Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Konzept für schweizerische staatlich anerkannte eID-Systeme

Auftraggeber	fedpol
Projektleiter	Markus Waldner
Autoren	Lorenz Müller, Markus Waldner
Klassifizierung	öffentlich
Status	informelle Konsultation

Änderungsverzeichnis

Datum	Version	Änderung	Autor
01.02.2015	0.1	Struktur und Inhalt basierend auf Diskussionsgrundlage eID Konzept Bund	L. Müller
10.02.2015	0.2	Entwurf	L. Müller, M. Waldner
30.03.2015	0.6	Präzisierung und Straffung der Terminologie; Rechtsetzungskapitel	L. Müller, M. Waldner, Urs Paul Holenstein, Daniel Stettler
14.04.2015	0.9	Version für die Ämterkonsultation	L. Müller, M. Waldner, R. Vanek
13.05.2015	0.95	Version für informelle Konsultation	L. Müller, M. Waldner, K. Good

Alle Formulierungen gelten gleichermassen für beide Geschlechter.

Eine eID dient zum Nachweis der eigenen Identität in der virtuellen Welt, vergleichbar mit Identitätskarte oder Pass in der physischen Welt.

Abstract

Der Bundesrat hat das EJPD beauftragt, ein Konzept und einen Entwurf für die rechtliche Ausgestaltung des künftigen elektronischen staatlichen Identifikationsmittels (elD) auszuarbeiten, das zusammen mit der neuen Identitätskarte (IDK) angeboten wird und EU-kompatibel ist. Die EU geht davon aus, dass ihre Mitgliedstaaten im Sinne der hoheitlichen Verantwortung nur für ihre eigenen Bürger staatlich anerkannte eID ausstellen, diese eID aber gegenseitig anerkennen können (Notifikation). Auch das vorliegende Konzept orientiert sich an diesem Modell und hat zum Ziel, die Abläufe für den Bezug und den Einsatz der staatlichen schweizerischen eID sowie den technischen Lösungsansatz festzulegen. In einem weiteren Schritt soll dann in der zweiten Jahreshälfte 2015 der zugehörige Rechtsetzungsentwurf erarbeitet und im Frühjahr 2016 in die Vernehmlassung gegeben werden.

Im Rahmen der Analyse bestehender (staatlicher) eID-Systeme wurden die Benutzerfreundlichkeit der eID und die Attraktivität der damit nutzbaren Angebote als wichtigste Erfolgsfaktoren identifiziert. Der erste Erfolgsfaktor führt unmittelbar zur Schlüsselfrage, ob es dem Staat gelingen kann, mit vertretbarem Aufwand eine langfristig attraktive eigene eID (realisiert als physisches Token, z.B. in Form eines Chips auf der Identitätskarte) herauszugeben oder ob dies aufgrund der raschen technologischen und sozioökonomischen Entwicklung besser dem freien Markt zu überlassen ist. Wichtig ist dabei die Erkenntnis, dass eine eID hauptsächlich für die Online-Authentifizierung gebraucht wird und dass genau dieser Prozess rasche Entwicklungszyklen durchläuft. Eine vom Staat abgegebene eID käme dabei bald ins Hintertreffen. Die Erfüllung des zweiten wichtigen Erfolgsfaktors liegt in der Verantwortung der übrigen Protagonisten des eID-Ökosystems und ist meist ein langjähriger Prozess. Ausdrücklich soll hier der im Rahmen des Vorhabens Identitätsverbund Schweiz (IDV-Schweiz) geplante nationale und internationale Föderierungsdienst für eID-Systeme erwähnt werden, welcher voraussichtlich eine zentrale Rolle für den Erfolg des schweizerischen eID-Ökosystems einnehmen wird und zudem die Schnittstelle zu den eID-Systemen der EU bieten soll.

Gestützt auf die in der Analyse gewonnen Erkenntnisse wird gemäss vorliegendem Konzept auf die Herausgabe einer eigenen staatlichen eID verzichtet. Dafür können sich heutige und zukünftige eID-Systeme staatlich anerkennen lassen (z.B. SuisseID, Mobile ID usw.), wenn diese die noch zu schaffenden gesetzlichen Bedingungen erfüllen. Darin eingeschlossen sind behördliche eID-Systeme, wie sie z.B. im Rahmen des Vorhabens IAM-Bund vorgesehen sind. Ziel ist es, dass jede Person für alltägliche Transaktionen ihre gewohnte eID einsetzen kann, ohne dabei zwingend und fortwährend auf staatliche eID-Infrastrukturen zurückgreifen zu müssen. Separat zu prüfen bleibt, ob für besonders heikle Transaktionen, z.B. im Bereich Vote électronique, zusätzlich ein eigenes und besonders sicheres Endgerät notwendig ist.

Die Lösung sieht vor, dass Personen die Identitätsattribute ihrer eID mit Hilfe eines neu durch den Bund zu schaffenden ID-Kontos staatlich beglaubigen können. Für die freiwillige Eröffnung des ID-Kontos ist in jedem Fall eine persönliche Vorsprache notwendig, damit die Identität der Person zweifelsfrei abgeklärt werden kann. Die Vorsprache erfolgt im selben organisatorischen Rahmen wie die Beantragung eines Passes oder einer IDK. Die Nutzung des ID-Kontos wird immer eine 2-Faktor-Authentifizierung erfordern. Bei der Eröffnung des ID-Kontos erhält der Antragsteller von der staatlichen Registrierungsstelle die Mittel für eine solche Authentifizierung in Form einer Kombination von Benutzernamen/PIN sowie eines jeweils per SMS übermittelten Einmalpasswortes auf ein persönliches Mobiltelefon. Später registriert der Kontoinhaber dann eine auf dem Markt beschaffte staatlich anerkannte eID für den Zugang zum Konto. Mit diesem Verfahren kann die Registrierung und Beglaubigung einer eID zeitlich sehr flexibel, auch später, erfolgen.

Unter Abwägung der Benutzerakzeptanz, der Risiken und der Kosten sowie der Resultate der durchgeführten Ämterkonsultation ist das Projekt zum Schluss gekommen, dass der geschilderte Lösungsvorschlag die vielschichtigen Anforderungen an eine staatliche eID am besten zu erfüllen vermag. Im Rahmen der informellen Konsultation soll dies nun validiert werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Das Literaturverzeichnis befindet sich in Kapitel 11 am Ende des Dokuments. Referenzen im Text werden in eckigen Klammern […] angegeben (IEEE Notation).

1 Einführung

1.1 Zweck des Dokuments

Das vorliegende Dokument beschreibt das Konzept für die schweizerischen staatlich anerkannten elektronischen Identifizierungssysteme (eID-Systeme), welche mit den eID-Systemen der EU interoperabel und damit notifizierbar [1] sind. Es beschreibt organisatorische, technische, finanzielle sowie erste rechtliche Aspekte der vorgesehen Realisierung und dient als Grundlage für die spätere Ausarbeitung des Rechtsetzungsentwurfs und der Detailkonzepte. Das Konzept soll Mitte 2015 in einer mit den interessierten Stellen der Verwaltung und Öffentlichkeit konsultierten Fassung der Departementsleitung EJPD zur Genehmigung vorgelegt werden. Danach soll der Rechtsetzungsentwurf erarbeitet werden und dem Bundesrat Mitte 2016 zur Eröffnung der Vernehmlassung unterbreitet werden.

1.2 Struktur des Dokuments

Eine Zusammenfassung des Konzeptes findet man im Kapitel 1.3 und die verwendete einheitliche Terminologie, welche sich auf Begriffe abstützt, die im Kontext der europäischen eID-Systeme [1] gebräuchlich sind, in Kapitel 1.4. In Kapitel 2 wird die Ausgangslage mit dem Auftrag des Bundesrates, dem internationalen Umfeld und den bisherigen Erkenntnissen über eID-Systeme dargestellt. Die Ausgangslage führt zum Grundsatzentscheid, dargestellt in Kapitel 3, keine eigene staatliche eID herauszugeben, sondern den staatlichen Anteil am eID-Ökosystem auf ein notwendiges Minimum zu beschränken. Basierend auf dem Grundsatzentscheid werden in Kapitel 4 Ziele für staatlich anerkannte eID-Systeme und das eID-Ökosystem insgesamt definiert, wobei dem für die Akzeptanz wichtigen Themenkreis „Nutzen“ ein eigenes Unterkapitel gewidmet ist. Anschliessend werden in Kapitel 5 die Anforderungen konkretisiert. Schliesslich folgt in Kapitel 6 die Beschreibung der Lösungskomponenten, welche sich in staatlich zu realisierende und weitere Elemente unterteilen. Dem Thema Datensicherheit und Datenschutz ist ein separates Unterkapitel gewidmet. In Kapitel 7 werden die rechtlichen Voraussetzungen für eine Notifizierung der nationalen eID-Systeme in der EU behandelt sowie eine erste Gesetzgebungsanalyse vorgenommen. In Kapitel 8 wird schliesslich die Umsetzung mit Kostenschätzungen und den Risiken für den staatlichen Beitrag dargelegt. In Kapitel 9 folgt eine Ausführung der Auswirkungen auf die Gesellschaft, die Wirtschaft und den Staat, einschliesslich einer sehr vorläufigen Gebührenberechnung.

Im Anhang in Kapitel 10 folgen erläuternde Erklärungen zu Elementen und Annahmen, die im Konzept verwendet werden und in Kapitel 11 folgen schliesslich die Quellenangaben.

1.3 Zusammenfassung

Die „**E-Government-Strategie Schweiz**“ [2] [3] hat zum Ziel, dass sowohl die Wirtschaft als auch die Bevölkerung die wichtigen Geschäfte mit den Behörden elektronisch abwickeln können. Das priorisierte Vorhaben „B2.15 National und im EU-Raum barrierefrei anerkannte elektronische Identität“ [4] ist einer der Bausteine zur Umsetzung dieser Strategie des Bundesrates.

Sind in der physischen Welt Ausweise wie Pass oder Identitätskarte die Mittel zum Nachweis der eigenen Identität, so sind es in der elektronischen Welt die **elektronischen Identifizierungsmittel (kurz eID)**, auch bezeichnet als elektronische Identitäten. eID werden in der Regel von **Identitätsdienstleistern (IdP)** herausgegeben. Mit einer eID kann sich eine natürliche Person gegenüber einem **vertrauenden Beteiligten** (z.B. einem Internetportal) authentifizieren sowie Personenidentifizierungsdaten, genannt **Identitätsattribute** (wie z.B. Name, Alter, usw.), elektronisch nachweisen.

Dazu beweist die Person gegenüber ihrer eID ihre physische Präsenz und ermöglicht dadurch ihre **Authentifizierung** bei einem vertrauenden Beteiligten. Auf ausdrückliches Verlangen der Person können mit Hilfe der eID Identitätsattribute der Person auf vertrauenswürdige Art und Weise an einen vertrauenden Beteiligten übermittelt werden. Die eID ist dem vertrauenden Beteiligten unter einem eindeutigen Identifikator bekannt, unter dem die Person beim vertrauenden Beteiligten registriert ist. Eine eID ist also das sichere Bindeglied zwischen der physischen Person und ihrer elektronischen Repräsentation bei einem vertrauenden Beteiligten. Eine Person kann mehrere eID und damit elektronische Identitäten besitzen. Natürliche Personen, vertrauende Beteiligte, Identitätsdienstleister und der Staat als Garant für die wichtigsten Identitätsattribute der Personen bilden zusammen ein eID-Ökosystem. Die wichtigsten Begriffe des eID-Ökosystems sind in Abbildung 1 aufgeführt.

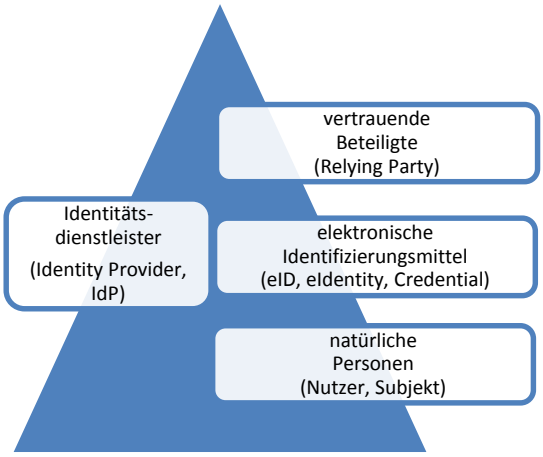

Abbildung 1 – Begriffe des eID-Ökosystems

Im Kontext der anstehenden Erneuerung der Schweizer Ausweise Pass und Identitätskarte (IDK) hat der **Bundesrat am 19.12.2012 das EJPD beauftragt, ein Konzept für zukünftige staatlich anerkannte elektronische Identifizierungsmittel der Schweiz zu erarbeiten**, welche mit den eID-Systemen der EU (eIDAS-Verordnung [1]) interoperabel und damit notifizierbar sind. Das vorliegende Dokument beschreibt dieses Konzept und versucht, die im eID-Ökosystem bestehenden hohen, aber teilweise diffusen Erwartungen mit den praktischen Erfahrungen bereits implementierter Identifizierungssysteme zu verschmelzen. Selbstverständlich ist eine wichtige Voraussetzung für den Nutzen und damit den Erfolg des Vorhabens, dass in der Bevölkerung, der Privatwirtschaft und bei den Behörden tatsächlich ein Bedarf für eine Verlagerung von Dienstleistungen in die online Welt und für den elektronischen Nachweis von Identitätsattributen besteht. Obwohl die fortschreitende technologische Entwicklung, die umfassende Verbreitung des Internets und die technologieaffinen jüngeren Generationen[1] einen solchen sozioökonomischen Wandel begünstigen, braucht es dazu eine aktive Mitarbeit aller Protagonisten im eID-Ökosystem.

Ein erster **Konzeptentwurf** ging davon aus, dass das elektronische Identifizierungsmittel direkt in die neue Identitätskarte (IDK mit Chip) integriert wird. Dies entspricht dem Modell von zahlreichen anderen staatlichen eID, z.B. denjenigen von Deutschland (nPA), Estland oder Belgien. Nach einer Prüfung der Benutzerakzeptanz von solchen Lösungen im Herbst 2014, sowie gestützt auf die Resultate der im Sommer 2014 durchgeführten ersten Ämterkonsultation, hat sich das EJPD entschlossen, das Konzept nochmals zu überarbeiten. Einerseits blockiert die lange Gültigkeit einer IDK von 10 Jahren technologische Weiterentwicklungen, andererseits bedingt eine konventionelle Kartenlösung immer auch eine entsprechende elektronische Schnittstelle und ein passendes Lesegerät. Dieses ist oft auf die Installation von Treibern und zusätzlichen Applikationen angewiesen, welche einen hohen fortwährenden Entwicklungs- und Supportaufwand seitens Bund nach sich ziehen würden. Hinzu kommt, dass nicht alle modernen Endgeräte über die notwendigen Schnittstellen (wie z.B. USB oder NFC) verfügen und so die Verwendbarkeit einschränken. Deshalb ist die Akzeptanz einer solchen Lösung als sehr fraglich bis schlecht zu beurteilen, wie aktuell implementierte Systeme zeigen. **In der Folge wurde eine Integration der staatlichen eID in die IDK als nicht zielführend beurteilt**. Die staatlich anerkannte eID soll deshalb über einen anderen Weg realisiert werden, welcher moderner, flexibler und skalierbarer ist.

[1] Generationen Y und Z, „Internet Generation“ oder „Digital Natives“, ab den späten 80-ern geboren, sehr gut vernetzt und dauernd online.

Das **überarbeitete Konzept** sieht vor, dass der Staat nur diejenigen Elemente in Form eines subsidiären staatlichen Identitätsdienstes selbst bereitstellt, welche aus Gründen der Rechtssicherheit und Wirtschaftlichkeit zwingend durch ihn selbst bereitgestellt werden müssen. Das Konzept geht von der Voraussetzung aus, dass Personen zum Einführungszeitpunkt einer staatlichen eID im Jahr 2020 dasjenige elektronische Identifizierungsmittel aus dem freien Markt einsetzen wollen, welches modern ist, alltäglich, bequem und mobil genutzt werden kann, wenig bis nichts zusätzlich kostet, und die individuellen Sicherheitsbedürfnisse gerade genügend gut abdeckt.

Aus diesem Grund sollen die staatlich anerkannten eID nicht monopolistisch durch den Staat selbst, sondern durch **mehrere staatlich anerkannte Identitätsdienstleister** (IdP) herausgegeben werden. Nur im sehr unwahrscheinlichen Fall, dass im Schweizer eID-Ökosystem keinerlei staatlich anerkennbare eID angeboten würden, müsste der Staat selbst ein täglich nutzbares Identifizierungsmittel herausgeben (Rückfalllösung). Staatlich anerkannte Identitätsdienstleister sind solche, die ihr Identifizierungssystem nach den rechtlichen Vorgaben des Staates zertifizieren lassen und gestützt darauf vom Staat eine Lizenz erhalten können, um eID mit staatlich beglaubigten Identitätsattributen herausgeben zu dürfen. Dieser Vorgang entspricht im Grundsatz der Notifikation im EU-Raum, jedoch auf nationaler Ebene. Falls die Schweiz später das zugehörige staatlich anerkannte eID-System notifiziert, wird mit einer solchen eID jede Person die eigene Identität im EU-Raum grenzüberschreitend und medienbruchfrei nachweisen können.

Damit eine Person ihre eID mit staatlich beglaubigten Identitätsattributen unterlegen kann, schafft der Staat neu ein **persönliches ID-Konto mit einem Siegeldienst**. Mit diesem kann eine Person freiwillig einzelne staatliche Identitätsattribute online gegenüber staatlich anerkannten IdP beglaubigen. Das eID-Konto soll initial folgende Attribute enthalten, die insgesamt als **Personenidentifizierungsdaten** bezeichnet werden: a) amtlicher Name, b) Vornamen, c) Geburtsdatum, d) Geschlecht, e) Geburtsort[2], f) Heimatort, g) Nationalität, h) (leer)[3], i) Gesichtsbild, j) Unterschriftsbild, k) Ausweisnummer Pass und l) Ausweisnummer IDK sowie zusätzlich das m) Datum der letzten staatlichen Identifikation. Weitere staatliche Identitätsattribute können zusätzlich aufgenommen werden, sollte im eID-Ökosystem dafür ein Bedarf und eine Rechtsgrundlage bestehen. **Wichtig für das Verständnis** ist, dass weder ein IdP noch ein vertrauender Beteiligter unbesehen Zugriff auf diese Attribute erhalten. Es ist immer die Person, welche einzelne oder mehrere Attributwerte explizit und bewusst an den staatlich anerkannten IdP übermittelt und damit beglaubigt. Sollte also eine Person z.B. ihr Geburtsdatum dem IdP nicht übermitteln wollen, muss sie das auch nicht tun, kann aber dennoch die übrigen Attribute beglaubigen. Die Überprüfung, ob die vom IdP geführten Attributwerte mit den staatlichen Beglaubigungen übereinstimmen, liegt indes in der alleinigen Verantwortung des IdP. Gesichts- und Unterschriftsbild können von der Person zusätzlich als Datei zur weiteren Verwendung aus dem ID-Konto heruntergeladen werden, nachdem sich die Person gegenüber ihrem ID-Konto authentisiert hat.

Nach der eIDAS-Verordnung **haftet der Staat bei den der EU notifizierten Identifizierungssystemen** dafür, dass die Registrierung, also die Verbindung von natürlicher Person, Identifizierungsmittel und den Identitätsattributen, zum Zeitpunkt der Ausstellung des elektronischen Identifizierungsmittels korrekt ist. Aus diesem Grund übernimmt der Staat die Registrierungsdienstleistung

---

[2] Bei den Schweizer Ausweisen wird aktuell der Heimatort statt wie weltweit üblich der Geburtsort genannt. Heimatort und Geburtsort sind in einem eID-System unterschiedliche Attribute und müssen deshalb genau unterschieden werden. Im Sinne der internationalen Interoperabilität wird empfohlen, auch den Geburtsort in das CH-eID-System aufzunehmen.

[3] Hier war die AHVN13 zur Qualitätssicherung in den Bereichen elektronisches Patientendossier und Vote électronique sowie zur elektronischen Abwicklung von AHV/IV-Geschäftsfällen vorgesehen gewesen. Sie wurde aber im Rahmen der Ämterkonsultation aufgrund der Stellungnahmen des Bundesamtes für Sozialversicherungen und des EDÖB aus der Liste der Attribute entfernt. Beide Ämter haben auf die Zweckbindung der AHVN13 und das potentielle Datenschutzrisiko bei einer missbräuchlichen Verwendung durch vertrauende Beteiligte hingewiesen.

und akzeptiert für den Zugang zum ID-Konto nur ein starkes Authentifizierungsmittel, das er der Person selbst ausgestellt hat, oder eID von staatlich anerkannten und dementsprechend lizenzierten Identitätsdienstleistern. Staatlich anerkannte eID-Systeme müssen mindestens das Sicherheitsniveau „substanziell" gemäss eIDAS-Verordnung unterstützen.

In der **Praxis** wäre der Ablauf für die Eröffnung und Nutzung eines ID-Kontos wie folgt:

- In einem ersten Schritt beantragt eine Person das ID-Konto und registriert dabei ihre Mobiltelefonnummer. Sie kann den Antrag online mit dem Internetantrag auf www.schweizerpass.ch oder je nach Kanton auch telefonisch oder im Rahmen der persönlichen Vorsprache stellen. Ob eine Person beim Internetantrag auch gleich eine eID bei einem staatlich anerkannten IdP online bestellen kann, soll noch geprüft werden. Der Antrag auf das ID-Konto kann vorteilhaft als Kombi mit einem Pass und/oder einer Identitätskarte erfolgen.
- In einem zweiten Schritt muss die Person auf einer staatlichen Registrierungsstelle persönlich vorsprechen. Die Person wird von Staates wegen identifiziert, die registrierte Mobiltelefonnummer wird verifiziert, die Personenidentifizierungsdaten werden festgestellt und in dem persönlichen online ID-Konto abgelegt. Nach dem Bezahlen der Gebühren wird das ID-Konto aktiviert und der Person wird Benutzername mit PIN für den initialen Zugang zum ID-Konto zugestellt oder direkt übergeben.
- In einem dritten Schritt meldet sich die Person mit dem Benutzernamen und PIN sowie dem auf die registrierte Mobiltelefonnummer gesandten Einmalpassort am ID-Konto an. Danach kann sie eine oder mehrere staatlich anerkannte eID im ID-Konto registrieren. Damit werden diese eID ebenfalls akzeptierte Authentifizierungsmittel für den Zugriff auf das ID-Konto und die Person kann für jede dieser eID beim herausgebenden IdP einzelne Identitätsattribute staatlich beglaubigen. Der IdP bewahrt die Beglaubigung auf und kann für den Inhaber der eID entsprechende Bestätigungen zuhanden von vertrauenden Beteiligten ausstellen. Sowohl die Registrierung einer eID als auch die Attributbeglaubigungen erfordern Transaktionsbestätigungen, welche via Quittungsmeldung und erneut zugesandte Einmalpassworte auf die Mobiltelefonnummer des ID-Konto Inhabers eingeholt werden. Zudem wird es voraussichtlich möglich sein, direkt aus dem ID-Konto eine eID bei einem staatlich anerkannten IdP zu bestellen.

