Beilage 05

Konzeptstudie

Positionierung einer staatlichen eID im Identitäts- und Zugangsmanagement

An	fedpol eID Projektgruppe
Von	[redacted]
Klassifizierung	intern
Status	Diskussionsgrundlage für weiteres Vorgehen im Bereich eID
Datum, Version	10.11.2014 / V2.01

Änderungsverzeichnis

Datum	Version	Änderung	Autor
25.8.2014	1.0	Erster Entwurf	[redacted]
29.10.2014	2.0	Konsolidiertes Konzept	[redacted]
10.11.2014	2.01	Überarbeiter Text	[redacted]

Vorbemerkung:

Auf verschiedenen Ebenen wurden Vorabklärungen zum Nutzen und der Nutzbarkeit einer eID Funktion in einem staatlichen Identifikationsmittel getätigt. Es hat sich gezeigt, dass die bisher in Nachbarstaaten verfolgten Ansätze und die teilweise ausgerollten Systeme mit hoher Regeldichte die Erwartungen bezüglich Einsatz in der Praxis nicht erfüllen konnten. Für eine erfolgreiche staatliche eID Lösung muss das Grundkonzept vermehrt und flexibel an den Bedürfnissen der Bürger, der Wirtschaft und der Behörden ausgerichtet werden. Nutzerfreundlichkeit und einfache Schnittstellen zu bestehenden identitätsbasierten Diensten sind zwingende Voraussetzungen für die Akzeptanz einer staatlichen eID. Eine eID Lösung und die entsprechende Regulierung müssen sich in die nationalen und internationalen Systeme des Identitäts- und Access Management (IAM) integrieren und so offen sein, dass sie jeweils bei Bedarf an neue erfolgreiche Entwicklungen im IAM Ökosystem [1] angepasst werden können.

Diese Anforderung führt zu einem auf die Kernfunktion der staatlichen Ausstellung und Garantie von Identitäten konzentrierten und damit subsidiären Lösungskonzept für die staatliche eID. Die tägliche Authentifizierung der Personen im Feld gehört nicht dazu. Vielmehr nutzt die vorgeschlagene Lösung für eine schweizerische eID (CH-eID) die sich entwickelnden Authentifizierungsmethoden des freien Marktes und wird im IAM entsprechend positioniert.

Im vorliegenden Dokument wird ein eID-System skizziert, das diese Vorgaben berücksichtigt und die staatliche eID in eine universelle IAM Architektur mit getrenntem Authentifizierungsmodell integriert, wie es zum Beispiel von der FIDO Alliance propagiert wird [2] und wie es sich offensichtlich in der Praxis bereits durchzusetzen beginnt.

Die Begriffsverwendung [3] in diesem Dokument ist im Glossar definiert.

Inhaltsverzeichnis

1 Ausgangslage und Rahmenbedingungen

1.1 Auftrag des Bundesrates

Das EJPD wurde vom Bundesrat am 19. Dezember 2012 beauftragt, in Zusammenarbeit mit der BK, dem EVD, UVEK und EFD, eine Vernehmlassungsvorlage für ein künftiges staatliches elektronisches Identifizierungsmittel (eID), welches zusammen mit der neuen Identitätskarte angeboten wird, bis Mitte 2014 vorzulegen. Mit der eID sollen eine starke Online-Authentisierung und der Online-Nachweis von Identitätsattributen (z.B. Name oder Alter) für alle Schweizerinnen und Schweizer ermöglicht werden.

1.2 Bisherige Arbeiten

Mit dem Aussprachepapier «Einführung einer staatlichen elektronischen Identität (eID) zusammen mit der neuen Identitätskarte (IDK) -Vorentscheide und weiteres Vorgehen» vom 18. März 2014 hat das EJPD den BR über seinen Vorentscheid für die staatliche Ausgestaltung der eID informiert. Gestützt auf das Aussprachepapier und den entsprechenden Bundesratsbeschluss wurde ein Konzept und ein Entwurf für die rechtliche Ausgestaltung („eID-Gesetz") erarbeitet und vom 23. Juni bis 11. Juli 2014 bei den Ämtern konsultiert.

Die vorgeschlagene eID-Lösung orientierte sich am neuen Personalausweis (nPA) von Deutschland, der in Bezug auf Datenschutz und Sicherheit vorbildlich realisiert wurde. Genauso wie der nPA erfüllt die bisher bei fedpol und im BJ andiskutierte staatlich eID implizit zwei eigentlich unterschiedliche Zwecke. Einerseits sollte die eID auf der IDK (eIDK) einer vertrauenden Partei die Feststellung ermöglichen, dass sie im Moment mit der angenommenen Person interagiert (Authentifizierung) und andererseits sollte die eID der IDK gewisse Identitätsattribute zu einer Person liefern (Identifizierung) bzw. die Richtigkeit solcher Attribute staatlich bestätigen können. Authentifizierung und Identifizierung haben zwar wesentliche Bezugspunkte, erfüllen aber unterschiedliche Bedürfnisse. Die klassische IDK erfüllt in der Welt der direkten Begegnungen zwischen Personen beide Funktionen, wobei in einer konkreten Anwendungssituation oft nur eine Authentifizierung oder ein Nachweis für bestimmte Identitätsattribute verlangt wird.

In der Welt der Begegnungen zwischen einer Person und einer vertrauenden Partei über ein zwischengeschaltetes elektronisches Medium (Internet, Telefon, Automaten) sind ebenfalls eine Reihe von vertrauensbildenden Absicherungsmassnahmen nötig. Diese umfassen situationsbedingt die Feststellung, dass die Person einer bei der vertrauenden Partei registrierten Entität entspricht (Authentifizierung), die allfällige Erhebung zusätzlicher Identitätsattribute (Identifizierung) insbesondere für die Erstregistrierung bei der Aufnahme einer Beziehung und eine Absicherung der gegenseitigen Mitteilungen (Transaktionsabsicherung).

1.3 Reflexion

Im Nachgang zur Ämterkonsultation stellte sich die Frage, ob das zur Beurteilung vorgelegte Konzept einer staatlichen eID zu wenig auf die eigentliche Kernfunktion, die Identifizierung, fokussiert war. Insbesondere muss hinterfragt werden, ob die klassische IDK wirklich der richtige physische Träger einer solchen eID ist und ob das Konzept nicht wesentlich vereinfacht werden könnte. Es gab gleich mehrere Gründe für eine kritische Reflexion des Vorschlags. Erstens erhärteten sich ab Juni 2014 die Indizien, dass der nPA in Deutschland keine Akzeptanz findet, weil er zwar perfekt, aber in der täglichen Handhabung zu kompliziert ist [4]. Zweitens zeichnete sich ab, dass die Umsetzung des geplanten Konzepts in der Schweiz trotz gewissen Vereinfachungen hohe Betriebskosten für den Bund verursachen würde (Kundensupport, dauernde Aktualisierung der Lesesoftware). Drittens trat fast zeitgleich eine mächtige Allianz von Firmen auf den Markt, welche ein neues universelles Konzept für die starke Online-Authentisierung basierend auf persönlichen mobilen Geräten vorantreibt (FIDO-Allianz). Und viertens ergab die durchgeführte Ämterkonsultation wertvolle

Hinweise, namentlich in Bezug auf die Verwendung der AHVN13 und den Einsatz der eID als Identifikationsmittel durch Banken, die in der Konzeption berücksichtigt werden müssen.

Darüber hinaus hat sich bei Gesprächen mit anderen Ländern bestätigt, dass für einen Erfolg einer eID zusätzlich Fördermassnahmen notwendig sind. Das SECO hat dazu die Konzeption eines umfassenden 'Identitäts-Ökosystems' in Auftrag gegeben. Dabei wird u.a. geprüft, ob auch in der Schweiz ein Anreizsystem geschaffen werden soll, welches den Aufbau entsprechender Einsatzmöglichkeiten der eID bei staatlichen Diensten und Angeboten der Privatwirtschaft fördert und dazu eine Unterstützung anbietet.

1.4 Weiteres Vorgehen

In einer Standortbestimmung kam das EJPD zum Schluss, dass die erarbeiteten Konzepte und die rechtliche Ausgestaltung unter Einbezug der oben genannten Befunde nochmals kritisch geprüft werden sollen. Am 11. August 2014 wurde in einer Sitzung mit Vertretern des BJ und der fedpol beschlossen den eingangs genannten Entwurf des eID Gesetzes, der in die Ämterkonsultation gegeben wurde, grundsätzlich zu überarbeiten und damit den ursprünglichen Zeitplan für die Einführung eines eID Gesetzes mit Einverständnis der Departementsleitung zu verlassen. Eine Überarbeitung des Konzepts und der Grundannahmen erweist sich als zwingend um einen Erfolg der staatlichen eID zu ermöglichen.

Die Priorisierung der Sicherheit und des Datenschutzes zu Lasten der Nutzerfreundlichkeit und der einfachen Anwendbarkeit muss differenzierter betrachtet werden. Es macht auch wenig Sinn ein langfristig gültiges eID-System stark an den momentanen Stand der Technik auszurichten. Das eID-System sollte konzeptionell deutlich über der Ebene der technischen Realisierung spezifiziert werden, so dass zukünftige technische Entwicklungen problemlos integriert werden können.

Die Planung des EJPD sieht vor, dass diese Arbeiten zur Überprüfung des Konzepts einschliesslich der Erstellung eines Zeitplans für das weitere Vorgehen bis Mitte 2015 abgeschlossen werden können. Danach werden die Arbeiten für die rechtliche Umsetzung einschliesslich Vernehmlassung und die vorgesehene öffentliche Ausschreibung der Schweizer Identitätskarte wieder aufgenommen.

2 Zielsetzung und Strategie

Dieses Memo ist ein Startpunkt für die weitere Diskussion wie in der Schweiz eine sinnvolle Positionierung und Umsetzung einer staatlichen eID erreicht werden kann. Es ist notwendig nochmals eine vertiefte Abklärung der Bedürfnisse im Zusammenhang mit der Authentifizierung und Identifizierung von Personen im Feld zu treffen. Eine staatliche eID soll vertrauenden Parteien in der Wirtschaft, den Behörden und der Gesellschaft die Möglichkeit geben, einer Person bei der Registrierung in ihrem IAM System staatlich garantierte Identitätsattribute zuzuordnen oder über spezialisierte Identitätsdienste bereits verifizierte Attribute abzurufen.

Die schweizerische Lösung soll zudem mit den europäischen Systemen interoperable sein und insbesondere die Voraussetzungen für die Notifizierbarkeit gemäss der eIDAS Verordnung (Art 6,7,9) erfüllen. Gleichzeitig muss sie sich auch an den internationalen Trends im IAM-Ökosystem orientieren, wie zB. den Arbeiten und Spezifikationen von NIST zur digitalen Authentifizierung, der FIDO Alliance zur Authentifizierung und Transaktionsabsicherung sowie der zunehmend akzeptierten Sicherheitsarchitektur der GlobalPlatform Organisation für mobile Geräte, die mit dualen Betriebssystemumgebungen arbeitet, wobei eine davon als Trusted Execution Environment (TEE) speziell in der Hardware abgesichert ist (siehe Anhang 1). Generell muss davon ausgegangen werden, dass Authentifikationsmittel vermehrt mit Hilfe von ausgerollter und sich ständig erneuernder Consumer-Elektronik realisiert werden und dedizierter Hardware sich auf geeignete Einschübe beschränkt (zB SIM Karten).

