenquellen wie ISA, Infostar

usw.), d) Erarbeitung und Pflege der organisatorischen und technischen Vorgaben für die Anerkennung von IdP und staatlich anerkannten E-ID-Systemen, e) Beschaffung (öffentliche Ausschreibung) der beim Bund notwendigen IdP-Dienstleistungen, f) Pflege und Publikation der Liste der anerkannten IdP sowie g) Informationsbeschaffung über aktuelle technologische Entwicklungen im Bereich E-ID und zugehörige Fragen der IKT-Sicherheit. Bei der AID wird die personelle Ressource für a) die Anerkennung von IdP (Überprüfen der Konformitätsnachweise) und b) die Überwachung der anhaltenden Konformität der anerkannten IdP und E-ID-Systeme eingesetzt.

Die Höhe der Betriebskosten kann sich im Rahmen der kommenden Ausarbeitung des IKT-Detailkonzepts noch ändern.

3.4.3 Ausgaben des Bundes für IdP-Dienstleistungen

Da der Bund die für seine Portale notwendigen Identitätsdienstleistungen bei den staatlich anerkannten IdP beschaffen muss, fallen Ausgaben an. Diese Ausgaben werden durch die Einsparungen mit dem Wegfall von aktuellen oder zukünftigen IM-Insellösungen des Bundes sowie den Kosteneinsparungen durch die Vereinfachung von Geschäftsprozessen mehr als aufgewogen.

3.4.4 E-ID-Einnahmen Bund

Da der SID ab Betriebsaufnahme für die Übermittlung und die Aktualisierung der an die IdP übermittelten Personenidentifizierungsdaten Gebühren erhebt, werden Einnahmen für den Bund generiert. Bei rund 10 Mio. Abfragen pro Jahr wird die Gebühr voraussichtlich bei einem tiefen zweistelligen Rappenbereich pro Übermittlung liegen. Bei vier Aktualisierungen der Attribute pro Jahr liegen die Kosten für eine E-ID auf dem Sicherheitsniveau Gold so bei deutlich unter einem Franken. Zudem kann der Bund für die Anerkennung und die periodische Überprüfung der Konformitätsnachweise der IdP und ihrer E-ID-Systeme Gebühren erheben.

3.4.5 Betriebliche Erfolgsrechnung

Die Einführung staatlich anerkannter E-ID-Systeme ist ein mehrjähriges, strategisches Vorhaben. Bezüglich Verbreitung der E-ID dürfen deshalb keine unrealistischen Erwartungen formuliert werden, wie dies auch die Erfahrungen anderer Länder zeigen. Bei der E-ID handelt es sich, wie damals bei der brieflichen Stimmabgabe, um ein innovatives Werkzeug, welches in der Bevölkerung zuerst Vertrauen gewinnen muss.

Zudem müssen neben der Etablierung der E-ID auch eine genügende Anzahl attraktiver Online-Anwendungen durch die vertrauenden Beteiligten bereitgestellt werden. Als Investitionsschutzmassnahme könnte gesetzlich vorgesehen werden, dass alle Behörden, die Bundesrecht vollziehen und auf ihren Internet-Portalen eine Authentifizierung verlangen, grundsätzlich verpflichtet werden, auch staatlich anerkannte E-ID-Systeme akzeptieren zu müssen.

Die Betriebskosten des Bundes sollen mittelfristig vollständig durch die Gebühreneinnahmen für die Attributübermittlung und Gebühren für die Anerkennung von IdP kompensiert werden, so dass das Vorhaben für den Bundeshaushalt kostenneutral wird. Zu Beginn wird aber eine „Anschubfinanzierung“ resp. die oben erwähnte „Defizitgarantie“ notwendig sein.

4 E-ID in der Praxis

4.1 Einführung

Dieses Kapitel soll einen Einblick in mögliche zukünftige Anwendungen von staatlich anerkannten E-ID geben. Im Kapitel werden bewusst etwas vereinfachte Begriffe (z.B. „amtliche Personalien“ statt „beim Bund registrierte Personenidentifizierungsdaten“ oder „Aussteller“ statt „Anbieter von Identitätsdienstleistungen / IdP“) verwendet.

4.2 Ausstellung einer E-ID

In einem ersten Schritt hat die Kundin oder der Kunde die freie Wahl, welches der angebotenen E-ID Produkte ihre oder seine Bedürfnisse am besten erfüllt. Angebotene E-ID unterscheiden sich etwa im Sicherheitsniveau, dem Trägermedium (Smartphone, USB-Stick, Smartcard usw.) oder den damit zusammen angebotenen Zusatzdiensten, wie etwa die elektronische Signatur oder die Transaktionsabsicherung. Es ist zulässig, gleichzeitig mehrere staatlich anerkannte E-ID zu besitzen.

In einem zweiten Schritt bezieht die Kundin oder der Kunde die gewählte E-ID. Dies beinhaltet einen Registrierungsprozess beim Aussteller und kann im einfachsten Fall online erfolgen; im Regelfall wird aber eine persönliche Vorsprache beim Aussteller oder zumindest eine Video-identifizierung notwendig sein. Dabei wird die Kundin oder der Kunde anhand eines amtlichen Ausweises identifiziert, mit ihrem/seinem Einverständnis die amtlichen Personalien beim Bund abgerufen, die E-ID personalisiert, der Kundin oder dem Kunden übergeben und vom Aussteller aktiviert.

In einem dritten Schritt kann die Inhaberin oder der Inhaber die E-ID bereits einsetzen. Da staatlich anerkannte E-ID durch die Standardisierungsvorgaben auf den Portalen über weite Strecken identisch funktionieren, ist die Gewöhnungszeit für die Inhaberinnen und Inhaber gering. Dies gilt insbesondere auch bei einen Wechsel des Ausstellers.

4.3 Rückgabe oder Verlust einer E-ID

Geht eine E-ID verloren oder soll sie aus anderen Gründen nicht mehr eingesetzt werden können, kann sie die Inhaberin oder Inhaber beim Aussteller jederzeit sperren oder löschen lassen. Alle Aussteller von staatlich anerkannten E-ID sind verpflichtet, entsprechende Meldestellen anzubieten und gesperrte E-ID in einer Sperrliste zu führen. Diese Sperrliste wird von den vertrauenden Beteiligten konsultiert, wenn sich eine Person mit einer E-ID anmeldet.

4.4 Einsatz einer E-ID

4.4.1 E-Demokratie und E-Partizipation

Die Entwicklung des Internets beeinflusst auch die politische Meinungs- und Willensbildung. Die Bundeskanzlei hat 2011 im Auftrag des Bundesrates einen Bericht zur E-Demokratie und zur E-Partizipation ausgearbeitet [41]. Darin wird der Einfluss des Internets auf die Volksrechte analysiert und werden Zukunftsperspektiven aufgezeigt. Bereiche, in denen Inhaberinnen und Inhaber von E-ID mittelfristig über elektronische Medien am politischen Geschehen partizipieren können, sind:

- Volksabstimmungen

- Eidgenössische Wahlen
- Eidgenössische Volksinitiativen und Referenden
- Eidgenössische Petitionen[28]
- Vernehmlassung und Anhörungen[29]
- Parlamente - Behörden - Gerichte

Im Rahmen der demokratischen Willensbildung folgt nach der Information und der Konsultation die Entscheidung. Das elektronische Abstimmen wird unter dem Stichwort Vote électronique [42] seit der ersten Internetabstimmung am 19. Januar 2003 in Anières (GE) von der Bundeskanzlei und den Kantonen schrittweise vorangetrieben. Nach einer ersten Etappe mit Pilotversuchen in den drei Kantone GE, NE und ZH, die in enger Zusammenarbeit mit dem Bund durchgeführt wurden, hat sich der Bundesrat am 31. Mai 2006 für eine Einführung von Vote électronique in Etappen ausgesprochen. Anlässlich der Volksabstimmung vom 05.06.2016 haben 5 Kantone den elektronischen Stimmkanal angeboten.

Aufsehen erregte im Jahr 2009 das Referendum gegen die Einführung des biometrischen Passes, weil es nicht von einer etablierten Partei frühzeitig angekündigt und dann in herkömmlicher Art und Weise organisiert wurde, sondern weil die Gegner „Facebook“ für die Mobilisierung der Stimmberechtigten nutzten. In einer Motion[30] hatte eine Nationalrätin schon im Jahr davor den Bundesrat aufgefordert, „die gesetzlichen Grundlagen zu schaffen, die es möglich machen, in Pilotprojekten Unterschriften für Initiativen und Referenden elektronisch zu sammeln. Das Projekt E-Collecting ist parallel zu den Projekten E-Voting und E-Government voranzutreiben.“

Der Bundesrat bekräftigte in der Antwort auf die Motion seinen Vorschlag, bei der Digitalisierung der Volksrechte in Etappen vorzugehen. 1. Etappe: Elektronisches Abstimmen. 2. Etappe: Elektronisches Wählen. 3. Etappe: Elektronisches Unterschriftensammeln. 4. Etappe: Elektronische Wahlvorschläge.

4.4.2 E-Government

Obwohl der Begriff E-Government wohl einige Überschneidungen mit anderen Bereichen in diesem Kapitel 4 birgt, seien hier folgende Möglichkeiten eines Einsatzes einer staatlich anerkannten E-ID kurz erwähnt, welche heute teilweise schon mit eigenen Anmeldeverfahren online sind:

- Ausfüllen von Online-Formularen bei Behörden, z.B. für den Umzug, das Einholen von Bewilligungen oder die Beantragung von Ausweisen.
- Zugriff auf Steuerdossiers und Mehrwertsteuerabrechnungen
- Zugriff auf Portale wie E-VERA für Auslandschweizer
- Zugriff auf Portale der Motorfahrzeugkontrollen
- Bestellung eines Strafregisterauszuges

Inhaberinnen und Inhaber von staatlich anerkannten E-ID können sich auf allen Behördenportalen, welche den geplanten eindeutigen Personenidentifikator unterstützen, ohne aufwendige vor-

[28] Alle Personen – also nicht nur Stimmberechtigte – haben das Recht, sich schriftlich mit Bitten, Anregungen und Beschwerden zu jeglicher staatlicher Tätigkeit an zuständige Behörden zu wenden.

[29] Im Vernehmlassungsverfahren werden die Unterlagen durch die Bundeskanzlei in elektronischer Form veröffentlicht. Die Eingabe der Stellungnahme in elektronischer Form ist zulässig, die elektronische Abwicklung des gesamten Verfahrens und die Auswertung der Stellungnahmen sind derzeit aber noch nicht möglich.

[30] 08.3908. Motion Jacqueline Fehr. Stärkung der Demokratie durch E-Collecting. 17.12.2010 Abgeschrieben, weil seit mehr als zwei Jahren hängig.

herige Registrierung sicher anmelden. Beim Bund werden dies gemäss dem aktuellen Gesetzesentwurf alle Portale sein, die eine elektronische Anmeldung verlangen.

4.4.3 E-Health

Die Einführung des elektronischen Patientendossiers ist bereits für 2017 geplant [9]. Inhaberinnen und Inhaber eines elektronischen Patientendossiers respektive ihre gesetzlichen Vertreter müssen sich daran sicher anmelden können. Mit staatlich anerkannten E-ID wird dies möglich sein.

Es ist absehbar, dass für jedes Kind bei seiner Geburt oder im Rahmen der ersten ärztlichen Kontrolle ein solches Dossier eröffnet und anschliessend laufend nachgeführt wird. Bei einem allfälligen Spitalaufenthalt kann den Gesundheitsfachpersonen Zugriff auf das elektronische Dossier gegeben werden und nach Spitalaustritt stehen dem Hausarzt für die Kontrollbehandlungen die medizinischen Daten zur Verfügung. Mittels einer E-Health-App könnte die Patientin oder der Patient zukünftig Gesundheitsdaten registrieren und bei Bedarf der Gesundheitsfachperson zur Verfügung stellen.

Denkbar ist, dass der Patient zukünftig ein E-Rezept erhält, mit dem er die für die Behandlung notwendigen Medikamente bei einer Online-Apotheke bestellen kann. Im Weiteren könnte auch eine medizinische Online-Beratung eingebunden werden (E-Consultation).

4.4.4 E-Education

Die Digitalisierung hat in den Volks- und Hochschulen schon lange Einzug gehalten. So stehen heute vermehrt digitale Lehrmittel zur Verfügung, welche oft erst nach einer Anmeldung am Portal der Schule oder des Lehrmittelverlages zugänglich sind. Auch Zeugnisse oder Schulinformationen werden immer öfter elektronisch angeboten. Mit einer E-ID können Schülerinnen und Schüler Zugriff auf diese Ressourcen der Schule erhalten.

Die Eltern wiederum haben mittels ihrer E-ID Zugriff auf Informationen der Schule und bestätigen digital die Einsichtnahme ins Zeugnis ihres Kindes, um ihren Rechten und Pflichten während der Schul- und Ausbildungszeit nachzukommen.

Auf einer höheren Schulstufe sind heute schon das Einschreiben und die Fächerbelegung über elektronische Medien möglich. Auch diese erfordern eine elektronische Anmeldung, welche mit der staatlich anerkannten E-ID sicher erfolgen kann. Im Hochschulbereich sind dann auch Einsätze der E-ID über die Landesgrenzen hinweg wahrscheinlich.

4.4.5 E-Commerce

Inhaberinnen und Inhaber können die E-ID bei Online-Shops einsetzen, um sich zu Registrieren und sich später erneut sicher anzumelden. Online-Shops können und sollen gesetzlich nicht gezwungen werden, staatlich anerkannte E-ID zu akzeptieren. Aus Sicht der Inhaberin oder des Inhabers ist es jedoch sehr praktisch, wenn diese es dennoch tun. Denn dann müssen sie sich nicht mit x-verschiedenen unterschiedlichen Benutzernamen und Passworten herumschlagen, sondern können ihre staatlich anerkannte E-ID universell einsetzen. Da für staatlich anerkannte E-ID zudem ein transparenter Rechtsrahmen geschaffen wird, sind auch die Rechte und Pflichten klar geregelt. So soll es den Online-Shops als vertrauende Beteiligte z.B. verboten werden, mit den vom IdP übermittelten staatlichen Personenidentifizierungsdaten zu handeln. Solche Daten werden vom ausstellenden IdP nur übermittelt, wenn die Inhaberin oder der Inhaber damit ausdrücklich einverstanden ist.

Zudem ist es mit der E-ID sehr einfach und zuverlässig möglich, sein Alter nachzuweisen. Sei es nun ein Höchstalter für Angebote für Jugendliche oder aber auch ein Mindestalter für Angebote für Erwachsene oder auch Pensionierte.

4.4.6 E-Payment

Das Bezahlen mit Mobile Payment wird immer beliebter. Mit der E-ID geht es noch einfacher, den digitalen Identitätsnachweis für das Erlangen einer digitalen Bezahllösung zu erbringen. Im Rahmen der Registrierung kann der Identitätsnachweis medienbruchfrei digital erfolgen, wodurch die Anwendung schnell freigeschaltet und genutzt werden kann. Mobiles Bezahlen ist on- aber auch offline möglich und für den ganzen E-Commerce-Bereich eine zukunftsträchtige Lösung.

4.4.7 E-Banking

E-Banking gewinnt laufend an Bedeutung. Gemäss dem Bundesamt für Statistik nutzten 2015 über 49% der Bevölkerung die Möglichkeiten von E-Banking [1]. Auch hier ist die sichere Registrierung und Anmeldung beim Portal zwingend für die vertrauenswürdige Geschäftsabwicklung. Eine staatlich anerkannte E-ID auf dem Sicherheitsniveau Gold oder Platin könnte die proprietären Lösungen der Banken ersetzen und ihnen so mittelfristig grosse Einsparungen bringen.

4.4.8 E-Ausweise

Etwas weiter in die Zukunft geblickt, aber immerhin schon von einigen Firmen [43] [44] versuchsweise angeboten, sind „hoheitliche elektronische Ausweise“, kurz E-Ausweise. Das sind quasi die elektronischen Pendants zu physischen hoheitlichen Ausweisen wie Pass, Identitätskarte oder auch Führerausweis.