Wie konventionelle Ausweise haben die Identitätsattribute im ID-Konto eine beschränkte Gültigkeit und müssen von Zeit zu Zeit erneuert werden. Solange die Identitätsattribute im ID-Konto gültig sind und eine Person über eine autorisierte eID verfügt, kann sie für sich ohne erneute Vorsprache weitere anerkannte eID registrieren und auch Identitätsattribute beglaubigen.

In drei Sätzen zusammengefasst: Der Staat gibt kein eigenes elektronisches Identifizierungsmittel heraus, sondern schafft den Rechts- und Standardisierungsrahmen für eine Pluralität von staatlich anerkannten eID, welche durch lizenzierte Identitätsdienstleister herausgegeben werden. Diese eID können durch Personen mit Schweizer Staatsbürgerschaft auf freiwilliger Basis mit beglaubigten Attributen ihrer staatlichen Identität unterlegt werden. Mit wenigen Ausnahmen erfolgt der tägliche Einsatz einer solchen eID innerhalb der Schweiz ohne jeden weiteren Rückgriff auf staatliche Identitätsdienstleistungen[4], denn die Hauptakteure sind die Personen mit eID, die vertrauenden Beteiligten und die eID herausgebenden staatlich anerkannten Identitätsdienstleister.

[4] Staatlich anerkannte IdP können die Echtheit der Identitätssiegel überprüfen. Vertrauende Beteiligte können eine staatliche Liste mit gesperrten IdP-Lizenzen (z.B. bei Verlust der Lizenz des IdP) abfragen. Falls nach einer Notifizierung eine eID international eingesetzt wird, dann werden die Daten in den beteiligten Ländern über die nationalen Pan European Proxy Server (PEPS) geleitet.

Folgende **staatlichen Beiträge zum eID-Ökosystem** (in Abbildung 2 blau gefärbt) müssen für staatlich anerkannte eID mit staatlich beglaubigten Identitätsattributen umgesetzt werden:

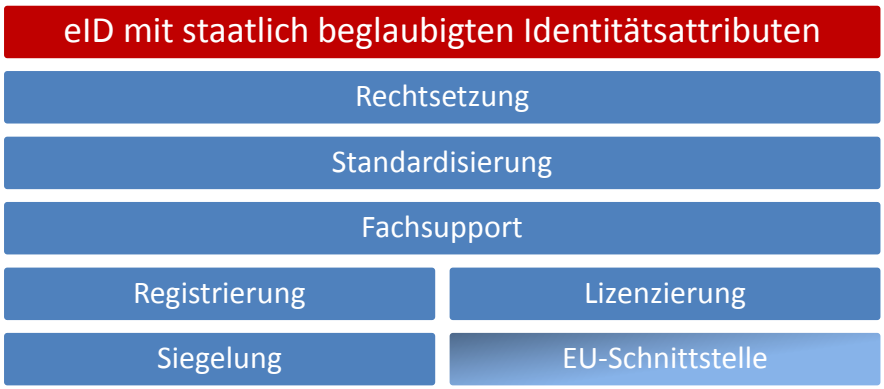

Abbildung 2 – Staatliche Beiträge zum eID-Ökosystem

- **Rechtsetzung**: Für staatlich anerkannte eID mit staatlich beglaubigten Identitätsattributen müssen ein formellgesetzlicher Rechtsrahmen und die notwendigen Ausführungsbestimmungen geschaffen werden. Hierbei müssen die Notifizierbarkeit gegenüber der EU und die damit verbundenen Haftungsbestimmungen beachtet werden. Zudem sollte im Rahmen der Rechtsetzungsarbeiten auch eine Verpflichtung für Behörden geschaffen werden, staatlich anerkannte eID für ihre Online-Dienste zu verwenden. Weiter sollten mögliche rechtliche Hürden für die Umstellung von konventionellen auf elektronische Abläufe beseitigt werden, wo dies innert nützlicher Frist mit vertretbarem Aufwand möglich ist.
- **Standardisierung**: Für eine durchgängige und barrierefreie Funktion des eID-Ökosystems müssen die Teilsysteme einheitliche technische und organisatorische Standards einhalten. Die staatlich anerkannten eID-Systeme der Schweiz müssen auf der Protokollebene vollständig interoperabel sein. Es soll wenn immer möglich auf bestehende Standards (wie etwa ISO- oder ITE-Standards) zurückgegriffen werden. Für die Zertifizierung staatlich anerkannter eID und IdP können zum Beispiel entsprechende „CC Protection Profiles“[5] geschaffen werden. Da die europäische Interoperabilität der eID als wirtschaftliches Ziel angestrebt wird, erscheint uns auch die hauptsächliche Verwendung der von eIDAS geprägten Begrifflichkeiten sehr sinnvoll.
- **Fachsupport**: Dieser unterstützende Dienst umfasst die fachliche Unterstützung der Registrierungsstellen, Support der ID-Kontoinhaber für die Nutzung der ID-Konto, Unterstützung der staatlich anerkannten IdP in den Bereichen Lizenzierung und Siegelung, sowie die interne und externe Kommunikation im Bereich der staatlichen eID-Dienstleistungen. Aufgrund der komplexen, oft wenig greifbaren Materie und der vielen Beteiligten ist eine eingängige und aufklärende Kommunikation für den Erfolg wichtig. In Abstimmung mit den Beteiligten des eID-Ökosystems soll deshalb in Zusammenarbeit mit dem Programm E-Government Schweiz eine professionelle Kommunikationsstrategie in Auftrag gegeben und umgesetzt werden. Dies umfasst auch die auf den Registrierungsstellen notwendigen Informationsmaterialien und Ausbildungen. Der Fachsupport umfasst auch - delegiert an den zuständigen Leistungserbringer des Bundes - den 2nd- und 3rd-Level-Support gegenüber den staatlich anerkannten IdP im Zusammenhang mit den technischen

[5] CC steht für Common Criteria for Information Technology Security Evaluation und ist ein weltweit anerkannter Standard (ISO/IEC 15408) für die Überprüfung der Sicherheit von Informationstechnologien. Pro Technologiekategorie wird jeweils ein sogenanntes Protection Profile (Schutzprofil) entwickelt, das die Sicherheitsanforderungen spezifisch definiert und Basis des Prüfprozesses ist.

Systemen des Bundes. Der direkte Endkundensupport für eine eID erfolgt aber immer direkt durch den Herausgeber der eID.

- **Registrierung**: Die Registrierung umfasst die Identifizierung der natürlichen Person, die Feststellung ihrer staatlichen Personenidentifizierungsdaten und die Erfassung und Validierung der Mobiltelefonnummer, die für den Zugriff auf das persönliche ID-Konto gebraucht wird. Diese Aufgaben übernehmen die so genannten Registrierungsstellen. Da grosse Synergien zur Beantragung eines Schweizer Passes bestehen, sollen die Passstellen der Kantone und Schweizer Auslandvertretungen die Aufgaben der Registrierungsstellen übernehmen, was kostengünstige Kombiangebote zulässt. Dazu muss ihnen der Bund eine technische Lösung für die Eröffnung des ID-Kontos und die Erfassung der Mobiltelefonnummer zur Verfügung stellen. Da die für Schweizer Ausweise notwendigen Identitätsattribute im Informationssystem Ausweisschriften (ISA) bearbeitet werden, sollen möglichst alle Daten für das ID-Konto aus ISA bezogen werden. Die Gültigkeit einer Registrierung ist wie die Gültigkeit von Pass oder IDK zeitlich beschränkt und muss periodisch erneuert werden (10 Jahre für Erwachsene, 5 für Jugendliche und Kinder).
- **Siegelung**: Die Siegelung bedingt die Entwicklung und den Betrieb eines sicheren Datenverarbeitungssystems für die online ID-Konten einschliesslich des Internetportals für den sicheren Zugriff durch die berechtigten Personen (IAM-System). Für die Anmeldung im Portal werden alle staatlich anerkannten eID-Systeme unterstützt, was durch die sich abzeichnende Standardisierung für die online Authentifikation stark erleichtert wird. Zudem muss vom Bund eine technische Lösung für die Erstellung und die Validierung der Siegel gegenüber den lizenzierten IdP realisiert werden. Da der Zugriff auf das ID-Konto mit eID erfolgt, welche von staatlich anerkannten IdP stammen, soll der 1st-Level-Support für ihre eID von diesen IdP erbracht werden (Ausnahme: Zugriff mit Benutzernamen/PIN und OTP für die Erstregistrierung einer eID). Vom Bund wäre im Wesentlichen 2nd- und 3rd-Level-Support für die Beglaubigungssiegel und den Validierungsdienst gegenüber den IdP zu leisten. Sollte eine Person mit den beglaubigten Attributen nicht einverstanden sein, so muss sie sich wie bei den übrigen Schweizer Ausweisen an die zuständige Registrierungsstelle wenden. Inwiefern es zweckmässig wäre, das ID-Konto zu einem Portal auszubauen, über welches weitere E-Government-Anwendungen erreicht werden können, die eine starke und sichere Authentifizierung der Person verlangen (z.B. in den Bereichen Steuern, Bewilligungen, Strafregister, Sozialversicherungen usw.), müsste noch zusammen mit dem priorisierten Vorhaben Identitätsverbund Schweiz (IDV-Schweiz) und der Bundeskanzlei als Betreiberin von www.ch.ch abgeklärt werden.
- **Lizenzierung (Zertifizierung)**: Um eine Lizenz als staatlich anerkannter Identitätsdienstleister zu erhalten, müssen die IdP in regelmässigen Abständen den Nachweis erbringen, dass sie alle rechtlichen, organisatorischen und technischen Vorgaben einhalten. Dazu sollen sie sich nach den im Rahmen der gesetzlichen Regelungen zu bestimmenden Normen und Richtlinien durch eine von der Schweizerischen Akkreditierungsstelle (SAS) anerkannte Zertifizierungsstelle zertifizieren müssen. Für die Verwaltung von IdP-Lizenzen muss der Bund eine neue Applikation entwickeln, welche auch eine im Internet frei zugängliche Validierung von solchen Lizenzen durch die vertrauenden Beteiligten erlaubt. Da nur mit einer Hand voll lizenzierter IdP gerechnet wird und die Abfrage im Internet mit Standardtechniken automatisiert erfolgen kann, hält sich der Aufwand des Bundes in Grenzen. Die im Rahmen des Vorhabens IAM-Bund zu schaffende IdP- und Föderierungs-Lösung kann aus unserer Sicht als staatlich anerkanntes eID-System in das mit dem vorliegenden Konzept vorgeschlagene Modell eingebunden werden. Sie müsste allerdings – wie alle anderen staatlich anerkannten IdP – zertifiziert werden.
- **EU-Schnittstelle (optional)**: Mit einer Notifizierung ist die Einhaltung der Vorgaben der eIDAS-Verordnung der EU verbunden, welche für die Schweiz a priori nicht rechtlich verbindlich sind und deshalb eine staatsvertragliche Regelung vorzunehmen ist (vgl. diesbezüglich Ausführungen unter Ziff. 7.2.2). Notifiziert die Schweiz ein staatlich anerkanntes eID-System, so muss sie für ih-

re eigenen E-Government-Dienste, bei denen sie die Schweizer eID zulässt, auch uneingeschränkt alle anderen notifizierten eID zulassen, sofern diese über das mindestens gleiche Sicherheitsniveau verfügen („substanziell“ gemäss eIDAS-Verordnung[6]). Zudem ist die technische Schnittstelle zu den eID-Systemen der EU-Länder zu schaffen. Sollte die Schweiz eines oder mehrere ihrer eID-Systeme der EU notifizieren, muss für die Abwicklung von eID-Transaktionen mit den anderen Ländern ein nationaler Pan European Proxy Server (PEPS) [5] geschaffen werden, welcher die Schnittstelle zwischen den beteiligten eID-Systemen bildet. Die Entwicklung und der Betrieb des PEPS sowie der Akt der Notifikation selbst sind jedoch nicht Bestandteil des geplanten Umsetzungsprojekts des EJPD. Die nationalen und internationalen Föderierungsdienste sind ein Teil des Vorhabens Identitätsverbund Schweiz (IDV-Schweiz), welches in der Verantwortung des SECO liegt.

Mit der Umsetzung dieser Lösungselemente muss der Bund neue Aufgaben wahrnehmen. Nach den vorliegenden Aufwandschätzungen sind zur **Umsetzung CHF 6.3 Mio.** und für den **Betrieb CHF 2.1 Mio.** jährlich notwendig. Bedingt durch neue Aufgaben sind darin zusätzliche personelle Ressourcen beim EJPD (fedpol) im Umfang von 300 Stellenprozenten enthalten. Die Finanzierung ist durch den mit dem Bundesratsbeschluss vom 16.12.2011 bewilligten Verpflichtungskredit nur teilweise abgedeckt. Im Rahmen der für Mitte 2016 geplanten Vernehmlassung soll dem Bundesrat ein revidiertes Finanzierungskonzept vorgelegt werden.

Die Registrierungsstellen der **Kantone** und **Schweizer Auslandvertretungen** müssen einen neuen Geschäftsfall abdecken, nämlich die oben beschriebene Eröffnung des ID-Kontos mit der Registrierung und Validierung einer Mobiltelefonnummer. Dies kann zu einem noch zu bestimmenden personellen Mehrbedarf führen.

Die Investitionen und Betriebsausgaben müssen mittelfristig durch **kostendeckende Gebühreneinnahmen** kompensiert werden. Ob in der Anfangsphase auch eine Anschubfinanzierung durch den Bund möglich und politisch gewünscht ist, bleibt abzuklären. Wie hoch diese Gebühren tatsächlich ausfallen, kann verständlicherweise noch nicht definitiv abgeschätzt werden. Eine informative Überschlagsrechnung ohne Amortisation der Projektkosten hat ergeben, dass eine Registrierung rund CHF 30 kostet, sofern sie im Rahmen eines Antrages für einen Pass erfolgt (sonst CHF 80). Darin nicht enthalten sind die Kosten für die durch die Personen selbst zu beschaffende eID, welche durch den Markt bestimmt werden und je nach Preismodell des IdP auch null sein können.

Die Beglaubigung von Personenidentifizierungsdaten erstreckt sich im vorliegenden Konzept nicht auf in der Schweiz lebende **Personen mit ausländischer Staatbürgerschaft**, sondern orientiert sich am EU-Modell, welches davon ausgeht, dass jeder Mitgliedsstaat ein nationales eID-System für seine Bürger aufbaut und dieses dann notifizieren kann. Diese Einschränkung schliesst ausländische Personen aber nicht grundsätzlich vom Gebrauch der staatlich anerkannten eID aus, denn auch diese Personen können eine solche eID bei einem IdP beziehen und als Authentifizierungsmittel nutzen. Sie können lediglich keine Attributbestätigungen mit beglaubigten Identitätsattributen an vertrauende Beteiligte liefern. Analoges gilt für juristische Personen, deren Attribute im Handelsregister und nicht im ID-Konto hinterlegt sind.

Als **Projektrisiken** werden einerseits die Unsicherheiten bezüglich des tatsächlichen Bedarfs und andererseits die Unsicherheiten bezüglich der Akzeptanz einer konkreten staatlich regulierten eID-Lösung angesehen. Aus diesen Gründen begnügt sich der Staat bei der vorgeschlagenen Lösung mit der elektronischen Beglaubigung von Identitätsattributen, nutzt aber gleichzeitig die Stärken des Marktes für innovative eID. Wichtig ist, dass parallel das oben erwähnte Vorhaben IDV-Schweiz

[6] Die eIDAS-Verordnung definiert in Art. 8 in Anlehnung an die Sicherheitsniveaus 2-4 („Medium“, „High“, „Very High“) des ISO Standards 29115:2013 [33] die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ für elektronische Identifizierungsmittel. Das Sicherheitsniveau „substantiell“ verlangt eine sichere Zweifaktor-Authentifizierung.

umgesetzt wird und die Behörden wo sinnvoll verpflichtet werden, staatlich anerkannte eID zu akzeptieren.

Die **Umsetzung des Projektes** zur Einführung von staatlich anerkannten elektronischen Identifizierungsmitteln kann voraussichtlich unter Einbezug der notwendigen Schaffung der formellgesetzlichen Grundlagen bis 2020 erfolgen. Die Federführung liegt im EJPD unter Beteiligung der BK, des EDA, EDI, EFD, WBF und des UVEK.

1.4 Begriffe und Abkürzungen

Im Bereich Identitäts- und Zugangsmanagement verwenden die involvierten Parteien eine Reihe von Begriffen, die zwar oft ähnlich aber nicht immer deckungsgleiche Bedeutungen haben. Auch in diesem Dokument werden Begriffe verwendet, die ganz spezifische Sachverhalte bezeichnen und hier zu Beginn in Tabelle 1 definiert und spezifiziert sind. Basis für die hier verwendeten Definitionen sind die Begriffsbestimmungen der eIDAS-Verordnung Art 3, wo nötig ergänzt mit Definitionen aus weiteren Quellen (z.B. ZertES [6], eCH-0107 [7], Mondinis Begriffsbestimmungen [8] und weitere Dokumente [9]). Einige wenige Begriffe sind für das vorliegende Konzept präzisiert oder eingeschränkt worden.

Tabelle 1 – Begriffe und Abkürzungen

Begriff und Abkürzung	Definition und Erläuterung
Attributbeglaubigung	Staatliche Attributbestätigung in Form eines Siegels für die Prüfsumme eines Identitätsattributs aus einem staatlichen ID-Konto, erstellt durch den Staatlichen Identitätsdienst (SID) zuhanden eines staatlich anerkannten IdP.
Attributbestätigung	Signierter Datensatz, der bestätigt, dass der Wert eines Identitätsattributs auf einem bestimmten Qualitätsniveau überprüft ist; zum Beispiel können Attributbestätigungen für Identitätsattribute durch einen staatlich anerkannten Identitätsdienstleister gebunden an eine bestimmte eID geleistet werden.
Authentifizierung	Elektronischer Prozess zwischen einem Authentifizierungsdienst und einer Authentifizierungsanwendung, der die Bestätigung der elektronischen Identifizierung einer Person ermöglicht; sie beinhaltet die Verifikation von einem oder mehreren Authentifizierungsfaktoren und bestätigt dies unter einem der Authentifizierungsanwendung und dem Authentifizierungsdienst bekannten Identifikator. Eine Authentifizierung erfolgt je nach Sicherheitsstufe auf dem Niveau „niedrig“ (begrenztes Vertrauen), „substanziell“ (substanzielles Vertrauen) und „hoch“ (noch höheres Vertrauen). Vgl. auch Kapitel 10.3.3 im Anhang.
Authentifizierungsanwendung	Anwendung auf dem Endgerät einer Person, welche mittels einer eID gegenüber einem Authentifizierungsdienst in einem standardisierten Verfahren eine Authentifizierung der Person ermöglicht.
Authentifizierungsdienst	Elektronischer Dienst, der in einem standardisierten Verfahren mit einer Authentifizierungsanwendung eine Authentifizierung einer Person durchführt. Überprüft der Authentifizierungsdienst die Authentifizierung durch eine eID ohne Rückgriff auf einen Föderationsdienst, wird dies hier als Direktmodus bezeichnet.

Begriff und Abkürzung	Definition und Erläuterung
Authentifizierungsfaktor	Charakteristik (Faktor) in Form eines materiellen oder virtuellen Gegenstandes, eines Geheimnisses oder einer biometrischen Eigenschaft, die einer bestimmten Person zugeordnet ist. Die Gesamtheit der Authentifizierungsfaktoren, die für eine Authentifizierung überprüft werden, wird als Authentifizierungsmittel bezeichnet.
Elektronisches Identifizierungssystem (eID-System)	Elektronisches System, in dessen Rahmen Personen elektronische Identifizierungsmittel ausgestellt werden; staatlich anerkannt werden eID-Systeme, wenn die ausgestellten eID und die herausgebenden IdP den einschlägigen schweizerischen gesetzlichen Anforderungen genügen.
Elektronisches Identitätsökosystem (eID-Ökosystem)	Gesamtheit aller natürlichen und juristischen Personen, vertrauender Beteiligter und Identitätsdienstleister, die elektronische Identifizierungssysteme nutzen oder zu deren Betrieb beitragen inklusive das organisatorische, prozedurale, rechtliche und technische Umfeld.
Elektronisches Identifizierungsmittel (eID)	Materielle und/oder immaterielle Einheit, die zur Authentifizierung einer Person bei Authentifizierungsdiensten verwendet wird (die Authentifizierungsfunktion allein wird oft auch als Authentifikator bezeichnet); sie kann nebst dem evtl. verbindungsabhängigen Identifikator weitere Identitätsattribute enthalten oder mit solchen in eindeutiger Weise verbunden sein. Elektronische Identifizierungsmittel können verschiedene Sicherheitsstufen der Authentifizierung und der Identifizierung unterstützen.
Elektronisches Siegel	Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt und logisch mit ihnen in unveränderbarer Weise verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen; sie sind dem Siegelersteller eindeutig zugeordnet und identifizieren diesen.
Föderationsdienst	Dienst eines IdP, der im Auftrag eines vertrauenden Beteiligten eine Person authentifiziert und dem vertrauenden Beteiligten die erfolgreiche Authentifizierung bestätigt. Eine eID, die für eine Authentifikation bei einem Föderationsdienst gebraucht wird, wird hier als eID im Föderationsmodus bezeichnet.
Identifikator	Name (Zeichenkette) einer materiellen oder immateriellen Einheit, die innerhalb eines Namensraumes durch den Namen eindeutig bestimmt ist. Ein Identifikator einer eID kann in einem Initialisierungsprozess von einem Dienst einer bestimmten Person zugeordnet werden, er wird dann auch zu einem Identitätsattribut der Person für diesen Dienst.