Die Basis für eine staatliche eID ist eine sichere erste Authentifizierung und Identifizierung der Person in einem staatlich kontrollierten Erfassungs- und Ausgabeprozess. Der Staat definiert auch Vorgaben zum Mechanismus, wie die Person die garantierten Identitätsattribute danach einer vertrauenden Partei über elektronische Medien vorweisen kann. Ein solcher elektronischer Identitätsnachweis erfolgt immer in Kombination mit einer hinreichend vertrauenswürdigen Authentifikation der sich ausweisenden Person. Die elektronische Fernauthentifizierung auf einem definierten Sicherheitsniveau ist ein Hauptprozess im IAM auf dem auch die Nutzung einer eID aufbaut. Die zivilen Identitätsattribute haben in der Regel eine langfristige Gültigkeit und die Überprüfungsmechanismen können vom Staat bestimmt werden. Die Authentifizierung im Feld hingegen unterliegt raschen technischen Entwicklungen und wird bereits durch viele Systeme von unterschiedlichen Institutionen realisiert.

Es ist deshalb anzustreben, die staatliche eID auf die optimale Realisierung und Anwendbarkeit (federation, „2nd mile") der Identifizierungsfunktionen zu konzentrieren und den Authentifizierungsprozess soweit als möglich den etablierten und neu aufkommenden Mechanismen im IAM-Ökosystem zu überlassen.

2.1 Anforderungen und Prioritäten für eine staatliche eID

Im IAM-Ökosystem ist die eID nur ein Werkzeug um eine Vertrauensbeziehung zwischen einem Nutzer und einer vertrauenden Partei aufzubauen. Sie ist die (lästige) Eintrittshürde, welche der Nutzer und die vertrauende Partei nehmen müssen, um danach viel mächtigere und nutzenbringendere Transaktionen zu tätigen oder Identitätsattribute auszutauschen. Wie hoch dieses Absicherungsniveau sein soll, bestimmen Nutzer und vertrauende Partei gemeinsam: für nicht heikle Transaktionen vermutlich eher tief, für heikle Transaktion aber eher hoch. Ein eID-System muss auf diese unterschiedlichen Bedürfnisse eingehen können, um erfolgreich zu sein. Zudem sollte das eID-Werkzeug im gesamten IAM-Ökosystem seine Funktion erfüllen können.

Die wichtigsten Anforderungen für den Gebrauch eines neuen Werkzeugs im IAM-Ökosystem sind nach Priorität geordnet:

- Unmittelbarer Nutzen für die Anwender und für die der eID vertrauenden Parteien
- Einfachheit und Komfortgewinn beim Einsatz der eID
- Einfache Integrierbarkeit in bestehende Systeme
- Interoperabilität über europäische Landesgrenzen hinweg
- Sicherheit für und Schutz von privaten Daten bei der Anwendung

Last but not least sollte das schweizerische eID-System (CH-eID) für den Staat und die Anwender vertretbare Kosten und keinen unnötigen Aufwand verursachen. Bestehende Abläufe in der Verwaltung und im Kontakt mit den Bürgern sollen soweit als möglich genutzt und bei Bedarf erweitert werden. Die CH-eID soll in den anstehenden grösseren Entwicklungsprojekten des eGouvernements (IAM Projekt des Bundes, eHealth, eVoting etc) als Baustein für den Nachweis der staatlichen Identitätsattribute eingesetzt werden und entsprechende Schnittstellen sind bereitzustellen und gesetzlich abzustützen.

2.2 IAM-Hauptprozess - Authentifizierung

Die notwendige Basis für eine sichere Durchführung einer beliebigen identitätsbasierten Transaktion ist die wechselseitige Authentifizierung der involvierten Parteien. Dies bedeutet, dass sich beide Parteien zuerst gegenseitig kennenlernen und sich bei jeder neuen Begegnung wiedererkennen können.

Das Fundament für eine sichere gegenseitige Authentifizierung ist ein Entdeckungs- und Registrierungsprozess, bei dem die möglichen Authentifizierungsfaktoren der involvierten Parteien abgeklärt (Entdeckung) werden und mindestens je ein Merkmal festgestellt und ausgetauscht wird (Registrierung), das eineindeutig und unbestreitbar jeder der Parteien zugeordnet ist. Für eine spätere Wiedererkennung (Authentifizierung) muss dann je mindestens ein solches Merkmal gegenseitig überprüft werden können.

Wünschenswert ist, dass die ausgetauschten Merkmale und deren Überprüfung nur von den beiden involvierten Parteien ausgewertet werden können (Schutz der Privatsphäre) und dass anstelle von personenbezogenen Merkmalen kryptographische Tokens, die für eine erfolgreiche Authentifikation stehen, ausgetauscht werden (Datenschutz). Solche Konzepte, Mechanismen und Methoden, die für eine wechselseitige Authentifizierung notwendig sind, werden zum Beispiel durch die Entwürfe für die FIDO Standards beschrieben und spezifiziert (siehe dazu Anhang 3).

2.3 Identifizierung und Transaktionsabsicherung

Für die weitere Diskussion ist die Feststellung wichtig, dass die Authentifizierung (Wiedererkennung einer Person) der IAM-Hauptprozess ist. Auf einer erfolgreichen Authentifizierung lassen sich Subprozesse aufsetzen, wie zum Beispiel die Verifikation von zusätzlichen Identitätsattributen, die Absicherung von Transaktionen oder auch weitere komplexe Kombinationen solcher Prozesse wie das eVoting. Je nach Charakter der identitätsbasierten Leistung kann es notwendig sein, dass zusätzliche Identitätsattribute der einen oder anderen Partei ausgetauscht und bestätigt werden (Identifizierung) und/oder dass die Richtigkeit der Transaktionsdaten bestätigt werden (Transaktionsabsicherung) (siehe Anhang 4). Die eID wird für die Abdeckung zusätzlicher Identifizierungsanforderungen und punktuell auch für die Absicherung von Transaktionen gebraucht, falls letztere auf gewisse Identitätsattribute wie zum Beispiel das Alter angewiesen sind.

3 Positionierung der staatlichen eID

Die Entstehung eines unmittelbaren Nutzens für die Anwender ist die wichtigste Anforderung an die eID. Im täglichen Gebrauch bei der Aufnahme einer identitätsbasierten Geschäftsbeziehung zwischen einem Kunden und einem Dienstleister (Vertrauende Partei, VP) liefert der Kunde die nötigen Identitätsattribute an den Dienstleister und es wird definiert, wie sich der Kunde in Zukunft ihm gegenüber authentifizieren muss (Authentifizierungsform und –niveau). Der Dienstleister wird je nach Charakter der geplanten Beziehung oder Transaktion gewisse Überprüfungen der gelieferten Identitätsattribute und insbesondere deren Zuordnung zur authentifizierten Person vornehmen wollen. Dazu wird er meist auf einen möglichst einfach verfügbaren Identitätsnachweis eines vertrauenswürdigen Dritten zurückgreifen. In der physischen Begegnung ist dies sehr oft ein staatlicher Ausweis. In der Onlinewelt können spezialisierte Identitätsdienstleister (Identity Provider, IdP) eine entsprechende Bestätigung liefern, wenn der Kunde vorgängig mit dem IdP einen Authentifizierungsprozess vereinbart und hinreichend überprüfte Identifikationsattribute hinterlegt hat. Mit der eID kann der Kunde verlangte Identitätsattribute mit staatlicher Garantie direkt oder via einen unmittelbar eingeschalteten IdP liefern und die beiden Parteien können die erwünschte identitätsbasierte Transaktion sofort durchführen.

3.1 Identitätsdienstleister (IdP)

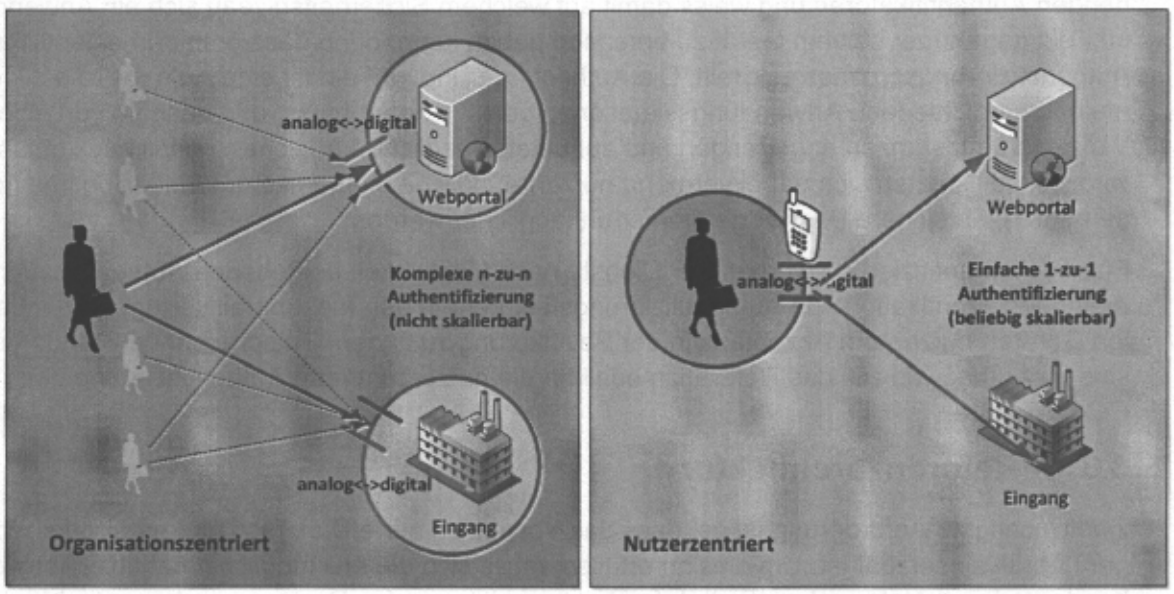
Es gibt bereits eine ganze Reihe von IdP oder IdP ähnlichen Diensten (Identity Broker), die speziell im Umfeld der Onlinebezahlsysteme entstanden oder im Aufbau begriffen sind (Apple, Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace, SuisseID Providers, OpenID, Telcom Operators, Zertifikatsausteller, Kreditkartenorganisationen, Banken, Behörden und viele mehr). Für die erste Erfassung von Identitätsattributen greifen viele dieser

Dienste auf leicht verfügbare Identitätsattribute, wie zum Beispiel Email Adressen, Kreditkartennummern, Telefonnummern und ähnliche, leicht elektronisch verifizierbare Attribute zurück, jeweils in der Hoffnung oder Erwartung, dass diese Attribute letztendlich via Ausstellungsprozess mit staatlich garantierten Identitätsattributen verbunden sind. Es ist klar, dass dies natürlich nicht immer der Fall ist und die Identifizierung von Personen deshalb mangelhaft sein kann.