E-Ausweise können bei einer physischen Begegnung mit einer vertrauenden Beteiligten zum Nachweis der eigenen Identität verwendet werden, etwa für einen Altersnachweis in einem Verkaufspunkt oder auch bei einer Identitätsüberprüfung. Dabei wird der Inhaberin oder dem Inhaber auf der Anzeige eines geeigneten Trägergerätes ein lesbares Bild des E-Ausweises angezeigt, das mit einer geeigneten Leseapplikation via IdP elektronisch überprüft werden kann. Dies hilft, eine gedankliche Brücke zwischen der rein elektronischen E-ID und den konventionellen Ausweisen zu schaffen.

Selbstverständlich sind es nicht einfach „Bilder“ von Ausweisen, welche bei E-Ausweisen kontrolliert werden, sondern im Hintergrund wirken die Verfahren und Sicherheitsmechanismen einer klassischen staatlich anerkannten E-ID. Die für E-Ausweise notwendigen zusätzlichen Funktionen können aber ohne grossen Aufwand seitens IdP und vertrauende Beteiligte umgesetzt werden.

4.4.9 Elektronische Signaturen

Mit der Revision des Bundesgesetzes über die elektronische Signatur (ZertES) [45] ist es möglich, elektronische Signaturen als „Vertrauensdienst“ online anzubieten. Die Inhaberin oder der Inhaber einer staatlich anerkannten E-ID kann sich also bei einem entsprechenden Anbieter online Registrieren und die Dienstleistung, z.B. serverbasierte qualifizierte elektronische Signaturen, unmittelbar nutzen. Da die staatlich anerkannte E-ID auf dem erforderlichen Sicherheitsniveau verfügbar ist, erübrigt sich ein Vorsprechen beim Anbieter des Signaturdienstes, was Zeit und Kosten spart.

4.4.10 Abonnemente

Da mit der geplanten staatlich anerkannten E-ID ab dem Sicherheitsniveau Gold auch das staatlich verbürgte Gesichtsbild (Foto des Ausweises) übermittelt werden kann, können auch Ausweise, welche ein Foto erfordern, online bestellt werden. Dies könnte zum Beispiel für Anbieter im öffentlichen Verkehr aber auch für den Tourismus interessant sein. Die Inhaberinnen und Inhaber von E-ID müssen so nicht am Schalter anstehen, sondern können die benötigten Ausweise

mit Foto online lösen und z.B. auf eine App oder per Post nach Hause gesandt erhalten.

Der E-ID könnten mittels Mobilitäts-App zusätzliche Funktionen angeschlossen werden. Dabei kann für die Registrierung und Anmeldung die E-ID genutzt und Abonnemente und Billette online über die Mobilitäts-App eingekauft und nachgewiesen sowie die Kosten für eine separate Abonnement- oder Billettausgabe eingespart werden.

4.4.11 Sharing Economy

Die Sharing Economy, auch Collaborative Economy [46], wächst immer weiter und darin ist noch viel Potential vorhanden. Die Collaborative Economy (Car-Sharing, Wohnungs-Sharing, Freelancer-Plattformen, usw.) ist dabei oft auf die sichere Identifizierung der Geschäftspartnerin oder des Geschäftspartners angewiesen. Dieses Bedürfnis kann mit staatlich anerkannten E-ID auf den verschiedenen Sicherheitsniveaus abgedeckt werden.

4.4.12 Cloud Computing

Ebenso wie die Virtualisierung verspricht Cloud Computing Kostenvorteile gegenüber konventionellen Systemen. Mit Cloud Computing lassen sich IKT-Systeme wesentlich effizienter auslasten als dezidierte Einzelsysteme und so die IKT-Ressourcen nachhaltiger planen und einsetzen. Zum Schutz vor unerlaubtem Zugriff auf die Daten in der Cloud können E-ID in Kombination mit weiteren kryptographischen Verfahren eingesetzt werden.

4.4.13 Social Media

Obwohl Personen in den Social Media auch mit einem Pseudonym unterwegs sein können, gibt es Anwendungen, z.B. Foren mit besonderen Mitgliederanforderungen, welche eine vertrauenswürdige Registrierung erfordern. So sind Foren, welche für Kinder oder Jugendliche bestimmt sind, vor Erwachsenen zu „schützen“. Mit staatlich anerkannten E-ID ist dies sehr einfach möglich, da mit der E-ID ein zuverlässiger Altersnachweis erbracht werden kann.

5 Informations- und Datenschutz

5.1 Einführung

Informations- und Datenschutz und die IKT-Sicherheit im Allgemeinen sind für das Vertrauen in staatlich anerkannte E-ID wichtig. Das aktuelle Benutzerverhalten im Markt zeigt jedoch auch, dass die Benutzerfreundlichkeit einer Lösung für die Akzeptanz entscheidend ist. Von der Industrie werden grosse Anstrengungen unternommen, sichere und dennoch benutzerfreundliche Endgeräte, welche sich als Träger von E-ID eignen, auf den Markt zu bringen (z.B. Mobiltelefone mit Trusted Execution Environment [47]). Es gilt also, eine gangbare Balance zwischen Sicherheit und Benutzerfreundlichkeit zu finden.

Das vorliegende Konzept geht von einer Aufgabenteilung zwischen Staat und Markt aus, womit implizit das grundsätzliche Vertrauen in marktwirtschaftlich erbrachte Identitätsdienstleistungen vorausgesetzt wird. Obschon die Sicherheit aller Komponenten, Systeme und beteiligten Organisationen im E-ID-Ökosystem wichtig ist, kann der Staat nicht alle Sicherheitsmassnahmen gegen alle Bedrohungen im gesamten E-ID-Ökosystem implementieren und verantworten. So kann ein staatlich anerkannter IdP zum Beispiel neben den Personenidentifizierungsdaten weitere Attribute aus anderen Quellen erfassen und verwalten. Die Verantwortung dafür muss der IdP aber selbst tragen.

Gestützt auf das Bundesgesetz über den Datenschutz (DSG), die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV), die Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV), die Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) und das IKT-Sicherheitsleitbild der Bundesverwaltung sollen deshalb die Bedrohungen und Risiken im E-ID-Umfeld bestimmt und die notwendigen Massnahmen umgesetzt werden. Dazu werden für die beteiligten Systeme eine Schutzbedarfsanalyse (einschliesslich RINA) und ISDS-Konzepte erarbeitet und die Anforderungen des IKT-Grundschutzes umgesetzt werden.

Durch die Schaffung einer formellgesetzlichen Grundlage für staatlich anerkannte E-ID sollen ergänzende Datensicherheits- und Datenschutzvorgaben für die beteiligten Organisationen und technischen Systeme erlassen werden.

5.2 Eindeutiger Personenidentifikator

Im E-ID-Ökosystem ist der eindeutige Personenidentifikator für die Datenintegrität - hier verstanden als korrekte Zuweisung von Personenidentifizierungsdaten zur Person – und das Vertrauen in E-ID sehr wichtig. So hat die ZAS[31] im Bereich der Sozialversicherungen mit der Schaffung des UPI („Unique Person Identification“, AHVN13) genau dieses Ziel bereits umgesetzt und kann so die korrekte Geschäftsabwicklung sicherstellen.

Zu einem EPID lassen sich bei Bedarf sektorielle Identifikatoren bilden. Sei dies durch eine Einwegfunktion oder durch eine tabellarische Zuordnung, wie dies im Falle der E-Patientennummer bereits geschieht, welche bei der ZAS zusammen mit der AHVN13 gespeichert ist.

Ein EPID führt unseres Erachtens entgegen der manchmal geäusserten Meinung zu keiner Minderung des Schutzes der persönlichen Daten. Im Gegenteil, er vermindert die Gefahr von Verwechslungen oder Inkonsistenzen von Personenidentifizierungsdaten, welche der betroffenen

[31] Die Zentrale Ausgleichsstelle ZAS (ZAS) ist eine Hauptabteilung der Eidgenössischen Finanzverwaltung. Sie betreibt den Dienst „ZAS-UPI“, welcher natürlichen Personen eine AHVN13 zuteilt, sowie eine „Clearingstelle“ zur Datenberichtigung.

Person schaden können. Zudem vermeidet ein EPID die für eine eindeutige Identifizierung üblicherweise zwingend notwendige Offenlegung von weiteren Personenidentifizierungsdaten wie Name, Vorname und Geburtsdatum, die jedermann ohne weiteres im täglichen Leben einer physischen Person zuordnen kann.

5.3 Schutzbedarf

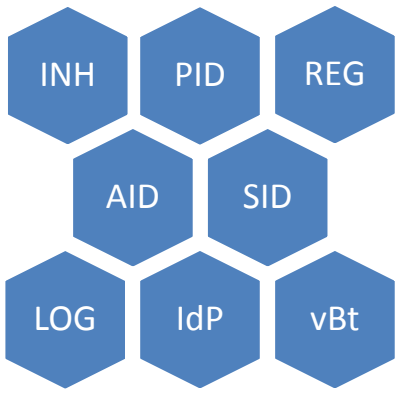
Die Schutzbedarfsanalyse hat aufgezeigt, dass staatlich anerkannte E-ID-Systeme Personendaten gemäss DSG verarbeiten, welche im Einzelfall besonders schützenswert sein können. Nämlich dann, wenn aus dem Foto einer Person, welches auf dem Sicherheitsniveau Gold und Platin übermittelt wird, Informationen zur Rassen- oder Religionszugehörigkeit oder den Gesundheitszustand einer Person herausgelesen werden können.

Nach ISchV sind die Personenidentifizierungsdaten weder als vertraulich noch geheim sondern als intern zu klassifizieren. Bezüglich Verfügbarkeit der Infrastruktur des Bundes bestehen keine erhöhten Anforderungen, bezüglich Integrität und Nachvollziehbarkeit hingegen schon. Da der Bund nach vorliegendem Konzept für seine Portale von den staatlich anerkannten IdP IAM-Dienstleistungen beziehen wird und diese je nach Portal auch BCM-relevant sein können, sind nach RINA besondere Sicherheitsmassnahmen zu ergreifen. Diese Sicherheitsmassnahmen finden auch Eingang in die Gesetzgebung.

5.4 Schutzobjekte

Aus Sicht Datenschutz ist der Mensch das Schutzobjekt und die Technik das Risiko. Aus Sicht IKT-Sicherheit ist die Technik das Schutzobjekt und der Mensch das Risiko. Die Priorität zur Bestimmung der Schutzmassnahmen geht im ersteren Fall von Recht über Organisation zur Technik, um zweiten Fall genau umgekehrt.

Nachfolgende Abbildung gibt einen groben Überblick über die Schutzobjekte staatlich anerkannter E-ID-Systeme, für welche aus Sicht Datenschutz und IKT-Sicherheit Massnahmen zu definieren sind (Legende nachstehend):



Skizze 16: Schutzobjekte

Abk.	Details
INH	Inhaberin oder Inhaber einer staatlich anerkannten E-ID einschliesslich der von ihr/ihm verwendeten technischen Infrastruktur wie Smartphone, Tablet oder PC.

Abk.	Details
REG	Personenregister, welche beim Bund die Personenidentifizierungsdaten enthalten (Infostar, ISA, ZEMIS, ZAS-UPI), einschliesslich des Personals und der technischen Systeme.
PID	Einzelner Datensatz mit Personenidentifizierungsdaten wie Name, Vorname, Geburtsdatum, Foto usw.
LOG	Protokolldaten über die Übermittlung von Personenidentifizierungsdaten und die Verwendung staatlich anerkannter E-ID, welche von den beteiligten Stellen gesammelt werden (müssen).
AID	Anerkennungsstelle für Identitätsdienstleister einschliesslich des Personals und der technischen Systeme.
SID	Schweizerische Stelle für elektronische Identität einschliesslich des Personals und der technischen Systeme.
IdP	Anbieter von Identitätsdienstleistungen einschliesslich des Personals und der technischen Systeme, welche für die Herausgabe der staatlich anerkannten E-ID im Einsatz stehen
vBt	Vertrauende Beteiligte, einschliesslich des Personals und der technischen Systeme, welche im Zusammenhang mit dem Einsatz einer staatlich anerkannten E-ID stehen.

Tabelle 6: Legende Schutzobjekte

5.5 Risiken

Aus Bedrohungen und Schwachstellen entstehen Risiken, welche zu einem Schaden führen können. Ein Risiko ist die Wahrscheinlichkeit, dass sich eine Bedrohung realisiert, multipliziert mit dem Schadenspotenzial. Bedrohungen für die IKT-Sicherheit sind zum Beispiel vorsätzliche Handlungen von Innen- oder Aussentätern, höhere Gewalt und technisches Versagen und menschliche Unzulänglichkeiten wie Nachlässigkeit oder Irrtum. Bedrohungen für den Datenschutz sind zum Beispiel ungenügende rechtliche Regelungen, vorsätzliche Handlungen von Innen- und Aussentätern und Fehlfunktionen von IKT-Systemen.

Die grössten Risiken für staatlich anerkannte E-ID-Systeme sind:

Abk.	Risiko
INH	Verletzen der Sorgfaltspflicht und Identitätsmissbrauch Auch staatlich anerkannte E-ID müssen gemäss den Vorgaben und mit der notwendigen Umsicht eingesetzt werden. Ein Verletzen der Sorgfaltspflicht wäre z.B. das Notieren der PIN auf einer E-ID oder der vollständige Verzicht auf Virenscanner. Identitätsmissbrauch wäre die Nutzung der eigenen E-ID durch Dritte, z.B. indem diese dem Dritten (z.B. dem Lebenspartner) zur Nutzung überlassen wird.
REG	Datendiebstahl Die in den Personenregistern beim Bund verzeichneten Daten müssen insbesondere gegen den Massendatendiebstahl und die Datenverfälschung im Einzelfall geschützt werden.

Abk.	Risiko
PID	Datenverfälschung Eine Verfälschung eines Datensatzes mit Personenidentifizierungsdaten kann zu einem Schaden führen.
LOG	Datenmissbrauch Beim Einsatz von IKT, wie sie auch die E-ID sind, fallen grundsätzlich Protokolldaten an, welche ausgewertet werden können. Diese Protokolldaten müssen gegen missbräuchliche Verwendung, wie z.B. unerlaubte Profilbildung, geschützt werden.
AID	Verletzen der Sorgfaltspflicht Die Anerkennung und die Aufsicht über IdP muss mit der notwendigen Sorgfalt und Unabhängigkeit durchgeführt werden. Dazu sind vom SID sorgfältig erarbeitete Schutzprofile notwendig.
SID	Datendiebstahl und Datenverfälschung, fehlendes IKT-Sicherheitswissen Die vom SID bearbeiteten Daten müssen gegen Diebstahl und Verfälschung geschützt werden. Unter Datendiebstahl wird auch eine unzulässige Übermittlung von Personenidentifizierungsdaten an einen IdP verstanden. Die vom SID für die Anerkennung der E-ID-Systeme bereitgestellten Schutzprofile müssen den aktuellen Technologien und Bedrohungen entsprechen.
IdP	Datendiebstahl Die E-ID-Systeme der staatlich anerkannten IdP müssen insbesondere gegen den Massendatendiebstahl und die Datenverfälschung im Einzelfall geschützt werden. Unter Datenverfälschung wird auch eine technische Fehlfunktion der E-ID oder eine fehlerhafte Registrierung einer Person verstanden.
vBt	Datendiebstahl und Datenmissbrauch Die technischen und organisatorischen Prozesse beim vBt müssen einen fehlerfreien Einsatz einer staatlich anerkannten E-ID zulassen. Ein Fehler wäre z.B. eine nicht korrekt durchgeführte Authentifizierung. Die Daten beim vBt sollen insbesondere gegen Massendatendiebstahl und Datenmissbrauch geschützt sein.

Tabelle 7: Grösste Risiken

Weitere Risiken grundsätzlicher Art sind:

Abk.	Risiko
NUL	Fehlende Anbieter von Identitätsdienstleistungen Falls sich kein Anbieter von staatlich anerkannten E-ID im Markt etabliert, ist das Konzept der Aufgabenteilung zwischen Staat und Markt gescheitert. Davon ausgehend, dass dennoch eine staatlich anerkannte E-ID eingeführt werden soll, muss eine Rückfalllösung bestehen.
FIN	Monopol eines Anbieters von Identitätsdienstleistungen Das Konzept beruht auf der Annahme, dass sich im E-ID-Ökosystem mehrere Anbieter von staatlichen E-ID etablieren und so ein Wettbewerb besteht. Falls kein Wettbewerb zustande kommt gilt es zu verhindern, dass die Preise für staatlich anerkannte E-ID eine Fehlentwicklung nehmen.