Begriff und Abkürzung	Definition und Erläuterung
Identifizierung (elektronische)	(Elektronischer) Prozess der Verwendung von Identitätsattributen um eine Person eindeutig zu bestimmen. Im Kontext der staatlich anerkannten eID ist die Verwendung von Personenidentifizierungsdaten gemeint[7]. Vgl. auch Kapitel 10.2.2 im Anhang.
Identität	Menge der Attribute (namentliche Eigenschaften) einer Person.
Identitätsattribut	Mit einem Namen bezeichnete Eigenschaft einer Person, die diese näher beschreibt; das Attribut besteht aus dem Attributnamen (Beispiel „Vorname“) und dem Attributwert (Beispiel „Heidi“); optional können einem Attribut weitere Merkmale zugeordnet werden wie Datentyp, Vertrauensgrad in Korrektheit des Attributs etc.
Identitätsdienstleister (IdP)	Anbieter und Betreiber von Vertrauensdiensten (insbesondere Authentifizierung, Identifizierung und evtl. Föderation) für ein eID-System; er kann solche Dienste für seinen internen Bedarf oder für Dritte erbringen; ein IdP, der ein staatlich anerkanntes eID-System betreibt und die entsprechende Lizenz vom Staat hat, wird als staatlich anerkannter Identitätsdienstleister, IdP oder eID-Herausgeber bezeichnet.
Identitäts- und Zugangsverwaltung (IAM)	Als Identitäts- und Zugangsverwaltungssysteme (Identity and Access Management – IAM) werden die Systeme von vertrauenden Beteiligten bezeichnet, die Identitäts- und Zugangsdaten der nutzenden Personen verwalten und die Authentifizierungsprotokolle durchführen.
Notifizierung	Anmeldung, Beschreibung und Nachweis der Erfüllung der Anerkennungskriterien für ein von der EU gemäss eIDAS-Verordnung anerkanntes eID-System. Eine Notifizierung bedingt eine reziproke Anerkennung aller bereits notifizierten eID-Systeme. Für die Schweiz ist eine staatsvertragliche Regelung notwendig.
Person	Natürliche Person; im Kontext dieses Konzepts ist damit immer eine Schweizerin oder ein Schweizer gemeint.

[7] In der IT Begriffswelt kann jedes Identitätsattribut zur Identifizierung verwendet werden. Mit der hier gemachten Einschränkung nähert sich der Begriff dem Verständnis einer staatlichen Registrierungsstelle an, die unter Identifizierung die Feststellung von staatlichen Personenidentifizierungsdaten versteht.

Begriff und Abkürzung	Definition und Erläuterung
Personen-identifizierungsdaten	Datensatz, der es ermöglicht, die Identität einer Person festzustellen; im Kontext der schweizerischen staatlich anerkannten eID enthält der für eine vollständige staatlich Identifizierung ausreichende Datensatz initial die Attribute: a. amtlicher Name; b. Vornamen; c. Geburtsdatum; d. Geschlecht e. Geburtsort ; f. Heimatort; g. Nationalität; Diese Daten werden in diesem Konzept auch als Identitätsdaten bezeichnet. Zusätzlich gehören auch noch h. (leer)[8]. i. Gesichtsbild, aufgenommen bei der initialen Registrierung; j. Unterschriftsbild, aufgenommen bei der initialen Registrierung; k. Ausweisnummer des Passes; l. Ausweisnummer der IDK; m. Datum der initialen Registrierung; zu den schweizerischen Personenidentifizierungsdaten.
Registrierung	Prozess einer Regierungsstelle, bei dem die Identität einer Person amtlich festgestellt wird, ihre Personenidentifizierungsdaten erfasst werden und eine eID mit diesen Daten verbunden wird; für schweizerische eID-Systeme registriert der Staat eine staatlich anerkannte eID als digitalen Ausweis für den Zugang zum ID-Konto.
Registrierungsstelle	Bezeichnet eine staatliche Stelle, die eine initiale Identifizierung und Registrierung einer Person vornehmen und deren Personenidentifizierungsdaten amtlich feststellen kann; die Passstellen bei den Kantonen und Auslandvertretungen der Schweiz sind Registrierungsstellen.

[8] Vgl. Fussnote 3 auf Seite 8.

Begriff und Abkürzung	Definition und Erläuterung
Staatlicher Identitätsdienst (SID)	Gesamtheit der folgenden staatlichen Dienstleistungen der Schweiz, die für staatlich anerkannte elektronische Identitätsmittel erbracht werden: a) Initiale physische Überprüfung der Identität einer Person; Erstellung eines ID-Kontos und Registrierung einer staatlich anerkannten eID als Authentifizierungsmittel für den Zugang zum ID-Konto bei einer Registrierungsstelle (Registrierungsdienst); b) Erstellung, Überprüfung und Validierung von elektronischen Siegeln für staatlich beglaubigte Identitätsattribute (Siegeldienst); c) Registrierung, Aufsicht und Lizenzierung von staatlich anerkannten Identitätsdienstleistern, die ein staatlich anerkanntes eID-System betreiben (Lizenzierungsdienst , entspricht der Aufsichtsstelle in der eIDAS-Verordnung). Zusätzlich Rechtsetzung, Standardisierung, Fachsupport mit Kommunikation und (optional) EU-Schnittstelle.
Staatliches Identitätskonto (ID-Konto)	Online Konto, das die staatlichen Personenidentifizierungsdaten einer Person mit schweizerischer Staatsbürgerschaft enthält. Nach einer erfolgreichen Registrierung eines der Person gehörenden Identifizierungsmittels erhält die Person den Zugang zu ihrem Konto und kann gegenüber staatlich anerkannten IdP ihre Identitätsattribute beglaubigen (Siegel).
Trusted Execution Environment (TEE)	Isolierte und vertrauenswürdige Laufzeitumgebung für Applikationen auf mobilen Endgeräten. Auf dem TEE können nur speziell dafür freigeschaltete Applikationen ausgeführt werden.
Validierung	Prozess der Überprüfung und Bestätigung der Gültigkeit eines elektronischen Siegels, eines Zertifikats, einer Bestätigung oder einer Lizenz.
Verifikation	Prozess des elektronischen Erkennens einer Person durch Überprüfung des Authentifizierungsmittels der Person (einem oder mehreren Authentifizierungsfaktoren) mittels eines geeigneten Messprotokolls; Zuordnung eines Identifikators (Übergang von der realen Welt der Person zur digitalen Repräsentation der Person).
Vertrauender Beteiligter (vBt)	Natürliche oder juristische Personen, die einen Vertrauensdienst oder die von einem Vertrauensdienst erstellten Dokumente und Zertifikate nutzt und diesen vertraut; zum Beispiel kann ein vBt einer eID eines IdP vertrauen.
Vertrauensdienst	Elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird, und Dienstleistungen wie Erstellung, Überprüfung, Validierung und Bewahrung von elektronischen Identitäten, Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln einzeln oder in Kombination erbringt; ein IdP aber auch Dienste des SID sind Beispiele für Vertrauensdienste.

2 Ausgangslage

Mit der Verbreitung des Internets und der hohen Verfügbarkeit von leistungsfähigen Mobilgeräten können Geschäfte immer einfacher von der physisch realen in die online Welt verlagert werden. Die gut ausgebildeten und technologieaffinen jüngeren Generationen, welche sehr gut vernetzt und ständig online sind, begünstigen diesen sozioökonomischen Wandel. In beiden Welten haben Geschäftspartner Sicherheitsbedürfnisse bezüglich der Identität und Authentizität des Gegenübers. Diese werden durch unterschiedliche Massnahmen des Identitätsmanagements abgedeckt, welche von anonymen Authentifizierungen, über die Akzeptanz von behaupteten bis hin zur Überprüfung von Identitäten mittels staatlich beglaubigter Identifizierungsmittel reichen können. Für letztere zeigt man in der physischen Welt seinen Identitätsausweis. Gestützt darauf erfolgt - meist unbewusst - eine biometrische Authentifizierung anhand des Fotos. Ist diese erfolgreich und der Ausweis gültig, vertraut man den auf dem Ausweis stehenden Identitätsattributen wie Name, Vorname oder Geburtsdatum. Ein einfacher und breit etablierter Prozess, den es in die online Welt abzubilden gilt.

2.1 Anlass und Auftrag

Das Pendent zum Identitätsausweis ist in der elektronischen Welt das elektronische Identifizierungsmittel (eID). Auch eine eID soll in einem bestimmten Rechtsrahmen die Authentizität und Identität einer Person garantieren. Dazu soll die Möglichkeit geschaffen werden, ein staatlich anerkanntes elektronisches Identifizierungsmittel mit staatlich beglaubigten Identitätsattributen aufzuwerten. Ein solches Identifizierungsmittel wird in mehreren Strategien des Bundes thematisiert, sei es als direktes Ziel oder als Voraussetzung für die Erreichung weiterer Ziele („Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz“ vom März 2012 [10] und die „E-Government Strategie Schweiz“ vom Januar 2007 [2]).

Zuletzt hat der Bundesrat im Jahr 2012 das EJPD beauftragt [11], ein Konzept für eine staatlich anerkannte eID zu erarbeiten, welche sowohl im schweizerischen eID-Ökosystem als auch im EU-Raum eingesetzt werden kann. Um diesen Auftrag zu erfüllen hat das EJPD eine Projektgruppe eingesetzt, die bis Mitte 2015 das vorliegende Konzept für die nachfolgende Gesetzgebung und Umsetzung erarbeitet.

2.2 Internationales Umfeld (EU)

Auf europäischer Ebene wurde 2014 die Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung [1]) verabschiedet. Nebst der Regelung von Vertrauensdiensten (elektronische Signatur, Siegel, Zeitstempel, Einschreib-Zustelldienste und Webseiten-Zertifikate) enthält die Verordnung Vorschriften für elektronische Identifizierungssysteme, welche notifiziert und damit zwischen den Mitgliedstaaten anerkannt werden können. Die Mitgliedstaaten werden gleichzeitig verpflichtet, dort wo sie für den Zugang zu Behördendiensten eine nationale eID verlangen, auch die übrigen europäischen Identifizierungssysteme zu akzeptieren, sofern diese auf der erforderlichen Sicherheitsstufe notifiziert wurden.

Da die Schweiz nicht Mitglied der EU ist, ist die eIDAS-Verordnung für sie nicht verbindlich, und es besteht auch im Rahmen der bestehenden bilateralen Abkommen mit der EU keine Verpflichtung für die Schweiz zur Übernahme der EU-Verordnung. Die schweizerische Lösung soll jedoch die Bedingungen für die Notifizierung an die EU auch erfüllen (vgl. Kapitel 7 und Anhang 10.1), damit in Zukunft – gestützt auf ein entsprechendes mit der EU noch abzuschliessendes Abkommen (vgl. diesbezüglich Ausführungen unter Ziff. 7.2.2) – ein medienbruchfreier Einsatz von staatlich anerkannten schweizerischen eID über die Landesgrenzen hinweg möglich sein wird.

In mehreren europäischen Staaten, aber auch in einer beträchtlichen Zahl von Schwellenländern sind heute bereits staatliche eID, 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 eID eingeführt haben.

2.3 Nationales elektronisches Identitätsökosystem

Unter dem Begriff elektronisches Identitätsökosystem (eID-Ökosystem) wird die Gesamtheit aller betroffenen Beteiligten und das organisatorische, prozedurale, rechtliche und technische Umfeld verstanden, in der eine eID eingesetzt wird. In einem fortgeschrittenen eID-Ökosystem können folgende und weitere Fragestellungen online und in Echtzeit beantwortet werden [12] [13]:

- Ist die Person X diejenige, für die sie sich ausgibt und wie sicher ist dies?
- Ist die Person X diejenige, die als Kunde A registriert ist und wie sicher ist dies?
- Ist die Person X berechtigt ein vorgewiesenes Zahlungsmittel zu benutzen?
- Welche Nationalität hat die Person X, wie alt ist sie, ...?
- Wo ist die Person X niedergelassen, ist sie greifbar für eine Betreibung oder Klage?
- Hat die Person X eine Vertretungsbefugnis für die Firma F, wenn ja, welche?
- Ist die Person X tatsächlich Notar, Geometer, Grundbuchbeamter, ... und wie sicher ist dies?

Abbildung 3 zeigt das eID-Ökosystem, welches von allen Inhabern von eID, den Anbietern von elektronischen Identifizierungsmitteln (Identitätsdienstleister - IdP), den Anbietern von Vertrauensdiensten, die ihre Dienste auf eID aufbauen, den staatlichen Stellen als mögliche Garanten von eID und den vertrauenden Beteiligten (vBt) gebildet wird. Unter letztere fallen auch die Anbieter von Online-Diensten mit E-Government- und E-Business-Portalen.

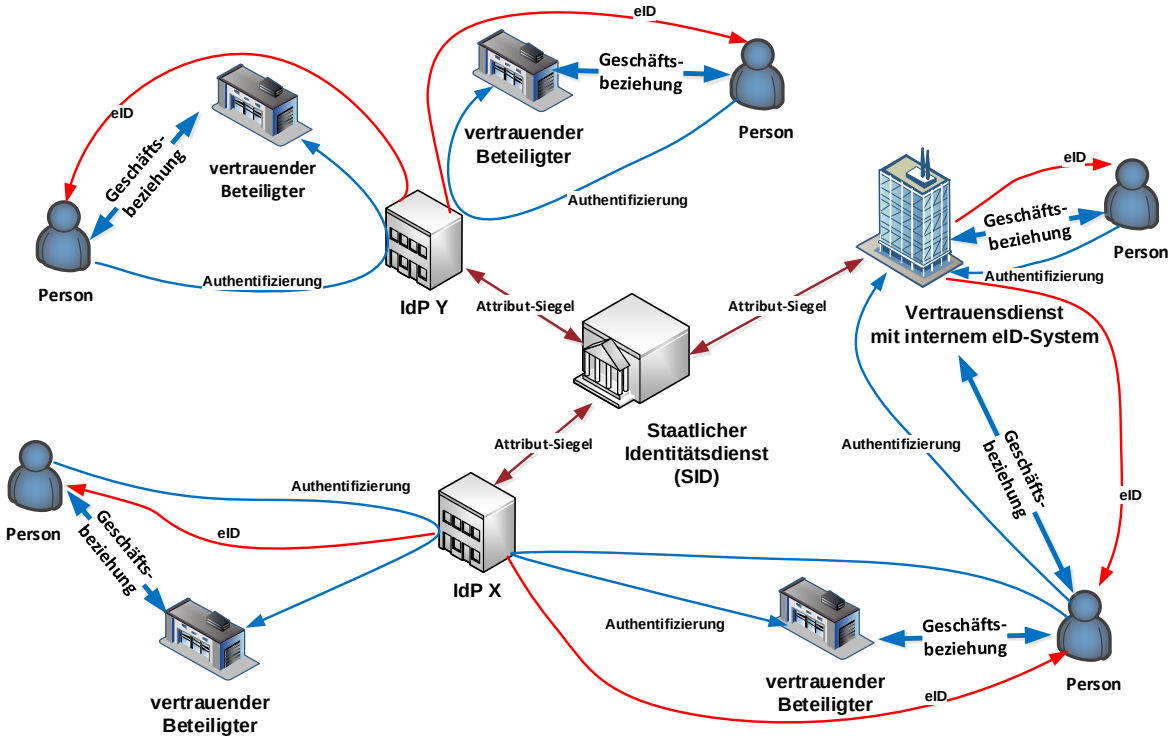

Abbildung 3 – Teilnehmer des eID-Ökosystems

Die Gesamtheit der Komponenten des eID-Ökosystems, welche die Nutzung eines elektronischen Identifizierungsmittels ermöglichen, wird als eID-System bezeichnet (IdP als Herausgeber von eID und involvierte staatliche Stellen). Staatlich anerkannt werden eID-Systeme, die den schweizerischen gesetzlichen Anforderungen genügen. Ein **staatlicher Identitätsdienst (SID)** stellt die dazu nötigen Dienste bereit und wirkt als Aufsichtsstelle. In einer fortgeschrittenen Entwicklung wird das eID-Ökosystem mehrere staatlich anerkannte eID-Systeme und eine Vielzahl von öffentlichen und privaten vertrauenden Beteiligten umfassen. Staatlich anerkannte eID-Systeme sollen für alle Beteiligten attraktiv und wirtschaftlich sein. Sie müssen sich jederzeit flexibel an technologische und gesellschaftliche Entwicklungen anpassen können.

Bereits heute agieren im schweizerischen eID-Ökosystem zahlreiche IdP, die eine eID anbieten, wie z.B. SuisseID, Mobile ID, Google ID, Apple ID, Open ID, Banken und so weiter. Es existieren auch verwaltungsinterne Lösungen mit einer persönlichen Smartcard, wie zum Beispiel diejenige für die Authentifizierung beim SSO-Portal des EJPD. Alle haben eine unterschiedliche Verbreitung, Benutzerfreundlichkeit, Funktionalität und Sicherheit. All dies sind Kandidaten, die ihre Dienste an die gesetzlichen Bestimmungen für staatlich anerkannte eID-Systeme anpassen und damit ihre eID zu einer staatlich anerkannten eID aufwerten können. Damit geniesst eine eID im Markt ein höheres Vertrauen und kann von den Nutzern breiter angewendet werden. Denn nach einer entsprechenden Lizenzierung erhalten die IdP als staatlich anerkannte IdP Zugang zum schweizerischen staatlichen Identitätsdienst für die Besiegelung von Identitätsattributen. So können die vertrauenden Beteiligten die Garantie haben, dass ihre Partner auf dem erwünschten Sicherheitsniveau identifiziert bzw. authentifiziert sind. Falls die Schweiz ein solches eID-System europäisch notifiziert, können die schweizerischen Nutzer ihre eID medienbruchfrei für Auslandgeschäfte einsetzen.

Beispielhaft für eine bestehende Lösung, welche für eine staatliche Anerkennung in Frage kommt, sei die SuisseID kurz erläutert. In den Jahren 2009-2010 hat der Bund im Rahmen des dritten Pakets der konjunkturellen Stabilisierungsmassnahmen unter Federführung des SECO und in Zusammenarbeit mit den vier anerkannten Anbietern von Zertifizierungsdiensten nach ZertES [6] die SuisseID [14] lanciert. Eine SuisseID besteht aus einem Set von standardisierten Geräten und Diensten, die spezifisch auf die sichere elektronische Identifizierung (starke Authentifizierung mit Verifikation von zwei Authentifizierungsfaktoren und Bestätigung von Identitätsattributen) ausgerichtet sind. Die SuisseID kann grundsätzlich in verschiedenste Geräte einzeln oder zusammen mit anderen Komponenten eingebaut werden, z.B. in einen USB-Stick oder eine Smartcard; denkbar wäre auch eine Integration in ein mobiles Gerät mit abgesichertem Bereich (Trusted Execution Environment –TEE [15]). Für die starke Authentifizierung stellt die SuisseID ein Schlüsselpaar, ein X.509-Zertifikat und eine Authentifizierungseinheit (Computer-Chip, Betriebssystem, Speicher) zur Verfügung und verifiziert die Nutzerpräsenz durch die Authentifizierungsfaktoren Besitz (Träger der Suisse ID) und Geheimnis (PIN). Zusätzliche Identitätsattribute befinden sich in einem zentralisierten Server, welcher die Ausweisdaten des SuisseID-Inhabers bereit hält und sie nach erfolgter starker Authentifizierung dem Inhaber zuhanden eines Dienstanbieters beweisbar abgibt. Die initiale Zuordnung der SuisseID zu einer berechtigten Person beruht auf der Überprüfung eines staatlichen Identitätsausweises.

2.4 Bisherige Erkenntnisse

In einem ersten Ansatz ist die Projektgruppe davon ausgegangen, dass sich eine schweizerische eID am Modell der bereits seit mehreren Jahren eingeführten eID im neuen deutschen Personalausweis (nPA) ausrichten kann. Es häuften sich aber 2014 die Indizien, dass die eID im nPA keine Akzeptanz findet, weil sie zwar bezüglich Sicherheit perfekt, aber in der täglichen Handhabung zu kompliziert und für den betreibenden Staat zu teuer ist [16]. Auch andere eID-Lösungen, die zusätzliche Infrastrukturkomponenten bei den Endnutzern verlangen, haben Akzeptanzprobleme; so wird zum Beispiel die belgische eID [17] meist nur für das Ausfüllen der Steuererklärung verwendet, weil

die Bürger dazu verpflichtet werden und die eID der österreichischen Bürgerkarte wird nur von einer ganz kleinen Minderheit verwendet [18] (im Gegensatz zu der ebenfalls angebotenen Lösung auf dem Smartphone). Auch die SuisseID hat sich in der Schweiz trotz grosser Erwartungen bisher nur als Nischenprodukt etablieren können. Als Schwächen bzw. Gründe für die eingeschränkte Verbreitung der SuisseID werden insbesondere die aufwendige und teure Beschaffung, die wenig komfortable Installation, die auf drei Jahre limitierte Gültigkeitsdauer der Zertifikate, sowie der Mangel an Anwendungen und internationaler Interoperabilität genannt [19]. Dagegen fallen z.B. bei der Mobile ID keine direkten Kosten für den Nutzer an – diese werden über einen Nutzungsvertrag den vertrauenden Beteiligten belastet.

Fast alle eID-Systeme in Europa, die unabhängig von konkreten Geschäftsfällen die Sicherheit gegenüber Benutzerfreundlichkeit priorisieren, haben Akzeptanzprobleme [20] [21].

Es hat sich in der Folge gezeigt, dass es sinnvoll ist, die beiden Prozesse „Authentifizierung“ und „Identifizierung“ explizit zu unterscheiden, da sie im eID-Ökosystem in unterschiedlichen Phasen und wie Abbildung 4 zeigt in sehr unterschiedlicher Häufigkeit gebraucht werden [22] [23] [24].