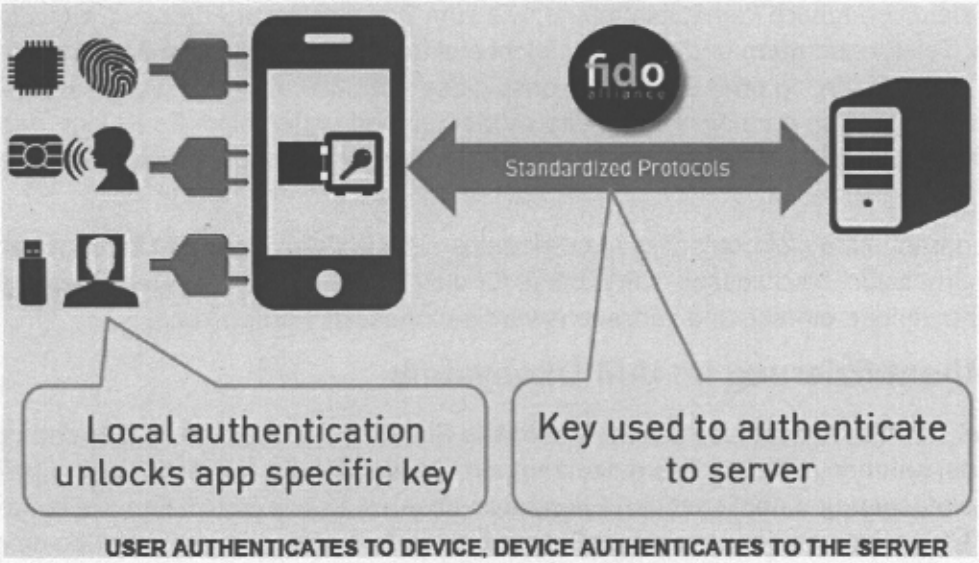
Ein staatlich garantiertes elektronisches Identifikationsmittel in Form einer eID kann genau diese Unsicherheitslücke schliessen, wenn diese für die IdP Dienste bei der Registrierung der Nutzer unmittelbar, einfach und vertrauenswürdig eingesetzt werden kann.

3.2 Authentifizierung im IAM-Ökosystem

Wie in Kapitel 2.2 erläutert, ist die Authentifikation die Eintrittshürde, welche Nutzer und vertrauende Partei nehmen müssen. Das nutzerzentrierte Modell für die Authentifizierung basiert auf der einfachen und nahliegenden Erkenntnis, dass es für alle Beteiligten viel einfacher ist, den Übergang von der physischen Präsenz zu einer digitalen Repräsentation einer Person (analog-zu-digital) in ein Gerät zu integrieren, das möglichst nahe und im ständigen Besitz des Nutzers ist, als in jeder Organisation komplexe Erkennungssysteme für Personen zu unterhalten. Die Authentifizierung verlagert sich deshalb von einem organisationszentrierten Modell zu einem nutzerzentrierten Modell mit der Nutzerverifikation gegenüber einem persönlichen Gerät. Dieser Paradigmenwechsel ist zentral für die weiteren Überlegungen.



Diese Erkenntnis führt zum Konzept der persönlichen Authentifikationssysteme, im FIDO-Modell als Authentifikatoren bezeichnet (siehe die Erläuterung im Anhang). Die neueren Generationen von mobilen Geräten mit sogenannten Trusted Execution Environments (TEE) ermöglichen die einfache Implementierung und die Interoperabilität von FIDO-Authentifikatoren in der heterogenen Infrastruktur des IAM Ökosystems. Das von FIDO entwickelte Architekturmodell für die nutzerzentrierte Authentifizierung, mit verschiedenen Authentifikatoren unterschiedlicher Stärke und an bestimmte Dienste gebunden, kann als generisches Beispiel für zukünftige Authentifizierungslösungen angesehen werden und entwickelt sich zum Referenzmodell für Authentifizierung im IAM Ökosystem.



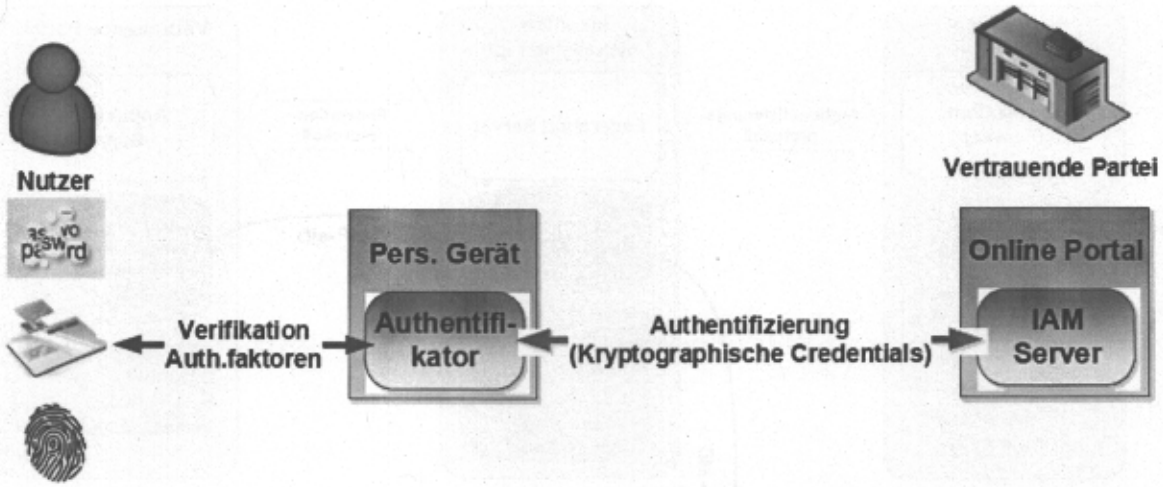
USER AUTHENTICATES TO DEVICE, DEVICE AUTHENTICATES TO THE SERVER

Je nach Charakter des IdP Dienstes definiert dieser einen (oder mehrere) Authentifizierungsprozess für seine Kunden auf dem von ihm benötigten Absicherungsniveau (die Absicherungsniveaus können gemäss eIDAS, ISO/IEC-29115 oder nach weiter verfeinerten Modellen klassifiziert werden). Er erfasst die Charakteristiken der dem Kunden zur Verfügung stehenden Authentifikatoren und weiss damit auf welchem Sicherheitsniveau sich ein Anwender im Feld gegenüber seinem Gerät zu erkennen geben kann, ohne dass er in den eigentlichen Authentifizierungsprozess eingreift. Die Authentifizierung im Feld ist eine Aufgabe, die allgemein für verschiedene Anwendungssituationen gelöst werden muss, und deshalb von einer Vielzahl von Instanzen angegangen und auf unterschiedlichen Absicherungsniveaus gelöst wird. Aktuell setzten sich dabei vermehrt nutzerfreundliche biometrische Verifikationsmethoden durch, da sichere Passwörter immer unhandlicher werden.

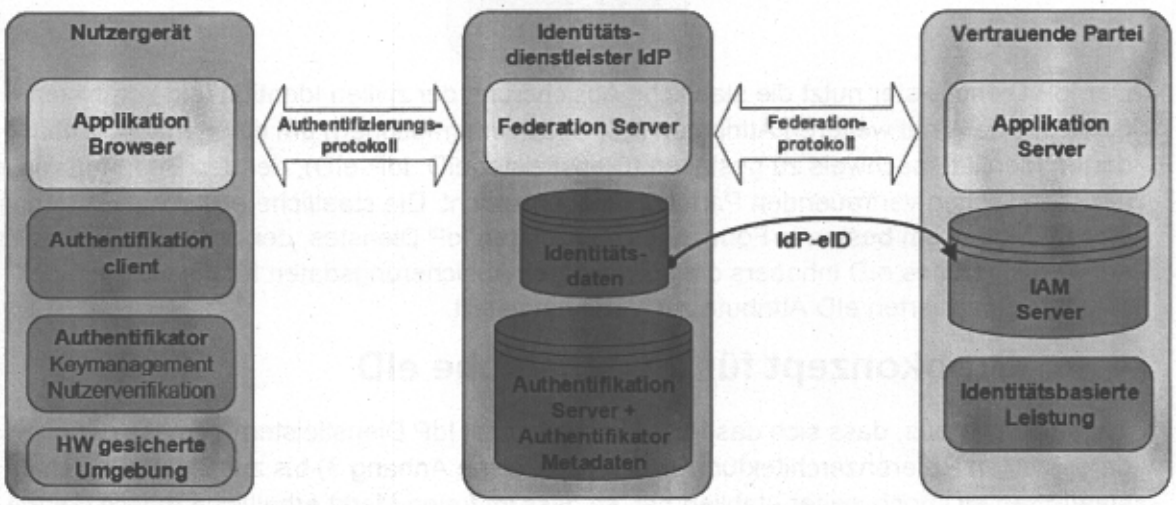
Für die Authentifizierung werden IdP Dienste nach Möglichkeit bestehende Authentifikationsmethoden (Verifikation von Authentifizierungsfaktoren) in den fast überall verfügbaren mobilen Geräten nutzen um Akzeptanz in der Bevölkerung zu finden. Entsprechende Standards sind im Aufbau wie zB. das Referenzmodell für die nutzerzentrierte Authentifizierung der FIDO Alliance.

3.3 Referenzarchitektur

Zweitwichtigste Anforderung ist es, dass das Vorweisen der eID einfach und mehr oder weniger überall einsetzbar ist. Um dies zu erfüllen, muss sich die eID möglichst nahtlos in bestehende und vom Nutzer akzeptierte Infrastrukturen integrieren. Das generische und in der IT-Welt zunehmend akzeptierte Architekturmodell für identitätsbasierte digitale Dienstleistungen, das zum Beispiel auch von der FIDO Alliance propagiert wird, trennt die Funktion der Authentifizierung von der Identifizierung des Nutzers. Die nutzerzentrierte Authentifizierung wird lokal von einem Gerät im Feld durchgeführt, das unter dessen Kontrolle ist. Auf dem Nutzergerät ist eine abgesicherte Funktion (Authentifikator) realisiert, die feststellt, ob eine bestimmte Person sich mit den verlangten Faktoren ausgewiesen hat. Bei erfolgreicher Erkennung des Nutzers (Verifikation) aktiviert der Authentifikator einen verbindungsspezifischen Schlüssel, der für die Abwicklung einer Transaktion mit dem Dienstleister notwendig ist. Dieser Mechanismus wird vom Nutzer gebraucht um sich bei allen Dienstleistern zu authentifizieren; gleichzeitig erfolgt durch den Schlüsseltausch implizit jeweils auch eine Authentifizierung des Dienstleisters gegenüber dem Nutzer.