Abk.	Risiko
KET	Verkettung von Schadensereignissen An staatlich anerkannten E-ID sind zahlreiche Einzelsysteme (wie Infostar, ISA, IdP usw.) beteiligt, welche organisatorisch und technisch gekoppelt werden. Es muss verhindert werden, dass das Versagen eines Teilsystems die anderen Teilsysteme ebenfalls zu Fall bringt.
KOV	Kontrollverlust über staatlich anerkannte E-ID-Systeme Eine Kontrolle staatlich anerkannter E-ID-Systeme durch ausländische Stellen wäre politisch nicht zu vertreten. Sie sollen „in der Hand“ der Schweiz sein.
AUS	Ausspähung staatlich anerkannter E-ID-Systeme Staatlich anerkannte E-ID verfügen als solche ausser den Personenidentifizierungsdaten über keine weiteren Merkmale einer Person. Insbesondere geben sie keine Auskünfte über Mitgliedschaften, Funktionen, politische Gesinnungen und Fähigkeiten von Personen. E-ID können jedoch zur Beschaffung solcher Informationen genutzt werden, insbesondere wenn ein Identitätsmissbrauch stattfindet.

Tabelle 8: Weitere Risiken

Eine vertiefte Risikobetrachtung gemäss dem „Handbuch Risikomanagement Bund vom 29. April 2013“ wird im Rahmen der Erarbeitung des Detailkonzepts und der Ausführungsbestimmungen zum E-ID-Gesetz durchgeführt.

5.6 Sicherheitsmassnahmen

Gestützt auf die Schutzbedarfsanalyse (Kapitel 5.3), die Liste der Schutzobjekte (Kapitel 5.4) sowie der Risiken (Kapitel 0) sind nachfolgend die wichtigsten Sicherheitsmassnahmen aufgeführt, welche für staatlich anerkannte E-ID-Systeme ergriffen werden sollen:

Abk.	Sicherheitsmassnahmen
INH	gegen Verletzung der Sorgfaltspflicht und des Identitätsmissbrauch Rechtliche Vorgaben (z.B. Handhabung, Meldepflicht); aktive Information der Inhaberinnen und Inhaber.
REG	gegen Datendiebstahl Keine zusätzlichen Massnahmen. Die Personenregister werden heute schon konform mit den Vorgaben vom Bund betrieben.
PID	gegen Datenverfälschung Konsequente Einführung eines eindeutigen Personenidentifikators; Signatur der Personenidentifizierungsdaten.
LOG	gegen Datenmissbrauch Rechtliche Vorgaben (z.B. Verbot von Handel mit Profilen); Audits im Rahmen der Anerkennung und Aufsicht.
AID	gegen Verletzung der Sorgfaltspflicht Kontrollierte Prozesse (ev. ISO27000-Zertifizierung); Personensicherheitsprüfung.

Abk.	Sicherheitsmassnahmen
SID	gegen Datendiebstahl und Datenverfälschung, fehlendes IKT-Sicherheitswissen Aktuelle Personenidentifizierungsdaten; kontrollierte Prozesse (ev. ISO27000-Zertifizierung); Personensicherheitsprüfung; Digitale Signatur; sicherer Kommunikationskanal; Datensparsamkeit; Sperrlisten (z.B. mit verstorbene Inhaberinnen und Inhaber); konsequente Weiterbildung und Zusammenarbeit mit IKT-Sicherheitsspezialisten.
IdP	gegen Datendiebstahl Aktuelle Personenidentifizierungsdaten; Verwendung eines eindeutigen Personenidentifikators; rechtliche Vorgaben (z.B. Schutzprofile nach ISO/IEC 15408, Datenhaltung in der Schweiz, Haftung, Löschfristen, Sperrlisten); staatliche Anerkennung und Aufsicht; technologisch aktuelle Vorgaben für die Anerkennung ; kontrollierte Prozesse (ev. ISO 27000-Zertifizierung); Personensicherheitsprüfung.
vBt	gegen Datendiebstahl und Datenmissbrauch Rechtliche Vorgaben (z.B. Haftung, Vorgaben für den Schutz der Personenidentifizierungsdaten); kontrollierte Übermittlung von Personenidentifizierungsdaten durch den IdP (z.B. die AHVN13 gestützt auf eine Whitelist).
NUL	gegen fehlende Anbieter von Identitätsdienstleistungen Attraktive Rahmenbedingungen für IdP; Rückfalllösung (Herausgabe einer E-ID durch Bund).
FIN	gegen ein Anbietermonopol Attraktive Rahmenbedingungen für IdP; rechtliche Vorgaben für Preise.
KET	gegen die Verkettung von Schadensereignissen Lose Kopplung der Systeme; Risikoanalyse und BCM; geregelte Verantwortlichkeiten.
KOV	gegen den Kontrollverlust über staatlich anerkannte E-ID-Systeme benutzerzentrische Systeme (z.B. ausdrückliche Einverständnis für die Übermittlung von Personenidentifizierungsdaten); rechtliche Vorgaben und Sicherheits-EK („Schweizer Recht und Gerichtsstand“, „Datenbearbeitung in der Schweiz“, „Keine Pflicht zur Datenherausgabe“); geregelte Verantwortlichkeiten.
AUS	gegen Ausspähung von staatlich anerkannten E-ID-Systemen Rechtliche Vorgaben (z.B. Datensparsamkeit, Verbot von Profilbildung, Löschfristen); Sicherheits-EK („Keine Pflicht zur Datenherausgabe“)

Tabelle 9: Sicherheitsmassnahmen

6 Rechtsetzung

6.1 Allgemein

Durch die Schaffung eines transparenten Rechtsrahmens sollen folgende Ziele erreicht werden:

- Minderung resp. Verhinderung von Identitätsmissbrauch und Identitätsverfälschung in der digitalen Welt;
- Förderung des sicheren elektronischen Geschäftsverkehrs unter Privaten und mit Behörden; und
- Interoperabilität und Durchgängigkeit von E-ID-Systemen innerhalb der Schweiz und mit der EU (Notifikation).

Die Vorgaben werden durch das noch zu schaffende E-ID-Gesetz, die zugehörigen Ausführungsbestimmungen sowie die notwendigen Standards gebildet und umfassen die rechtlichen, organisatorischen und technischen Vorgaben für

- den Inhalt, die Ausstellung, den Betrieb, die Verwaltung, den Entzug und den Einsatz staatlich anerkannter E-ID;
- die staatliche Anerkennung von IdP und die Aufsicht über anerkannte IdP sowie ihre E-ID-Systeme;
- die Schnittstelle zur Übermittlung staatlicher Personenidentifizierungsdaten an IdP;
- die Interoperabilität der E-ID-Systeme.

Die gesamte Regulierung muss so ausgestaltet werden, dass damit ein Vertrauensrahmen für ein nachhaltiges E-ID-Ökosystem entsteht, das Basis für die weitere Entwicklung der digitalen Märkte ist. Wo möglich und sinnvoll ist auf internationale Standards oder im Markt bereits etablierte Vorgaben abzustützen. In dem bestehenden dynamischen technischen Umfeld der E-ID ist es unbedingt sinnvoll, die Regelung der technischen und organisatorischen Feinheiten auf Stufe Ausführungsbestimmungen zu regeln. So soll das Gesetz lediglich die Ziele der Kategorien von E-ID, hier Sicherheitsniveaus genannt, definieren. Wie diese technisch und organisatorisch ausgestaltet werden, soll der Bundesrat entscheiden können, einschliesslich Einschränkungen bezüglich Weitergabe von bestimmten Attributen (z.B. die AHVN13) an bestimmte vertrauende Beteiligte. Hingegen soll das Gesetz die Konsequenzen bei einem Missbrauch durch die beteiligten Stellen regeln, z.B. kann beim anerkannten IdP ein Entzug der Zulassung möglich sein.

Welches Sicherheitsniveau für welche Art der Anwendung in Frage kommt, wird grundsätzlich von den vertrauenden Beteiligten definiert. So kann für Vote électronique ein anderes Sicherheitsniveau der E-ID gewählt werden, als es für die E-Health-Anwendungen vorgeschrieben oder für E-Education notwendig ist.

6.2 Verhältnis zu anderen Gesetzen

Im Rahmen der Rechtsetzungsarbeiten werden Berührungspunkte mit anderen Gesetzen im Detail geprüft und ausgewiesen. Gegebenenfalls werden im Rahmen der „Änderung anderer Erlasse“ auch Anpassungen vorgenommen. Klare Regelungen bezüglich Haftung und Verantwortung der IdP und/oder Zertifizierungsdienste werden angestrebt.

7 Anhang

7.1 Begriffsdefinitionen

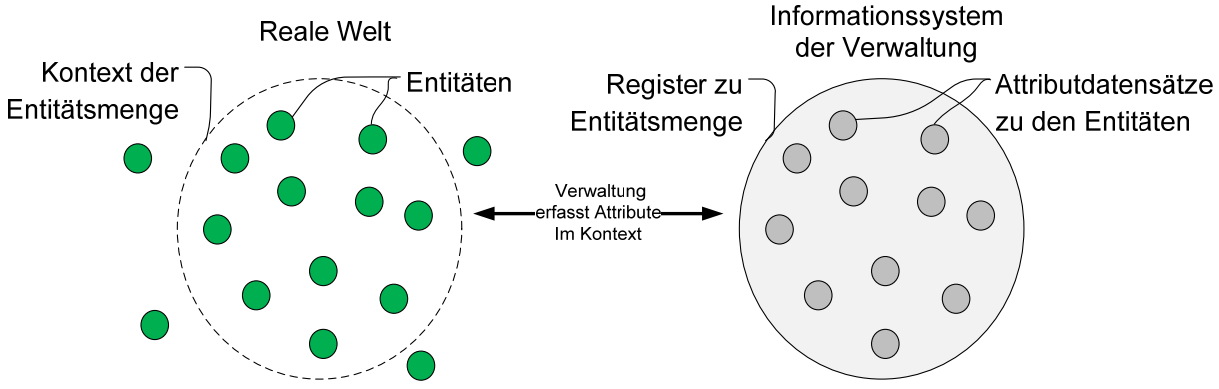
Im Kontext des E-ID-Konzepts 2016 und damit auch für den Gesetzgebungsentwurf (Bundesgesetz über anerkannte elektronische Identifizierungseinheiten) verwenden wir eine Reihe von Begriffen, deren Bedeutungen hier definiert und in einen semantischen und logischen Zusammenhang gebracht werden. Die folgenden Abschnitte erklären die verwendeten Begriffe soweit als nötig, ohne alle Details des wissenschaftlichen Diskurses abzubilden.

A. Grundbegriffe

Der Grundbegriff der Identität ist ein sehr facettenreicher Begriff, der in seinen vielen Bedeutungen philosophisch, psychologisch, rechtlich, ökonomisch und technisch vielfach analysiert wurde und wird. Eine gute Übersicht ist zum Beispiel durch das europäische Network of Excellence - FIDIS geschaffen worden [48]. Im Kontext des Rechtssetzungsverfahrens wird der Begriff der Identität in einer etwas eingeschränkten rechtlichen und technischen Sichtweise gebraucht, wie er zum Beispiel durch NIST [49] und die EU [2] gebraucht wird. Unser Definitionsschema basiert auch auf dem Informationsmodell aus den eCH-Standards [50] [7] [51].

1. Entitäten, Entitätsmengen und Attribute

Ausgangspunkt in diesem Ansatz ist die Aussensicht aus der Position einer Verwaltung[32] auf eine Menge von materiellen oder immateriellen Einheiten in der realen Welt, die als **Entitäten** bezeichnet werden. Die Gesamtheit der relevanten Entitäten ist durch den Verwaltungskontext definiert und wird als **Entitätsmenge** bezeichnet[33]. Eine **Entität** wird aus Sicht und im Kontext der Verwaltung eine Reihe von Eigenschaften haben, die durch sie mit einer gewissen Sicherheit festgestellt werden können und die dann eine Entität als Datensatz von **Attributen** in einem Informationssystem der Verwaltung repräsentieren.



Skizze 17: Attribute als für den Verwalter relevante Eigenschaften der Entitäten

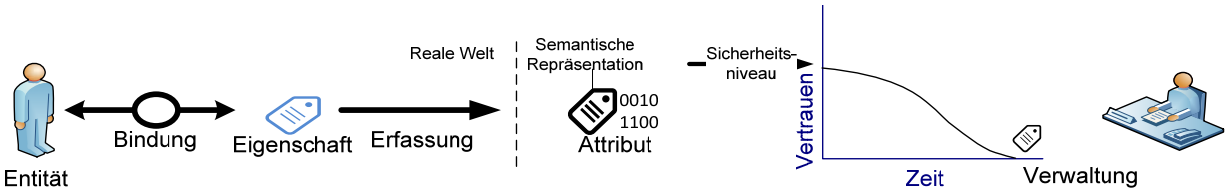
Ein Attribut setzt sich zusammen aus dem **Attributnamen**, dem **Attributwert** und allfällig weiteren Metadaten wie z.B. einer Datentypisierung oder einem Gültigkeitsdatum. Der Name definiert die semantische Bedeutung des Attributs und damit den Bereich der möglichen Attributwerte. Der Attributwert ist das Resultat einer Attributbestimmung für eine einzelne Entität.

---

[32] Die Verwaltung ist eine Instanz, die Entitäten verwaltet und ihnen Rollen oder Rechte zuordnen kann. Typischerweise ist dies eine vertrauende Beteiligte, ein Identitätsdienstleister oder eine staatliche Organisation.

[33] In den eCH-Standards [7] [51] [50] wird die Entität nur als Person verstanden und dann als *Subjekt* bezeichnet. Die Entitätsmenge und die dazugehörige Verwaltung entsprechen den Begriffen *Namensraum und Ressource.*

Dem Attributwert zugeordnet ist implizit auch die Sicherheit, mit der ein Attributwert bestimmt wurde und auf der das Vertrauen der Verwaltung in die Richtigkeit der Zuordnung basiert. Das Vertrauen der Verwaltung ergibt sich aus der Stärke der Bindung der Eigenschaft zur Entität, dem Gewähr, dass der zugehörige Attributwert richtig erfasst wurde, bzw. der Verlässlichkeit der Quelle, aus der das Attribut bezogen wurde, und aus der verflossenen Zeit seit der Attributbestimmung. So ist zum Beispiel die Feststellung der Echtheit einer bestimmten SIM-Karte sehr sicher, hingegen ist die Bindung des Handys als Träger der SIM-Karte zur Person nicht sehr stark. Auf der anderen Seite ist ein biometrisches Merkmal fest mit der Person verbunden, bei der Messung verbleibt aber eine gewisse Unsicherheit, ob der festgestellte Attributwert richtig erfasst und zugeordnet wurde. Je nach Kontext ist das resultierende Vertrauen der Verwaltung in die Richtigkeit des Attributwerts und dessen Zuordnung zu einer Person ausreichend oder nicht. Generell nimmt das Vertrauen in eine einmal gemachte Attributbestimmung mit der Zeit ab. Deshalb werden Attribute ab und zu neu erfasst, um die Stärke des Vertrauens aufrecht zu erhalten.



Skizze 18: Sicherheit eines Attributs und zeitabhängiges Vertrauen

Falls der Wert eines Attributs für alle Entitäten mit ausreichender Sicherheit bestimmt ist, kann die zugrundeliegende Entitätsmenge in Teilmengen aufgeteilt werden, in denen je alle Entitäten den gleichen Attributwert zugeordnet haben[34]. Ein Beispiel dafür ist die Partition einer Menge von Personen nach dem Attribut *Geburtsdatum*. Die einzelnen Teilmengen dieser Partitionierung sind durch die Personen gebildet, die je das gleiche Geburtsdatum als Attributwert haben. Verschiedene und voneinander unabhängige oder nur schwach korrelierte Attribute führen zu unterschiedlichen Partitionen der Entitätsmenge. Es gibt dabei Attribute, die eine Entitätsmenge stark partitionieren und solche, die Entitäten nur gering separieren oder keine neue Information bieten, wie zum Beispiel das Geburtsjahr, wenn das Geburtsdatum schon bekannt ist.