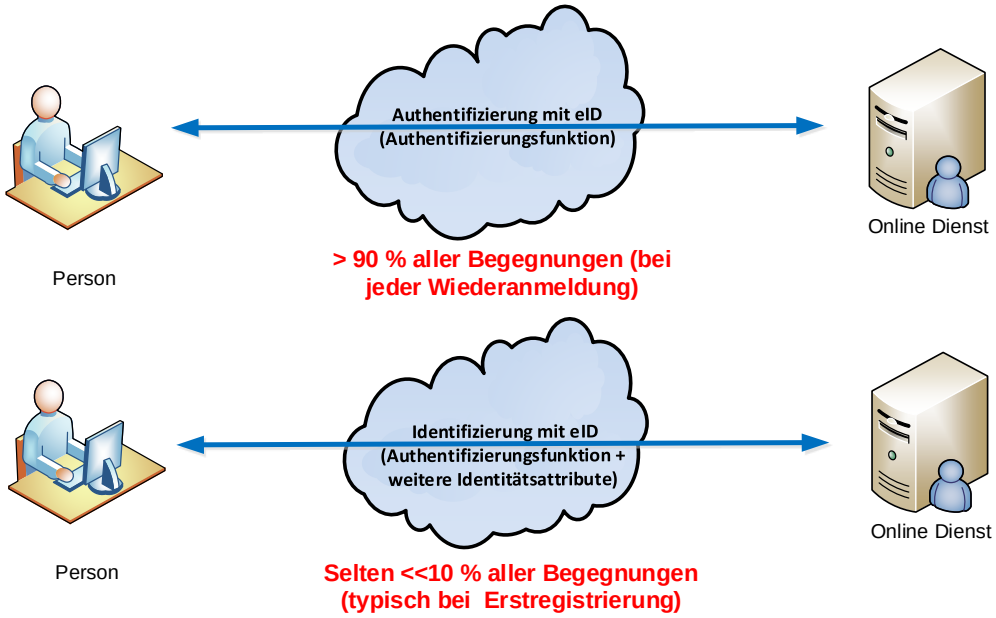

Abbildung 4 – Authentifizierung und Identifizierung

Die Authentifizierung ist ein Prozess bei dem eine Bestätigung für die Identifizierung einer Person eingeholt wird. Dies im Unterschied zu der Identifizierung mit staatlichen Identitätsattributen, bei der zusätzlich zur Authentifizierung eine Reihe von weiteren Identitätsattributen erfasst wird, welche eine Person eindeutig bestimmen. Eine Identifizierung mit Personenidentifizierungsdaten wird üblicherweise nur bei der erstmaligen Begegnung durchgeführt, wobei auch die digitale Form der Bestätigung (Identifikator) für zukünftige Authentifizierungen festgelegt wird (weitere Erläuterungen finden sich im Anhang 10.2).

Da für den elektronischen Nachweis von Identitätsattributen immer eine Authentifizierung vorausgesetzt wird, ist eine gesicherte, anwendungsfreundliche und interoperable Authentifizierung Voraussetzung für die Nutzung und Verbreitung einer eID. Genau in diese Richtung gehen die Arbeiten einer breit abgestützten Allianz von IT-Firmen, welche ein neues universelles Konzept für die starke online Authentifizierung in Form eines interoperablen Standards basierend auf persönlichen mobilen Geräten vorantreibt (FIDO-Allianz) [25].

Die entscheidenden Kriterien für eine brauchbare Authentifizierungslösung und damit eine brauchbare eID sind Benutzerfreundlichkeit, standardisierte Einsetzbarkeit und Sicherheit [26].

Die Einführung eines schweizerischen eID-Systems muss in Abstimmung mit der unsicheren Evolution des internationalen (vgl. Kapitel 2.2) und nationalen (vgl. Kapitel 2.3) eID-Ökosystems erfolgen. Nur wenn auch attraktive Online-Dienstleistungen zur Verfügung stehen, wird mit einem vertretbaren Marketing die wirtschaftlich notwendige Akzeptanz einer qualifizierten eID mit zusätzlichen Personenidentifizierungsdaten erreicht werden können. Viele heutige eID-Systeme realisieren die Authentifizierung lediglich durch die gesicherte Übermittlung des Identifikators der eID. Die vertrauenswürdige Zuordnung und starke Bindung einer eID an eine Person durch die Verifikation von mehreren Authentifizierungsfaktoren und die Feststellung von staatlich beglaubigten Identitätsattributen wird noch kaum gemacht. Dies ist eine Lücke, die durch staatlich anerkannte eID gefüllt werden kann. Die Risiken bezüglich Akzeptanz und Anwendungspalette müssen bei der Projektumsetzung jedoch berücksichtigt werden.

Die Einführung von staatlich anerkannten eID-Systemen wird zumindest zu Beginn in den Bereichen Investitionen, Regulierung und Architektur auch den Charakter eines Explorationsprojektes haben.

Einige Staaten kombinieren auf ihren nationalen Identitätskarten die eID- und die ePass-Funktion, da sich beide auf dem gleichen Chip unterbringen lassen. Die ePass-Funktion stammt aus dem Bereich der biometrischen Pässe und ist durch die International Civil Aviation Organisation (ICAO) weltweit genormt. Sie ermöglicht bei Grenzkontrollen eine automatisierte biometrische Verifikation des Ausweisinhabers. Sie bietet jedoch in ihrer standardisierten Form keine 2-Faktor-Authentifizierung, wodurch sie per se als staatlich anerkannte eID nicht geeignet ist. Gemäss aktuellem Ausweisgesetz [27] muss zudem in jedem Fall auch eine Identitätskarte ohne Chip angeboten werden. Allen diesen Lösungen gemeinsam ist, dass sie ein Lesegerät und eine Applikation (PC-Programm oder App) benötigen und damit einen erheblichen Supportaufwand verursachen, welcher für die Anwender und die Betreiber unbefriedigend ist.

Eine Kopplung von ePass- und eID-Funktion ergibt zwar gewisse Synergien bei der Hardware, schafft jedoch auch zusätzliche Abhängigkeiten im bereits vielschichtigen eID-Bereich.

Tatsache ist, dass im heutigen eID-Ökosystem bereits zahlreiche „E-Komponenten“ installiert oder geplant sind. Seien das Produkte von Identitätsdienstleistern (wie SuisseID, Mobile ID, IAM-Bund) oder auch Portale der Privatwirtschaft oder der öffentlichen Hand.

Mit Vorteil wirken staatlich anerkannte eID-Systeme nicht konkurrenzierend, sondern ergänzend und integrierend auf bereits bestehende Lösungen im eID-Ökosystem.

Wichtig für den Erfolg sind zudem die Interoperabilität und der Aufbau eines Föderierungsdienstes zwischen den verschiedenen eID-Lösungen (vgl. auch [28]). Nur so erreichen möglichst alle eID mit vertretbarem Aufwand möglichst alle vertrauenden Beteiligten. Genau dies ist das Ziel des Vorhabens Identitätsverbund Schweiz (IDV-Schweiz [29]) in der Verantwortung des SECO und genau deshalb ist es so wichtig, dass dieses Vorhaben parallel zur Lancierung der staatlich anerkannten eID-Systeme umgesetzt wird.

Für den Erfolg sind die Interoperabilität und gegenseitige Anerkennung der eID im nationalen und internationalen eID-Ökosystem sehr wichtig.

Last but not Least ist die Einführung einer staatlichen eID eine kommunikative Herausforderung. Ein gemeinsames Vokabular und Informationskonzept vereinfacht die Kommunikation auf allen Stufen und kann die Akzeptanz massgeblich beeinflussen.

Der Information und Kommunikation sind besondere Beachtung zu schenken, insbesondere auch im Bereich der Unterstützung der vollziehenden Behörden und Endkunden.

3 Grundsatzentscheid

Die Feststellungen und Erkenntnisse in Kapitel 2.4 führten zu folgendem Grundsatzentscheid: 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 elektronischen Identifizierungsmitteln nicht als Monopol durch den Staat erfolgen.

Folglich beschränkt sich **der staatliche Beitrag zu den eID-Systemen der IdP auf die notwendige staatliche Verankerung**, nämlich der Schaffung des notwendigen Rechtsrahmens für staatlich anerkannte elektronische Identifizierungssysteme und der Infrastruktur für die Ausstellung von Beglaubigungen für eID von Personen mit Schweizer Staatsbürgerschaft (Abbildung 5). Auf die Herausgabe einer eigenen eID durch den Staat soll jedoch verzichtet werden. Schweizerische staatlich anerkannte eID-Systeme müssen die Sicherheitsstufe „substanziell“ (2-Faktor-Authentifizierung) gemäss [1] erreichen.

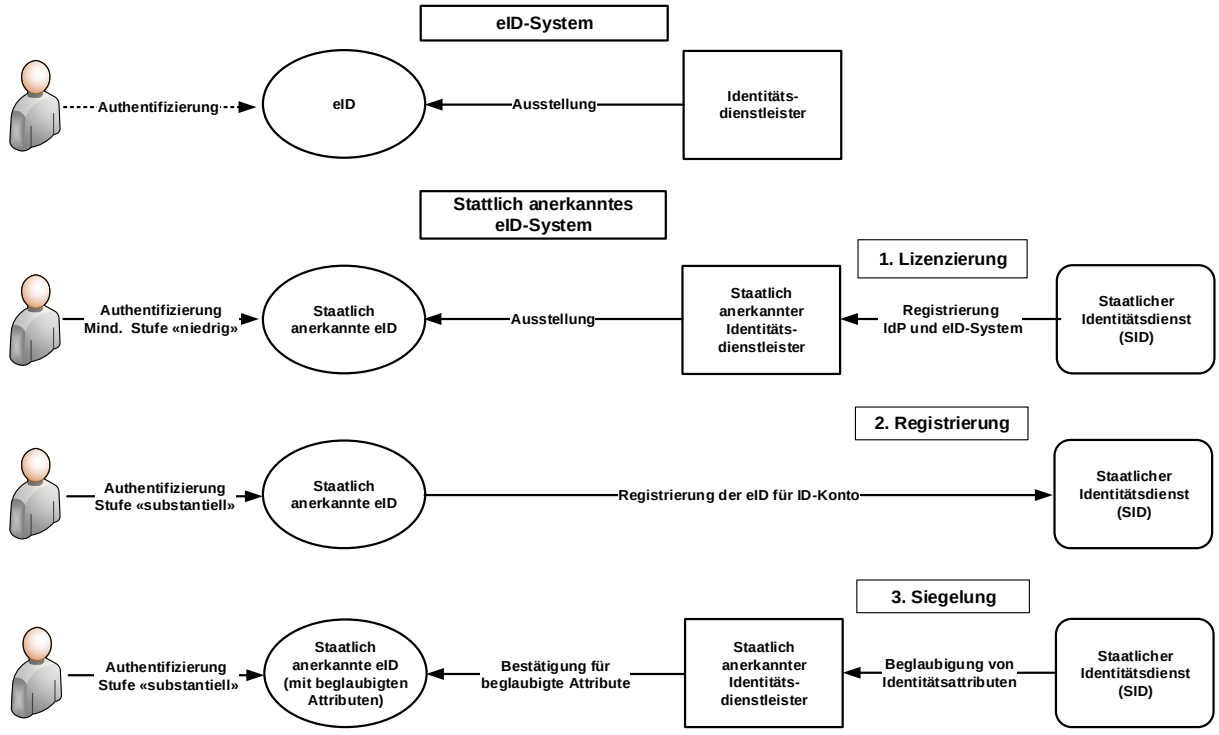

Abbildung 5 – Staatliche Beiträge: Lizenzierung, Registrierung und Siegelung

Grundsätzlich können auch alle ausländischen Staatsbürger eine staatlich anerkannte eID bei einem IdP beziehen und diese als Authentifizierungsmittel nutzen. Die staatliche Beglaubigung von Identitätsattributen ist aber nur für schweizerische Staatsbürger vorgesehen. Allerdings können In

der Schweiz wohnhafte Personen der EU unter Umständen von ihrem Heimatstaat eine notifizierte eID erhalten, wie dies von der EU vorgesehen ist (vgl. auch Kapitel 9.2).

4 Ziele

In die Formulierung von konkreten Zielen für das eID-System fliessen die in den Kapiteln Ausgangslage (vgl. Kapitel 2) und Grundsatzentscheid (vgl. Kapitel 3) gennannten Erkenntnisse und Vorentscheide mit ein. Gewisse Ziele muss das staatlich anerkannte eID-System als solches erfüllen, andere Ziele können nur vom eID-Ökosystem insgesamt erfüllt werden.

Staatlich anerkannte eID-Systeme sollen einen namhaften Beitrag leisten, um den Übergang der Schweiz zu einer fortgeschrittenen Informationsgesellschaft weiter voranzutreiben und ein System von Sicherheit und Vertrauen im elektronischen Geschäftsverkehr aufzubauen.

4.1 Strategie

Gelegentlich wird die Meinung vertreten, es sei sinnlos, ein eID-System einzuführen, ohne gleichzeitig für die entsprechenden Anwendungen zu sorgen. Trotzdem wird im Rahmen dieses Projektes nur die Voraussetzung für die Herausgabe von staatlich anerkannten eID geschaffen. Dies mit folgender Begründung:

- Ein eID-Ökosystem ist ein komplexes Gebilde mit zahlreichen Komponenten und Teilnehmern, welche zusammenspielen müssen. Es ist schlicht nicht möglich, alle diese Entitäten im Rahmen des gleichen Vorhabens zu entwickeln.
- Der Staat muss die Basis (z.B. den Rechtsrahmen) für die breite Anwendbarkeit von staatlich anerkannten eID in seinem Hoheitsgebiet schaffen und die Nutzung mit entsprechenden Kommunikationsmassnahmen und verwaltungsinternen Vorgaben fördern (z.B. mit einer Pflicht für Behörden zur Verwendung der staatlich anerkannten eID). Analoges muss von allen Akteuren im eID-Ökosystem auf allen Ebenen geleistet werden.
- Die weiteren für ein funktionierendes eID-Ökosystem notwendigen Komponenten, seien es weitere Vertrauensdienste, Identitätsdienstleister oder identitätsbasierte Anwendungen, sollen von den Akteuren im Markt bereitgestellt werden. Soweit es Aufgaben der öffentlichen Hand sind, beispielsweise der Zugriff auf gewisse Register oder E-Government-Anwendungen, sollen die entsprechenden Vorhaben separat durchgeführt und im Rahmen der vorstehend erwähnten E-Strategien koordiniert werden.
- Es ist nicht immer nötig, dass derselbe Akteur gleichzeitig die Infrastruktur und die Anwendungen dieser Infrastruktur zur Verfügung stellt. Zahlreiche Beispiele zeigen, dass die Bereitstellung der richtigen Infrastruktur-Elemente zum richtigen Zeitpunkt ganze Zweige von Anwendungen gleichsam explosionsartig entwickeln lassen kann. Strassen, Schienen und Stromnetze sind solche Beispiele, oder - aus neuerer Zeit - insbesondere das Internet bzw. TCP/IP und http oder die Kommunikationsinfrastruktur für mobile Geräte.

Um also die vom Bundesrat vorgegebenen Strategien erfolgreich umzusetzen, braucht es neben staatlich anerkannten eID-Systemen zusätzliche Komponenten und Leistungen aller Akteure des eID-Ökosystems.

4.2 Nutzen

Die direkten Nutzniesser von benutzerfreundlichen und vielfältig einsetzbaren staatlich anerkannten eID sind die Bevölkerung, die Privatwirtschaft und die Behörden (vgl. auch [30]). Dies soll im Folgenden durch die Schilderung von einigen möglichen zukünftigen Anwendungsfällen illustriert werden (vorbehältlich der Schaffung der notwendigen Rechtsgrundlagen und technischen Systeme). Für die detaillierten Abläufe sei auf Kapitel 10.4 im Anhang verwiesen.

4.2.1 Bevölkerung

Fall 1: Heidi de Maienfeld ist eine moderne und vielbeschäftigte Frau. Sie erledigt so viele Geschäfte wie möglich im Internet. So spart sie sich Zeit, welche ja immer knapp ist. Es stört sie, dass sie für einige Geschäfte immer noch vorbeigehen und ihren Identitätsausweis zeigen muss. Um sich bei Online-Diensten anzumelden, hat sie sich vor einiger Zeit von ihrem Identitätsdienstleister eine eID für ihr Smartphone gekauft. Die eID unterstützt neben einer PIN auch die praktische Fingerabdruckfunktion. Als sie kürzlich einen neuen Pass bestellen wollte, hat sie auf www.schweizerpass.ch gesehen, dass sie ihrer eID staatlich beglaubigte Identitätsattribute unterlegen kann und so bei zahlreichen Stellen eine persönliche Vorsprache unnötig wird. Sie entschliesst sich im günstigen Kombiangebot mit dem neuen Pass auch gleich das online ID-Konto zu bestellen, das dafür benötigt wird. Sie muss bei der Anmeldung auch eine persönliche Mobiltelefonnummer angeben, die bei der persönlichen Vorsprache auf dem Passbüro schliesslich noch verifiziert wird. Einige Tage später erhält sie noch ihren Benutzernamen und die PIN per Post. Sie meldet sich im ID-Konto mit Benutzernamen, PIN und einem Einmalpasswort an, welches sie per SMS auf die gemeldete Mobiltelefonnummer ihres Smartphones erhalten hat, und registriert ihre eID mit einer Authentifikation bei ihrem IdP. Im ID-Konto kann sie dann auswählen, welche Identitätsattribute sie beglaubigen lassen will. Sie entscheidet sich für Namen, Vornamen, Nationalität und Geburtsdatum. Ihre Auswahl bestätigt sie mit einem neuen Einmalpasswort, welches sie zusammen mit einer Auswahlquittung automatisch auf ihr Smartphone erhalten hat. Der staatliche Identitätsdienst beglaubigt nun im Hintergrund die gewählten Attribute ihrem Identitätsdienstleister, bei dem sie die eID bezogen hat. Heidi surft noch auf der Webseite ihres Wunsch-Telecom-Providers und bestellt sich mit ihrer eID eine SIM-Karte für ihr neu erworbenes Tablet. Da sie die benötigten Identitätsattribute mit der eID via ihren Identitätsdienstleister online nachweisen kann, klappt das gänzlich ohne Vorsprache (siehe auch Anhang 10.4.1). Heidi de Maienfeld ist zufrieden.

Fall 2: Peter de Maienfeld hat einen noch länger gültigen Pass und eine ebensolche IDK. Da jedoch seine Frau davon schwärmt, wie bequem Online-Geschäfte mit einer staatlich anerkannten eID seien, entschliesst er sich, das preislich attraktive Einführungsangebot eines der staatlich anerkannten Identitätsdienstleister zu nutzen. Er surft auf www.schweizerpass.ch, füllt den Antrag für das ID-Konto aus und bestellt sich gleich seine eID beim IdP, was sehr bequem geht, da die notwendigen Angaben zu seiner Person automatisch aus dem Internetantrag für das ID-Konto übernommen werden. Wie seine Frau erhält er einige Tage nach der persönlichen Vorsprache auf dem Passbüro seinen Benutzernamen und PIN. Auch die bestellte eID trifft bei ihm Zuhause ein und er kann die von ihm gewählten Identitätsattribute bei der ersten Anmeldung im ID-Konto beglaubigen. Da Peter de Maienfeld einen risikoreichen Beruf ausübt und viel unterwegs ist, eröffnet er für sich vorsorglich ein elektronisches Patientendossier. Peter de Maienfeld hat seinem IdP auch das Ausweisfoto übermittelt und beglaubigt. Das Foto nutzt er darauf um bei der SBB ein Halbtax-Abonnement und auf der Webseite der Bergbahn das Monats-Abonnement für den Skilift zu bestellen. Er freut sich, dass er zukünftig weniger Schlage stehen muss. So was könnte auch seine Tochter und seinen Sohn dazu bringen, eine eID zu nutzen, denkt er sich.

Fall 3: Tobias de Maienfeld, der Bruder von Peter de Maienfeld, muss eine neue IDK haben. Er kann den Schwärmereien für das Internet nichts abgewinnen. Er will nur eine neue IDK für den Gang auf die Post und seine Ferienreisen in Europa. Und das ohne für Schnickschnack zu zahlen,

den er nicht braucht. Als er bei der persönlichen Vorsprache auf der Gemeinde erfährt, dass er tatsächlich eine solche IDK ohne Mehrkosten kaufen kann, ist er zufrieden.

4.2.2 Privatwirtschaft

Fall 1: Eine Bank weiss, dass der Kampf um neue Kunden hart ist. Sie will deshalb innovative Lösungen für die Eröffnung von neuen Geschäftsbeziehungen anbieten. Dazu hat sie einen Internetantrag entwickelt, bei dem ein Neukunde alle notwendigen Angaben machen und staatlich beglaubigte Identitätsdaten mit Hilfe der eID direkt via seinen IdP online bestätigen kann. Besonders genial findet das Unternehmen, dass auch das Ausweisfoto und die Unterschrift staatlich beglaubigt online geliefert werden können. So sind wichtige Sicherheitsauflagen erfüllt, ohne dass der Kunde vorbeikommen oder zusätzliche Unterlagen auf dem Postweg einreichen muss. Das spart nicht nur dem Kunden Aufwand und Zeit.

Fall 2: Ein KMU betreibt einen Online-Shop mit Medizinalprodukten und gewährt Senioren einen deutlichen Preisnachlass. Dazu hat es mit seinen Lieferanten spezielle Vergünstigungen ausgehandelt und sich verpflichtet, das jeweilige Alter der Kunden verlässlich und nachweisbar zu prüfen. Das Unternehmen hat sich daher entschlossen, die Altersprüfung auf staatlich anerkannte eID abzustützen, welche einen garantierten Altersnachweis erlauben. Der Kunde kann sich beim Bezahlvorgang direkt aus dem Online-Shop bei seinem IdP anmelden und den Altersnachweis erbringen lassen. Auf das Einscannen oder Einsenden von Ausweiskopien konnte so verzichtet werden. Gleichzeitig wird implizit eine sichere Authentifizierung im Web-Shop erreicht, ohne dass das KMU ein aufwändiges Identitäts- und Zugang-Managementsystem betreiben muss. Nach anfänglichen kommunikativen Herausforderungen funktioniert die Sache reibungslos und zur Zufriedenheit der Beteiligten.

Fall 3: Ein Telecom-Unternehmen bietet seinen Kunden eine attraktive Lösung zur Online-Authentifikation in Form einer eigenen eID an, welche zusammen mit Smartphones funktioniert. Es ist überzeugt, dass nur solche Authentifizierungslösungen die nachhaltige Kundenakzeptanz gewinnen können, welche praktisch sind und täglich gebraucht werden können. Das Unternehmen hat bisher explizit darauf verzichtet, eine Garantie für die der eID hinterlegte Identität zu übernehmen. Mit Hilfe der staatlichen Beglaubigung von Identitätsattributen ist dies jedoch nun möglich und den Kunden kann eine vollwertige eID mit staatlich garantierten Identitätsdaten angeboten werden. Zuvor musste das Unternehmen beim Bund eine Lizenz einholen und den Nachweis erbringen, dass es die Anforderungen für ein staatlich anerkanntes eID-System erfüllt. Dafür kann die herausgegebene eID nun auch mit dem ID-Konto und zahlreichen weiteren E-Government-Angeboten verwendet werden, was den Marktanteil weiter erhöht.