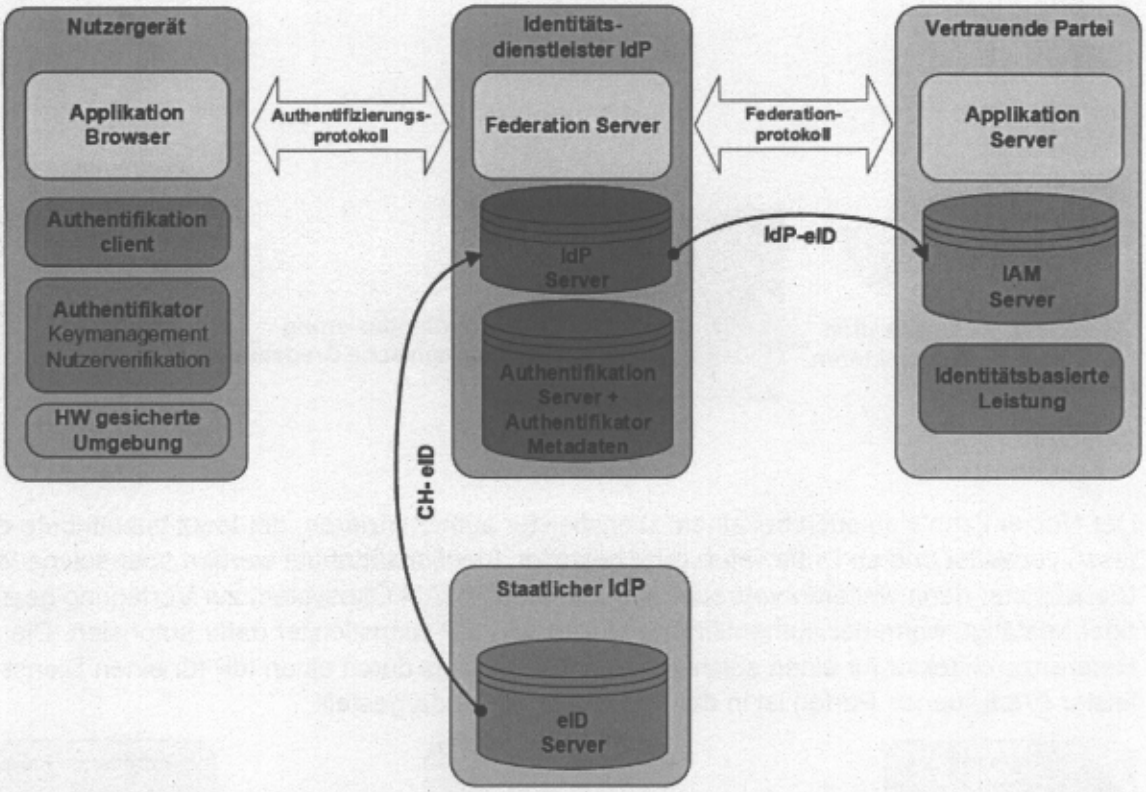
Der Nutzer kann sich auch bei einem Dienstleister authentifizieren, der Identitätsattribute erfasst, verwaltet und an Dritte liefert oder bestätigt. Identitätsattribute werden über solche IdP Dienstleister dann weiteren vertrauenden Diensten im IAM Ökosystem zur Verfügung gestellt oder bestätigt, wenn der authentifizierte Nutzer den IdP Dienstleister dafür autorisiert. Die Referenzarchitektur für einen solchen Identitätsnachweis durch einen IdP für einen Dienstleister (Vertrauende Partei) ist in der folgenden Skizze dargestellt.



Insbesondere kann der Nutzer einem solchen IdP Dienstleister auch seine staatlich garantierten Identitätsattribute zur Verfügung stellen, wenn gewisse Voraussetzungen bezüglich Sicherheitsniveau der Nutzerauthentifizierung erfüllt sind. Solche IdP Dienstleistungen können von Brokern für beliebige vertrauende Parteien im IAM Ökosystem geleistet werden oder als Proxy-Service von grossen Anbietern von identitätsbasierten Diensten im eigen IAM System selbst betrieben werden.

3.4 Rolle der eID im IAM Ökosystem

Die staatliche eID bringt den grössten Nutzen für alle Seiten, wenn der Anwender sie, ähnlich wie eine IDK in der physischen Erstbegegnung, in der Online Erstregistrierung bei einer vertrauenden Partei (Dienstleister) einsetzen kann. Im IAM Ökosystem lagern vertrauende Parteien die Authentifizierung und die Identifizierung immer mehr an IdP Dienstleister aus oder betreiben spezialisierte IAM Systeme mit IdP Funktionalität. Deshalb wird der Normalfall eines Einsatzes der staatlichen eID die Erstregistrierung von staatlichen Identitätsattributen in einem IdP Server sein. Die schematische Integration einer solchen staatliche Identitätsdienstleistung im Referenzmodell ist in der folgenden Skizze dargestellt.



Der IdP Dienstleister nutzt die staatliche Absicherung der zivilen Identität und kombiniert diese allenfalls mit weiteren Attributen (zB. Bezahlinformationen) um einen massgeschneiderten Identitätsnachweis zu gestalten (Dienstleister eID, IdP-eID), der den Bedürfnissen einer spezifischen vertrauenden Partei optimal entspricht. Die staatliche eID integriert sich in diesem Modell am besten in Form eines subsidiären IdP Dienstes, der den operativen IdPs auf Verlangen des eID Inhabers die notwendigen Absicherungsdaten für die Nutzung der staatlich garantierten eID Attribute zur Verfügung stellt.

4 Grobkonzept für die staatliche eID

Wir setzen voraus, dass sich das IAM-Ökosystem mit IdP Dienstleistern gemäss der oben dargestellten Referenzarchitektur (FIDO Modell, siehe Anhang 3) bis zur Einführung einer staatlichen eID noch weiter etabliert hat, so dass im freien Markt erhältliche mobile Geräte (Smartphones, Tablets, Notebooks etc) immer mit entsprechenden Lösungen (Clients, Authentifikatoren) ausgerüstet werden können. Zudem werden die Geräte, auf denen die Authentifikations-Clients installiert sind, akzeptabel sicher sein und sinnvollerweise über eine Trusted Execution Environment (TEE) verfügen (vgl. Anhang 1). Diese Annahmen sind kaum einschränkend, da sie der natürlichen Entwicklung zur mobilen IT-Welt entsprechen, wie sie bereits heute im Gang ist [5]. Die Annahme stellt auch keine unerwünschte Ausrichtung auf einen momentanen Stand der Technik dar, sondern erlaubt praktisch alle möglichen technischen Entwicklungsrichtungen.

4.1 Staatliche eID Funktion

Die staatliche eID Funktion beinhaltet die Absicherung staatlich garantierter Identitätsattribute der zivilen Identität, wie Namen, Geburtsdaten oder ein eindeutiger Personenidentifikator, wie er zum Beispiel in der eGovernment Strategie als wichtige Massnahme im Hinblick auf ein kundenfreundliches Einstiegsportal für staatliche elektronische Dienstleistungen verlangt wird. Diese Daten (siehe Anhang 2) werden im Rahmen des Antragsprozesses für einen Pass oder eine IDK zuverlässig – eben staatlich – ermittelt und im Falle der genannten Ausweise im ISA abgespeichert.

Die staatliche Bereitstellung von Identitätsattributen in elektronischer Form via einen CH-IdP und die Integration des IdP Dienstes in das oben vorgestellte Referenzmodell ist der notwendige Beitrag zum IAM Ökosystem, der vom Staat realisiert werden muss, wenn er eine staatliche eID herausgibt. Im Rahmen der Ausstellung der eID muss sichergestellt werden, dass nur die berechtigte Person diese nutzen und weiteren IdP Diensten bzw vertrauenden Parteien zur Verfügung stellen kann.

4.2 eID Prozesse

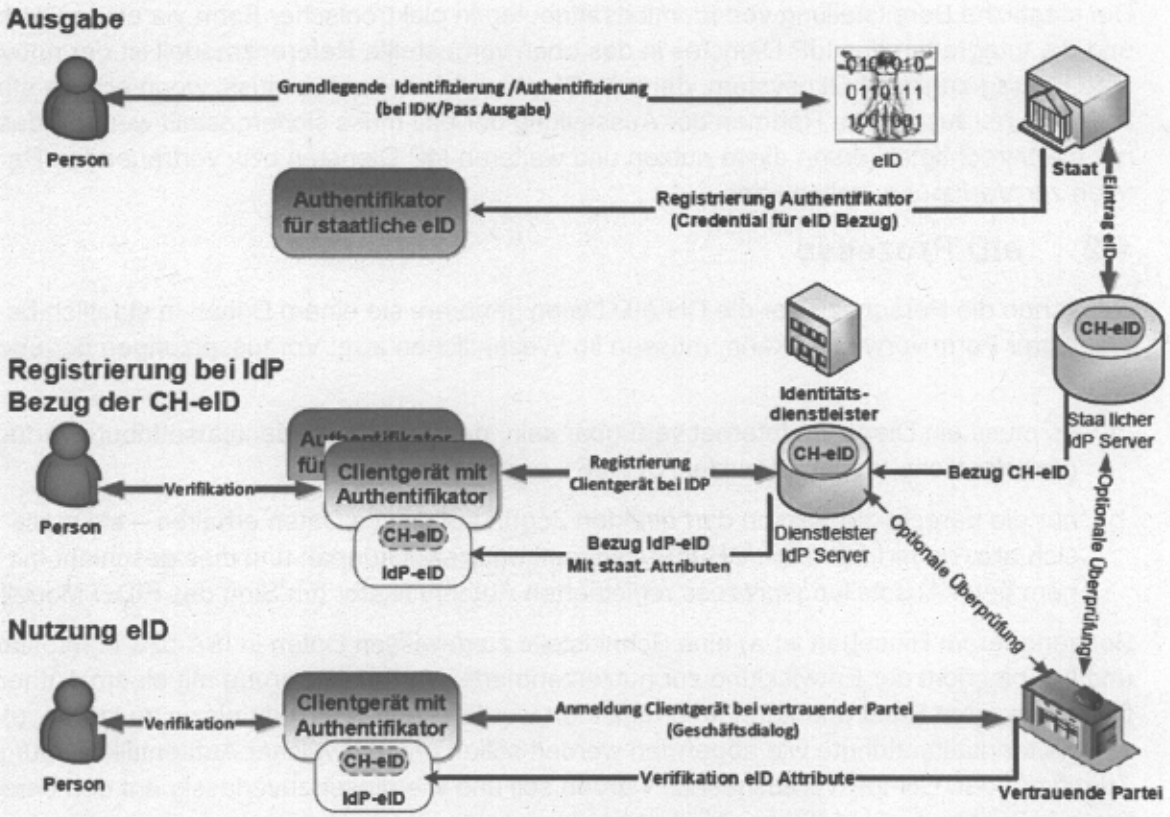
Damit nun die Person, zu der die CH-eID Daten gehören, sie einem Dritten in staatlich beglaubigter Form vorweisen kann, müssen im Wesentlichen zwei Voraussetzungen gegeben sein:

a. es muss ein Dienst im Internet verfügbar sein, der über diese Identitätsattribute verfügt (der staatliche Identity Provider, CH-IdP); und

b. nur die berechtigte Person darf direkten Zugriff auf dieses Daten erhalten – sie muss sich also gegenüber dem CH-IdP stark authentisieren können und dies geschieht mit einem beim Ausstellungsprozess registrierten Authentifikator (im Sinn des FIDO Modells).

Bei genauerem Hinsehen ist a) eine Schnittstelle zu gewissen Daten in ISA bzw in Infostar und b) entspricht der Entwicklung zur nutzerzentrierten Authentifizierung mit einem Authentifikator, der vom Staat anerkannt und registriert werden kann. Es bleibt einzig zu klären, (i) welche Identitätsattribute wie abgerufen werden sollen und (ii) welcher Authentifikator für den Zugriff auf den CH-IdP vorausgesetzt werden soll und wie dieser zuverlässig auf den berechtigten Nutzer beim CH-IdP registriert werden kann.