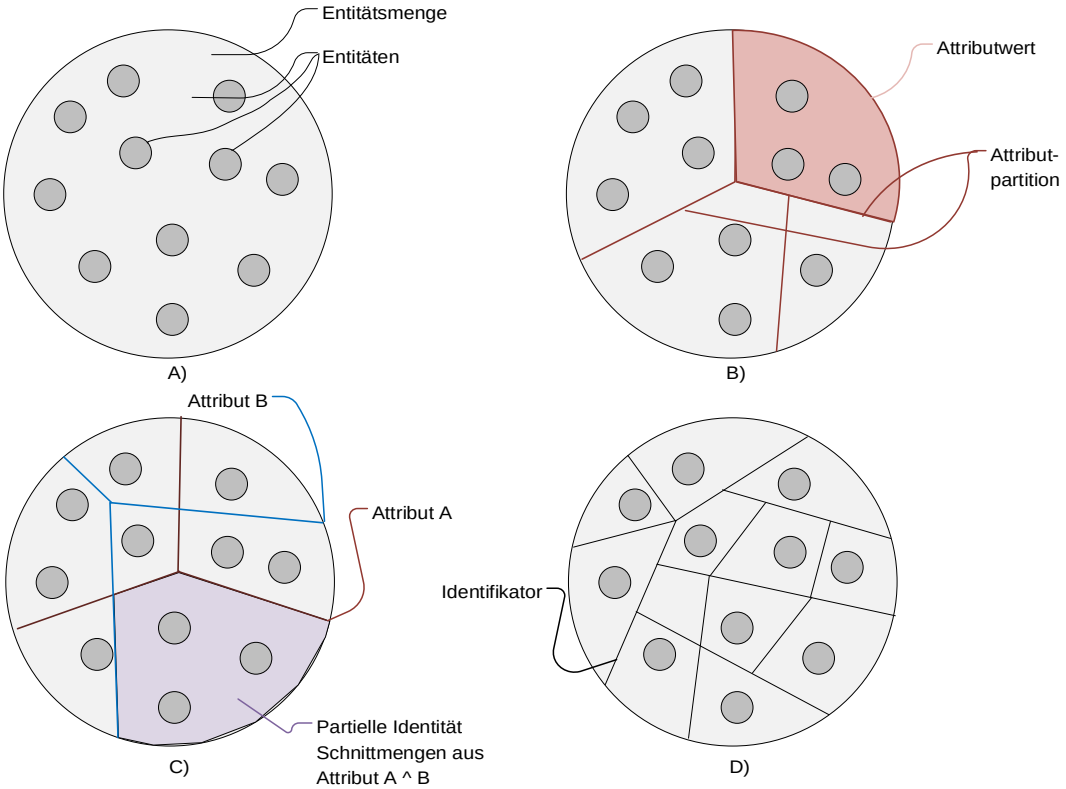
2. Kombination von Attributen

Durch mehrere möglichst unabhängige Attribute kann eine Entitätsmenge, genauer die Menge der zu den Entitäten gehörenden Datensätze mit den erfassten Attributen, so mehrfach partitioniert werden. Nur wenn in den Schnittmengen dieser Attributpartitionen je nur noch maximal ein einziger einer Entität zugeordneter Attributdatensatz verbleibt, können alle Entitäten in der Entitätsmenge durch die sie repräsentierenden Datensätze mit den erfassten Attributen unterschieden werden. In diesem Fall ist die Kombination der festgestellten Attribute auf der entsprechenden Vertrauensstufe **identifizierend**. Generell wird ein Datensatz von Attributen für eine Entität als **partielle Identität** bezeichnet. Sind die Attribute identifizierend ist es eine identifizierende partielle Identität.

[34] Formal ist eine Attributbestimmung eine Abbildung von der Entitätsmenge in den Raum der Attributwerte. Eine eindeutige Partition der Entitätsmenge ergibt sich nur, wenn für jede Entität ein Attributwert auf einem verlangten Sicherheitsniveau eindeutig bestimmt ist. Die Partition der Entitätsmenge ergibt sich dann aus den Urbildern der einzelnen Attributwerte.

Falls in einer partiellen Identität nur Attribute sind, deren Schnittmengen nicht alle Entitäten separieren, verbleibt eine gewisse Anonymität, die der grössten nicht separierten Teilmenge entspricht. Beispielsweise verbleibt mit der partiellen Identität *Name* und *Geburtsdatum* in der Entitätsmenge der Einwohnerschaft der Schweiz, eine gewisse Anonymität, da es mehrere Personen mit gleichem Namen und Geburtsdatum gibt. Gibt es ein einzelnes Attribut, das die Anonymität bereits vollständig auflöst, nennt man ein solches Attribut einen **Identifikator[35].**

Skizze 19 zeigt die symbolische Darstellung einer A) Entitätsmenge mit den einzelnen Entitäten (repräsentiert durch ihre Attributdatensätze) und B) Partition dieser Menge durch ein namentliches Attribut und die Teilmenge, die durch einen bestimmten Attributwert definiert ist. Die C) Kombination von Attributen (Schnittmengen von Partitionen einer partiellen Identität). Ein einzelnes Attribut das alle Entitäten in der Entitätsmenge separiert, ist D) ein Identifikator.



Skizze 19: Datensätze zu Entitätsmengen und partielle Identitäten.

Oft wird ein Identifikator von einer Verwaltung einer Entitätsmenge zugeordnet und kann dann von weiteren Verwaltern, in deren Interessenkontext Teilmengen der umfassenderen Entitätsmenge relevant sind, ebenfalls als vollständig identifizierendes Attribut genutzt werden. In der Einwohnerschaft der Schweiz ist zum Beispiel die AHVN13 ein solcher Identifikator, der von der ZAS den Personen in der Schweiz zugeteilt und dann von verschieden Instanzen als Identifikator genutzt wird.

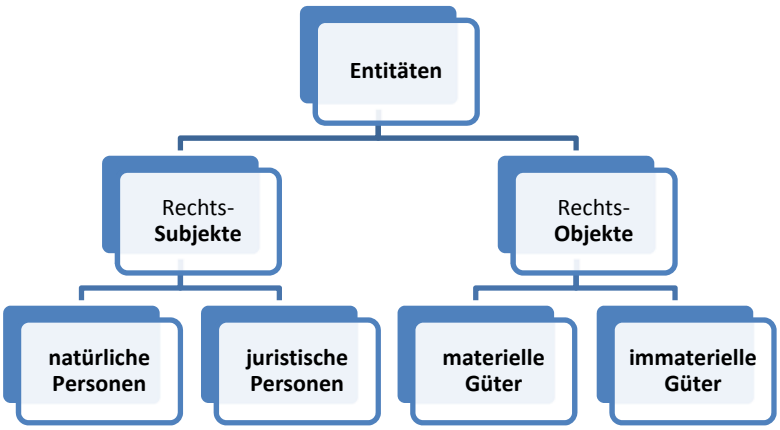
3. Klassen von Entitätsmengen

Basierend auf einem Rechtsrahmen lassen sich Entitäten in Rechtssubjekte und in Rechtsobjekte unterteilen. **Rechtsubjekte** sind Träger von Rechten und Pflichten. Dagegen sind **Rechtsobjekte**

[35] Eine identifizierende partielle Identität als Repräsentation einer Entität in Form von Attributen mit einem Identifikator wird in den eCH Standards als *eIdentity* bezeichnet. Der Begriff eIdentity wird jedoch oft mit unterschiedlichen semantischen Bedeutungen verwendet. Deshalb ziehen wir den Term ‚identifizierende partielle Identität' vor.

Gegenstände, über die ein Rechtssubjekt verfügen und für sich beanspruchen kann. Rechtssubjekte sind **natürliche Personen** (Menschen) und **juristische Personen** (z.B. Unternehmen oder Institutionen). Rechtsobjekte sind **materielle Güter** (z.B. Immobilien oder Mobilien) und **immaterielle Güter** (z.B. Patente, Urheberrechte, Geldforderungen oder auch Software).

Obschon im Prinzip die elektronische Identifizierung im Kontext des Internet of Things (IoT) für alle Arten von Entitäten relevant ist, beschränkt sich das E-ID Gesetz gemäss Auftrag auf die Rechtssubjekte (natürliche) Personen. Folgerichtig konzentriert sich die weitere Diskussion auf *natürliche Personen*, die im Kontext der schweizerischen E-ID die relevanten Entitätsmengen bilden.



Skizze 20: Kategorisierung der Entitäten in Rechtssubjekte und -objekte.

4. Person – Personenstamm, E-ID Ökosystem

Jede Person ist durch ihre sozialen und wirtschaftlichen Tätigkeiten Mitglied von vielen kontextspezifischen Entitätsmengen, die wir in Anlehnung an den Begriff Kundenstamm in der Folge als **Personenstamm** bezeichnen[36]. Eine **Person** kann Bürgerin oder Bürger eines Staates, Mitarbeiter oder Mitarbeiterin eines Unternehmens, Kundin oder Kunde eines Geschäftes, Mitglied einer Partei, eines Klubs oder weiterer Gruppierungen sein. Gemeinsam sind allen solchen Gruppierungen, dass der Personenstamm der zugehörigen Personen durch ein Regelwerk (Gesetz, Kontrakt, Statuten etc.) bestimmt ist und von der Kontext definierenden Organisation verwaltet wird. Ist die Organisation ein Staat und das Regelwerk durch Verfassung, Gesetze und Anwendungsregeln bestimmt, nennen wir den dadurch definierten Personenstamm **Bevölkerung.** Für eine bestimmte Bevölkerung wird die Gesamtheit aller Personen und der verwaltenden Instanzen, die innerhalb der Bevölkerung solche kontextabhängigen Personenstämme definieren, als **Identität Ökosystem** bzw. **E-ID-Ökosystem** bezeichnet.

5. Personenidentifikator, Personenidentifizierungsdaten

Innerhalb eines spezifischen Kontextes ist eine Person durch eine identifizierende partielle Identität auf einer gewissen Vertrauensstufe eindeutig bestimmt. Ein Attribut, das für sich alleine alle Personen in einem Personenstamm identifiziert, ist ein **Personenidentifikator**. Bezieht sich ein solcher Identifikator auf eine ganze Bevölkerung eines Staates, bezeichnen wir ihn als **Eindeutigen Personenidentifikator (EPID)**. Die AHVN13 ist ein Beispiel für ein Attribut, das im Personenstamm der vom ZAS erfassten Bevölkerung identifizierend und somit ein EPID ist.

[36] Ein Personenstamm ist zu einem bestimmten Zeitpunkt durch die Menge der sie repräsentierenden Datensätze der partiellen Identitäten bei der Verwaltung fest definiert. Im Lauf der Zeit können Datensätze für Personen neu erfasst oder gelöscht werden. Der Personenstamm entwickelt sich entsprechend.

Die vom Staat erfassten und verwalteten Attribute werden als **Personenidentifizierungsdaten (PID)** bezeichnet. Mit den Personenidentifizierungsdaten kann eine Person in der Bevölkerung eindeutig identifiziert werden. Meist genügt dazu nur eine kleine Auswahl solcher Daten, wie zum Beispiel *Name*, *Vorname* und *Geburtsdatum*, die als partielle Identität in der Schweiz de facto identifizierend ist[37].

Ist für eine Bevölkerung, als staatlich definierter Personenstamm, ein EPID definiert, gibt es die Möglichkeit aus diesem EPID für jeden untergeordneten Personenstamm unterschiedliche Personenidentifikatoren abzuleiten (sektorielle Identifikatoren) oder deren Gültigkeit sogar zeitlich zu begrenzen (transiente Identifikatoren). Abgeleitete Identifikatoren können dazu dienen aus Datenschutz Gründen eine Identifikation quer über verschiedene untergeordnete Personenstämme zu verhindern. Abgeleitete Identifikatorsysteme müssen von der Verwaltung des staatlichen Personenstamms administriert oder zumindest beaufsichtigt werden, da nur diese Instanz die relative Anonymität zwischen Personenstämmen mit unterschiedlich abgeleiteten Identifikatoren auflösen kann.

6. Identität einer Person

Die **Identität** einer Person ist eine idealisierte Verallgemeinerung der partiellen Identitäten einer Person. Sie setzt sich im Prinzip aus allen Attributen zusammen, die in allen möglichen Kontexten zugeordnet werden könnten und für die insgesamt ein hinreichendes Vertrauen besteht, dass sie zum Zeitpunkt der Feststellung genau die richtige Person beschreiben. Im Kontext eines E-ID-Ökosystems mit staatlich erfassten Identitätsdaten für die gesamte Bevölkerung, wird Identität oft als Synonym für die staatlich erfasste partielle Identität mit den Personenidentifizierungsdaten verwendet, welche präziser als **zivile** oder **staatliche Identität** bezeichnet wird.

7. Attributklassen

Bei den Attributen ist zu unterscheiden zwischen solchen, die durch die Verwaltung eines Personenstamms den Personen zugewiesen werden, solchen, welche die Person unabhängig von einem Regelwerk als persönliches Merkmal hat und solchen, die ihr vom übergeordneten staatlichen Regelwerk, das die Bevölkerung und die zivile Identität der Personen definiert, oft lebenslang zugeordnet sind.

i. Zugewiesene Attribute

Dies sind im Prinzip öffentlich bekannte aber vom Kontext des Personenstamms abhängige Attribute einer Person wie zum Beispiel Mitgliedschaftslizenz in einem Verein, Kundennummer bei einer vertrauenden Beteiligten, Personalnummer, Prokura einer Gesellschaft, UserID für den Zugang zu einem Dienst etc. Sie dienen dazu die im Personenstamm erfassten Mitglieder relativ zum Kontext zu identifizieren und ihnen Rollen zuzuordnen. Berufsorganisationen führen für ihre Mitglieder Personenregister mit solch zugewiesenen Attributen wie zum Beispiel Qualifikation, Spezialisierungen, Akkreditierungen, Berechtigungen usw. Solche Attribute können von allen verwaltenden Organisationen ihren Personenstämmen zugewiesen werden. Sie sind meistens ergänzend zu den Personenidentifizierungsdaten und haben oft nur im spezifischen Kontext eine Bedeutung.

ii. Persönliche Attribute als Authentifizierungsfaktoren

Dies sind der Person zugehörige Attribute wie zum Beispiel biometrische Eigenschaften, ausgedachte oder angeeignete Geheimnisse wie z.B. PIN Codes oder auch der Besitz eines persönli-

[37] Die Verwechslungsrate mit diesen drei Attributen ist in der schweizerischen Bevölkerungen auf dem ppm-Niveau

chen Werkzeugtyps, wie zum Beispiel eine personifizierte Smartcard oder ein Ausweis. Grundsätzlich sind solche Attribute privat und können von einer Verwaltung nur mit dem Einverständnis und der Mitwirkung der Person erfasst und zu einer identifizierenden partiellen Identität hinzugefügt werden[38]. Sie dienen insbesondere dazu die Authentizität einer Person zu überprüfen. Für eine Authentifizierung macht die Person das persönliche Attribut der Verwaltung des Personenstamms soweit bekannt, dass diese später eine Überprüfung des Vorhandenseins des persönlichen Attributs durchführen kann. So erfasste persönliche Attribute sind meist nur innerhalb des Personenstamms überprüfbar definiert, für den sie erfasst sind. Die Erfassung und Überprüfung kann auch indirekt via ein Gerät erfolgen, das persönliche Originalattribute erfasst und überprüft und nur das Resultat der Überprüfung weiterleitet. Ein E-ID-Authentifikator ist eine typische Realisierung eines solchen Gerätes. Im Fall des E-ID-Authentifikators sind der Identifikator und die Sicherheitselemente des Geräts Teil der bei der Verwaltung (IdP) registrierten partiellen Identität des Inhabers des Authentifikators. Andere Beispiele für solche Geräte sind die von Banken verteilten Authentifikatoren, die die Präsenz der Person mit PIN-Code oder biometrisch erfassen und einen nur einmal gültigen Code als Bestätigung für eine erfolgreiche Überprüfung erzeugen. Ein so zugewiesenes Attribut repräsentiert dann die dahinter liegenden persönlichen Attribute.