Fall 4: Ein im Dienstleistungsbereich tätiges Unternehmen bietet heute seinen Kunden eine eigene Authentifikationslösung für das Login an. Es akzeptiert aber auch andere eID, wenn sie als sicher genug eingestuft werden. Wie beim Online-Bezahlen mit Kreditkarten führt das dazu, dass der Kunde beim Login „seine“ eID-Variante anwählen muss und das Unternehmen alle akzeptierten eID-Varianten in seine Lösung integrieren muss. Dies ist dank der für staatlich anerkannte eID-Systeme verlangten Standardisierung nur noch mit geringem Aufwand verbunden. Das Unternehmen prüft daher den Business-Case, ob es nicht als Identitäts- und Föderationsdienstleister am Markt auftreten und seine Lösung als staatlich anerkannte eID positionieren soll. In dieser Rolle würde es die Authentifizierung und die Bestätigung von Identitätsattributen für die Kunden von vertrauenden Unternehmen durchführen. Dies hätte den Vorteil, dass die vertrauenden Unternehmen nur noch ein einfaches Protokoll für die Zugangsverwaltung unterstützen müssen, was für sie eine grosse Vereinfachung darstellt und von der eID herausgebenden Unternehmung verrechnet werden könnte.

Fall 5: Ein heutiger eID-Anbieter will seine Geschäftstätigkeit in Zukunft vermehrt auf das Anbieten von Vertrauensdiensten fokussieren. Unter Vertrauensdiensten sind zum Beispiel qualifizierte elektronische Signaturen aber auch elektronische Zeitstempel und Verschlüsselungen zu verstehen.

Durch die staatlich anerkannten eID-Systeme wird der für seine Dienstleistungen besonders wichtige vertrauenswürdige Online-Zugang und die sichere Identifizierung sichergestellt. Dadurch kann er seine Kostenstruktur optimieren und seine Marktposition als Dienstleister weiter ausbauen.

4.2.3 Behörden

Fall 1: Eine Gemeinde ist fortschrittlich und bietet auf ihrem Online-Portal zahlreiche Dienstleistungen an. Aber sie seien aus Sicherheitsüberlegungen an Grenzen gestossen, meint der zuständige Kanzleichef. Doch die staatlich anerkannten eID und die damit einhergehende sichere Authentifizierung und Identifizierung werde es den Gemeinden erlauben, zahlreiche neue Online-Dienstleistungen anzubieten. Und gleichzeitig könne das Risiko eines Missbrauchs weiter gesenkt werden.

Fall 2: Die konsularischen Dienste des EDA können ihre Online-Dienstleistungen für die Auslandschweizer gestützt auf staatlich anerkannte eID ausbauen. Dadurch kann die Dienstleistungsqualität gesteigert und gleichzeitig Kosten gespart werden. Da mehr Geschäfte online abgewickelt werden können, sind auch weniger persönliche Vorsprachen notwendig, was wiederum teure Anreisen und die notwendigen personellen Ressourcen reduziert.

4.3 eID-System

Die Einführung von staatlich anerkannten eID-Systemen, deren Identitätsattribute beglaubigt werden können, dient der Erreichung folgender Ziele (Priorität 1 = zwingend, Priorität 2 = wünschenswert):

Tabelle 2 – Ziele staatlich anerkanntes eID-System

Nr.	Ziel	Priorität	Bemerkungen
Z11	Personen mit Schweizer Staatsbürgerschaft sollen elektronische Identifizierungsmittel mit Bestätigungen für staatlich beglaubigte Identitätsattribute für den Einsatz in der Online-Welt beziehen können. (Verfügbarkeit)	1	Der Staat sorgt für die staatliche Beglaubigung von Personenidentifizierungsdaten, gibt selber jedoch keine zusätzliche eID heraus. Die Bestätigungen werden von den IdP geliefert.
Z12	Das elektronische Identifizierungsmittel mit staatlich beglaubigten Personenidentifizierungsdaten muss der berechtigten Person ausschliesslich, eindeutig und sicher zugeordnet sein. (Sicherheit, Privatheit)	1	Der Staat sorgt dafür, dass nur eID mit einer Authentifizierung auf substanziellem Sicherheitsniveau durch staatliche Beglaubigungen aufgewertet werden.
Z13	Identitätsdienstleister (IdP), die staatlich anerkannte eID herausgeben, müssen vertrauenswürdig sein und über sichere operative Prozesse verfügen. (Vertrauenswürdigkeit)	1	Der Staat lizenziert Identitätsdienstleister als Herausgeber von staatlich anerkannten eID, wenn sie eine geeignete Sicherheitszertifizierung haben.
Z14	Die staatlich anerkannten eID der Schweiz können auf einfachste Weise und sicher für den elektronischen Geschäftsverkehr (E-Government, E-Business) verwendet werden. (Benutzerfreundlichkeit)	1	Die staatliche Beglaubigung von Attributen führt nicht zu einer Verschlechterung des einfachen Einsatzes einer eID.
Z15	Vertrauende Beteiligte im eID-Ökosystem sollen staatlich anerkannte eID-Systeme rasch und problemlos nutzen können. (Einsetzbarkeit)	2	Vertrauende Beteiligte können staatlich anerkannte eID in ihren IAM-Systemen in standardisierter Form einsetzen.

Nr.	Ziel	Priorität	Bemerkungen
Z16	Die folgenden im ID-Konto verfügbaren Personenidentifizierungsdaten können staatlich beglaubigt werden: a. amtlicher Name; b. Vornamen; c. Geburtsdatum; d. Geschlecht e. Geburtsort ; f. Heimatort; g. Nationalität; h. (leer)[9]; i. Gesichtsbild, aufgenommen bei der initialen Registrierung j. Unterschriftsbild, aufgenommen bei der initialen Registrierung k. Ausweisnummer des Passes; l. Ausweisnummer der IDK; m. Datum der initialen Registrierung; Die Attribute a) bis g) sind ausreichend für eine eindeutige Identifizierung und werden auch als Identitätsdaten bezeichnet.	1	Es ist denkbar, dass später weitere Attribute im ID-Konto erfasst werden können. Die Beglaubigung für die Attribute „Gesichtsbild“ und „Unterschriftsbild“ sind nur für die digital unveränderten Originalbilddateien möglich (keine Gesichts- oder Unterschrifterkennung). Die Bilder können deshalb von einem vBt nur als Referenz genutzt werden. Damit eine eID im internationalen Geschäftsverkehr als notifizierte eID genutzt werden kann, müssen alle Attribute a) bis g) beglaubigt sein.
Z17	Authentifizierungslösungen für staatlich anerkannte eID-Systeme sollen soweit als möglich nach internationalen Standards definiert werden und auf gleicher Sicherheitsstufe jeweils austauschbar und interoperabel sein. (Standardisierung)	2	Austauschbarkeit innerhalb von Standards garantiert die Weiterentwicklung der eID-Systeme der Schweiz. Insbesondere soll das Authentifizierungsprotokoll unabhängig von der Personenverifikationsmethode immer gleich funktionieren (z.B. nach FIDO Standardisierung [25]).
Z18	Ein schlanker und für alle Beteiligten attraktiver Rechtsrahmen schafft die nötige Rechtssicherheit für staatlich anerkannte eID-Systeme. (Rechtssicherheit)	1	Der zu schaffende rechtliche Rahmen soll keine überhöhten Eintrittshürden aufweisen, aber dennoch die nötige rechtliche Sicherheit schaffen. Zudem soll er kompatibel mit der eIDAS-Verordnung der EU sein.

[9] Vgl. Fussnote 3 auf Seite 8.

4.4 eID-Ökosystem

Folgende Ziele sollen durch das eID-Ökosystem nach Einführung von eID-Systemen erreicht werden:

Tabelle 3 – Ziele eID-Ökosystem

Nr.	Ziel	Priorität	Bemerkungen
Z21	Staatlich anerkannte eID und staatlich bestätigte Personenidentifizierungsdaten werden von allen schweizerischen Behörden akzeptiert und sind europäisch notifizierbar. (Akzeptanz, Notifizierbarkeit)	1	Vorausgesetzt ist eine hinreichend vertrauenswürdige Authentifizierung, die mit dem Gebrauch der eID einhergeht (Sicherheitsstufe „substanziell“).
Z22	Das eID-Ökosystem stellt weitere Vertrauensdienste, z.B. die qualifizierte elektronische Signatur sowie erweiterte Attributsdienste (z.B. zum Nachweis von Berufen) oder spezielle Anwendungen wie z.B. eHealth mit dem elektronischen Patientendossier oder Vote électronique, bereit, die eID nutzen. (Verbreitung)	2	Der Staat arbeitet mit privaten und öffentlichen Diensten zusammen um die Erreichung dieses Ziels zu ermöglichen.
Z23	Der staatliche Beitrag bietet für in der Schweiz bestehende eID-Lösungen (z.B. die SuisseID) einen Aufwärtspfad hin zur staatlich anerkannten eID bzw. für deren Anbieter zum lizenzierten Identitätsdienstleister. (Subsidiarität)	2	Heutige eID-Herausgeber sind potenzielle Nutzer eines staatlichen Identitätsdienstes. Die Behörden sind Nutzer von staatlich anerkannten eID-Systemen.
Z24	Die Bevölkerung wird über die Einsatzmöglichkeiten von staatlich anerkannten eID auf breiter Ebene informiert und zum Gebrauch ermuntert. (Marketing)	1	Staat und Herausgeber sorgen für die Information über Anwendungen und die Sicherheit der eID-Systeme.

5 Anforderungen

5.1 eID-Systeme – staatlicher Beitrag

Die Anforderungen an den staatlichen Beitrag (**Staatlicher Identitätsdienst – SID**) für die Bereitstellung von staatlich anerkannten eID mit beglaubigten Personenidentifizierungsdaten sind:

Tabelle 4 – Anforderungen eID-System Staat

Nr.	Funktionale Bedürfnisse und Anforderungen	Priorität	Bemerkungen
A11	Die Personenidentifizierungsdaten eines eID-Antragstellers werden im gleichen Identifikationsprozess festgestellt, wie er auf den heutigen Passstellen etabliert ist.	1	Der initiale Identifikationsprozess auf den Registrierungsstellen wird nicht oder nur marginal beeinflusst.
A12	Die festgestellten Identitätsattribute werden von einem zentralisierten staatlichen Vertrauensdienst (Staatlicher Identitätsdienst – SID) in einem Identitätskonto (ID-Konto) verwaltet, zu dem ausser dem staatlichen Dienst ausschliesslich die für das Konto registrierte Person online Zugang hat.	1	Jede identifizierte Person hat ein persönliches Identitätskonto (ID-Konto). Für den Zugang wird nebst dem initialen Authentifizierungsmittel (PIN, OTP) eine staatlich anerkannte eID als Authentifizierungsmittel registriert.

Nr.	Funktionale Bedürfnisse und Anforderungen	Priorität	Bemerkungen
A13	Für den Zugang zu seinem ID-Konto muss sich der Nutzer auf dem Sicherheitsniveau „substanziell“ authentifizieren; das Konto wird im Rahmen des initialen Identifikationsprozesses an eine staatlich anerkannte eID gebunden; weitere staatlich anerkannte eID auf gleichem oder höherem Sicherheitsniveau können vom Nutzer später zusätzlich registriert werden.	1	Der Staat anerkennt eID, die eine Authentifikation auf dem Sicherheitsniveau „substanziell“ oder „hoch“ erlauben; dies bedingt zwingend die Verifikation von zwei Authentifizierungsfaktoren
A14	Beglaubigungen für Identitätsattribute werden nur an staatlich anerkannte IdP geliefert, deren Infrastruktur und Organisation zeitgemässe Sicherheitsanforderungen erfüllen und die entsprechend zertifiziert sind.	1	Um eine Lizenz als staatlich anerkannter IdP zu erhalten, muss dieser den Nachweis für die Sicherheitszertifizierung erbringen.
A15	Die Gültigkeit einer staatlichen Attributbeglaubigung kann jederzeit vom IdP, der diese erhält, online beim SID nachgeprüft werden.	1	Validierungsdienste werden vom SID entsprechend verfügbar gemacht.
A16	Eine Attribut Beglaubigung wird vom Staat zum Zeitpunkt der Beglaubigung für den Zeitpunkt der initialen Identifizierung ausgestellt, sofern dem Staat keine in der Zwischenzeit erfolgte Änderung der Gültigkeit von zu beglaubigenden Attributen bekannt ist. Der Staat führt kein Logbuch über ausgestellte Beglaubigungen an staatlich anerkannte IdP; diese werden von jedem IdP in ihrem IAM-System für die eID verwaltet.	2	Bei jeder Verlängerung der Gültigkeit einer eID oder bei der Neuausstellung einer eID muss vom IdP eine neue Beglaubigung eingeholt werden.
A17	Die ID-Kontonummer identifiziert das ID-Konto; sie kann vom Nutzer über die Gültigkeit der erfassten Attribute hinaus beibehalten werden. Die eID muss aber nicht einen einzigen eindeutigen Identifikator haben. Eindeutig muss der Identifikator nur pro Verbindung mit einem vBt sein; dies kann zum Beispiel ein Schlüssel für den Verbindungsaufbau sein	2	Dies im Gegensatz zur Pass- oder IDK-Nummer. Die eID hingegen hat ein vom IdP definiertes Identifikatorsystem, das nicht vom Staat verwaltet wird. Jeder IdP führt ein IAM-System und kann auch als Föderationsdienst auftreten.
A18	Die Identitätsattribute werden pro Person und pro IdP beglaubigt; eine Beglaubigung wird nur mit explizitem Einverständnis des ID-Kontoinhabers erstellt.	2	Beglaubigungen sind für staatlich anerkannte IdP bestimmt und in keiner Weise übertragbar.
A19	Die Datenverwaltung der eID-Systeme und die erbrachten Leistungen müssen durch Gesetz und Verordnung abgestützt sein.	1	Es braucht eine formell gesetzliche Grundlage für die Bearbeitung und Aufbewahrung der Identitätsdaten sowohl beim SID wie bei den IdP.

5.2 eID-System –Beitrag der Dienstleister

Bereits bestehende und zukünftige Identitätsdienstleister (IdP) können die von ihnen herausgegebene eID mit staatlich beglaubigten Identitätsattributen aufwerten, sofern sie und die von ihnen herausgegebene eID die gesetzlichen Anforderungen für ein staatlich anerkanntes eID-System erfüllen. Damit dies möglich wird, muss sich ein IdP beim Bund registrieren und lizenzieren lassen. Eine solche Zulassung ist an bestimmte Anforderungen gebunden, deren Erfüllung vom IdP bei der Registrierung und jeder Lizenzerneuerung bestätigt werden muss.

Tabelle 5 – Anforderungen eID-System IdP

Nr.	Pflichten und Anforderungen	Prio-rität	Bemerkungen
A21	Für jede von einem IdP herausgegebene staatlich anerkannte eID muss festgelegt sein, wie sich der Nutzer authentifizieren muss.	1	Definition des minimalen Sicherheitsniveaus für die Authentifizierung und allfällig mögliche Verstärkungsschritte.
A22	Jede staatlich anerkannte eID muss mindestens auch eine Authentifizierung auf einem Sicherheitsniveau erlauben, welches für die Nutzung des ID-Kontos verlangt wird; die minimal verlangte Authentifizierungsstärke (Sicherheitsniveau der Authentifizierung) für die eID kann jedoch unter derjenigen liegen, welche für den ID-Konto Zugang verlangt wird.	1	Ein Nutzer soll im Prinzip alle identitätsbasierten Dienste mit dem gleichen standardisierten Authentifizierungsverfahren nutzen können. Situationsabhängig kann die eID aber unterschiedliche Authentifizierungsfaktoren verifizieren.
A23	Jede staatlich anerkannte eID muss immer dem Herausgeber (IdP) zugeordnet werden können; staatliche Attributbeglaubigungen sind mit der Lizenz des Herausgebers verknüpft; jede Attributbestätigung für eine Person mit eID wird vom IdP so geliefert, dass ein vertrauender Beteiligter feststellen kann, welche Attribute staatlich beglaubigt sind.	1	Die Lizenznummer des herausgebenden IdP ist Teil der Attributbeglaubigung; im Streitfall um vom IdP bestätigte Attribute einer eID muss der IdP belegen, dass er eine entsprechende Beglaubigung der Attribute besitzt.
A24	Ein IdP, der eID herausgibt, prüft ob die Prüfziffer des Attributwerts in der staatlichen Beglaubigung derjenigen des Attributwerts entspricht, der in seinem IAM-System für die eID erfasst ist; er bewahrt die erhaltenen staatlichen Beglaubigungen im seinem IAM Konto zur ausgestellten eID auf.	2	Der IdP ist verantwortlich dafür, dass von ihm ausgestellte Attributbestätigungen überprüft, richtig und der richtigen eID zugeordnet sind.
A25	Jedes staatlich anerkannte eID-System ist – vorbehältlich staatsvertraglicher Barrieren – gemäss EU-Verordnung im Prinzip notifizierbar; Im Einzelfall einer eID wird jedoch verlangt, dass der für eine Personenidentifizierung ausreichende Datensatz beglaubigt ist: Attribute von a) bis g) (Identitätsdaten nach Z16)	1	eID von lizenzierten Herausgebern mit dem ausreichenden Satz von beglaubigten Personenidentifizierungsdaten werden insbesondere auch von schweizerischen Behörden akzeptiert.
A26	In der Schweiz muss nach der Einführungsphase mindestens ein staatlich anerkannter IdP eine notifizierte eID anbieten.	2	Bei Bedarf kann der Staat einen geeigneten IdP-Dienst bereitstellen oder beauftragen.
A27	Ein staatlich anerkannter IdP sorgt dafür, dass ein vertrauender Beteiligter die Integrität der von ihm herausgegebenen staatlich anerkannten eID und der zugehörigen Attributsbestätigungen verifizieren kann.	2	Integration in eine anerkannte PKI-Infrastruktur mit Zertifikatskette; Bereitstellung einer öffentlich zugänglichen online Prüfinfrastruktur.
A28	Für jedes staatlich anerkannte eID-System muss eine klar definierte Supportorganisation bereitgestellt werden.	2	Hoher Standardisierungsgrad für eID-Systeme und zugehörige Supportleistungen sind erwünscht.

5.3 eID-Ökosystem

Über die zwingenden Anforderungen an staatlich anerkannte eID und IdP hinaus sollte das eID-Ökosystem die nachstehenden Bedürfnisse und Anforderungen im Sinne von Optimierungen erfüllen.

Tabelle 6 – Anforderungen eID-Ökosystem

Nr.	Bedürfnisse und Anforderungen	Priorität	Bemerkungen
A31	Staatlich anerkannte eID sollten für den Nutzer überall sicher und einfach einsetzbar sein.	1	Einsetzbarkeit und Benutzerfreundlichkeit sind von den Akteuren gemeinsam zu fördern.
A32	Vertrauende Beteiligte sollten die Identifizierung mittels staatlich anerkannten eID mit minimalem Aufwand in ihre IAM Systeme integrieren und nutzen können.	1	Standardisierung, Einsetzbarkeit und geringe Kosten sind Voraussetzung für die Verbreitung.
A33	Vertrauende Beteiligte und IdP sollen bevorzugt standardisierte, interoperable eID-Systeme für die Abdeckung der Authentifikationsbedürfnisse nutzen.	2	Einheitliche und einfache Protokolle führen zu Benutzerfreundlichkeit; z.B. mit eID, die eine Authentifikation gemäss FIDO-Spezifikation ermöglichen.
A34	IdP und vertrauende Beteiligte sollten die verlangten Sicherheitsniveaus für die Authentifizierung an internationalen Standards ausrichten und stufenweise Erhöhungen mit zusätzlich messbaren Authentifikationsfaktoren ermöglichen (step-up und Kontext basierte Authentifikation)	2	eID integriert in Trägergeräte neuester Bauart (z.B. Smartphones mit TEE) ermöglichen eine stufengerechte Authentifikation.
A35	Neue identitätsbasierte Dienste von vertrauenden Beteiligten sollen die vorhandene eID-Infrastruktur nutzen; dies soll zwingend für behördliche Dienste sein.	1	Behördliche Dienste akzeptieren staatlich anerkannte eID; z.B. Vote électronique, eHealth, E-Government, E-Partizipation
A36	Informations- und Supportmassnahmen aller Akteure erfolgen im Hinblick auf eine einheitliche Wahrnehmung und vermehrten Einsatz von staatlich anerkannten eID.	2	Die führenden Akteure des eID-Ökosystems arbeiten zusammen, um die staatlich anerkannten eID-Systeme zu propagieren.
A37	Alle staatlich anerkannten eID sollen im Prinzip von allen vBt, die eID akzeptieren, anerkannt sein. Die IdP verpflichten sich entsprechende Interoperabilitätsanforderungen zu erfüllen und Tarifsysteme zu entwickeln, die mit dieser Anforderung im Einklang sind.	2	Vertrauende Beteiligte sollen, wenn es nicht wirtschaftlich plausible Gründe dagegen gibt, alle staatlich anerkannten eID für ihre Authentifizierungsbedürfnisse akzeptieren.

5.4 Sicherheit und Datenschutz

Ein hohes Sicherheits- und Datenschutzniveau ist für den Einsatz von eID-Systemen und Vertrauensdiensten unerlässlich. Entwicklung und Einsatz solcher elektronischer Mittel müssen sich auf eine angemessene Verarbeitung personenbezogener Daten durch Dienstanbieter und Identitätsdienstleister stützen. Dies ist umso wichtiger, als eine derartige Verarbeitung die Grundlage unter anderem für eine möglichst zuverlässige Identifizierung und Authentifizierung natürlicher (oder juristischer) Personen sein soll.

Sicherheitsanforderungen kann der Staat für den Zugang zum ID-Konto und für die Lizenzierung von IdP für die Bezugsberechtigung von Attributbeglaubigungen festlegen. Die Sicherheitsmecha-

nismen im eID-Ökosystem werden dagegen meist auf internationaler Ebene einerseits durch Angebot und Nachfrage im Markt und andererseits durch Standards und Regulierungen bestimmt.

Die konkreten Sicherheitsrisiken und Schutzmechanismen für die persönlichen Daten werden im Kapitel 6.5 vertieft diskutiert.