Für die Einführung einer eID in der Schweiz müssen somit die Ausgabe, die Authentifizierung für die Bezugsberechtigung der eID beim staatlichen CH-IdP, bei der Registrierung bei einem IdP Identitätsdienstleister und die operative Nutzung der eID Attribute definiert werden. Wichtig sind auch die Schnittstellen zum IAM Projekt des Bundes und zu den weiteren Projekten im Bereich eHealth, eVoting und generell eGovernement. Die folgende Skizze zeigt diese drei Hauptabläufe schematisch.



Beim Design der eID Lösung müssen die einschlägigen internationale Standards berücksichtigt und die Interoperabilität zumindest zum europäischen System garantiert sein. Die Rahmenbedingungen in Europa werden einerseits durch die eIDAS Verordnung der EU und nationale Gesetze definiert und andererseits werden sich wohl aus Gründen der Interoperabilität noch weitere Standards entwickeln (zB. Storck).

4.2.1 Grundlegende Identifizierung und Authentifizierung

Die Erfassung und Verwaltung der grundlegenden Zuordnung einer Identität zu einer Person ist eine Aufgabe, die der Staat seit langem für alle Staatsbürger wahrnimmt. Im Rahmen dieser Aufgabe sind bereits Ausgabeprozesse für Identitätsnachweise wie die Ausstellung von IDKs und Pässen definiert und operativ. Ein ganz ähnlicher Prozess ist für die Ausgabe einer eID notwendig und kann somit in die etablierten Ausstellungsprozesse integriert werden. Lediglich der Formfaktor des Identitätsmittels ändert. Statt Informationen auf gesichertem Papier werden die eID Attribute in der sicheren ISA Datenbank erfasst. Die CH-eID wird von ISA (und evt Infostar) in einen CH-IdP Server exportiert, der von der gleichen Instanz wie die ISA Datenbank betrieben wird[1]. Genauso wie die erste Abgabe eines klassischen Ausweises an die Person gesichert ist, muss auch die Ausgabe der Zugangs- und Nutzungsberechtigung für die CH-eID an eine Person abgesichert sein.

4.2.2 Authentifizierung für die Bezugsberechtigung

Für den Bezug der CH-eID muss definiert sein, wie sich der Nutzer im Feld authentifizieren muss, damit er seine CH-eID bei einem IdP Dienstleister oder bei einer vertrauenden Partei mit IAM System einsetzen kann. Dies geschieht durch die Registrierung eines anerkannten Authentifikators (zB. FIDO zertifiziert) in einem persönlichen Gerät des Nutzers (BYOD), der mindestens zwei Authentifizierungsfaktoren (2F) verifiziert. Der Staat definiert dabei, was für

[1] Es ist Aufgabe des ISA Betreibers zu definieren, ob der Identity Provider Server direkt oder über eine zwischengeschaltete DB auf die eID Daten der ISA DB zugreift.

weitere sicherheitstechnische Anforderungen geeignete Authentifikatoren für eine solche Registrierung erfüllen müssen (dies kann für ganze Gerätegenerationen und Herausgeber spezifiziert werden, ähnlich der Typenprüfung für Fahrzeuge[2]). Zusätzlich wird der Staat selbst im Rahmen der eID Ausstellung auf Wunsch des erfassten Nutzers auch einen FIDO kompatiblen 2F-Authentifikator abgeben können, der auf ihn registriert ist und durch den zwei Authentifizierungsfaktoren des Nutzers verifiziert werden. Dies könnte zum Beispiel eine Smart Card mit Lesegerät mit PIN Eingabe und integrierter NFC Schnittstelle sein. In jedem Fall muss der Staat aber dafür sorgen, dass die Person, die auf ihre CH-eID Funktion zugreift, auf einem definierten Sicherheits- und Verifikationsniveau authentifiziert wird (Voraussetzung für die allfällige EU Notifizierbarkeit des CH-eID-Systems gemäss eIDAS Verordnung). Da typischerweise die geeigneten Authentifikatoren in Geräten implementiert sind, die, verglichen mit der CH-eID, kurze Lebenszeiten haben, muss ein einfacher und sicherer Mechanismus definiert werden, wie Authentifikatoren erneuert und von einem Gerät zum anderen übertragen werden können.

4.2.3 Registrierung bei den IdPs und Nutzung der CH-eID

Wenn ein Nutzer seine CH-eID bei einem IdP seiner Wahl hinterlegen will, muss er sich bei diesem mit einem Authentifizierungsprozess anmelden, der vom IdP bestimmt wird. Der IdP leitet dann die Anfrage für die Lieferung der CH-eID an den staatlichen CH-IdP weiter. Damit die Lieferung erfolgt, muss sich der Nutzer auch noch gegenüber dem CH-IdP mit dem staatlich registrierten Authentifikator authentifizieren und die Auslieferung der CH-eID Daten an den IdP seiner Wahl bestätigen. Der CH-IdP erzeugt dann einen eID Verifikationsrekord, der es dem bezeichneten und nur diesem IdP erlaubt die vom Nutzer zur Verfügung gestellten CH-eID Identitätsattribute zu überprüfen und diese Überprüfung auch gegenüber Dritten zu bestätigen. Der IdP kann den auf ihn lizenzierten eID-Rekord aber nicht direkt weitergeben, da eine Bestätigung und Überprüfung der CH-eID Daten nur unter seinem Namen möglich ist. Der IdP kann jedoch mit den bestätigten Identitätsattributen und allfällig weiteren ergänzenden Attributen dem Nutzer anwendungsspezifische Beglaubigungen für seine Identität (IDP-eID) ausstellen, die dieser in einem Geschäftsdialog direkt einer vertrauenden Partei vorweisen kann. Der IdP, der eine aus den CH-eID Attributen abgeleitete Beglaubigung (IdP-eID) an den Nutzer übergibt, muss diese an einen bestimmten Authentifikator knüpfen, damit sie gültig ist. Der verlangte Authentifizierungslevel ist Teil der IdP-eID.

Für das Vorweisen einer solchen IdP-eID muss sich der Nutzer mit dem richtigen Authentifikator anmelden. Vertrauende Parteien können eine IdP-eID nur in Kenntnis des ausstellenden IdPs auswerten, auf den der staatliche eID Rekord lizenziert ist. Die vertrauende Partei kann mit den in der Beglaubigung gelieferten Informationen (kryptographisch verarbeitet Daten, Zertifikate, Signaturen, Schlüssel, MAC, Zeitstempel etc) die Richtigkeit der staatlichen Identitätsattribute via IdP und CH-IdP nachprüfen. Damit ist die Sicherheitskette Person – Client/Authentifikator – IDP Server – CH-IdP Server - eID etabliert.

4.2.4 Authentifizierung im Feld

Der eigentliche Authentifizierungsprozess im Feld ist nicht mehr in der Verantwortung des staatlichen eID Herausgebers sondern in der Verantwortung der Instanz, die einen IdP-eID-bezugsberechtigten Authentifikator herausgibt, beziehungsweise in der Verantwortung des IdP beziehungsweise der vertrauenden Partei, welche den Authentifikator akzeptiert. Die vertrauende Partei weiss jedoch auch, auf welchem Sicherheitsniveau der Nutzer sich beim CH-IdP authentifiziert hat, als er die CH-eID dem IdP Dienst verfügbar gemacht hatte, und auf welchem Sicherheitsniveau er sich beim Bezug der vorgezeigten Beglaubigung vom IdP

[2] In Estland sind zum Beispiel nebst der nationalen eID-Karte auch spezielle SIM Karten oder von Banken herausgegeben Authentifikatoren akzeptiert (eServices in Estonia: a success story, June 2014; SIA report; http://www.secureidentityalliance.org/index.php/resources)

(IdP-eID) authentifiziert hatte. Es ist in der Verantwortung der vertrauenden Partei vom Nutzer eine IdP-eID Beglaubigung zu verlangen, die nur mit Authentifizierungen auf dem erwünschten Sicherheitsniveau ausgestellt werden kann.

Normalerweise wird eine vertrauende Partei die IdP-eID mit den integrierten stattlich garantierten Attributen der zivilen Identität nur bei der Erstregistrierung brauchen. Für die weiteren Kontakte unter der erfassten Identität wird die vertrauende Partei nur noch eine Authentifizierungsmethode mit dem Nutzer vereinbaren. Diese kann natürlich auf dem gleichen Authentifikator beruhen, wie sie für den Zugang zum CH-IdP oder zum Dienstleister IdP genutzt wird. Es ist im Interesse aller Beteiligten, wenn möglichst wenige und dafür sichere Authentifikatoren eingesetzt werden.

Obschon gemäss der obigen Positionierung der Staat nicht direkt für die Authentifizierung im Feld verantwortlich ist, wird er für ein sicheres eID Konzept auf eine vertrauenswürdige Authentifizierung im IAM Ökosystem aufbauen wollen. Dies erreicht er mit der Definition einer ‚best practic', welche Authentifizierungsniveaus für eine bestimmte Nutzung der eID Attribute verlangt werden sollte.

4.3 Sicherheitsmassnahmen für die CH-eID

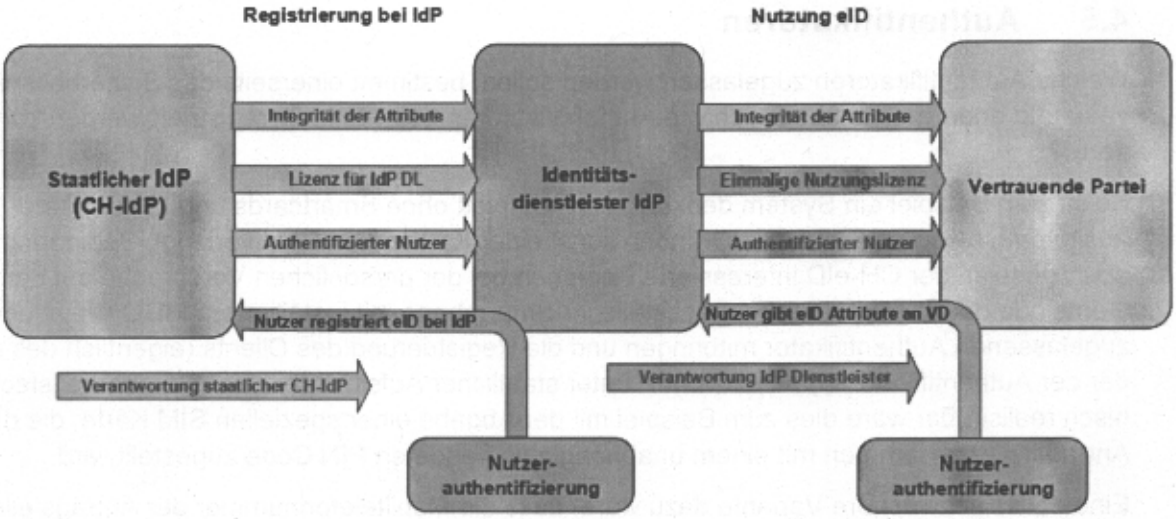
Die Nutzung der staatlichen CH-eID wird durch den Einbezug von marktnahen IdP Dienstleistern flexibler. Der Staat (CH-IdP) liefert die staatlichen eID Attribute nur in einer Form, die es dem empfangenden IdP erlaubt diejenigen Attribute auf Richtigkeit zu überprüfen, die ihm vom berechtigten Nutzer der CH-eID zur Verfügung gestellt werden. Das Protokoll für die Nutzung der eID Attribute muss immer die folgenden drei Absicherungsfunktionen erfüllen:

- Sicherstellen, dass nur die berechtigte Person die CH-eID nutzt (Authentifikation der Person mit dem staatlich registrierten Authentifikator)
- Sicherstellen, dass die CH- eID nur authentische Attribute beinhaltet (Integrität der Daten)
- Sicherstellen, dass die CH-eID einer vertrauenden Partei nur in einer Form geliefert wird, die es dieser und nur dieser erlaubt von der Person freigegebene Attribute zu überprüfen (Nutzungslizenz)

Die Absicherung der Integrität der CH-eID Daten und die Erteilung der Nutzungslizenzen an vertrauende Parteien sind CH-eID spezifische Aufgaben, die vom IdP Dienst übernommen bzw vom staatlichen Herausgeber der CH-eID Daten gesteuert werden.