Oft werden die persönlichen Attribute auch als **Authentifizierungsfaktoren** bezeichnet und in die drei Kategorien **biometrisch, wissensbasiert** und **besitzbasiert** eingeteilt. Alleinstehende Attribute, die auf einer messbaren Eigenschaft basieren, wie zum Beispiel biometrische Charakteristiken, sind für grössere Personenstämme meist kaum als Identifikatoren verwendbar, da es fast immer Personen gibt, die innerhalb der Messgenauigkeit und der angestrebten Sicherheit nicht unterscheidbare Attributwerte haben[39]. Für kleinere und vorgängig eingeschränkte Personenstämme können messbare Attribute aber sehr wohl identifizierend sein. Im Normalfall dienen sie jedoch dazu eine behauptete partielle Identität, zu der sie gehören, durch eine nochmalige Erfassung und eine Verifikation zu bestätigen. Zum Beispiel überprüft eine Verwaltung, ob das Passwort, das eine Person bei einer Anmeldung eingibt, dem Passwort entspricht, das er zusammen mit der UserID für die Person registriert hat. Oder der Polizist überprüft durch einen Kontrollblick, ob das Gesichtsbild der Person mit demjenigen der partiellen Identität übereinstimmt, die auf der IDK festgehalten ist.

iii. Attribute der staatlichen Personenidentifizierung

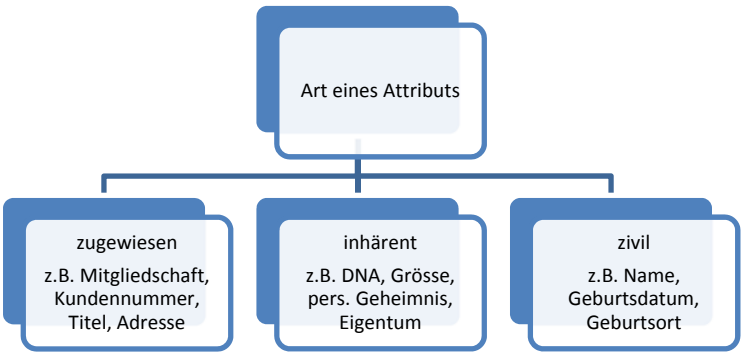
Die dritte Kategorie sind Attribute, die einer Person nach staatlichen Regeln und durch einen staatlichen Identitätsverwaltungsprozess meist direkt von Geburt[40] weg zugeordnet werden und als zivile Identität das Individuum in der gesamten Bevölkerung identifizieren. Diese Personenidentifizierungsdaten werden in staatlichen Personenregistern verwaltet. Beispiele für vom Staat verwaltete Attribute sind *Name, Vorname, Geburtsdatum, Geburtsort* etc. Sie werden im Kontext der Abstammung, des Örtlichkeit und des Kalenderdatums einer neuen Entität *Person* bei der Geburt zugewiesen, bei jeder Ausweiserstellung überprüft und beim Tod entsprechend markiert. Aber auch die *Nationalität*, die *Passnummer* oder *Adressdaten* gehören zu diesen Attributen. Sie sind jedoch im Gegensatz zu den meisten anderen Personenidentifizierungsdaten nicht unbedingt lebenslang gültig oder haben sogar eine explizit beschränkte Lebensdauer.

---

38 In der Forensik ist die Mitwirkung der Person nicht bewusst, erfordert von der Polizei als verwaltende Instanz aber grosse zusätzliche Anstrengungen um eine identifizierende partielle Identität mit erfassten persönlichen Attributen zu verbinden.

39 Es gibt gewisse Ausnahmen, so ist zum Beispiel das Irisbild einer Person ein identifizierendes Attribut innerhalb der gesamten Weltbevölkerung. Mit der Einschränkung bezüglich eineiiger Zwillinge gilt dies auch für die DNA.

40 Es gibt natürlich Staaten, die Personenidentifizierungsdaten kaum oder mangelhaft erfassen, oder auch Personen, die aus irgendwelchen Gründen versuchen die Verbindung zu ihren Personenidentifizierungsdaten und damit zu ihrer zivilen Identität zu brechen. In solchen Fällen kann ein Staat einer Person neue Personenidentifizierungsdaten zuordnen, die in seiner Bevölkerung gelten.



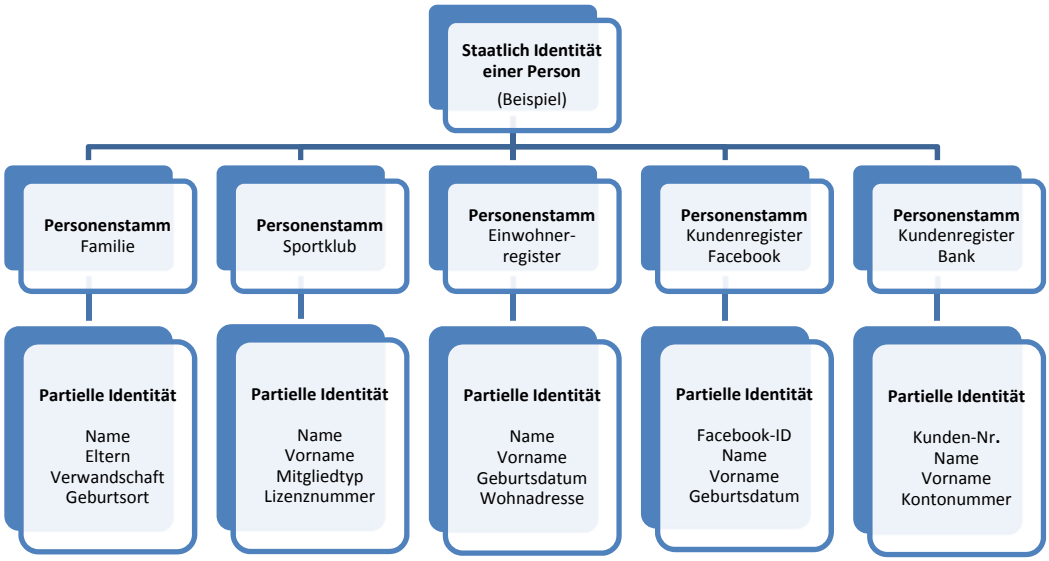
Skizze 21: Kategorien von Attributen, die in partiellen Identitäten erfasst sein können

8. Hierarchie der Personenstämme

Der von einem Verwalter in seinem Kontext definierte Personenstamm ist in den meisten Fällen eine Teilmenge eines umfassenderen Personenstammes, für den bereits gewisse Attribute festgestellt oder zugeordnet sind. Zuoberst in einer solchen Hierarchie von Personenstämmen steht die gesamte Bevölkerung eines Identitäts-Ökosystems mit den Personenidentifizierungsdaten der zivilen Identität. Die Attribute der zivilen Identität werden mittels der Personenstandsregister des Staates verwaltet und das Vertrauen in die richtige Zuordnung der erfassten Attribute zu den Personen wird in der Schweiz durch wiederholte Überprüfung dieser Daten bei jeder Ausweiserstellung immer wieder neu aufgebaut.

Die Attribute der Personenidentifizierungsdaten werden oft auch in untergeordneten Personenstämmen erfasst, so dass die zivile Identität des Staates und die partielle Identität im untergeordneten Personenstamm die gleiche Person bestimmt. So wird zum Beispiel ein E-Commerce Unternehmen seinen Kundenstamm möglichst in den staatlichen Rechtsrahmen einordnen wollen und erfasst deshalb insbesondere auch Attribute, die für eine solche Einordnung wichtig sind, und die Kundin oder den Kunden als Person mit ihrer zivilen Identität im Staat identifizieren.

Die verschiedenen Personenstämme können sich überschneiden und werden somit teilweise durch identische partielle Identitäten mit identischen Attributen repräsentiert. So sind zum Beispiel der Namen und das Geburtsdatum einer Person in vielen Registern von Personenstämmen Teil der erfassten partiellen Identität. Aus Datenschutzüberlegungen kann es sinnvoll sein, dass sich partielle Identitäten bestimmter Personenstämme möglichst nicht überschneiden, damit zwischen ihnen keine Verbindung hergestellt werden kann. Dies könnte zum Beispiel durch eine Reduktion der staatlichen Attribute auf einen abgeleiteten sektoriellen Personenidentifikator erreicht werden. Der im vorliegenden Konzept eingeführte EPID bildet die Basis für eine solche Option. Ein EPID bietet in jedem Fall einen besseren Schutz der Privatsphäre als die heute übliche Alternative aus *Name*, *Vorname* und *Geburtsdatum*, die in der Praxis zum Beispiel via soziale Netzwerke sehr einfach durch jedermann einer bestimmten Person zugewiesen werden kann. Skizze 22 zeigt Beispiele für verschiedene Personenstämme, die in ihren Attributdatensätzen Personenidentifizierungsdaten einbauen. Solche Personenstämme sind teilweise überschneidend und ihre partiellen Identitäten haben meist als Kern Attribute aus den Personenidentifizierungsdaten des Staates.



Skizze 22: Beispiele für verschiedene Personenstämme

B. Identitätsmanagement (IdM), Identitätsmanagement System (IdMS)

Die Verwaltung der Daten der partiellen Identitäten eines Personenstamms, deren Sicherung und Wartung und die Durchführung der Identifizierung und der Authentifizierung einzelner Personen wird als **Identitätsmanagement (IdM)** bezeichnet. Die Gesamtheit der Werkzeuge für die Erfüllung dieser Aufgaben ist ein **Identitätsmanagement System (IdMS)**. Der Kern eines IdMS besteht aus dem Personenregister mit den erfassten Attributen der partiellen Identitäten und definierten Prozessen wie das Register gepflegt, genutzt und administriert wird.

9. Lebenszyklus einer partiellen Identität im IdM

Die Hauptphasen des Lebenszyklus einer partiellen Identität einer Person in einem IdM sind die **Registrierung** einer neuen Person, die **Wiederanmeldung** einer bereits erfassten Person und die **Löschung** von ausgeschiedenen Personen. Nicht mehr direkt zu den Kernaufgaben eines IdM gehört die Rollen- und Rechtezuteilung, die jedoch noch oft als Teil eines Gesamtsystems betrachtet werden[41]. Einwohner-, Steuer- oder Personenstandsregister von Behörden, Kundenregister von sozialen Medien, Unternehmen und Banken, aber auch Mitgliederlisten von Vereinen oder Schulrodels sind Beispiele für solche IdMS.

i. Registrierung einer Person im IdM

Für die Registrierung einer neuen Person muss ihre partielle Identität im Kontext der verwaltenden Organisation erstellt oder aus einem IdMS eines übergeordneten Personenstamms bezogen werden. Teil der partiellen Identität ist ein kontextspezifischer Identifikator, der die gesamte partielle Identität der Person im Personenstamm repräsentiert. Auch der Identifikator kann spezifisch

[41] Oft werden die Rollenzuteilung und damit die Gewährung von Rechten zur Nutzung der Dienste der Organisation, die ein IdM betreibt, als Teil eines Gesamtsystems beschrieben, das als Identity and Access Management (IAM) System bezeichnet wird. Für eine korrekte Rollenzuteilung nach den Vorgaben der Organisation braucht es eine vorgängige Registrierung und für die Ausübung einer Rolle eine vorgängige Anmeldung und damit zwingend die Funktionalität eines IdM. Bei der Verwaltung von Zugangsrechten handelt sich jedoch um zusätzliche Aufgaben, die unter dem Begriff des Accessmanagements zusammengefasst werden. Für ein effizientes Systemdesign ist jedoch eine Trennung der Verwaltung der Zugriffsrechte vom IdM empfohlen [7].

für das IdMS definiert oder aus einem übergeordneten Personenstamm bezogen werden.

Bei der Registrierung wird die partielle Identität einer Person im IdMS auf dem von der Verwaltung definierten Sicherheitsniveau erfasst. Dazu gehört mindestens ein persönliches (geheimes) Attribut als referenzierender Authentifizierungsfaktor (**Bindung**), der in geschützter Weise erfasst oder zusammen mit der Person neu definiert wird**.** Gewisse Authentifizierungsfaktoren wie zum Beispiel biometrische Attribute müssen dabei von der Person nicht in jedem Fall offenbart, sondern können in einem geschlossenen Gerät (Authentifikator) in indirekter Form als Referenzdaten abgegeben werden[42]. Nebst Authentifizierungsfaktoren werden weitere Attribute erfasst z.B. gewisse Personenidentifizierungsdaten, die mit den bekannten Attributen eines übergeordneten oder bestehenden Personenstamms abgeglichen (**initiale Identifizierung)** werden. Meist sind dies Attribute der zivilen Identität. Nach erfolgter Registrierung wird das System für die Nutzung durch die berechtigte Person aktiviert.

ii. Wiederanmeldung beim IdM

Will eine registrierte Person später ihre Zugehörigkeit zu einem vom IdM verwalteten Personenstamm nachweisen, meldet sie sich mit dem zugeteilten Personenidentifikator oder einem zugehörigen Pseudonym (UserID etc.) an und behauptet damit, dass sie die richtige Person sei. Das IdMS wird dann eine **Authentifizierung** mittels der erfassten Authentifizierungsfaktoren durchführen, die zur behaupteten partiellen Identität der Person gehören. Für die Authentifizierung muss die Person nachweisen, dass sie aktuell über dieselben Authentifizierungsfaktoren (persönliche Attribute) verfügt, die anlässlich der Registrierung zu ihrer partiellen Identität erfasst wurden. Je nach Anzahl unabhängiger solcher Faktoren, die überprüft werden, spricht man von einer ein, zwei oder drei Faktoren Authentifizierung.

iii. Löschung oder temporäre Sperrung

Gehört eine Person nicht mehr zum Personenstamm der im IdM administriert wird, ist die bei der Registrierung erfasste partielle Identität zu löschen. Ebenfalls zu den Aufgaben eines IdM gehört die Beaufsichtigung der regulären Nutzung der erfassten partiellen Identität. Bestehen Zweifel, ob das Vertrauen in eine partielle Identität noch gerechtfertigt ist, kann deren Nutzung vorübergehend oder permanent gesperrt werden.

10. Basisprozesse eines Identitätsmanagement System (IdMS)

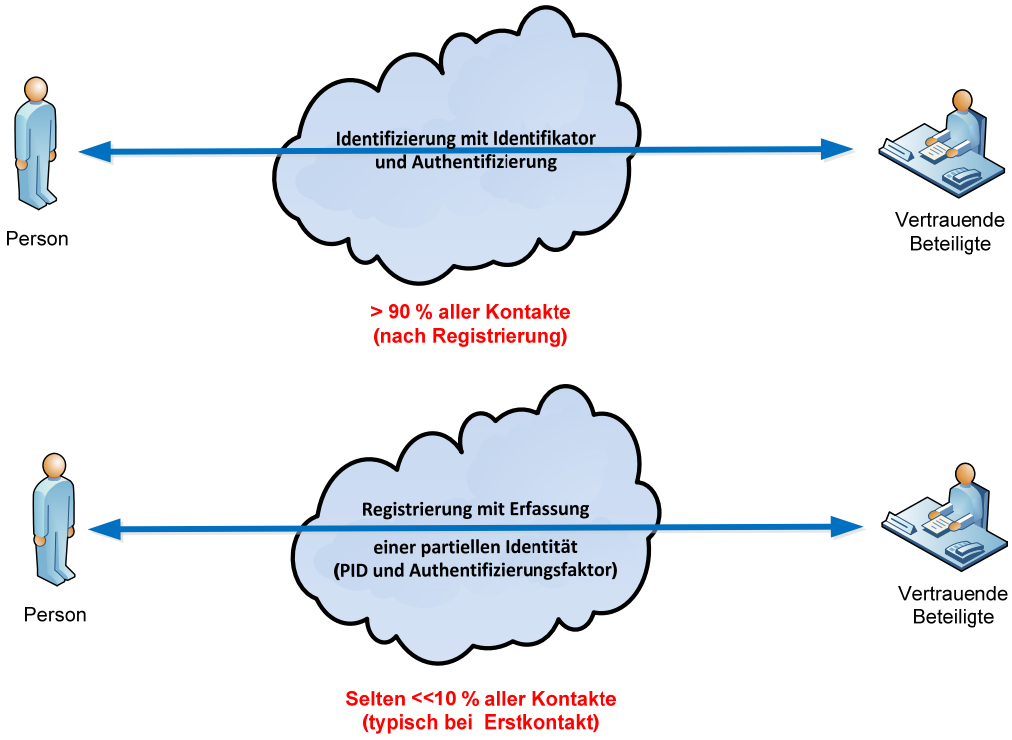
Die Identifizierung und die Authentifizierung einer Person sind die Basisprozesse das Identitätsmanagement. Der Betreiber eines IdM kann diese Prozesse auch als Dienstleistung für Dritte erbringen, die einen untergeordneten Personenstamms verwalten.