Tabelle 7 – Anforderungen Datensicherheit und Datenschutz

Nr.	Bedürfnisse und Anforderungen aus Sicht Datensicherheit und Datenschutz	Priorität	Bemerkungen
A41	Die Nutzung und Einsicht ins ID-Konto und der Bezug von Attributbeglaubigungen werden so geschützt, dass sie ausreichend gegen Missbrauch, Hacking und Angriffe jeder bekannten Art abgesichert sind.	1	Das ID-Konto wird durch Authentifizierung auf substantiellem Vertrauensniveau und durch rollenbasierte Rechte geschützt.
A42	Es werden vom staatlichen Identitätsdienst (SID) nie Identitätsattributwerte im Klartext anderen Instanzen als der authentifizierten berechtigten Person gezeigt und beglaubigte Identitätsattributwerte im Klartext nur im ausdrücklichen Auftrag des ID-Kontoinhabers ausschliesslich an staatlich anerkannte IdP geliefert.	1	Schutz vor Identitätsdiebstahl, Schutz der Privatsphäre der berechtigten Person; nur die berechtigte Person kann ihre Identitätsdaten gegenüber einem IdP oder vertrauenden Beteiligten offenlegen.
A43	Jedes vom SID beglaubigte Attribut ist einzeln abgesichert und nur für einen IdP und sein eID-System lizenziert; eine Überprüfung der Beglaubigung ist nur mit bekannter Lizenznummer möglich.	1	Beglaubigungen können nicht transferiert werden; Bindung an vertrauenswürdige staatlich anerkannte IdP; offengelegte Beglaubigungen können nicht missbraucht werden.
A44	Beschaffung und Support der IT-Infrastruktur für die betroffenen staatlichen Dienste und Regierungsstellen geschehen über etablierte, sichere Wege.	2	Kritische Elemente können nur von schweizerisch kontrollierten Firmen geliefert werden.
A45	Die Authentifizierung mit staatlich anerkannten eID kann auch unabhängig von Identitätsattributen für anonyme und/oder pseudonyme Authentifizierung genutzt werden.	2	Die Authentifikation einer Person erfolgt über einen unter Umständen rein verbindungsabhängigen Identifikator (zum Beispiel einen von der eID erzeugten Schlüssel) und ist kaum oder gar nicht profilierbar.
A46	Staatlich anerkannte eID, die von verschiedenen IdP oder vertrauenden Beteiligten genutzt werden, stellen zu jedem der Dienste einen unabhängigen gesicherten Kanal her. Die Sicherheitsparameter können als verbindungsabhängige Identifikatoren genutzt werden. Ihre Authentizität muss aber überprüft werden können.	2	eID mit einer interoperablen Authentifizierungsanwendung ermöglichen die ad hoc Eröffnung eines sicheren privaten Kanals zu Authentifizierungsdiensten; die Echtheit solcher eID wird durch öffentlich überprüfbare Zertifikate garantiert, die bei der Kanaleröffnung mitgeliefert werden (der FIDO-UAF Standard beschreibt zum Beispiel einen solchen Mechanismus [25]).

6 Lösungskonzept

Die Lösung für eID mit staatlich beglaubigten Identitätsattributen muss unter Berücksichtigung der Ausgangslage in Kapitel 2, des Grundsatzentscheids in Kapitel 3, der in Kapitel 4 genannten Ziele und der in Kapitel 5 definierten Anforderungen konzipiert werden. Ganz wichtig erscheint uns, dass die Lösung skalierbar ist und die Innovationskraft des eID-Ökosystems nicht behindert. Nur so kann sie den technologischen und sozioökonomischen Entwicklungen auch in 10 Jahren noch Stand halten. Deshalb konzentriert sich der Staat bei der vorgeschlagenen Lösung auf die Kernfunktion der vertrauenswürdigen Beglaubigung der staatlichen garantierten Personenidentifizierungsdaten (Z16) und auf die Schaffung von geeigneten Rechtsgrundlagen für eID-Systeme (Z18, A19).

Dagegen erfolgt die Bereitstellung der staatlich anerkannten elektronischen Identifizierungsmittel, also der eID, durch die im eID-Ökosystem vorhandenen staatlich anerkannten IdP, welche privatwirtschaftlichen oder behördlichen Ursprung haben können. Um staatlich anerkannt zu werden, müssen sie sich als lizenzierte IdP beim Bund registrieren und mittels Zertifizierung den Nachweis erbringen, dass sie die rechtlichen und operativen Vorgaben einhalten (Z13, Z17, Z18).

6.1 Übersicht

Die durch den Staat beizusteuernden Lösungselemente sind in Abbildung 6 dargestellt und werden in den nachfolgenden Kapiteln erläutert.

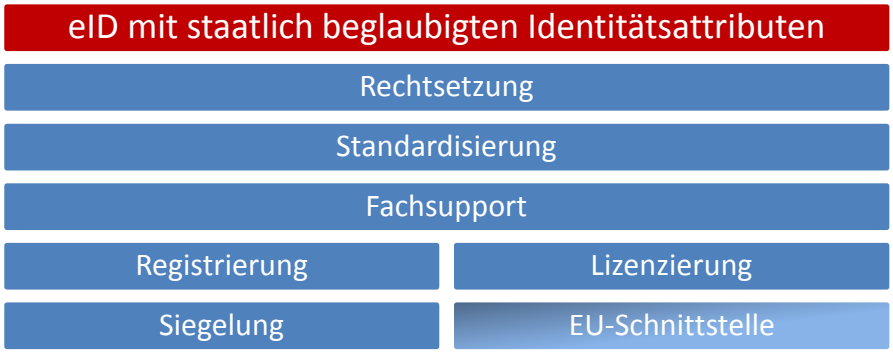

Abbildung 6 – Staatliche Beiträge zum eID-Ökosystem

Die Lösung sieht vor, dass

- der Bund den notwendigen Rechtsrahmen für staatlich anerkannte eID-Systeme schafft (Z18, A19) (vgl. Kapitel 6.4.1 und 7);
- der Bund definiert, welche technischen Standards und sonstigen Richtlinien für den Betrieb eines staatlich anerkannten eID-Systems einzuhalten sind (Z12 - Z15, Z17) (vgl. Kapitel 6.4.2);
- der Bund einen „Staatlichen Identitätsdienst (SID)“ betreibt (vgl. Kapitel 6.2), welcher alle für eine vertrauenswürdige Beglaubigung von Personenidentifizierungsdaten nötigen operativen und unterstützenden Dienste bereitstellt (Z11, Z16) (vgl. Kapitel 6.3); die nachstehende Abbildung 7 präsentiert den SID mit den einzelnen Diensten und zeigt die Interaktionsschnittstellen,
- die privaten und öffentlichen IdP ihre eID-Systeme, welche die gesetzlichen und reglementarischen Anforderungen erfüllen, beim Bund registrieren und staatlich anerkennen lassen können

und zum Betrieb eine Lizenz erhalten (Z11, Z13) („Lizenzierungsdienst“ des SID, vgl. Kapitel 6.2.3 und 6.3.8);

- für staatlich anerkannte eID-Systeme Anforderungen bezüglich Standardisierung, Interoperabilität, Sicherheit, Authentifizierungsstärke und Anwendbarkeit festgelegt werden (Z12 - Z15, Z17, A17, A21-A25, A31-A35, A41 - A44)
- der Bund einen öffentlichen Dienst zur Validierung der Lizenz bereitstellt, über den die vertrauenden Beteiligten die Gültigkeit der Lizenz eines staatlich anerkannten IdP überprüfen können (Z12, Z21, A27) (vgl. Kapitel 6.3.9);
- alle Schweizer auf den Registrierungsstellen (Passstellen) der Kantone und der Schweizerischen Auslandvertretungen neben den Schweizer Ausweisen auch ein staatliches online Konto (ID-Konto) mit den Personenidentifizierungsdaten (Z16, A11, A12) beantragen können (vgl. Kapitel 6.2.1 und 6.3.1);
- alle Schweizer die Möglichkeit haben, im Markt von einem lizenzierten IdP eine staatlich anerkannte eID mit geeigneter Authentifizierungsfunktion zu beziehen (Z11, Z23) (vgl. Kapitel 6.3.2);
- die Registrierungsstellen die Dienstleistung für die Personenidentifikation, die Eröffnung des ID-Kontos und die Registrierung einer staatlich anerkannten und auf die Person initialisierten eID für den Zugang zum Konto anbieten (Z11, Z12, A11, A13) („Registrierungsdienst“ des SID, vgl. Kapitel 6.2.1 und 6.3.3);
- alle ID-Kontoinhaber sich mit einem vom Staat verwalteten Authentifizierungsmittel (Z12) (2-Faktor Authentifizierung, vgl. Kapitel 6.2.1 und 6.3.1) bei der Erstanmeldung und bei Neuregistrierungen von eID im ID-Konto authentifizieren können;
- der Bund einen Beglaubigungsdienst für Personenidentifizierungsdaten („Siegeldienst“) (vgl. Kapitel 6.2.2 und 6.3.3) einrichtet (Z11, A11, A14), mit dem ID-Kontoinhaber staatliche Beglaubigungen für ausgewählte Attribute der Personenidentifizierungsdaten dem staatlich anerkannten IdP, welcher die eID ausgestellt hat (A18), in Form eines elektronischen Siegels zukommen lassen können;
- der Bund einen, den staatlich anerkannten IdP zugänglichen Validierungsdienst zur Überprüfung von staatlichen Beglaubigungen bereit stellt (A14 - A16, A43) („Siegeldienst“, vgl. Kapitel 6.2.2 und 6.3.3);
- der Bund den Gebrauch von eID fördert und in Zusammenarbeit mit Exponenten des eID-Ökosystems bei der Bevölkerung und vertrauenden Beteiligten propagiert (Z14, Z24, A35, A36)
- der Bund alle behördlichen Dienste auf Bundesebene verpflichtet, staatlich anerkannte eID im Online Verkehr als vollwertige Identifizierungsmittel zu akzeptieren und die entsprechende Anerkennung bei kantonalen und Gemeindebehörden zu fördern (Z21, Z22);
- der Bund vor einer Notifizierung im Rahmen eines separaten Vorhabens einen Dienst (Proxy Server / Identity Broker) für die länderübergreifenden Bestätigung von eIDAS-kompatiblen notifizierten eID-Systemen einrichtet (A25) [1] [5] (vgl. Kapitel 6.2.5); und
- der Bund eine eigene staatlich anerkannte und notifizierte eID herausgeben kann, sollte der freie Markt dies nicht in genügendem Mass tun (Z22, A26) (Rückfalllösung).

In den folgenden Kapiteln werden die einzelnen Lösungskomponenten im Detail beschrieben. Neben im Rahmen des vorliegenden Projekts staatlich zu realisierenden Komponenten (vgl. Kapitel 6.2.1 bis 6.2.4) müssen für eine funktionierende Gesamtlösung vom eID-Ökosystem selbst weitere wichtige Komponenten beigesteuert werden (A37, A45, A46) (vgl. Kapitel 6.4.5). Die Themen Authentifikation (vgl. Anhang 10.2), Datensicherheit und Datenschutz (vgl. Kapitel 6.5), sowie konkrete

Anwendungsbeispiele (vgl. Anhang 10.4) werden in eigenen Kapiteln oder in den Anhängen behandelt.

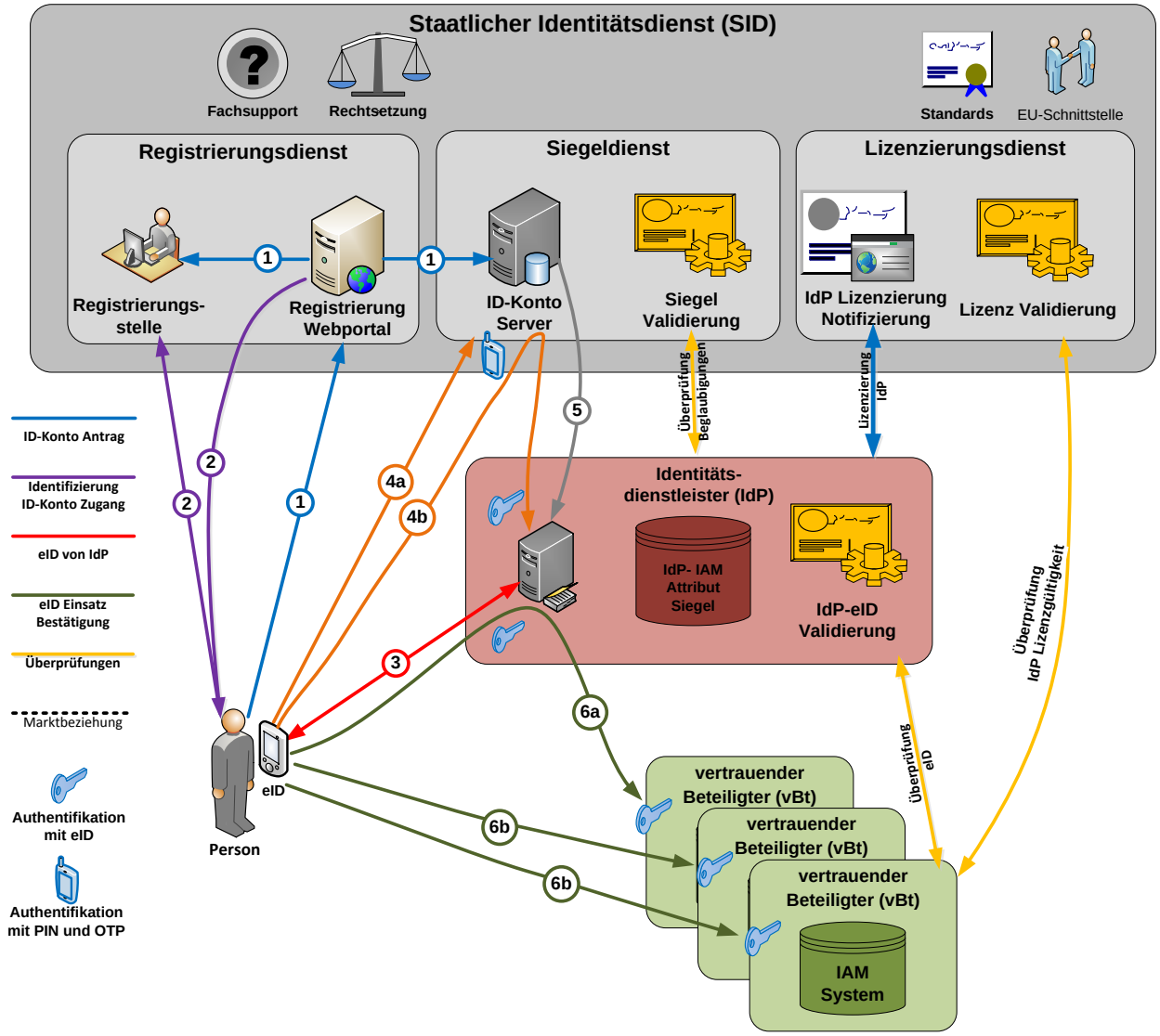

Abbildung 7 – Gesamtübersicht staatlich anerkanntes eID-System

Legende: Person bestellt, registriert, beglaubigt und nutzt eine staatlich anerkannte eID

1) Online Bestellung eines ID-Kontos (kann zusammen mit IDK/Pass oder separat bestellt werden), Personenidentifizierungsdaten werden erfasst und für ID-Konto vorbereitet, zusätzlich Erfassung der Telefonnummer eines persönlichen Geräts für die spätere Zusendung eines Einmalpassworts (One Time Password - OTP);

2) Identifizierung der Person und Erhebung der biometrischen Daten (Gesichtsbild, Unterschriftsbild), Überprüfung der persönlichen Telefonnummer für die Zusendung von Einmalpasswörtern (Faktor: Besitz des Geräts), anschliessend Zustellung der Zugangsdaten für die erstmalige Anmeldung beim ID-Konto bestehend aus einem Benutzernamen (Identifikator) und einer zusätzlichen PIN(Faktor: Geheimnis);

3) Person hat bereits eine staatlich anerkannte eID oder beschafft sich eine solche bei einem staatlich anerkannten IdP und initialisiert diese auf sich;

4) Person meldet sich beim ID Konto an (Identifikator und 2F-Authentifizierung aus 2: Benutzername und PIN + OTP) (4a) und registriert die eID für den zukünftigen Zugang zum ID-Konto. Bei der Registrierung der eID definiert die Person auch die Attribute, die beim eID herausgebenden IdP staatlich zu beglaubigen sind. Damit die Attributbeglaubigung vom IdP dem richtigen Account in seinem IAM zugeordnet werden kann, muss bei der Registrierung auch eine Anmeldung mit der eID beim IdP erfolgen (4b).

5) ID-Konto Server sendet die beglaubigten Personenidentifizierungsdaten über einen sicheren Kanal an den eID herausgebenden IdP, der diese überprüft und in seinem IAM dem eID Eintrag zur Person zuweist;

6) Person kann sich nun bei vertrauenden Beteiligten mit der eID registrieren und Attributbestätigungen mit beglaubigten Personenidentifizierungsdaten zukommen lassen (6a). Nach der Registrierung beim vertrauenden Beteiligten wird sich die Person mit der registrierten eID direkt (6b) oder via IdP föderiert (6a) authentifizieren.

Für den initialen Zugang zum ID-Konto hat die Person mit der PIN und dem OTP für das registrierte Telefon ein 2-Faktor Authentifizierungsmittel, das der Person vom Staat auf substanziellem Sicherheitsniveau (eIDAS Definition) zugeordnet ist. Dieses Authentifizierungsmittel wird jeweils nur dann gebraucht, wenn eine weitere eID für den Zugang zum ID-Konto registriert werden soll. Die Person bewahrt den Identifikator und die PIN an einem sicheren Ort auf und benutzt diese höchstens als Backup Authentifizierungsmittel, falls die registrierte eID nicht mehr funktioniert. Auch der Zugang zum ID-Konto wird voraussichtlich nur selten gebraucht, da eine Beglaubigung von Identitätsattributen im Normalfall nur einmal pro eID Lebensdauer nötig ist. Eine Erneuerung der Beglaubigung ist im Prinzip aber immer möglich und kann nötig werden, wenn ein vertrauender Beteiligter eine Attributbestätigung mit einer aktuellen Beglaubigung verlangt.

Für eine Authentifikation nach einer Erstregistrierung beim ID-Konto aber auch bei allen vertrauenden Beteiligten gibt es zwei Umsetzungsmöglichkeiten, wobei die Wahl der einen oder anderen Option vom spezifischen eID-System abhängt. Einerseits kann der IdP als zentralisierte Authentifizierungsinstanz für sein eID-System operieren und die Resultate von Authentifizierungen, die er durchführt, an die im vertrauenden Beteiligten und zum Beispiel auch an den ID-Konto Server senden (Föderationsmodus). Andererseits kann ein eID System so konzipiert sein, dass von der eID mit jedem vertrauenden Beteiligten ein neuer unabhängiger Kanal eröffnet wird, über den die Authentifizierung mittels der eID direkt ohne Einschaltung des IdP erfolgt (Direktmodus). Diese zweite Option wird zum Beispiel mit eID-Systemen ermöglicht, die eine Authentifikationsarchitektur nach dem FIDO Modell realisieren. Für den Zugang zum ID-Konto werden nach der Erstregistrierung, die zwingend immer mit dem in Punkt 1-4 beschriebenen Initialisierungsprotokoll abläuft, beide Authentifizierungsvarianten unterstützt (Z21). Heute sind in der Schweiz mit der Mobile ID und der SuisseID bereits beide Varianten von eID-Systemen vertreten. In der Industrie geht der Trend in Richtung direkter Authentifizierung [22], was auch anonyme und pseudonyme Authentifizierungen erlaubt (A45).

In Abbildung 8 ist der LifeCycle einer staatlich anerkannten eID mit beglaubigten Attributen und entsprechenden Bestätigungen an vertrauende Beteiligte schematisch aufgeführt. Die Skizze zeigt die Prozessschritte bis zum produktiven Einsatz. Für den vollständigen LifeCycle würden noch die Schritte Ablauf, Annullierung/Rückruf und Erneuerung der Beglaubigung folgen. Auf die evidente Darstellung wird in der Skizze zu Gunsten der Übersichtlichkeit verzichtet.