Der IdP Dienstleister kann weitere Attribute über andere Quellen erfassen und verwalten. Er übernimmt die Garantie für alle die von ihm verteilten oder bestätigten Attribute vollständig. Er ist auch verantwortlich dafür, dass die von ihm verwalteten Attribute nur im Einverständnis und mit geeigneter Authentifizierung des berechtigten Nutzers verwertet werden können. Der staatliche CH-IdP Dienst garantiert dabei nur die Integrität der von ihm gelieferten CH-eID Daten und die Authentizität des berechtigten Nutzers bei der Registrierung der CH-eID beim IdP Dienst. Das staatliche CH-IdP System sorgt dafür, dass sich der Nutzer bei einem IdP Dienst mit dem verlangten Sicherheitsniveau authentifizieren kann, so dass die Zusammengehörigkeit der staatlichen eID mit dem berechtigten Nutzer bei der Registrierung garantiert ist. Das staatliche eID-System garantiert die drei obgenannten Sicherheitsanforderungen in diesem Sinn bis zur Registrierung der CH-eID beim IdP Dienstleister.

Die Verantwortung für die Sicherheitsanforderungen sind für die verschiedenen Phasen im eID Einsatz in der folgenden Skizze dargestellt.



Selbstverständlich müssen zudem die einschlägigen Vorgaben des Datenschutzes und der Datensicherheit eingehalten werden. Wichtig ist, und das zeigen verschiedene Beispiele aus anderen Ländern, dass die Benutzerfreundlichkeit unter den Sicherheitsmassnahmen nicht zu kurz kommt.

4.4 Form und Nutzung der CH-eID Identitätsattribute

Die Identitätsattribute der CH-eID werden den IdPs auf Anweisung des berechtigten Nutzers und nur in verschlüsselter aber überprüfbarer Form zur Verfügung gestellt. Die Form der Daten garantiert, dass nur der vom Nutzer beauftragte (lizenzierte) und mit Identitätsattributen im Klartext direkt belieferte IdP die CH-eID Daten nutzen kann. Der IdP kann dann in der Beglaubigung (IdP-eID), die er für den Nutzer erstellt, staatliche und weitere Attribute im Klartext oder ebenfalls verschlüsselt integrieren. Auch jede Kombination davon ist denkbar. Die Überprüfung der staatlichen Attribute in einer solche IdP-eID ist aber nur mit der vom CH-IdP gelieferten Lizenz an den IdP möglich. Diese muss deshalb auch in die weitergereichte Beglaubigung eingefügt werden, damit eine vertrauende Partei die Vertrauenskette bis zum staatlichen CH-IdP nachprüfen kann.

Die Nutzung der eID mit Klartext Attributen würde dem Modus„Attributs-Transfer" und diejenige mit verschlüsselten Attributen dem Modus „Attribut-Verifikation" entsprechen. In jedem Fall ist es aber im Ermessen des Nutzers, ob er ein bestimmte Beglaubigung für eine Geschäftstransaktion an eine vertrauende Partei liefern will oder nicht.

Falls nur verschlüsselte Attributdaten bereitgestellt werden, braucht es eine spezielle Lösung um Ordnungsrelationsüberprüfungen zu machen, wie dies zum Beispiel beim Altersnachweis nötig ist. Das Problem könnte zum Beispiel mit einem Zusatzvektor von Stichdaten im Klartext gelöst werden, die eine Abgrenzung des Alters nach unten oder oben relativ zu den typischen Alterslimiten erlauben würde. Dies würde aber eine regelmässige Erneuerung der IdP-eID bedingen.

Offen ist auch, ob die Identitätsattribute bei jeder von einem IdP neu erstellten Beglaubigung für einen Nutzer beim CH-IdP neu abgerufen werden oder ob der IdP die CH-eID der registrierten Nutzer bei sich zwischenspeichert. Letzteres hätte den Vorteil einer etwas verringerten Last auf dem CH-IdP, würde aber den IdP verpflichten die aktuelle Rückrufliste des CH-IdP zu konsultieren.

4.5 Authentifikatoren

Welche Authentifikatoren zugelassen werden sollen, bestimmt einerseits das Sicherheitsniveau und andererseits aber auch wie Authentifikatoren beim CH-IdP registriert werden können.

So ist zum Beispiel ein System denkbar, das komplett ohne Smartcards und Lesergeräte auskommt, also weder auf der IDK noch sonst einer Karte einen Chip verlangt. Bedingung ist aber, dass an der CH-eID interessierte Personen bei der persönlichen Vorsprache auf der Gemeinde oder der kantonalen Passstelle ihr Smartphone mit installiertem FIDO Client und zugelassenen Authentifikator mitbringen und die Registrierung des Clients (eigentlich des oder der Authentifikatoren) beim CH-IdP unter staatlicher Aufsicht geschieht. Sicherheitstechnisch realisierbar wäre dies zum Beispiel mit der Abgabe einer speziellen SIM Karte, die dem Antragsteller zusammen mit einem unabhängig versendeten PIN Code zugestellt wird.

Eine etwas schwächere Variante dazu wäre, dass die Mobiltelefonnummer der Antragstellenden Person vor Ort registriert wird und der Person später - nach Prüfung des Antrages und der Erfassung der Daten im CH-IdP – mit einer SMS ein One Time Password (OTP) zur Aktivierung der zuvor von der Person beim CH-IdP registrierten Authentifikators zugesandt wird. Dies vielleicht auch in Kombination mit einem zusätzlichen Passwort, das er mit der IDK oder dem Pass zusammen zugeschickt erhält.

Beide Varianten haben den Nachteil, dass eine Nachregistrierung von anderen Clients (Authentifikatoren) oder auch bei einem Wechsel der Mobiltelefonnummer wahrscheinlich mit einer weiteren persönlichen Vorsprache bei den Behörden verbunden ist. Zu prüfen wird sein, ob dieses Erfordernis über ein Backup der auf dem Client gespeicherten Credentials oder durch die Selbstregistrierung von weiteren Clients auf dem CH-IdP umgangen werden könnte. Der grosse Vorteil dieser Varianten ist – wie bereits erwähnt – dass keinerlei Smartcards und Lesegeräte notwendig sind. Damit ein solches Verfahren sicher und nutzerfreundlich implementiert werden kann, müsste das Smartphone über eine Trusted Execution Environment (TEE) verfügen.

4.5.1 Authentifikator in einem Secure Element

Eine weitere Variante wäre, einen Authentifikator mittels einer NFC-fähige Smartcard als Secure Element zu realisieren. Zusammen mit einem Lesegerät mit NFC Schnittstelle und abgesichertem Display ergäbe sich dann ein vollwertiger Authentifikator. Das sichere Lesegerät könnte zum Beispiel ein App in einem sicheren Kompartement eines NFC Smartphones sein. Die Smartcard, die alle anderen Elemente des Authentifikators (aussert der sichere Display) enthält, kann entweder integriert in der IDK oder als separate E-Gov-Card abgegeben werden. Eine Smartcard hat prinzipiell natürlich eine noch kleinere Angriffsoberfläche als eine TEE in einem Smartphone und ermöglicht deshalb voraussichtlich eine zusätzlich leicht höhere Sicherheit. Diese Lösung hat aber den Nachteil, dass Lesegeräte mit sicherem Display oder mit einem Display in einer TEE notwendig sind. Vorteilhaft könnte weiter sein, dass auf der Smartcard zusätzliche Applikationen gespeichert werden könnten, insbesondere dann, wenn es sich um eine „universelle“ E-Gov-Card handelt.

4.5.2 Zusätzliche Nutzung

Ein weiterer Vorteil kann sein, dass die Karte zusammen mit einem separaten Lesegerät ein hoch sicheres System bilden kann, welche wahrscheinlich auch die Anforderungen im E-Voting- und E-Banking-Bereich zu erfüllen mag (z.B. Transaktionsabsicherung):

Die vertrauende Partei übermittelt die Daten der vereinbarten Transaktion zum Authentifikations-Client, der diese dem Nutzer anzeigt. Falls der Nutzer mit der Transaktionsquittung einverstanden ist, überträgt er die Daten in sein Lesegerät und bestätigt mittels einer Authentifizierung, dass er damit einverstanden. Die Quittung wird dann von der E-Gov-Karte signiert

und die Antwort wird auf der Anzeige des Lesegerätes angezeigt; diese überträgt man dann in den Authentifikations-Client ein und bestätigt so die Benutzerauthentisierung resp. die Transaktion.

Jede Kombination (Karte mit integrierter Tastatur und/oder Display usw.) ist denkbar. Wie die Erfahrungen von Deutschland zeigen, müsste ein Lesegerät mit Vorteil zusammen mit der Karte in einem „Sorglos-Package" an die Bürgerinnen und Bürger geben werden. Heutige e-Banking Systeme funktionieren zum Teil mit einem solchen Schema.

4.5.3 Selbstregistrierung mit E-Pass oder E-NAA

Die Registrierung von Authentifikations-Clients / Authentifikatoren könnte auch an einem Kiosksystem in den Passbüros erfolgen, sofern die Personen einen gültigen E-Pass besitzt und damit eine Zweifaktor-Authentifizierung sichergestellt werden kann. Kiosksysteme verhindern zwar nicht den Behördengang, entlasten jedoch die personellen Ressourcen vor Ort. Sie können mit Bankomaten verglichen werden und bilden eine Art Zwischenschritt zwischen der klassischen Vorsprache bei einer Behörde und der rein elektronischen Erledigung eines Behördengeschäfts. Gemäss Auskünften des BMI haben deutsche Kommunen gute Erfahrungen mit Kiosksystemen gemacht. Solche Systeme sind auch in Estland, das in der Anwendung von eID für staatliche Anwendungen führend ist, weit verbreitet. Auch die Schweiz kennt im Zusammenhang mit den E-Pässen bereits eine Art Kiosksystem: den Public Reader.