Der Unterschied zwischen den beiden Prozessen lässt sich einfach am Beispiel einer Online-Anmeldung bei einem Portal illustrieren. Ein Nutzer oder eine Nutzerin durchläuft beim ersten Kontakt mit dem Portal eine Registrierung, bei der sie im IdMS des Portals eine partielle Identität erstellt. Diese enthält insbesondere auch einen selbstgewählten (Pseudonym) oder zugeteilten (UserID, Anmeldenummer) Personenidentifikator. Gleichzeitig muss sie dem IdMS mindestens ein persönliches Attribut direkt (zum Beispiel als persönliches Passwort) oder via ein zwischengeschaltetes Medium (zum Beispiel die durch einen PIN Code freigeschalteten Sicherheitselemente einer SIM-Karte) als Teil der partiellen Identität offenbaren.

Wenn die Person sich später wieder beim Portal anmeldet, identifiziert sie sich mit dem Personenidentifikator, der im IdMS auf ihre partielle Identität zeigt (**Identifizierung**). Sie behauptet damit die im IdMS erfasste Nutzerin oder Nutzer zu sein. In einem weiteren Schritt beweist sie dies,

[42] Ein solches Gerät ist Teil des IdMS und liefert mit definierter Sicherheit das Resultat einer Überprüfung von Authentifizierungsfaktoren.

indem sie das im IdMS unter der gleichen partiellen Identität erfasste persönliche Attribut nachweist und sich damit authentifiziert (**Authentifizierung**). Dieser Nachweis erfolgt wieder direkt oder indirekt, so wie das persönliche Attribut bei der Registrierung erfasst wurde. Die Authentifizierung ist somit ein Prozess, bei dem eine Bestätigung für die behauptete Identität einer Person eingeholt wird. Die Wiederanmeldung mit Identifizierung durch einen Personenidentifikator und mit anschliessender Authentifizierung ist, verglichen mit der initialen Identifizierung mit Erfassung der partiellen Identität im Rahmen der Registrierung, ein sehr häufiger Prozess.



Skizze 23: Häufigkeit der Wiederanmeldung verglichen mit der Registrierung bei einer vBt.

11. Identifizierung einer Person

Basis der Identifizierung ist der Prozess der Feststellung und sicheren Zuordnung einer partiellen Identität zu einer Person, wobei von der Person mindestens auch ein persönliches Attribut als Authentifizierungsfaktor erfasst werden muss. Durch den Einbezug von staatlichen Personenidentifizierungsdaten kann die Identifizierung auch relativ zu einem übergeordneten (staatlichen) Personenstamm erfolgen. Ein übergeordneter Personenstamm kann bei einer Identifizierung die entsprechenden Daten direkt an den untergeordneten Personenstamm liefern. Zum Beispiel geschieht dies, wenn bei einer Identifizierung die Vorlage eines staatlichen Ausweises verlangt wird, der die wichtigsten Personenidentifizierungsdaten, wie *Name, Vorname, Geburtsdatum* etc. beinhaltet. In der Regel wird in einer identifizierenden partiellen Identität auch ein im Personenstamm eindeutiger Personenidentifikator erfasst. Dieser steht dann in diesem Personenstamm stellvertretend für die gesamte partielle Identität und kann für die Online-Anmeldung und damit für die Identifizierung gebraucht werden. Wird vom Staat für alle untergeordneten Personenstämme ein eindeutiger Personenidentifikator (EPID) definiert, kann dieser für die Identifizierung in der ganzen Bevölkerung und für viele vertrauende Beteiligte als Identifikator in ihren IdMS genutzt werden.

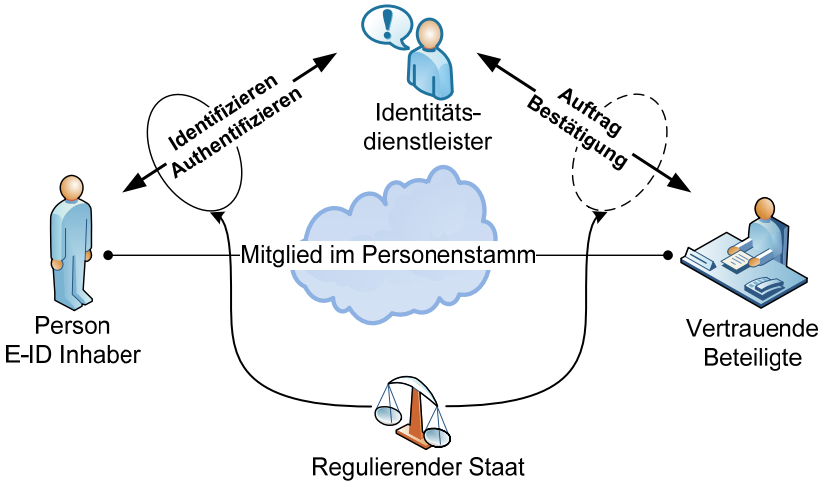
12. Authentifizierung einer Person

Authentifizierung ist der Prozess der Überprüfung der Zugehörigkeit einer partiellen Identität zu einer Person, die von dieser beansprucht wird. Es wird dabei verifiziert, dass die erfassten persönliche Attribute der partiellen Identität (Authentifizierungsfaktoren) mit einer gewissen Sicherheit tatsächlich zu der beanspruchenden Person im Personenstamm gehören. Die Überprüfung erfolgt durch den Vergleich von persönlichen Attributen, welche die Person im Moment der Authentifizierung liefert, mit den während der Registrierung der Person erfassten Authentifizierungsfaktoren. Die Stärke einer Authentifizierung ist abhängig von der Bindung der überprüften persönlichen Attribute an die Person und der Anzahl und dem Typ der überprüften Attribute. So hat zum Beispiel die Überprüfung einer Iris einer Person eine wesentlich höhere Signifikanz für die Bindung als die Abfrage eines vierstelligen PIN-Codes oder eines Passwortes. Eine Iris ist nach heutigem Wissen absolut einmalig. Viele Personen benutzen jedoch simple PIN-Codes oder Passwörter, die oft leicht zu erraten sind. Mit jedem zusätzlich überprüften unabhängigen Authentifizierungsfaktor wird eine Authentifizierung stärker. Das Vertrauen in eine Authentifizierung ergibt sich aus der Stärke der Authentifizierung und der Sicherheit, dass der Prozess nicht durch einen Angreifer verfälscht werden konnte. Eine Authentifizierung ist eine Momentaufnahme auf einem bestimmten Sicherheitsniveau und das Vertrauen in sie mindert sich mit der Zeit.

13. Elektronisches Identitätsmanagement

Wird das Identitätsmanagement über elektronische Medien abgewickelt, spricht man von einem **elektronischen Identitätsmanagement (E-IdM)** und dem zugehörigen **elektronischen Identitätsmanagement System (E-ID-System)**. Im E-IDM kommen nebst der Rolle der Person, die mit einem **elektronischen Identifikationsmittel (E-ID**) identifiziert wird und als **Inhaberin oder Inhaber** bezeichnet wird, und der Rolle der Verwaltung, die Personen identifiziert und authentifiziert und als **vertrauende Beteiligte(vBt)** bezeichnet wird, zwei weitere Rollen dazu und zwar diejenige der **Anbieter von Identitätsdienstleistungen (Identity Provider - IdP),** die E-ID ausstellt und das E-ID-System betreibt, und diejenige des **regulierenden Staates**. Die vertrauende Beteiligte, die dem IdP vertrauen muss, beauftragt den IdP die Prozesse der elektronischen Identifizierung und Authentifizierung von Personen durchzuführen. Die vBt betreibt dazu eine Informatikanwendung, als **vertrauender Dienst** bezeichnet, die mit dem E-ID-System des IdP über eine E-ID-Schnittstelle verbunden ist.

Der IdP betreibt ein E-ID-System und erfasst einen möglichst breit gefassten Personenstamm, so dass die Personenstämme möglichst vieler vBt abgedeckt sind und er so Identitätsdienstleistungen für einen grossen Kundenkreis machen kann. Zum E-ID-System gehört ein elektronisches Identifizierungsmittel (E-ID), das der IdP allen bei ihm registrierten Personen ausstellt und das ihm erlaubt alle Inhaber und Inhaberinnen einer solchen E-ID überall im virtuellen Raum zu authentifizieren. Der **regulierende Staat** definiert die rechtlichen, prozessualen, organisatorischen und technischen Rahmenbedingungen, innerhalb derer das E-IdM mit der Mitwirkung von IdP und ihrer E-ID-Systeme abgewickelt wird. Er definiert insbesondere auch wer wie welche Personenidentifizierungsdaten nutzen und verarbeiten darf. Er definiert damit den für die Entwicklung eines funktionierenden E-ID-Ökosystems nötigen Vertrauensrahmen.



Skizze 24: Aufgabenverteilung im elektronischen Identitätsmanagement

14. Elektronisches Identifizierungsmittel (E-ID)

Ein elektronisches Identifizierungsmittel (E-ID) ist eine materielle und/oder immaterielle elektronische Einheit (Authentifikator)[43], die zu einem E-ID-System gehört und die nach erfolgtem Registrierungsprozess zur Identifizierung und Authentifizierung einer Person im Personenstamm des Betreibers des E-ID-Systems verwendet wird. Die E-ID hat Schnittstellen, die eine direkte sichere Kommunikation mit dem zentralen Server des E-ID-Systems erlauben und sie enthält einen Identifikator, der bei der Registrierung der Inhaberin oder dem Inhaber zugeordnet wird. Die E-ID kann eine sicher mit der Einheit verbundene Authentifizierungsfunktion mit eingekapselten Referenzdaten für die persönlichen Authentifizierungsfaktoren der Inhaberin oder des Inhabers enthalten. Eine solche Authentifizierungsfunktion vergleicht bei einer Authentifizierung die bei der Registrierung erfassten Authentifizierungsfaktoren der Inhaberin oder des Inhabers mit aktuell erfassten persönlichen Attributen der Person und entscheidet, ob diese übereinstimmen und somit von der registrierten Inhaberin oder dem registrierten Inhaber kommen. Die E-ID kann nebst dem evtl. verbindungsabhängigen Identifikator weitere Identitätsattribute der Person enthalten oder ist via E-IdM des Personenstamms des IdP mit solchen in eindeutiger Weise verbunden.

i. Sicherheitsniveau einer E-ID

Elektronische Identifizierungsmittel können für verschiedene Sicherheitsniveaus konzipiert sein. Im Rahmen der europäischen eIDAS-Verordnung [2] werden drei Sicherheitsniveaus definiert (niedrig, substanziell, hoch), die im Wesentlichen den drei höheren Sicherheitsniveaus des ISO/IEC 29115 Standards [52] und den von NIST definierten Sicherheitsniveaus für die digitale Authentifizierung [6] entsprechen. Im Konzept für die schweizerische E-ID entsprechen diese Sicherheitsniveaus den drei eingeführten Sicherheitsniveaus (Silber, Gold, Platin). Die E-ID der drei Sicherheitsniveaus unterscheiden sich insbesondere durch den Ausstellungsprozess bei der Registrierung einer Person, durch die Authentifizierungsstärke der in die E-ID integrierten Authentifizierungsfunktion, durch unterschiedliche Sätze von Personenidentifizierungsdaten, die vom Staat übermittelt werden, und durch ihre unterschiedlich breite Anwendbarkeit.

[43] Ein Authentifikator ist vorerst lediglich eine elektronische Funktionseinheit. Er wird zur E-ID, nachdem im Registrierungsprozess die Einheit mittels der Authentifizierungsfunktion mit einer Person und deren Identitätsdaten mit dem Identifikator der Einheit verbunden sind.

ii. Staatlich anerkannte E-ID

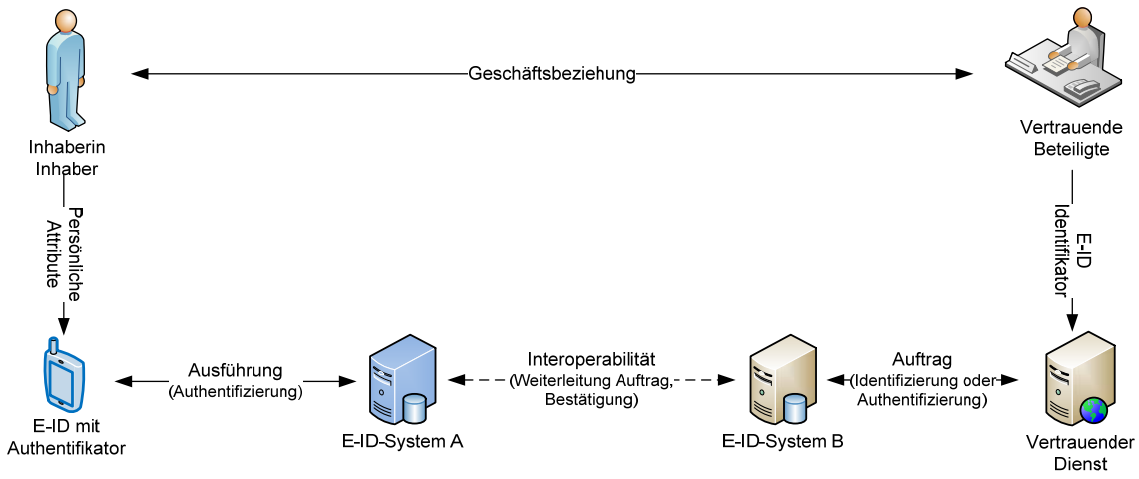
Das geplante *Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID Gesetz)* ist die rechtliche Grundlage für die staatliche Anerkennung von E-ID-Systemen und E-ID, die durch Identitätsdienstleister im Markt für berechtigte Personen der Bevölkerung der Schweiz angeboten werden. Die staatliche Anerkennung basiert auf einem Anerkennungsprozess, durch den die Aspekte technische und organisatorische Sicherheit entsprechend dem Sicherheitsniveau der E-ID, die Vertrauenswürdigkeit der ausstellenden IdP und die Interoperabilität des E-ID-Systems auf Erfüllung der gesetzlichen Anerkennungskriterien geprüft werden.

iii. Interoperabilität

Mit geeigneter Standardisierung der Schnittstellen und der Protokolle kann eine E-ID bzw. das zugehörige E-ID-System im Prinzip von allen vertrauenden Beteiligten für die Identifizierung und Authentifizierung von Inhaberinnen oder Inhabern genutzt werden. Dazu müssen die E-ID-Systeme untereinander interoperabel sein. Dank der Interoperabilität kann eine vertrauende Beteiligte für alle E-ID auf gegebenem Sicherheitsniveau, unabhängig vom ausstellenden staatlich anerkannten IdP, eine Identifizierung oder Authentifizierung einer Inhaberin oder eines Inhabers in Auftrag geben.