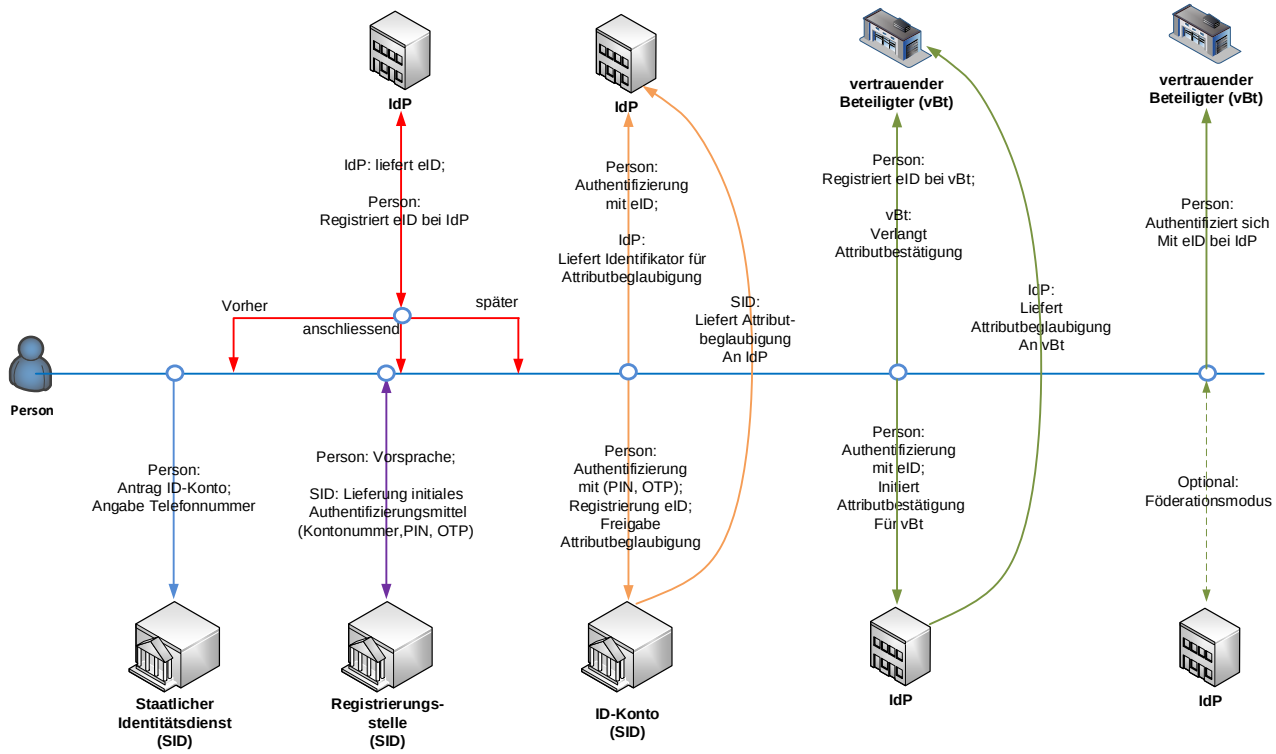

Abbildung 8 – eID Life Cycle

6.2 Architektur

Der staatliche Beitrag zum schweizerische eID System besteht aus einer Reihe von operativen und begleitenden Diensten, die im Staatlichen Identitätsdienst (SID) beim fedpol zusammengefasst sind und durch dieses geführt werden. Ein komplettes staatlich anerkanntes eID-System umfasst die folgenden Instanzen:

- Staatlicher Identitätsdienst mit den operativen Diensten
  - Registrierungsdienst mit den Registrierungsstellen in den Kantonen und schweizerischen Auslandvertretungen (Passstellen);
  - Siegeldienst für die Ausstellung und Validierung von Beglaubigungen;
  - Lizenzierungsdienst für die Akkreditierung und Lizenzierung von staatlich anerkannten eID-Systemen und IdP;

  und dem begleitenden Dienst
  - Fachsupport (Online 2nd und 3rd Level Supportorganisation) und Kommunikationsunterstützung);
- Identitätsdienstleister (IdP) mit folgenden Funktionalitäten
  - IAM-Infrastruktur für den sicheren Betrieb eines staatlich anerkannten eID-Systems;
  - Beschaffung, Herstellung oder Implementation von eID mit geschützter Verankerung in einer abgesicherten HW (Secure Element oder Integration in TEE von marktgängigen Geräten [15]); bevorzugt kompatibel mit interoperablen Authentifizierungsanwendungen (zum Beispiel „FIDO ready“ [25]);
  - Ausgabe und Initialisierung der eID an nutzende Personen;

- Authentifizierungsdienst für ausgegebene eID;
- Verwaltung der Lebenszyklen der ausgegebenen eID;
- Aufbewahrungs- und Pflegedienst für staatliche Attributbeglaubigungen;
- Ausgabe, Verwaltung und Validierung von Attributbestätigungen gegenüber vertrauenden Beteiligten und eID Inhabern;
- Support für betriebene eID-Systeme (Nutzersupport, technischer Support, Sicherheitsupdates, Anpassung an generelle IT-Entwicklungen).

- Vertrauensdienste und andere vertrauende Beteiligte mit
  - eigenem IAM System und Authentifizierungsserver, der eID registrieren und Attributbestätigungen beim IdP validieren kann oder
  - einer Föderationsanwendung, welche Identitätsdienstleistungen über den für die eID zuständigen IdP bezieht.
- Person (Nutzer) mit
  - einer eID und einem am Internet angeschlossenen Gerät, auf dem eine interoperable Authentifizierungsanwendung installiert ist und das eine Schnittstelle zum eID Trägermedium hat (typisch PC mit NFC- oder Smartcard-Schnittstelle) oder
  - einem persönlichen mobilen Gerät mit einem abgesicherten Kompartiment (TEE [15] oder Secure Element), in dem eine eID und eine interoperable Authentifizierungsanwendung installiert ist.
- Föderationsdienste des Identitätsverbundes Schweiz (IDV Schweiz, verantwortlich SECO)
  - Nationaler Föderationsdienst für staatlich anerkannte eID.
  - Internationaler Föderationsdienst für staatlich anerkannte eID. Pan-European-Proxy-Server (PEPS) nach dem STORK Modell für die transnationale Interoperabilität von notifizierten eID-Systemen.
- Kommunikations- und Informationsdienste für die Unterstützung der Einführung einer eID. Das Marketing von E-Government Leistungen liegt in der Verantwortung des Programms E-Government Schweiz.

Nur die erstgenannte Instanz „Staatlicher Identitätsdienst“ ist Bestandteil des hier vorliegenden Projektes. Alle anderen Instanzen sind Teil des eID-Ökosystems und werden von anderen privaten oder öffentlichen Institutionen und Personen bereitgestellt. Die organisatorische Struktur des staatlichen Teils des Systems (durchzogene Randlinien) mit den Schnittstellen zu den nichtstaatlichen Instanzen (unterbrochene Randlinien) ist in Abbildung 9 dargestellt.

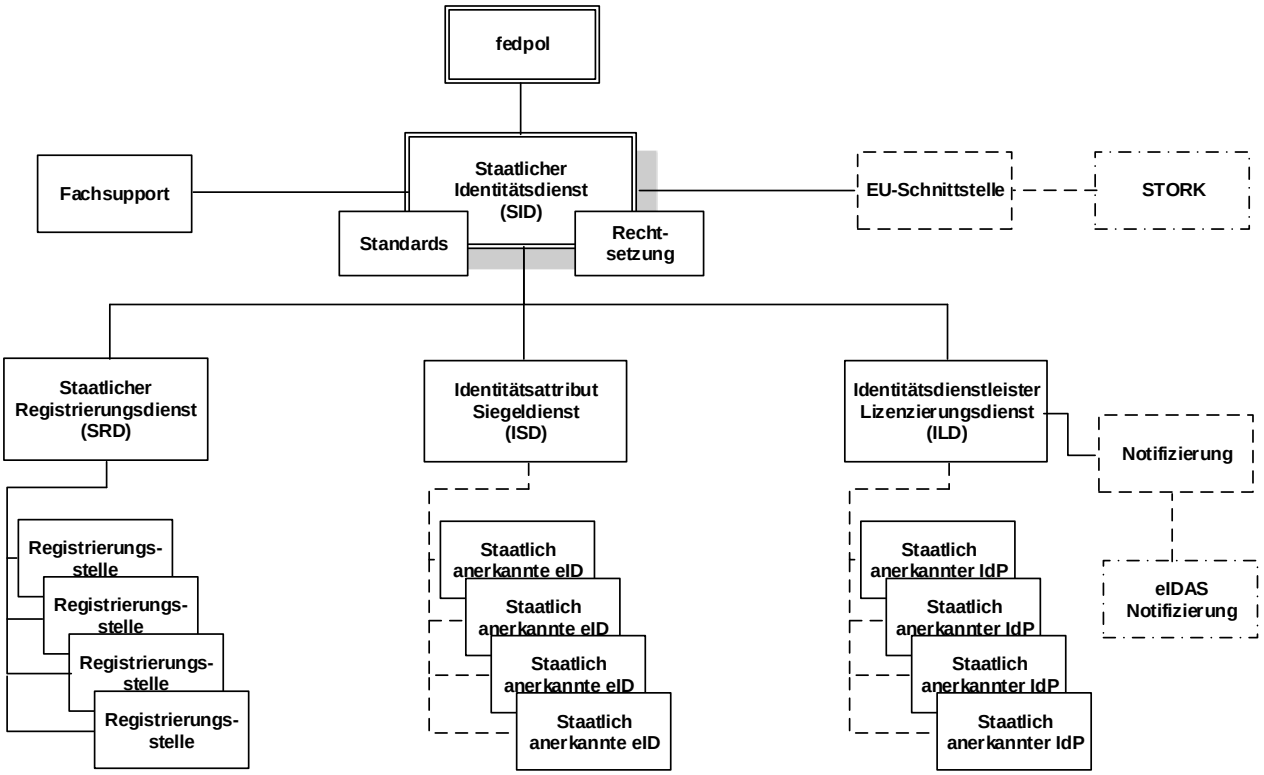

Abbildung 9 – Organisationsstruktur eines staatlich anerkannten eID-Systems

Die technische Infrastruktur des staatlichen Anteils für den Betrieb der eID-Systeme ist in Abbildung 10 schematisch dargestellt. Die meisten Komponenten sind im zentralen Dienst der SID konzentriert, der bei fedpol angesiedelt ist.

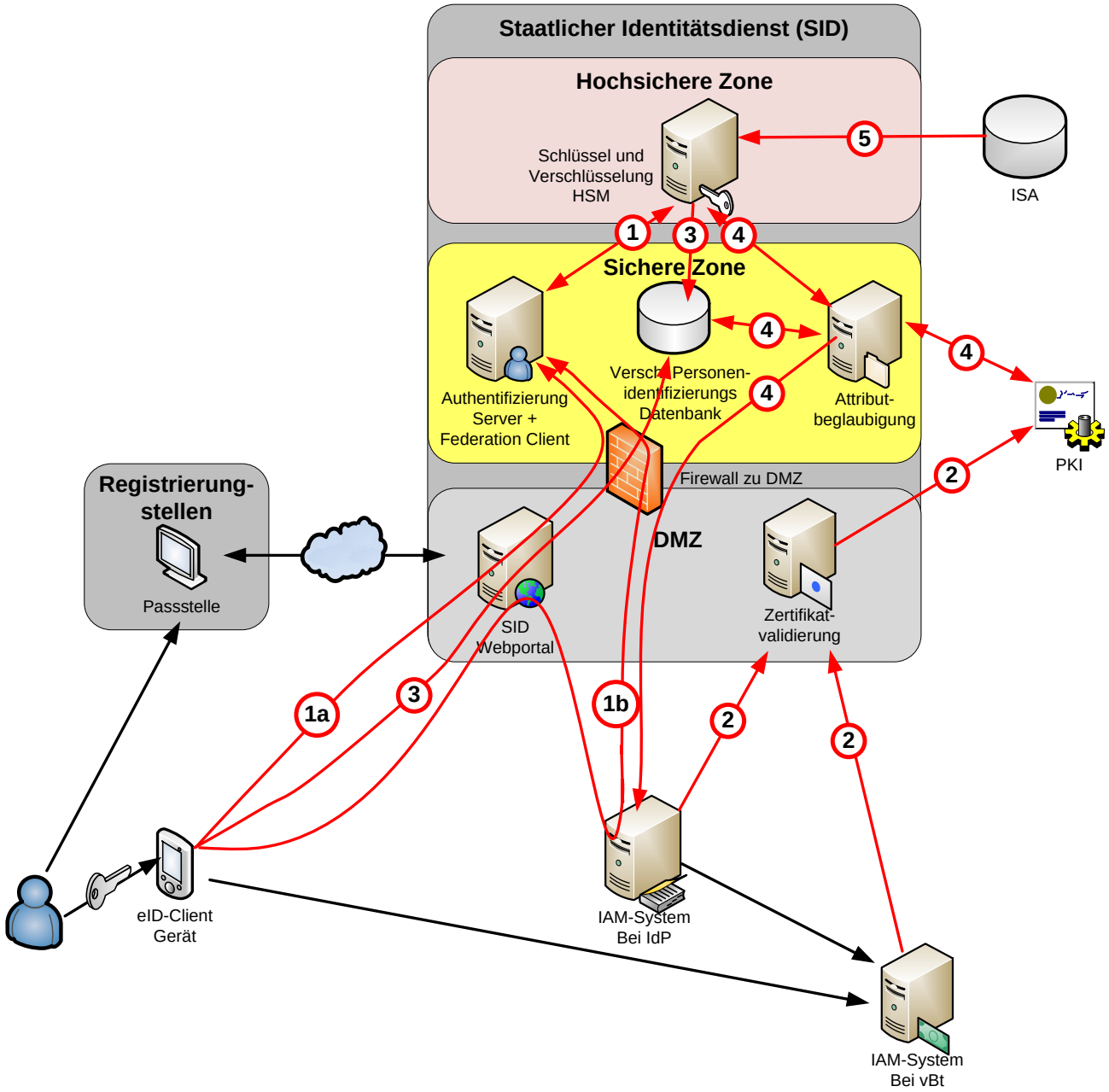

Abbildung 10 – Technische Infrastruktur und Schnittstellen des SID

Legende: Infrastruktur für SID (Aufgaben mit roten Pfeilen markiert)

1) Authentifizierungsserver für initialen Zugang mit PIN und OTP für jedes ID-Konto (1a), Client für Authentifizierungen durch IdP im Föderationsmodus (1b) und Authentifizierungsserver für eID mit verbindungsspezifischem Schlüssel im Direktmodus(1a);

2) Validierung von Attributbeglaubigungen und von IdP-Lizenzzertifikaten

3) Zugang für Inhaber des ID-Kontos zu seinen verschlüsselt abgespeicherten Personenidentifizierungsdaten (Entschlüsselung und Anzeige);

4) Zusenden von Attributbeglaubigungen an IdP;

5) Abfrage und Absicherung (Verschlüsselung) von Identitätsdaten aus der ISA-Datenbank, Ablage in verschlüsselter SID-Datenbank (Spiegelung);

Die Komponenten des SID Systems werden je nach Sicherheitsbedarf in unterschiedlich abgesicherte Zonen aufgeteilt, so dass die wichtigsten Sicherheitsprinzipien (minimale Angriffsoberfläche, Kompartementalisierung, gestaffelte Verteidigungslinien) stufen- und expositionsgerecht umgesetzt werden können. Das gesamte Sicherheitskonzept des SID wird geeignet zertifiziert.

6.2.1 Registrierungsdienst des SID

Der Registrierungsdienst besteht aus einem zentralen Teil und peripheren Elementen. Letztere sind integriert in die für die Schweizer Ausweise bestehenden Organisationsstrukturen und den für den Vollzug zuständigen Registrierungsstellen (Passstellen) bei den Kantonen und den schweizerischen Auslandvertretungen. Der zentrale Teil besteht aus einer Aufsichtsstelle beim Bund (fedpol). Die Aufgaben des Registrierungsdienstes sind:

- Bearbeitung der Anträge für ein ID-Konto;
- Feststellung der Identitätsdaten der Person;
- Erfassung der persönlichen Telefonnummer der Antragsteller;
- Eröffnung des ID-Kontos für berechtigte Personen;
- Physische Identifizierung der Person anlässlich der persönlichen Vorsprache;
- Erfassung der Attribute Gesichtsbild und Unterschriftsbild;
- Verifikation der Telefonverbindung über die registrierte Telefonnummer;
- Erfassung der Zustelladresse für die initialen Zugangsdaten zum ID-Konto (Benutzername und PIN; briefliche Zustellung der beiden Elemente an persönliche Adresse) oder Abgabe dieser Daten anlässlich der Vorsprache (die logistische Machbarkeit der zweiten Variante ist noch zu überprüfen);
- Inkasso der Gebühren;
- Freischaltung des ID-Kontos.

6.2.2 Siegeldienst des SID

Der Siegeldienst bietet die zentralen Dienstleistungen für die Attributbeglaubigungen und die IAM Infrastruktur für das Management der ID-Konten an. Die Aufgaben sind:

- HSM für das Schlüsselmanagement der verschlüsselten Einträge in der Datenbank mit den Personenidentifizierungsdaten mit automatisierten Schnittstellen zum Informationssystem Ausweisschriften ISA und evtl. Infostar in einer hochsicheren Netzwerkzone;
- Betrieb der verschlüsselten Datenbank mit den Personenidentifizierungsdaten in einer abgesicherten Netzwerkzone (sichere Zone) mit online Ver- und Entschlüsselung der Daten;
- Betrieb Webserver und Webportal für den Zugang zum ID-Konto in einer öffentlich zugänglichen Netzwerkzone (DMZ);
- Betrieb Authentifizierungsserver für den Zugriff auf das ID-Konto mit dem initialen Authentifizierungsmittel (PIN und OTP übermittelt an registriertes Telefon);
- Betrieb eID-Authentifizierungsserver für den Zugriff auf das ID-Konto mit staatlich anerkannten eID (Direktmodus);
- Betrieb Authentifizierungsclient für den Zugriff auf das ID-Konto mit starker Authentifizierung durch staatlich anerkannten IdP (Föderationsmodus);

- Empfang und Beantwortung der Aufträge für Attributbeglaubigungen von eID Inhabern;
- Betrieb der Public Key Infrastruktur (PKI) für Erstellung der Attributbeglaubigungen;
- Validierungsdienst für ausgestellte Attributbeglaubigungen.

6.2.3 Lizenzierungsdienst des SID

Der Lizenzierungsdienst evaluiert die Anträge für die Anerkennung als staatlich anerkannter IdP und verwaltet die Lizenzen für den Betrieb der staatlich anerkannten eID-Systeme. Seine Aufgaben sind:

- Empfang, Bearbeitung und Beantwortung von Lizenzierungsanträgen für den Status: „IdP mit staatlich anerkanntem eID-System“;
- Erstellung und Verwaltung der Lizenzen und der Lizenzzertifikate;
- Eröffnung und Freischaltung der sicheren Kanäle zwischen lizenzierten IdP und SID;
- Betrieb der Public Key Infrastruktur (PKI) für Erstellung der Lizenzzertifikate;
- Betrieb eines öffentlich zugänglichen Lizenzvalidierungsdienstes;
- Publikation der Namen der IdP mit staatlich anerkannten eID-Systemen in öffentlichem Online-register (Status der Lizenzen).

6.2.4 Fachsupport

Die operativen Dienste (Registrierungsdienst, Siegeldienst, Lizenzierungsdienst) werden im SID durch den Fachsupport mit folgenden Hilfestellungen unterstützt:

- Fachlicher und technischer Support (2nd und 3rd-Level) für den SID, für die Registrierungs-stellen (Beratung bei Problemen mit ID-Konto Eröffnung und Freischaltung, technische Hilfe), für die IdP (Beratung bei Problemen mit Attributbeglaubigungen und Zertifikatsvalidierun-gen),für die vertrauenden Beteiligten (Beratung bei Problemen mit Lizenzvalidierungen) und Support (1st-3rd-Level) für Personen mit ID-Konto (Hilfe bei Problemen mit initialem Zugang zu ID-Konto, Authentifizierung, Registrierung eID, Attributbeglaubigung);
- Schulung und Beratung von Mitarbeitern des SID und der Registrierungsstellen;
- Support und Kommunikationsunterstützung für die Implementierung von behördlichen Online Diensten, welche die eID als Zugangsausweis nutzen (alle Onlinedienste des Bundes sind verpflichtet staatlich anerkannte eID zu akzeptieren und entsprechende Authentifizierungs- oder Föderationsdienste zu betreiben bzw. zu nutzen, Kantons- und Gemeinde online Dienste werden ebenfalls unterstützt);
- Vorbereitung der EU-Notifikation von eID-Systemen auf Antrag der betreibenden IdP, welche ihr staatlich anerkanntes eID System bei der EU Kommission notifizieren und damit für alle vertrauenden Partner in ganz Europa via die STORK-PEPS Dienste nutzbar machen wollen. Ob diese vorbereitenden Arbeiten wie der Aufbau und Betrieb des PEPS eine Aufgabe des IDV-Schweiz resp. SECO sind, ist noch zu entscheiden.

6.2.5 EU-Schnittstelle (nicht Teil dieses Projektes)

Unter dem Begriff EU-Schnittstelle sind die Dienste und Instanzen zusammengefasst, die später dafür sorgen, dass die schweizerischen eID-Systeme via den vom STORK Projekt [5] ausgearbeite-ten Mechanismen Anschluss an das europäische interoperable Netz von eID-Systemen erhalten. Sie umfassen alle Aufgaben für

- den Aufbau und Betrieb des STORK-PEPS-Dienstes und
- die Organisatorische und technische Unterstützung für STORK Interoperabilitätsdienste.

Die EU-Schnittstelle kann zum jetzigen Zeitpunkt noch nicht klarer spezifiziert werden, ist aber auch nicht Teil des vorliegenden eID-Projekts. Sie wird später im Rahmen des Vorhabens IDV-Schweiz realisiert.

6.3 Prozesse

Das gesamte eID-System realisiert die notwendigen Prozesse und Abläufe um das Lebenszyklusmanagement der eID zu garantieren. Der Staatliche Identitätsdienst (SID) trägt mit einer Reihe von operativen (direkt das Lebenszyklusmanagement der eID betreffenden) und begleitenden (das Management der Vertrauensinfrastruktur betreffenden) Prozessen dazu bei.

Die operativen Prozesse, welche unter Beteiligung des SID, genauer des Registrierungsdienstes) und des Siegeldienstes, realisiert werden, sind:

- (O.1) Eröffnung eines ID-Kontos und Bezug des initialen Authentifizierungsmittels für den Zugang zum ID-Konto beim Registrierungsdienst,
- (O.3) Registrierung einer eID eines IdP und Beglaubigung von Identitätsattributen durch den Siegeldienst;
- (O.6) Einsicht in das ID-Konto, Registrierung weiterer eID und Auslösung von weiteren Beglaubigungen durch die berechtigte Person.

Die übrigen operativen Prozesse sind unter alleiniger Kontrolle der anderen Instanzen des eID-Systems. Es sind dies:

- (O.2) Bezug und Initialisierung einer staatlich anerkannten eID bei einem IdP durch eine Person;
- (O.4) Lieferung einer Attributbestätigung mit staatlich beglaubigten Identitätsattributen vom IdP an einen vertrauenden Beteiligten durch die für die eID berechtigte Person;
- (O.5) Revokation einer ausgestellten Attributbestätigung durch den IdP;
- (O.7) Revokation einer eID durch den ausstellenden IdP.