Die Zweifaktor-Authentifizierung kann dadurch geschehen, dass:

I. zusätzlich zum E-Pass eine Geheimzahl an die Inhaberin oder den Inhaber versandt wird; oder

II. die Identität mit einem biometrischen Merkmal (zB den Fingerabdrücken oder einer Gesichtserkennung) verifiziert wird; oder

III. nach Wahl der Person beides möglich ist.

Der Ablauf wäre also in etwa der Folgende: Die Person legt ihren E-Pass auf den Leser des Kiosks. Der Kiosk macht EAC und prüft die Gültigkeit des Dokuments. Bedingung ist natürlich, dass der Kiosk mit dem IS-HSM der Systemplattform E-DOC verbunden ist. Nun kann sich die Person entweder mit der Geheimzahl oder dem Fingerabdruck bzw einer Gesichtserkennung als zweiten Faktor authentisieren. Danach kann sie auf dem Bildschirm allerlei Behördengeschäfte erledigen, u.a. auch Authentifikatios-Clients / Authentifikatoren beim staatlichen CH-IdP registrieren oder löschen.

Bem: neben dem E-Pass eignen sich alle E-Dokumente, welche eine staatliche Identität bestätigen können, für das Kiosksystem. Also auch eine E-IDK oder je nach Anschauung also auch der NAA.

5 Referenzen

[1] eCH-0107: Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM); V2.0; 4.12.2013; www.eCH.ch

[2] UAF Architectural Overview, Review Draft; 9.2.2014; FIDO Alliance; fidoalliance.org/specifications/download

[3] Identitätsmanagement-eine visualisierte Begriffsbestimmung; D. Hühnlein; p 163 in Datenschutz und Datensicherheit 3; 2008

Verordnung (EU) Nr. 910/2014 vom 23.7.2014 (eIDAS Verordnung) und Glossar von [1]

[4] 3-Jahre Online Ausweisfunktion – Lessons Learned; J. Fromm et al.;Fraunenhofer Fokus; Okt. 2013

[5] The evolution of authentication; R. Lehmann, FIDO Alliance and NokNok Lab; preprint 2013

6 Glossar

AHVN13	Bezeichnung für die neue 13 stellige AHV Nummer, die keine unmittelbaren Rückschlüsse auf weitere persönliche Identitätsdaten des Inhabers zulässt.
Attribut	Namentliche Eigenschaft, die eine Person näher beschreibt.
Authentifizierung	Prozess der Bestätigung einer Behauptung über die Identität einer Person zB. durch Überprüfung von authentifizierenden Faktoren (Synonym: Authentifikation)
Authentifizierungs-faktor	Charakteristik in Form eines materiellen oder virtuellen Gegenstandes, eines Geheimnisses oder einer biometrischen Eigenschaft, die einer bestimmten Person zugeordnet ist
BYOD	Abkürzung für Bring Your Own Device. Dies entspricht der heutigen Situation in der IT Welt, wo Personen sehr oft die gleiche persönliche Infrastruktur im Berufs- wie im Privatleben brauchen und darauf vertrauen.
CH-eID	Schweizerische staatliche eID, welche ausschliesslich Attribute der zivilen Identität gemäss Anhang 2 enthält.
eID	Elektronisches Identifizierungsmittel ist eine materielle und/oder immaterielle Einheit, die Attributdaten der Identität in elektronischer Form enthält.
eIDK	Funktion der eID integriert in die Identitätskarte (IDK)
eID-System	System für die elektronische Identifizierung, in dessen Rahmen eIDs für die erfassten Personen erstellt werden
IAM	Identitäts- und Zugriffsverwaltung (Identity und Access Management)
IAM Ökosystem	Begriff, der die Gesamtheit der Instanzen und Nutzer von identitätsbasierten Diensten im Markt bezeichnet
Identifizierung	(Elektronischer) Prozess der Verwendung von Identitätsattributen um eine Person eindeutig zu bestimmen
Identität	Menge der Attribute (namentliche Eigenschaften) einer Person

Identitätsdienstleister (IdP)	Organisation, die eIDs verwaltet und herausgibt. Ein IdP stellt einen Authentifizierungsdienst und meist auch einen Attributbestätigungsdienst zur Verfügung.
MAC	Message Authentication Code; Prüfcode für die Integrität und die Authentizität von Daten
Ressource	Service oder Daten, auf welche eine Person zugreifen kann, wenn sie sich authentisiert hat und sie auf der Basis der benötigten Attribute autorisiert wurde (inklusive physische Ressourcen).
Verifikation	Prozess des elektronischen Erkennens einer Person durch Überprüfung von einem oder mehreren Authentifizierungsfaktoren mittels eines geeigneten Messprotokolls (Übergang von der physischen Welt der Person in die digitale Repräsentation der Person).
Vertrauende Partei (VP)	Natürliche oder juristische Person, die auf eine elektronische Identifizierung oder einen Identitätsdienstleister vertraut. Meist verwaltet sie eine Ressource und kann mittels eines IAM Systems Personen den Zugriff darauf ermöglichen.
Zivile Identität	Teilmenge der Identitätsattribute, die vom Staat erfasst und gepflegt werden und die eine Person im Staat eindeutig identifizieren

Anhang 1: Was ist ein Trusted Execution Environment (TEE)?

(Quelle: Wiki http://de.wikipedia.org/wiki/Trusted_Execution_Environment)

Eine Trusted Execution Environment (TEE) stellt eine sichere bzw. vertrauenswürdige Laufzeitumgebung für Applikationen zur Verfügung. Auf dem TEE können nur speziell dafür freigeschaltete Applikationen ausgeführt werden. Ein oder mehrere vertrauenswürdige Laufzeitumgebungen können parallel existieren, daneben können noch weitere unsichere oder ungeschützte Umgebungen existieren.

Ein TEE umfasst auch Peripheriegeräte, die zwischen Zugriffen aus sicheren und nicht-sicheren Applikationen oder Betriebssystemen unterscheiden können. Chipkarten, USB-Tokens oder Hardware-Sicherheitsmodule stellen ein TEE dar, bieten aber wegen der meist fehlenden Ein- und Ausgabekomponenten (Tastatur, Monitor) jedoch nur beschränkte Möglichkeiten.

Die TEE-Technologie kommt heute hauptsächlich auf Smartphones und Tablets zum Einsatz, z. B. für Digital Rights Management (DRM). Die Weiterentwicklung und Standardisierung dieser Technologie ist von entscheidender Bedeutung für Anwendungen wie Mobile-Banking und NFC-Zahlungsmöglichkeiten gesehen. Auch das Konzept Bring your own device (BYOD), die Schaffung eines privatem Bereich parallel zu einem sicheren Bereich für Firmendaten, stützt sich auf das TEE-Konzept.

Der Industrieverband GlobalPlatform (http://www.globalplatform.org/default.asp), der auch Spezifikationen für Laufzeitumgebungen auf Chipkarten und herausgibt, arbeitet an einer Standardisierung von TEEs. Eine Definition des Trusted Execution Environment im Sinne von GlobalPlatform wurde 2011 in einem White Paper zusammengefasst. Im Rahmen der Linaro-Initiative existiert auch eine Arbeitsgruppe, die den Zugriff auf ARM TrustZone basierte TEEs von Linux aus standardisiert.

Anhang 2: Identitätsattribute der staatlichen eID

a. amtlicher Name;
b. Vornamen;
c. Geburtsdatum;
d. Geburtsort;
e. Nationalität;
f. ausstellende Behörde;
g. Datum der Ausstellung;
h. Datum des Ablaufs der Gültigkeit;
i. Nummer und Art des Trägermediums;
j. Sozialversicherungsnummer;

Auf Verlangen der antragstellenden Person kann die eID zusätzlich Allianz-, Ordens-, Künstler- oder Partnerschaftsnamen enthalten.

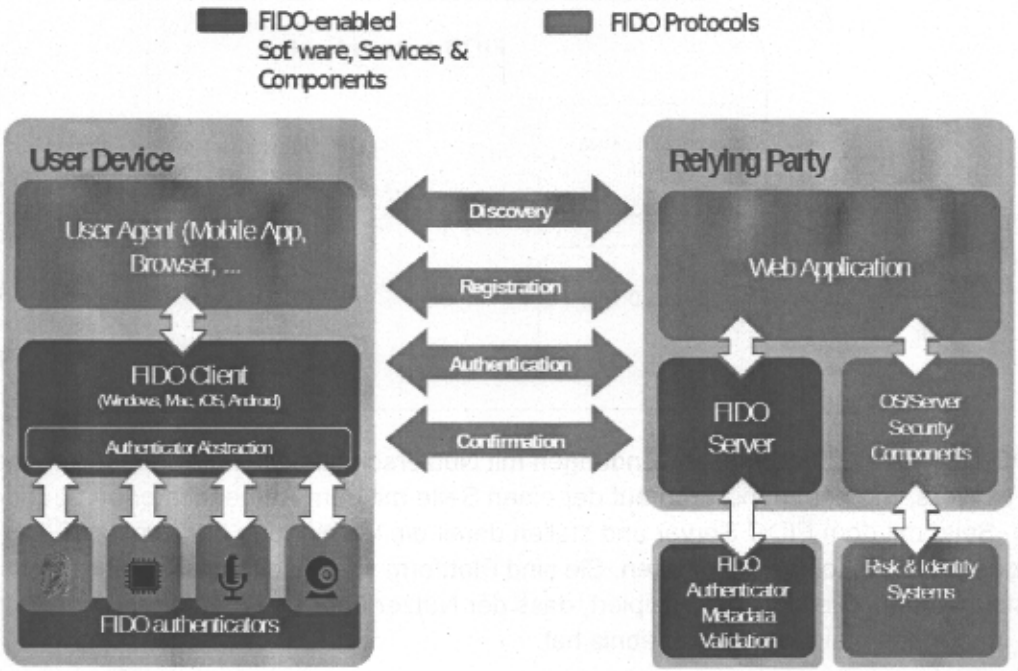
Anhang 3: FIDO Referenzmodell

Was ist FIDO?

Mit der FIDO Alliance ist 2012 ein u.E. sehr potenter Player im eID-Ökosystem aufgetaucht, in dem fast alle wichtigen Industriepartner des IT-Sektors vertreten sind. Die FIDO Alliance

hat ein wegweisendes Referenzmodell für die zuverlässige Authentifizierung einer Person gegenüber einem vertrauenden Online-System (vertrauende Partei) definiert. Architektur und Funktionen des Modells machen die online Authentifizierung a) einfach im Gebrauch b) sicher und die Privatsphäre schützend und c) durch Standardisierung interoperable über Dienstgrenzen hinweg. Das Authentifizierungsmodell liefert damit den Basisbaustein für den Online-Nachweis einer Identität über einen Online Identity Provider. In diesem Frühjahr hat FIDO bereits die Entwürfe der Spezifikationen für eine skalierbare interoperable starke Authentifizierung mit unterschiedlichen Authentifizierungsmethoden publiziert. Die propagierte Authentifizierungsarchitektur erlaubt die Einbindung von mehreren unterschiedlichen Authentifikatoren (auch als „first mile" bezeichnet) und die Federation der Authentifizierung zu unterschiedlichen vertrauenden Parteien (auch als „second mile" bezeichnet). In den Überlegungen zur schweizerischen eID muss diese auf globaler Ebene initiierte Standardarchitektur für Vertrauensdienste sicher berücksichtigt werden.

Das FIDO System lässt sich insbesondere auch in die Sicherheitsarchitektur der Trusted Execution Environment (TEE) der Global Platform Organisation abbilden, welche die Sicherheitsmechanismen der nächsten Generationen von mobilen Geräten bestimmen wird. Beide Technologien konvergieren zu einer nutzerfreundlichen sicheren Systemarchitektur für Vertrauensdienste, die über mobile und ortsgebundene Endgeräte genutzt werden können.