15. Interoperabilität in E-ID-Systemen

Es genügt die Interoperabilität zwischen allen Betreibern von E-ID-Systemen herzustellen um eine transparente Nutzung einer E-ID im ganzen E-ID Ökosystem zu erreichen. Eine Inhaberin oder ein Inhaber mit einer E-ID vom IdP A kann diese bei einer vertrauenden Beteiligten nutzen, deren vertrauender Dienst dem E-ID-System des IdP B angeschlossen ist. Dazu meldet sie oder er sich mit dem Identifikator der E-ID beim Portal des vertrauenden Dienstes an, der die Anfrage an das E-ID-System seines IdP B weiterleitet. Dieser stellt fest, dass die Sicherheitselemente der E-ID im E-ID-System des IdP A vorhanden sind und leitet den Authentifizierungs- oder Identifizierungsauftrag an das E-ID-System des IdP A weiter. Dieser führt den Auftrag entweder selbst aus und meldet das Resultat über den gleichen Weg zurück oder liefert die nötigen Sicherheitselemente an den IdP B, so dass dieser dann den Auftrag mit der E-ID des Inhabers ausführen kann. Technisch kann dies in ähnlicher Weise realisiert werden wie das Roaming in Mobilfunknetzen. Damit dies funktioniert müssen alle staatlich anerkannten E-ID-Systeme ein einheitliches Identifikatorsystem für ihre E-ID einsetzen. Dies könnte zum Beispiel aus IP-V6 Adressen, einem standardisierten E-Mail-Adressensystem oder einer anderen Form von einheitlich definierten Identifikatoren der E-ID bestehen.

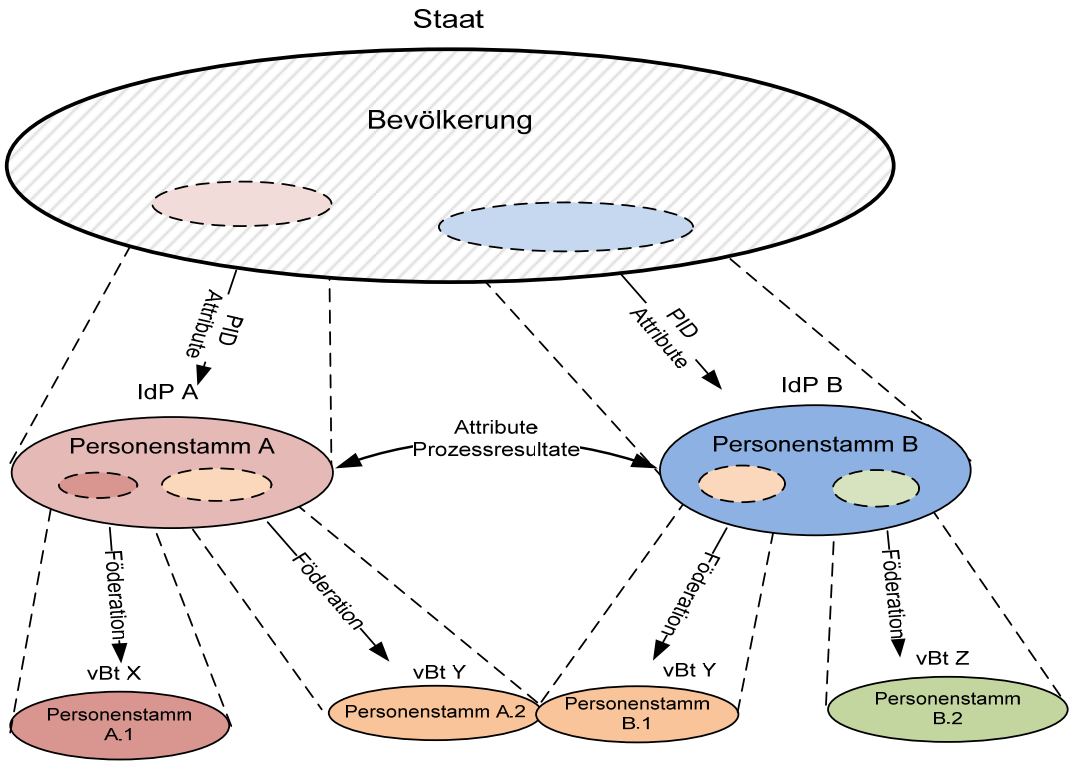


Skizze 25: Ablauf einer interoperablen Authentifizierung oder Identifizierung

i. Interoperable Nutzung von Personenidentifizierungsdaten

Auf der Basis der Interoperabilität zwischen den E-ID-Systemen der staatlich anerkannten IdP kann jede vBt, deren vertrauender Dienst mindestens einem anerkannten E-ID-System angeschlossen ist, für ihren Personenstamm die Identifizierungs- und Authentifizierungsmechanismen aller staatlich anerkannten E-ID nutzen. Die vBt bestimmt dabei das verlangte minimale Sicherheitsniveau. Die vBt kann im Registrierungsprozess mit Einverständnis der Inhaberin oder des Inhabers der E-ID auch Identitätsdaten aus den übergeordneten Personenstämmen der staatlich anerkannten IdP und damit staatlich registrierte Attribute der zivilen Identität übernehmen. Damit wird eine umfassende Interoperabilität der Personenidentifizierungsdaten im schweizerischen E-ID-Ökosystem für alle Inhaberinnen und Inhaber einer staatlich anerkannten E-ID erreicht. Die Interoperabilität der Identifizierung und Authentifizierung mit Abgleich von staatlich registrierten Attributen reicht über die Kette Staat, Identitätsdienstleister (IdP) bis zu den vertrauenden Beteiligten (vBt).

Wenn eine vertrauende Beteiligte eine Person in ihrem Personenstamm registriert, wird die notwendige Identifizierung vom Identitätsdienstleister durchgeführt und das Resultat der vBt mitgeteilt. Falls die E-ID staatlich anerkannt ist, kann der IdP dabei auf Wunsch der Inhaberin oder des Inhabers der vertrauenden Beteiligten auch Personenidentifizierungsdaten und insbesondere auch einen EPID aus staatlichen Registern übermitteln. Auch wenn sich eine Inhaberin oder ein Inhaber bei der vBt anmelden will, wird der IdP die notwendige Authentifizierung selbst machen oder dem zuständigen IdP weiterdelegieren und dann das Resultat der vBt mitteilen.



Skizze 26: Übertragungskette von Attributen

Skizze 26 zeigt die Übertragungskette von Attributen eines übergeordneten Personenstamms auf untergeordnete Personenstämme am Beispiel Staat - Identitätsdienstleister (IdP) – Vertrauende Beteiligte (vBt). An oberster Stelle steht der Personenstamm der gesamten Bevölkerung mit den Personenidentifizierungsdaten (PID). Bei der Interoperabilität mit Hilfe einer E-ID werden zwischen den IdP nicht nur Attribute sondern auch Prozessresultate der Identifizierung und Authentifizierung übertragen.

16. Staat als Attributverwalter und Anerkennungsstelle für das E-IdM

Der Bund betreibt das staatliche IdM für alle in der Schweiz registrierten Personen, die einen gültigen von den Schweizer Behörden ausgestellten Ausweis haben. Die staatliche unterstützte Identifizierung und Authentifizierung mittels diesen Ausweisen ist bereits heute für alle untergeordneten Personenstämme und ihre IdMS möglich. Mit der Einführung von staatlich anerkannten IdP als Anbieter von E-ID-Systemen wird zusätzlich die elektronische Übermittlung von Personenidentifizierungsdaten aus staatlichen Registern via einen staatlichen Proxydienst ermöglicht. IdP mit einem Angebot an staatlich anerkannten E-ID-Systemen können dieses Angebot nutzen. Für den Bereich der **staatlich anerkannten E-ID-Systeme** ist der oberste Personenstamm die gesamte schweizerische Bevölkerung, deren Personenidentifizierungsdaten in den staatlich geführten Registern Infostar, ISA, ISR, ZAS und ZEMIS verwaltet werden.

i. Schweizerischer Stelle für elektronische Identität (SID)

Der SID ist eine Verwaltungseinheit des EJPD, welche nach explizitem Einverständnis des Inhabers oder der Inhaberin einer E-ID ein vom Sicherheitsniveau der E-ID abhängiger Satz von Personenidentifizierungsdaten an das E-ID-System des IdP übermittelt. Sie hat dazu Zugriff auf die einschlägigen Personenregister der Schweiz (ISA, Infostar, ZEMIS, UPI-ZAS).

ii. Anerkennungsstelle für Identitätsdienstleister (AID)

Damit ein IdP ein staatlich anerkanntes E-ID-System betreiben kann, muss er einen Anerkennungsprozess für sich und seine E-ID-Systeme durchlaufen. Dieser beinhaltet die Überprüfung von technischen, organisatorischen und rechtlichen Anerkennungsvoraussetzungen. Dazu gehören insbesondere auch die Überprüfung der Einhaltung von Standards und das Vorhandensein von Schnittstellen für die interoperable Einbindung des anzuerkennenden E-ID-Systems in das schweizerische E-ID-Ökosystem.
Die AID ist eine Verwaltungseinheit beim EFD. Ihr obliegt die staatliche Anerkennung von IdP und deren E-ID-Systeme. Sie hat auch die Aufsicht über die Einhaltung der Voraussetzungen für diese Anerkennung.

7.2 Glossar

Auf der Basis der oben erklärten Begriffe und Zusammenhänge werden für die Gesetzgebung und das Konzept der staatlich anerkannten E-ID die folgenden Definitionen gebraucht.

Begriff	Abk.	Definition
Aktivierung		Freischaltung einer E-ID für den Betrieb durch den IdP nach erfolgter Ausstellung mit Registrierung der Inhaberin oder des Inhabers
Anmeldung		(Wieder)anmeldung einer Inhaberin oder eines Inhabers beim E-IdM (oder IAM) Systems einer vBt oder beim IdP mit der E-ID
Anerkennungsstelle für Identitätsdienstleister	AID	Siehe 3.3
Attribut		Namentlich definierte Eigenschaft einer Entität. Ein Attribut hat einen Attributnamen, einen Attributwert und weitere Charakteristiken wie zum Beispiel einen Datentyp oder ein Gültigkeitsdatum
Attributname		Semantischer Name der Eigenschaft, die als Attribut erfasst wird
Attributwert		Festgestellter Wert eines Attributs einer speziellen Entität (Person)
Attributdienst		Dienst für die Übermittlung von Identitätsattributen für Personen, die in Registern des Dienstes erfasst sind. Staatlich anerkannte IdP agieren als Attributdienst für Personenidentifizierungsdaten, die ihnen vom SID verfügbar gemacht werden. Auch der SID ist ein Attributdienst.
Authentifikator		Eine materielle und/oder immaterielle elektronische Einheit, die zu einem E-ID-System gehört. Sie hat Schnittstellen, die eine direkte sichere Kommunikation mit dem zentralen Server des E-ID-Systems erlauben und sie enthält einen Identifikator, der bei der Registrierung der Inhaberin oder dem Inhaber zugeordnet wird. Sie enthält eine sicher mit der Einheit verbundene Authentifizierungsfunktion mit Referenzdaten für die persönlichen Authentifizierungsfaktoren der Inhaberin oder des Inhabers enthalten.
Authentifizierungsfunktion		Funktion einer E-ID, die es erlaubt persönliche Attribute (Authentifizierungsfaktoren) der Inhaberin oder des Inhabers zu erfassen und mit den lokal abgespeicherten Werten zu vergleichen. Der Authentifizierungsfunktion entscheidet, ob eine Inhaberin oder ein Inhaber die richtige Person ist.
Authentifizierung authentifizieren		Siehe Anhang Abschnitt 12
Authentifizierungsfaktoren		Persönliche Attribute, die zur Authentifizierung einer Person gebraucht werden können. Man unterscheidet oft die drei Kategorien biometrisch, wissensbasiert und besitzbasiert
Bevölkerung		Hier die in den staatlichen Personenregistern erfassten und verwalteten Personen im Hoheitsbereich eines Staates
Eindeutiger Personenidentifikator	EPID	Eindeutig vom Staat den Personen der Bevölkerung zugeordneter Identifikator. Die AHVN13 ist ein EPID in der Schweiz.

Elektronisches Identitätsmanagement	E-IdM	Identitätsmanagement mit digitalen elektronischen Systemen
Elektronisches Identifizierungsmittel	E-ID	Authentifikator, der einer partiellen Identität der Inhaberin oder des Inhabers beim IdP zugeordnet ist, und dessen Authentifizierungsfunktion so initialisiert ist, dass sie die Authentifizierung der Inhaberin oder des Inhabers erlaubt.
Elektronisches Identitätsmanagement System	E-ID-System	System in dem E-ID ausgestellt, betrieben und verwaltet werden.
Elektronische Schnittstellen Anwendungen und Prozesse	E-ID-Schnittstelle	Standardisierte Komponente von E-ID-Systemen, die bei vertrauenden Diensten als Schnittstelle zum E-ID-System operiert. Sie garantiert einheitliche Formulare und Formate beim Einsatz der E-ID.
E-ID-Ökosystem		Gesamtheit aller Instanzen, die E-ID für eine Bevölkerung eines Staates einsetzen oder zu deren Betrieb beitragen.
Entität		Eine durch festgestellte Attribute individualisierbare Einheit
Entitätsmenge		Kontextabhängige Menge von Entitäten
Identifikator		Eindeutige Bezeichnung für eine Entität im Informationssystem eines Verwalters von partiellen Identitäten
Identitätsattribute		Siehe Attribute
Identifizierende Identitätsattribute		Partielle Identität mit Attributen, die eine Entität in einer Entitätsmenge eindeutig identifizieren
Identifizierung identifizieren		Siehe Anhang Abschnitt 11
Identität Ökosystem		Siehe E-ID-Ökosystem
Identität, zivile Identität		Gesamtheit aller Attribute, die für eine Person (Entität) erfasst werden können. Die zivile Identität entspricht den Attributen einer Person, die in staatlichen Personenregistern erfasst sind.
Identitätsdienstleister Identity Provider	IdP	Anbieter von Identitätsdienstleistungen, der ein E-ID-System betreibt und/oder nutzt.
Identitätsmanagement	IdM	Siehe Anhang Kapitel B
Identitätsmanagement System	IdMS	Siehe Anhang Kapitel B
Identitäts- und Zugangsmanagement	IAM	IdM mit angeschlossener Verwaltung von Rollen und Rechten für die erfassten Personen im Personenstamm
Identitäts- und Zugangsmanagement System	IAMS	Elektronisches System für das IAM
Identitätsdienstleistung		Hier ist damit immer eine Authentifizierung oder Identifizierung mit Übermittlung von Personenidentifizierungsdaten gemeint
Inaktivierung		Abschaltung einer E-ID im E-ID-System eines IdP
Inhaberin, Inhaber		Person, der von einem IdP eine staatlich anerkannte E-ID ausgestellt worden ist
Interoperabilität von E-ID		Netzwerk von sich gegenseitig vertrauenden und anerkennenden E-ID-Systemen mit einem definierten minimalen Sicherheitsniveau
Löschung		Definitive Inaktivierung einer E-ID

Natürliche Person		Person, die ein selbstständig handelndes Subjekt ist
Partielle Identität		Datensatz mit Attributen zu einer Entität
Person		Rechtssubjekt, hier meist als natürliche Person gebraucht
Personen-identifikator		Ein in einem Kontext definierter Name, der eine Person im Kontext eindeutig bezeichnet
Personenidentifizierungsdaten	PID	Attribute der zivilen Identität einer Person, die in den staatlichen Personenregistern erfasste sind. Die Personenidentifizierungsdaten sind hier auf eine gesetzlich definierte Teilmenge dieser Attribute eingeschränkt
Persönliche Attribute		Attribute, die für die Authentifizierung einer Person genutzt werden können, siehe Authentifizierungsfaktoren
Personenstamm		Menge von Personen, deren partielle Identitäten in einem IdM eines Verwalters erfasst sind.
Rechtssubjekt		Eigenständig handelnde Träger von Rechten und Pflichten; sie umfassen natürliche und juristische Personen
Registrierung		Registrierung bei IdP: Bindung einer Person an eine E-ID, Identifizierung der Person durch den IdP, Übermittlung von PID der Person durch den SID an den IdP anlässlich der Ausstellung einer E-ID Registrierung bei vBt: Erstanmeldung einer Inhaberin oder eines Inhabers bei einer vBt in dessen IdMS mit Übermittlung von Personenidentifizierungsdaten durch den IdP, der die E-ID ausgestellt hat
Schweizerische Stelle für elektronische Identität	SID	Siehe 3.2
Sicherheitsniveau		Siehe 2.6.1
Träger einer E-ID		Elektronische Einheit, in die ein Authentifikator bzw.eine E-ID integriert ist
Transaktionsabsicherung		Überprüfung der Abmachungen einer Transaktion
Vertrauende Beteiligte	vBt	Natürliche Person oder UID-Einheit, die für ihre Tätigkeit einen vertrauenden Dienst betreibt
Vertrauender Dienst		Eine Informatikanwendung, welche die Identitätsdienstleistung des E-ID-Systems nutzt und die nötigen Schnittstellen zwischen der Dienstleistung des vBt und dem E-ID-System bereitstellt.
Zugewiesene Attribute		Kontextabhängige Attribute, die einer Person in ihrer partiellen Identität im Personenstamm eines vBt oder IdP durch diesen zugewiesen werden

7.3 Literaturverzeichnis

Das Literaturverzeichnis enthält zuerst die zitierten Dokumente und anschliessend weitere Quellenangaben zu den im Konzept verarbeiteten Inhalten.

[1] Bundesamt für Statistik, «Informationsgesellschaft,» Schweizerische Eidgenossenschaft, 2016. [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04.html. [Zugriff am 20 Juli 2016].

[2] EU, «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 (eIDAS-Verordnung),» 23. Juli 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&qid=1422521123960&from=EN. [Zugriff am 29. Oktober 2015].

[3] E. Kommission, «Technical Specifications and procedures for Assurance for eID,» in *2015/1502*, 2015.

[4] FIDO Alliance, «UAF Architectural Overview, Review Draft,» 09. Februar 2014. [Online]. Available: https://fidoalliance.org/specifications/download/. [Zugriff am 12. April 2015].

[5] Lindemann, R., FIDO Alliance and Nok Nok Labs Inc., «The evolution of authentication,» 2013. [Online]. Available: http://www.springer.com/cda/content/document/cda_downloaddocument/9783658033705-c1.pdf. [Zugriff am 12. April 2015].

[6] D. N. S. P. 800-63-3, «Digital Authentication Guideline,» 12 Mai 2016. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3. [Zugriff am 15 Juni 2016].

[7] eCH, «eCH-0107 IAM Gestaltungsprinzipien v2.0,» 04. Dezember 2013. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0. [Zugriff am 12. April 2015].

[8] N. 8149, «Developing Trust Frameworks to Support Identity Federations,» NIST - National Institute of Standards and Technology; US DoC, 2016.

[9] Bundesamt für Gesundheit, «Bundesgesetz über das elektronische Patientendossier,» [Online]. Available: http://www.bag.admin.ch/themen/gesundheitspolitik/10357/10360/index.html?lang=de. [Zugriff am 23 07 2016].

[10] Schweizer Parlament, «Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03,» 19. Dezember 2003. [Online]. Available: http://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Zugriff am 12. April 2015].

[11] eCH Verein, «eCH - E-Governement Standards,» [Online]. Available: http://www.ech.ch. [Zugriff am November 2015].

[12] J. Fromm und et al., «3-Jahre Online Ausweisfunktion – Lessons Learned,» *Fraunhofer Fokus,* Oktober 2013.

[13] Belgische Regierung, «Portal belgium.be - Online Dienste der Belgischen Behörden,» [Online]. Available: http://www.belgium.be/de/online_dienst/. [Zugriff am 12. April 2015].

[14] BRZ-Presseservice, «Handy-Signatur gräbt der Bürgerkarte langsam das Wasser ab (Seite 54),» 27. März 2014. [Online]. Available: https://www.brz.gv.at/presse/pressespiegel/Pressespiegel-2014-03.pdf. [Zugriff am 12. April 2015].

[15] International Civil Aviation Organisation (ICAO), «Document 9303,» [Online]. Available: http://www.icao.int/Security/mrtd/pages/Document9303.aspx. [Zugriff am 26 07 2016].

[16] Bundesministerium des Innern, «Personalausweis,» [Online]. Available: http://www.personalausweisportal.de/DE/Home/home_node.html. [Zugriff am 26 07 2016].

[17] Government Technology, «Louisiana Considers Electronic Driver's License,» [Online]. Available: http://www.govtech.com/state/Louisiana-Considers-Electronic-Drivers-License.html. [Zugriff am 26 07 2016].

[18] CNET, «The driver's license of the future is coming to your smartphone,» [Online]. Available: http://www.cnet.com/news/your-future-drivers-license-could-go-digital/. [Zugriff am 26 07 2016].

[19] Gemalto, C. Mesnard, «Trusted National Mobile ID Schemes,» in *Secure Document World Conference, London 2016*, London, 2016.

[20] H. Steier, «Uns blieb das Lachen im Hals stecken,» *20 Minuten,* Bd. 22. September 2010; 11:14, Nr. Digital News, Sicherheit, p. http://www.20min.ch/digital/hardware/story/17220624, 2010.

[21] M. Quade und R. Wölfle, SuisseID in der Praxis - Grundlagen und Fallbeispiele zum elektronischen Identitätsnachweis der Schweiz, Basel: edition gesowip, 2010, p. 88.

[22] P. Müller, «Die SuisseID als Unterstützung für E-Voting, eine Analyse der Möglichkeiten und Handlungsoptionen,» Berner Fachhochschule, Wirtschaftsinformatik, Bern, 2011.

[23] S. Strauß und G. Aichholzer, «National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design. International Journal on Advances in Intelligent Systems,» pp. 12-23, Vol. 3, Nrs. 1&2 2010.

[24] Riedl, R., E-Government Institut Bern, BFH, «Von unterschiedlichen nationalen eID-Strategien zum einheitlichen europäischen Identitäts-raum – ein Ländervergleich,» 03. Juni 2014. [Online]. Available: http://e-government.adv.at/2014/pdf/2_1100_Riedl_eGovernmentKonferenz_20140603.pdf. [Zugriff am 12. April 2015].

[25] M. Horsch, «Die Open eCard App für mehr Transparenz, Vertrauen und Benutzerfreundlichkeit beim elektronischen Identitätsnachweis,» in *13. Deutscher IT-Sicherheitskongress des BSI*, Bonn, 2013.

[26] Nok Nok Labs Inc., «Four Barriers To Adabpt Strong Authentication,» 2013. [Online]. Available: https://www.noknok.com/sites/default/files/whitepapers/4barrierswhitepaper_0.pdf. [Zugriff am 12. April 2015].

[27] M. Richter, «Kriterien der Benutzerfreundlichkeit,» Philosophische Fakultät der Universität Zürich, http://www.michaelrichter.ch/literat_97.pdf, 1997.

[28] NIST, «National Strategy for Trusted Identities in Cyberspace (NSTIC),» [Online]. Available: http://www.nist.gov/nstic/index.html. [Zugriff am 26 07 2016].

[29] B. Fachhochschule, F. Wirtschaft und E.-G. Institut, «eID- Ökosystem Modell,» Juni 2015. [Online]. Available: https://www.egovernment.ch/index.php/download_file/force/271/3343/. [Zugriff am 8 August 2016].

[30] Bundesrat, «Strategie des Bundesrates für eine digitale Schweiz,» Schweizerische Eidgenossenschaft, 20. April 2016. [Online]. Available: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/strategie.html. [Zugriff am 15 Mai 2016].

[31] E-Government Schweiz, «E-Government-Strategie Schweiz,» 24. Januar 2007. [Online]. Available: http://www.egovernment.ch/egov/00833/00834/index.html?lang=de. [Zugriff am 12. April 2015].

[32] E-Government Schweiz, «Roadmap E-Government Schweiz,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00852/index.html?lang=de. [Zugriff am 12. April 2015].

[33] E-Government Schweiz, «Katalog priorisierter Vorhaben,» 2015. [Online]. Available: http://www.egovernment.ch/umsetzung/00847/index.html?lang=de. [Zugriff am 12. April 2015].

[34] Schweizerische Bundeskanzlei, «E-Demokratie und E-Partizipation,» 2011. [Online]. Available: http://intranet.bk.admin.ch/themen/06367/index.html?lang=de. [Zugriff am 08 05 2015].

[35] NSTIC- National Strategy for Trusted Identities in Cyberspace, «The Identity Ecosystem: Use Examples;,» [Online]. Available: http://www.nist.gov/nstic/identity-ecosystem.html [Zugriff am 13. April 2015].. [Zugriff am 13 April 2015].

[36] EU, «Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185252017&uri=CELEX:32015D0296. [Zugriff am 29 07 2017].

[37] EU, «Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185296675&uri=CELEX:32015R1501. [Zugriff am 29 07 2016].

[38] EU, «Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185318253&uri=CELEX:32015R1502. [Zugriff am 29 07 2016].

[39] EU, «Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung,» [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455185344281&uri=CELEX:32015D1984. [Zugriff am 29 07 2016].

[40] Zentrale Ausgleichsstelle, «Verteilter Clearingprozess,» [Online]. Available: http://www.zas.admin.ch/org/00721/00758/00911/index.html?lang=de. [Zugriff am 25 07 2016].

[41] Bundeskanzlei, «E-Demokratie und E-Partizipation,» [Online]. Available: https://www.bk.admin.ch/themen/06367/index.html?lang=de. [Zugriff am 22 07 2016].

[42] Bundeskanzlei, «Vote électronique,» [Online]. Available: https://www.bk.admin.ch/themen/pore/evoting/index.html?lang=de. [Zugriff am 22 07 2016].

[43] Österreichische Staatsdruckerei, «MIA (My Identity App),» [Online]. Available: https://www.staatsdruckerei.at/produkte/identitaetsmanagement/mia-my-identity-app/. [Zugriff am 26 07 2016].

[44] MORPHO, «Electronic Driver License,» [Online]. Available: http://www.morpho.com/en/now-your-smartphone-could-be-your-drivers-license-too. [Zugriff am 26 07 2016].

[45] Bund, «Bundesgesetz über die elektronische Signatur, ZertES,» [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20011277/index.html. [Zugriff am 24 07 2016].

[46] European Commission, «Collaborative economy,» [Online]. Available: http://ec.europa.eu/growth/single-market/strategy/collaborative-economy/. [Zugriff am 23 07 2016].

[47] «The Trusted Execution Environment, Delivering Enhanced Security at a lower cost to the mo-bile market,» Februar 2011. [Online]. Available: http://www.globalplatform.org/documents/GlobalPlatform_TEE_White_Paper_Feb2011.pdf. [Zugriff am 12. April 2015].

[48] K. R. e. a. (Eds), The Future of Identity in the Information Society, Berlin - Heidelberg: Springer-Verlag, 2009.

[49] NIST Hildegard Ferraiolo, Larry Feldman and Greg Witte, «NIST Special Publication 800-157 - Guidelines for Derived Personal Identity Verification (PIV) Credentials,» Dezember 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf. [Zugriff am 12. April 2015].

[50] eCH, «eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,» 04. September 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0171. [Zugriff am 13. April 2015].

[51] eCH, «eCH-0170 Qualitätsmodell für elektronische Identitäten,» 06. Juni 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170. [Zugriff am 12. April 2015].

[52] ISO, «ISO Standard 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework,» 27. März 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138. [Zugriff am 13. April 2015].

[53] D. Hühnlein, «Identitätsmanagement-eine visualisierte Begriffsbestimmung,» *Datenschutz und Datensicherheit, Heft 3,* p. 163, 2008.

[54] M. Jakobsson und S. Taveau, «The Case for Replacing Passwords with Biometrics,» 2012. [Online]. Available: http://mostconf.org/2012/papers/3.pdf. [Zugriff am 12. April 2015].

[55] J. Grant, «Digital Identity in 2019: a vibrant identity ecosystem,» 2014. [Online]. Available: http://secureidnews.com/news-item/digital-identity-in-2019-a-vibrant-identity-ecosystem/#. [Zugriff am 12. April 2014].

[56] M. Schröder und F. Morgner, «Abgeleitete Identitäten,» 2013. [Online]. Available: https://www.bundesdruckerei.de/sites/default/files/documents/2013/08/fachartikel_dud_abgeleitete_identitaeten.pdf. [Zugriff am 12 April 2015].

[57] Meister, Gisela, Giesecke & Devrient, «Abgeleitete Identitäten – ein Überblick,» 25. September 2014. [Online]. Available: http://www.cast-forum.de/workshops/programm/194. [Zugriff am 12. April 2015].

[58] Global Platform Inc., «A new model: The consumer-centric model and how it applies to the Mobile ecosystem,» März 2012. [Online]. Available: http://www.globalplatform.org/documents/Consumer_Centric_Model_White_PaperMar2012.pdf. [Zugriff am 12. April 2015].

[59] «OASIS - Advancing Open Standards for the Information Society,» [Online]. Available: https://www.oasis-open.org/. [Zugriff am 12. April 2015].

[60] OASIS, «OASIS - SAML Wiki,» [Online]. Available: https://wiki.oasis-open.org/security/FrontPage. [Zugriff am 12. April 2015].

[61] Schweizer Bundesrat, «Informationsgesellschaft in der Schweiz,» März 2012. [Online]. Available: http://www.bakom.admin.ch/themen/infosociety/. [Zugriff am 12. April 2015].

[62] EU, «STORK,» 2015. [Online]. Available: https://www.eid-stork.eu/. [Zugriff am 12. April 2015].

[63] Schweizer Bundesrat, «Bundesratsbeschluss zur Ausarbeitung eines Gesetzgebungspaketes zur Förderung des elektronischen Geschäftsverkehrs,» 19. Dezember 2012. [Online].

[64] SuisseID, «SuisseID,» 2015. [Online]. Available: http://www.suisseid.ch/de. [Zugriff am 12. April 2015].

[65] Mondinis Workshop, «Mondinis Study on Identity Management in eGovernment; Common Terminological Framework for Interoperable Electronic Identity Management; V2.01,» DG Information Society and Media; EU Commission, 23 November 2005. [Online]. Available: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf. [Zugriff am 13 April 2015].

[66] D. Miessler, «Daniel Miessler Blog; Security: Identification, Authentication, and Authorization,» [Online]. Available: https://danielmiessler.com/blog/security-identification-authentication-and-authorization/ . [Zugriff am 13 April 2015].

[67] G. Doe, «Difference Between Identification & Authentication;,» Demand Media; , [Online]. Available: http://science.opposingviews.com/difference-between-identification-authentication-3471.html . [Zugriff am 13 April 2015].

[68] I. 1. Standard, «Common Criteria for Information Technology Security Evaluation».

[69] R. Dholakia, «A question of Scale,» NokNok Labs, 2012.

[70] D. O'Shea, «Fido U2F & UAF Tutorial,» in *World e-ID Congress, Marseille 2014*, Marseille, 2014.

[71] Bundesversammlung, «Ausweisgesetz (AwG, SR 143.1),» 01 Jan 2013. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19994375/index.html. [Zugriff am 08 Mai 2015].

[72] SkIDentity, «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Zugriff am 09. Mai 2015].

[73] Verein eGov-Schweiz, «Bürgerdossier,» 2015. [Online]. Available: http://www.egov-schweiz.ch/media/archive2/eGov_Flyer_Buergerdossier_def.pdf. [Zugriff am 09. Mai 2105].

[74] E-Government Schweiz, «Identititätsverbund Schweiz (IDV Schweiz),» 2015. [Online]. Available: http://www.egovernment.ch/b206/index.html?lang=de. [Zugriff am 09. Mai 2015].

[75] «eID-Integration aus der Cloud,» 2015. [Online]. Available: www.skidentity.de. [Zugriff am 12. April 2015].

[76] H. STORCK 2.0, «STORK - Secure idenTity acrOss boRders linKed 2.0,» STORK 2.0 project group, [Online]. Available: https://www.eid-stork2.eu/. [Zugriff am 9 11 2015].

[77] Bundesamt für Statistik, «Nutzungszwecke,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=302#302. [Zugriff am 22 07 2016].

[78] Bundesamt für Statistik, «Nutzungshäufigkeit von Online-Fomularen,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30302.4.html?open=335#335. [Zugriff am 22 07 2016].

[79] Bundesamt für Statistik, «Nutzung des Internets,» [Online]. Available: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/03/key/ind16.indicator.30106.160204.html. [Zugriff am 22 07 2016].

[80] FINMA, «FINMA ermöglicht Video- und Online-Identifizierung,» 21 12 2015. [Online]. Available: https://www.finma.ch/de/news/2015/12/20151221-mm-videoidentifizierung/. [Zugriff am 15 7 2016].