*Zitat (Quelle: FIDO **U**niversal **A**uthentication **F**actor Architectural Overview, 2014): The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. The FIDO UAF Reference Architecture describes the components, protocols, and interfaces that make up the FIDO UAF strong authentication ecosystem.*

Ein FIDO System umfasst vier Interaktionen zwischen einem Nutzer und einem vertrauenden Dienst:

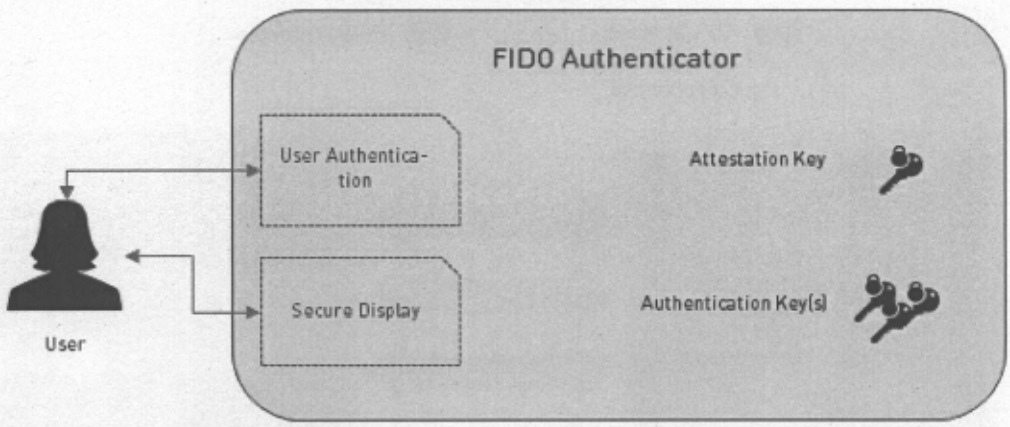
- Erstkontakt mit Bestimmung der möglichen sicheren Authentifikationsmethoden (Authentifikatoren) des Nutzers (Discovery)
- Registrierung der Authentifikationsmethoden mit Austausch verbindungsabhängiger Sicherheitselemente (Registration)

- (gegenseitige) Authentifizierung basierend auf den entdeckten und registrierten Authentifikationsmethoden (Authentification)
- Absicherung von Transaktionsdaten im gleichen Sicherheitsdispositiv und mit direkter Kommunikation mit dem Nutzer (Confirmation)

Wie funktioniert FIDO?

Auf einem FIDO kompatiblen Endgerät wird ein **FIDO Client** installiert, welcher die Schnittstelle zwischen FIDO Authentifikatoren und FIDO Servern bildet.

FIDO Authentifikatoren haben die Funktion von Schlössern. Ihre Aufgabe ist es, dem FIDO Server zu bestätigen, dass sich ein gültiger Schlüssel im Schloss befindet – sich der Benutzer also erfolgreich authentisiert hat. Je nach Schloss besteht ein gültiger Schlüssel aus einer gültigen Pin-Eingabe, biometrischen Daten wie Fingerabdruck oder Irisbilder, Smartcards mit gespeicherten Geheimnissen oder ein simples OK-Häkchen des Benutzers. Der Authentifikator übernimmt die Rolle des sicheren Elementes im Feld und besteht aus den vier Komponenten Nutzererkennungsmodul, sichere Anzeigemöglichkeit, verbindungsabhängige kryptographische Schlüssel und ein Zertifikat, das die Echtheit und Unversehrtheit des Authentifikators und damit der gelieferten Authentifizierungsschlüssel bestätigt.

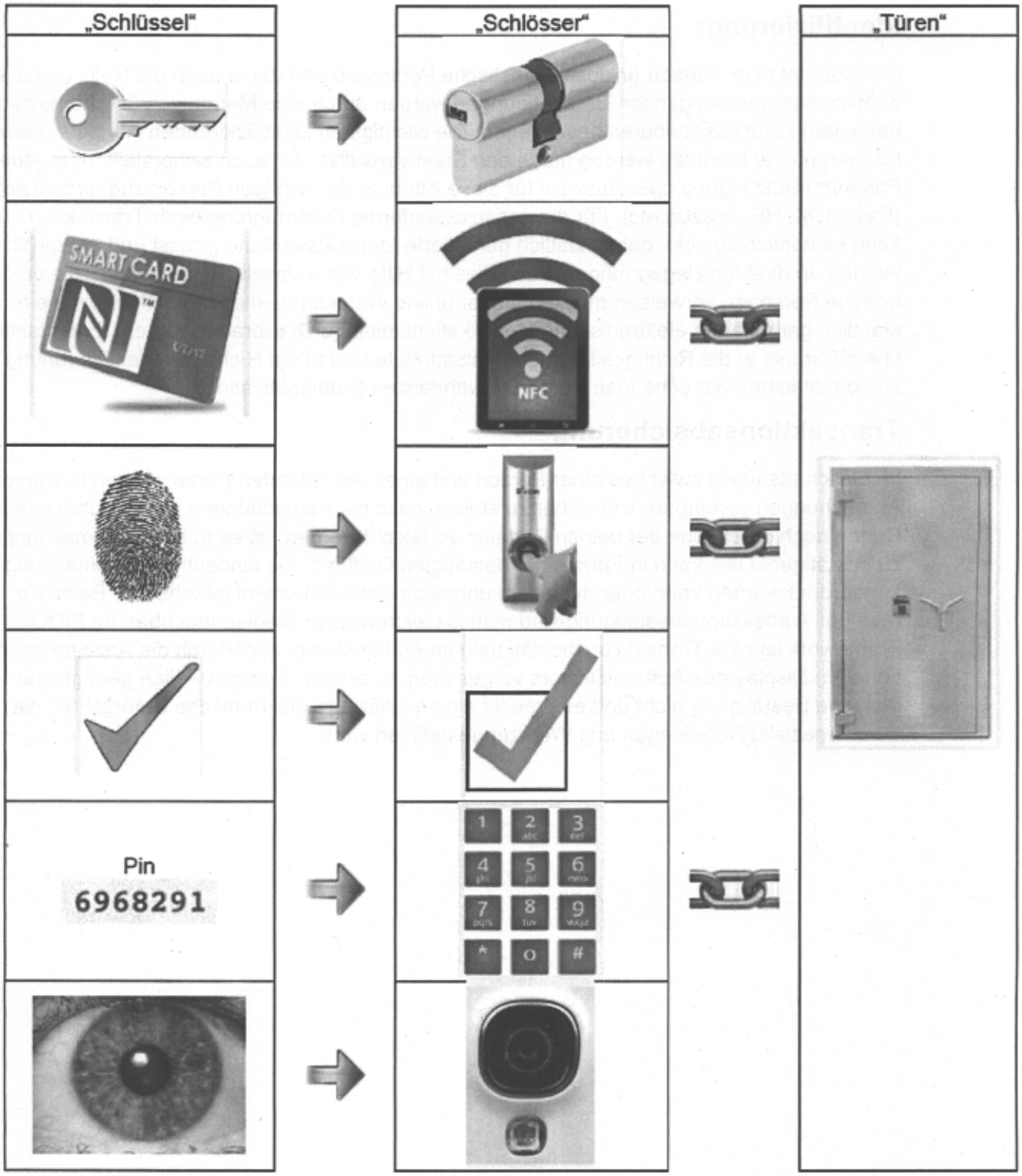


Die **FIDO Clients** sind Interfaceanwendungen mit Nutzerschnittstelle im Kommunikationsgerät des Nutzers. Sie kommunizieren auf der einen Seite mit dem Authenticator und auf der anderen Seite mit dem FIDO Server und stellen damit die Verbindung her, um das FIDO Authentifizierungsprotokoll durchzuführen. Sie sind Plattform spezifisch, müssen aber nicht individualisiert werden. Sie sind so konzipiert, dass der Nutzer über alle Plattformen und Geräte hinweg immer das gleiche Nutzererlebnis hat.

Die **FIDO Server** bei den Dienstanbietern haben die Funktion einer Türe zu den dahinter liegenden Dienstleistungsangeboten (z.B. Webseiten oder auch Attributverzeichnissen). Damit ein bestimmter FIDO Authentifikator eines bestimmten FIDO Client eines Endgerätes mit einem FIDO Server verwendet werden kann, muss er zuvor von diesem FIDO Server als geeignet anerkannt (Discovery) und registriert (Registration) werden. Ein FIDO Server kann die auf dem Endgerät vorhandenen Authentifikatoren abfragen und auch eine Kombination von Authentifikatoren verlangen. Jeder FIDO Authentifikator handelt mit jedem FIDO Server ein eigenes Pseudonym aus, so dass damit eine Profilbildung über verschiedene FIDO Server nicht möglich ist.

Abbildung 1 - FIDO System

Inhaber	User Device	Relying Parties
Wissen, Haben, Tun	FIDO Authentifikatoren	FIDO Server



Hinweis: Schlösser müssen auf Türen registriert () sein, damit sie funktionieren.

Anhang 4: Identitätsbasierte Prozesse

Identifizierung:

Die Identität einer Person (inklusive juristische Personen) und damit auch die Rolle und die damit zusammenhängenden Berechtigungen werden durch eine Menge von (zT. kontextabhängigen) Identitätsattributen beschrieben. Die wichtigsten identifizierenden Attribute (staatlich garantierte Identität) werden durch den Staat verwaltet, der auch sicherstellt, dass jede Form von Bestätigung oder Ausweis für diese Attribute der richtigen Person zugeordnet wird (Pass, IDK, HR-Auszug etc). Für die gesetzeskonforme Durchführung einer Transaktion kann es notwendig sein, dass staatlich garantierte Identitätsattribute erfasst und überprüft werden. In direkten Begegnungen, kann dies mit Hilfe von Ausweisen geschehen, die betroffene Personen vorweisen müssen. In der online Welt könnte diese Funktion durch ein staatlich garantiertes elektronisches Identifikationsmittel (eID) erbracht werden. Eine staatliche eID muss a) die Richtigkeit der Identitätsattribute und b) die Richtigkeit der Zuordnung zur identitätsbeanspruchenden Person gewährleisten (Authentifikation).

Transaktionsabsicherung

Im Geschäftsdialog zwischen einer Person und einer vertrauenden Partei werden bestimmte Abmachungen vereinbart. Um sicher zu stellen, dass die Abmachungen weder durch einen Dritten noch durch eine der beiden Parteien verfälscht werden, ist es nötig die Abmachungen zu bestätigen. Dies kann in Form einer bestätigten Quittung, die eindeutig der Abmachung zugeordnet werden kann oder mit einem unterschrieben Dokument geschehen. Beide Formen der Transaktionsbestätigung sind mittels elektronischer Medien machbar. Im FIDO Framework ist eine Transaktionsbestätigung im Architekturkonzept durch die Anzeige im (optionalen) Display des Authentifikators vorgesehen. In einigen wenigen Fällen genügt eine einfache Bestätigung nicht und es braucht eine qualifizierte elektronische Unterschrift, die durch spezielle Regelungen und Werkzeuge definiert wird.