Die Nummerierung der Prozesse (O.x) entspricht der kausalen Folge im Lebenszyklusmanagement einer eID. Abbildung 11 zeigt den sequentiellen Ablauf der wichtigsten operativen Prozesse (O.1) bis (O.4)

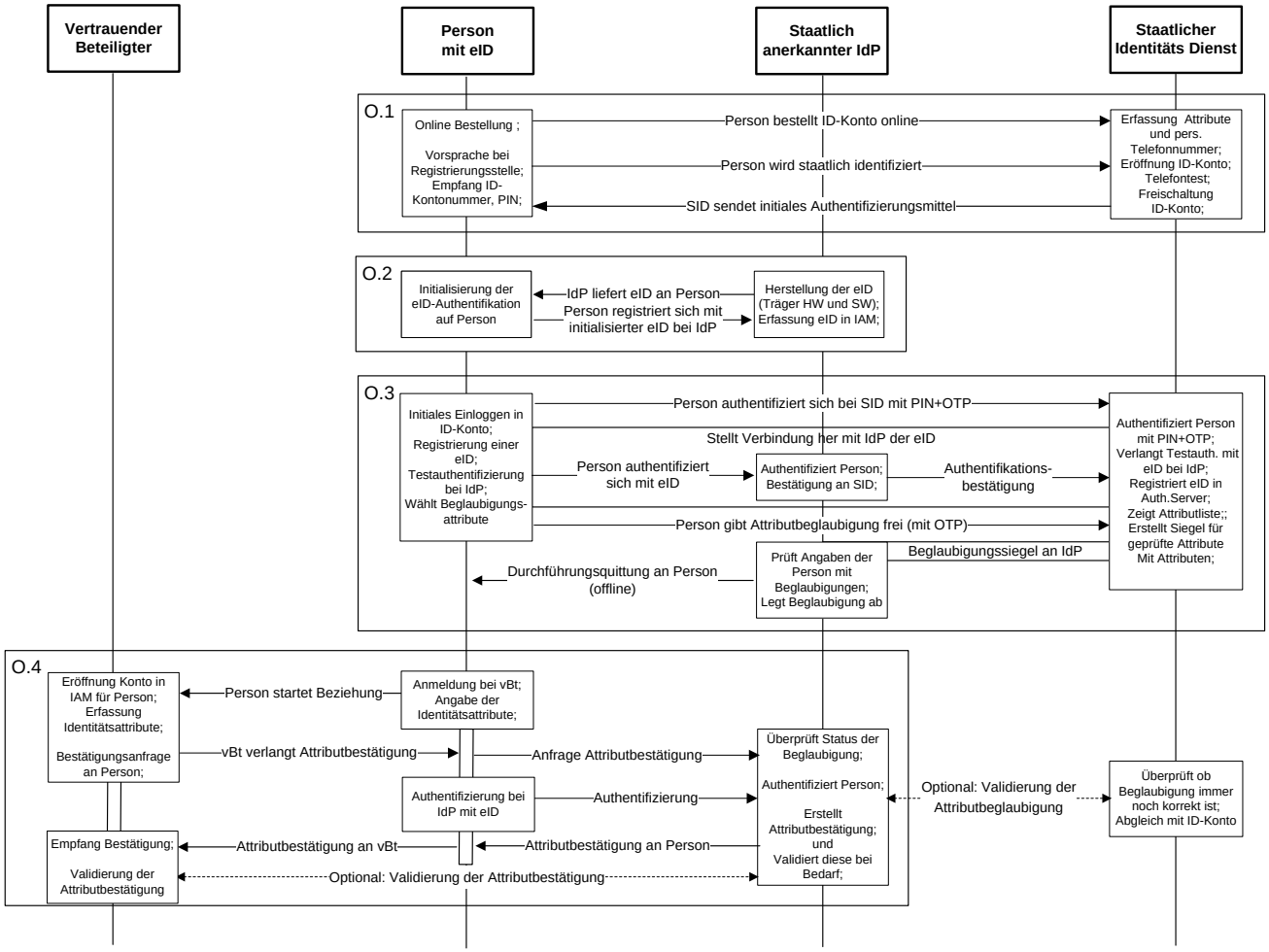

Abbildung 11 – Sequenzdiagramme der vier wichtigsten operativen Prozesse

Daneben unterstützt der SID durch seinen Lizenzierungsdienst auch die Durchführung von drei begleitenden Dienstprozessen, welche dem Aufbau einer Vertrauensinfrastruktur für das eID-System dienen. Es sind dies:

- (D.1) Anerkennung als staatlich anerkannter IdP und Ausgabe einer Lizenz an den IdP für den Betrieb eines staatlich anerkannten eID-Systems;
- (D.2) Validierung einer IdP Lizenz auf Anfrage eines vertrauenden Beteiligten;
- (D.3) Revokation einer Lizenz eines staatlich anerkannten IdP.

Es ist klar, dass in diesem Konzept nur die Prozesse und Abläufe beim SID verbindlich beschrieben werden können. Die Abläufe und Handlungen der vertrauenden Beteiligten, der Personen und der vom Staat bis auf gesetzliche Rahmenbedingungen unabhängigen IdP können hier nur im Sinne einer „best practice“ beschrieben werden. In den folgenden Detailbeschreibungen der einzelnen Abläufe sind die nicht vom SID kontrollierten Prozesse deshalb nur summarisch beschrieben.

6.3.1 (O.1) Eröffnung eines ID-Kontos

Voraussetzung für die Eröffnung eines ID-Kontos ist die staatliche Identifizierung der berechtigten Person anlässlich der persönlichen Vorsprache auf der staatlichen Registrierungsstelle. Im Rahmen der Identifizierung, welche identisch mit derjenigen für die Ausstellung einer IDK ist, werden die Personenidentifizierungsdaten festgestellt bzw. erfasst (Gesichts- und Unterschriftsbild). Das Ablaufprotokoll für die Eröffnung des ID-Kontos ist:

- Person bestellt das ID-Konto mit entsprechendem Anmeldeprozess (www.schweizerpass.ch), es wird dabei auch eine persönliche Mobiltelefonnummer angegeben;
- Das ID-Konto wird vom Registrierungsdienst vorbereitet und die Personenidentifizierungsdaten werden aus der ISA-Datenbank importiert;
- Die Person begibt sich zum vereinbarten Termin mit dem gemeldeten Mobiltelefon zur Registrierungsstelle, Person wird staatlich identifiziert, Gesichtsbild und Unterschriftsbild werden erfasst;
- Die Mobiltelefonnummer wird validiert (vor Ort senden und rückmelden eines OTP oder eventuell Anruf);
- Registrierungsdienst erfasst Zustelladresse für die Sendung des Benutzernamens und der PIN für den Zugang zum ID-Konto oder Benutzername und PIN werden direkt abgegeben;
- Person bezahlt Eröffnungsgebühr, ID-Konto wird eröffnet;
- Registrierungsdienst sendet Benutzername und PIN per Post an Zustelladresse der Person (falls nicht schon abgegeben).

Die Eröffnung des ID-Kontos ist damit abgeschlossen. Die Person kann sich mit dem initialen Authentifizierungsmittel (Benutzername, PIN, OTP auf Telefon) beim ID-Konto einloggen und die gespeicherten Personenidentifizierungsdaten einsehen.

6.3.2 (O.2) Bezug und Initialisierung einer staatlich anerkannten eID

Jeder IdP, der eine staatlich anerkannte eID herausgibt, beschafft die notwendigen Komponenten auf dem Markt und konfiguriert und betreibt diese so, dass sie innerhalb der gesetzlichen Vorgaben für die staatlich anerkannten eID seinen und den Bedürfnissen seiner Kunden möglichst gut entsprechen. Im Normalfall wird die eID und die allenfalls nötige zusätzliche Middleware folgende Eigenschaften und Varianten haben:

- Integriertes Messsystem oder abgesichertes Messprotokoll für die Verifikation der Authentifizierungsfaktoren, wie PIN oder Biometrie.
- Initialisierungsfunktion für die Erfassung der Referenzdaten für die Authentifizierungsfaktoren der Person, welche die eID in Besitz nehmen wird.
- Einen eindeutigen Identifikator für die eID mit den Varianten, dass
    - der Identifikator für jeden Dienst, welcher die eID nutzt, einzigartig und unabhängig von allen anderen Identifikatoren ist, unter denen die eID bei anderen Diensten bekannt ist (entspricht der FIDO Spezifikation, dort realisiert als Schlüssel für den Verbindungskanal) oder
    - der Identifikator für jeden Dienst der gleiche ist (wie zum Beispiel in der SuisseID in Form einer Seriennummer realisiert).
- Einen Bestätigungsmechanismus, meist in Form eines Zertifikates, der jedem vertrauenden Beteiligten, welcher die eID nutzt, bestätigt, dass der bei der Registrierung gelieferte Identifikator zu einer staatlich anerkannten eID mit bekannten Eigenschaften gehört.
- Abgesicherte Funktionen und Speicher für die sichere Durchführung von kryptographischen Protokollen und die allfällige Aufbewahrung von Attributen und Attributbestätigungen.
- Schnittstelle für die Durchführung von standardisierten Authentifizierungs- und Identifizierungsprotokollen mit Authentifizierungsanwendungen und Authentifizierungsservern, welche

solche standardisierte Protokolle abwickeln können (zum Beispiel ein Authentifizierungsprotokoll gemäss FIDO: siehe Anhang 10.3.2).

Ein wohl üblicher Ablauf für den Bezug und die Initialisierung einer eID für eine Person wird folglich wie folgt aussehen:

- Die Person bestellt (online oder offline) eine eID bei dem IdP, bezahlt die allfällige Gebühr und wird im IAM-System des IdP erfasst, entweder
  - mit Personenidentifizierungsdaten, geliefert durch die Person, oder
  - unter einem persönlichen Attribut (z.B. Emailadresse) oder
  - einem frei gewählten Pseudonym.
- Der IdP liefert die noch nicht initialisierte eID entweder als physisches Token oder als SW für ein abgesichertes Gerät (welches bereits im Besitz der Person ist) an die Person aus oder übergibt sie ihr anlässlich einer persönlichen Vorsprache.
- Die Person nimmt die eID in Besitz und personalisiert diese durch Festlegung der Authentifizierungsfaktoren (PIN, Biometrie), sie wird dadurch zur berechtigten Person für die eID.
- Die Person registriert die initialisierte eID noch beim IdP Authentifizierungsdienst (falls dies nicht schon vor der Auslieferung geschehen ist). Diese ist dann bereit für die Registrierung bei weiteren Diensten (vertrauende Beteiligte, SID etc.). Der Identifikator der eID zeigt im IAM System des IdP auf die erfassten Identitätsdaten der Person.

6.3.3 (O.3) Registrierung einer eID und Beglaubigung von Identitätsattributen

Im staatlichen ID-Konto kann die Person nun eine staatlich anerkannte eID eines IdP als weiteres Authentifizierungsmittel registrieren und ihre beim IdP angegebenen Personenidentifizierungsdaten online staatlich beglaubigen lassen. Dazu muss das folgende Protokoll durchlaufen werden:

- Die Person logt sich im ID-Konto mit dem Benutzernamen und dem initialen Authentifizierungsmittel ein und wählt die Option „Registrierung einer eID“; sie wählt dann aus einer Liste die eID des IdP, die sie sich im obigen Schritt beschafft hat;
- Der SID verbindet die Session mit dem zuständigen IdP mit einer Bestätigungsaufforderung an den IdP, die Person authentifiziert sich mit ihrer eID beim IdP auf dem Sicherheitsniveau „substanziell“, der IdP sendet die Bestätigung zusammen mit einem Identifikator für die erwartete Beglaubigungsmeldung zurück (Beglaubigungsidentifikator);
- Die eID wird im Authentifizierungsserver des SID als Authentifizierungsmittel für das ID-Konto registriert (Direktmodus oder Föderationsmodus);
- Anschliessend wird die Liste der beglaubigbaren Identitätsattribute angezeigt und die Person definiert die zu beglaubigenden Identitätsattribute; der Siegeldienst sendet ein OTP zusammen mit der Liste der gewählten Attribute auf das Telefon der Person, die mit der Rücksendung bestätigt, dass die gewählten Attribute für den IdP zu bestätigen sind (OTP-Verfahren);.
- Der Siegeldienst erstellt für jedes zu beglaubigende Attribut ein Beglaubigungssiegel. Ein Beglaubigungssiegel hat die folgenden Inhalte

  ```
  (Attributname; Attributwert; Lizenznummer IdP; Beglaubigungsdatum;
  Registrierungsdatum; Prüfziffer[Attributname; Attributwert, Lizenz-
  nummer IdP; Beglaubigungsdatum; Registrierungsdatum], Signatur über
  Prüfziffer, Zertifikat Siegeldienst)
  ```

- Die Liste mit allen Beglaubigungssiegeln wird dem IdP zusammen mit dem Beglaubigungsidentifikator über einen abgesicherten Kanal zugeschickt.
- Der IdP vergleicht die ihm von der Person mitgeteilten Attributwerte mit den Beglaubigungsdaten, überprüft die Prüfziffern in der Attributbeglaubigung und erfasst bei Übereinstimmung in seinem IAM System die beglaubigten Attribute der Person;
- Der IdP bewahrt die Beglaubigung in seinem IAM-System in Hinblick auf ein Audit oder eine notwendige Rückverfolgung auf;

Der beschriebene Ablauf kann allenfalls noch vereinfacht und verbessert werden. Es muss aber sichergestellt sein, dass nie eine Attributbeglaubigung für eine falsche eID ausgestellt wird. Die Verbindung Attributbeglaubigung zu eID ist durch die initiale Registrierung der eID beim ID-Konto durch die staatlich identifizierte Person gewährleistet.

6.3.4 (O.4) Ausstellung einer Attributbestätigung für einen vBt

Die Form und die zu erfüllenden Bedingungen für die Ausstellung einer Attributbestätigung mit als beglaubigt ausgewiesenen Identitätsattributen ist im Prinzip Sache des IdP, der die Beglaubigungen verwaltet. Eine gewisse Standardisierung, zum Beispiel des Namensraumes und der Vertrauensstufen der Attribute (Level Of Assurance), kommt jedoch der Interoperabilität und Sicherheit bei der Interpretation der Attribute zugute. Grundsätzlich kann der IdP eine solche Attributbestätigung online für jeden vertrauenden Beteiligten unmittelbar dann bereitstellen, wenn sich die Person beim vertrauenden Beteiligten registriert und den IdP zu einer solchen Bestätigung auffordert.

Eine andere Möglichkeit wäre die Attributbestätigung in Form eines SW-Sicherheitstokens, das an die eID gebunden ist, unmittelbar nach der Beglaubigung an die Person zu liefern. Die Person könnte das Token dann bei allen vertrauenden Beteiligten mit einer Authentifikation mittels eID ohne weitere Intervention des IdP vorweisen. Damit aber die Verbindung zwischen der Person (resp. eID) und dem Token mit den Identitätsattributen zuverlässig ist, muss die eID über einen eindeutigen immer gleichen Identifikator verfügen. Dies ist aber zum Beispiel bei einer FIDO-kompatiblen Authentifizierungslösung ganz bewusst ausgeschlossen, um einer Profilbildung vorzubeugen, was natürlich aus Datenschutzgründen vorzuziehen ist. In diesem Fall muss die Attributbestätigung jedes Mal direkt vom IdP kommen. Dieser könnte dann gleichzeitig auch die Authentifizierung als föderierter Dienst für die angeschlossenen vBt übernehmen.

Der IdP erstellt auch eine Policy in der festgehalten wird, ob und wie häufig bei einer weiteren Attributbestätigung vorgängig eine neue Attributbeglaubigung durchgeführt werden muss. Eine neue Beglaubigung kann auch jederzeit auf Verlangen eines vBt durchgeführt werden. Zudem kann er für eine vorliegende Attributbeglaubigung jederzeit eine Validierung der ausgestellten Beglaubigung machen. Das Protokoll dafür lautet:

- IdP sendet das Beglaubigungssiegel mit einer Validierungsanfrage an SID Validierungsdienst.
- Der Validierungsdienst überprüft das Zertifikat und verifiziert, ob der Attributwert im ID-Konto noch dem Wert im vom IdP zugestellten Attributsiegel entspricht.
- Falls beide Prüfungen erfolgreich sind, meldet dies der Validierungsdienst an den IdP zurück; sonst wird eine Fehlermeldung zurückgeschickt

Ob neben der durch die IdP-Policy oder den vBt initiierten Neubeglaubigung von staatlichen Attributen eine vom SID initiierte automatisierte Meldung an die lizenzierten IdP bei Attributänderungen im ID-Konto (z.B. bei Heirat oder im Todesfall) geschaffen werden soll, bleibt abzuklären. Dies hätte auch Konsequenzen für die Daten, die zu jedem ID-Konto gespeichert werden müssen (Beglaubigungsidentifikator des IdP müsste gespeichert werden) und für die heutige Schnittstelle zwischen dem Informationssystem Ausweisschriften und Infostar oder es müsste zusätzlich eine automatisier-

te Schnittstelle zwischen dem ID-Konto und Infostar geschaffen werden. Wir gehen heute davon aus, dass kein solcher Meldungsdienst vom SID bereitgestellt werden muss. Im Bedarfsfall muss der vBt oder der IdP eine entsprechende Anfrage an den SID richten.

Der Einsatz von beglaubigten Identitätsattributen ist jedoch nur dann nötig, wenn die geplante Geschäftsbeziehung zwischen Person und vertrauendem Beteiligten dies nötig macht. Ein vertrauender Beteiligter soll für jede Attributbestätigung eine Validierung der Gültigkeit durchführen können. Deshalb müssen Attributbestätigungen signierte Inhalte haben und das Signaturzertifikat enthalten. Jeder vertrauende Beteiligte kann dann die Sicherheitskette überprüfen. Dazu muss der IdP zwingend einen Onlinedienst für die Zertifikatsvalidierung verfügbar machen (Teil der Anforderungen für die staatliche Anerkennung und Lizenzierung).

6.3.5 (O.5) Revokation einer ausgestellten Attributbestätigung durch den IdP

Genauso wie die Ausstellung einer Attributbestätigung ist auch der Rückruf bzw. die Ungültigkeitserklärung für eine ausgestellte Attributbestätigung Sache des IdP. Er muss lediglich nachweisen können, dass er eine solche Möglichkeit hat. Vertrauende Beteiligte müssen solche Rückruflisten Online konsultieren können.

Ein Rückruf ist immer dann angebracht, wenn der IdP erfährt, dass

- Bestätigte Attributwerte von Identifizierungsdaten nicht mehr gültig sind,
- Die eID, die zu einer Attributbestätigung gehört, abhandengekommen oder korrumpiert ist oder
- Andere vom IdP festgelegte Kriterien für die Gültigkeit verletzt sind (zum Beispiel fehlende Bezahlung von Erneuerungslizenzen).

Ein Rückruf von Attributbestätigungen hat keinen direkten Einfluss auf das ID-Konto der Person.

6.3.6 (O.6) Nutzung ID-Konto und Registrierung weiterer eID

Der Zugang zum ID-Konto ist an eine Authentifizierung mit dem initialen Authentifizierungsmittel beziehungsweise einer staatlich anerkannten eID gebunden. Nach der Registrierung einer staatlich anerkannten eID (siehe 6.3.3), wird vom ID-Konto automatisch diese als Authentifizierungsmittel verlangt. Die berechtigte Person kann nun aber weitere eID vom gleichen oder von anderen IdP beschaffen, sie korrekt initialisieren (siehe 6.3.2) und sie dann als weiteres Authentifizierungsmittel für den Zugang zum ID-Konto registrieren. Das Protokoll einer solchen Zusatzregistrierung lautet dann (mit den Bezeichnungen eID1 für die ursprünglich registrierte eID und eID2 für die neue eID):

- Person meldet sich im ID-Konto an und authentifiziert sich mit ihrer eID1.
- Sie wählt die Option „Weitere eID registrieren“ und wird dann mit einem Assistenten durch die folgenden Schritte geführt.
- Person verbindet sich aus dem Konto mit dem ausstellenden IdP der eID2 und authentifiziert sich mit ihrer eID2. Der IdP bestätigt dem SID die Authentifikation mittels der eID2 und sendet den Beglaubigungsidentifikator.
- Der SID registriert nun die eID2 als Authentifizierungsmittel beim Authentifizierungsserver für das ID-Konto. Je nach eID Typ müssen auch bei dieser Zweitregistrierung die zwei Fälle (Direktmodus, Föderationsmodus) unterschieden werden:
- Nach der Registrierung der eID2 kann die Person analog zum Protokoll der Erstregistrierung einer eID dem IdP2 ebenfalls eine Attributbeglaubigung zukommen lassen (siehe 6.3.4). Da-

nach meldet sich die Person von dem ID-Konto ab. Sie hat nun mit der eID1 und der eID2 zwei gleichberechtigte Authentifizierungsmöglichkeiten für den Kontozugang.

Die Person kann das ID-Konto nutzen um alle seine vom Staat erfassten und aktuell gültigen Personenidentifizierungsdaten einzusehen. Er kann auch das Gesichts- und das Unterschriftsbild als Grafikdatei herunterladen. Weitere Nutzungsvarianten können später leicht verfügbar gemacht werden. Der Authentifizierungsserver des SID könnte rein technisch für andere E-Government Dienste als Föderationsserver dienen und damit für die Person ein generelles SSO zu diesen Diensten ermöglichen. Möglicherweise ist eine solche Funktion mit dem geplanten Föderationsdienst von IDV Schweiz obsolet.

6.3.7 (O.7) Revokation einer eID durch den ausstellenden IdP

Der Rückruf bzw. die Ungültigkeitserklärung einer eID ist Sache des ausstellenden IdP. Wird eine eID vom IdP zurückgerufen, ist er verpflichtet eine entsprechende Meldung an den SID zu machen:

- Der IdP teilt dem SID den zuletzt benutzten Beglaubigungsidentifikator, den Typ und, falls vorhanden, den eindeutigen Identifikator der betroffen eID mit.
- Der Authentifizierungsserver des SID löscht die Zugangsberechtigung für die betroffene eID. Falls kein eindeutiger Identifikator vorliegt, löscht er alle Zugangsberechtigungen, die auf einer eID vom selben Typ und selben IdP beruhen, die das ID-Konto betreffen, das durch den Beglaubigungsidentifikator identifiziert wird.
- Falls danach keine eID mehr als Zugangsausweis zum ID-Konto registriert ist, ist das ID-Konto nur noch mit dem initialen Authentifizierungsmittel (PIN+OTP) zugänglich. In diesem Fall muss die Person zuerst wieder eine neue eID registrieren (siehe 6.3.3) bevor Beglaubigungen ausgestellt werden können.

Der IdP darf einen solchen Rückruf nur machen, wenn die Verlässlichkeit der Authentifizierung nicht mehr gegeben ist oder wenn die eID als Authentifikator korrumpiert ist. Ungültig gewordene Attributbestätigungen oder Attributbeglaubigungen zu einer eID stellen keinen Rückrufgrund dar.

6.3.8 (D.1) Anerkennung als staatlich anerkannter IdP und Lizenz für eID-System

Damit ein IdP den Status eines staatlich anerkannten eID-Systembetreibers erhalten kann, muss er folgende Schritte unternehmen:

- Sicherheitszertifizierung seines IAM-Systems insbesondere seines Authentifizierungsdienstes nach CC mit einem geeigneten Protection Profile mindestens auf Stufe EAL5 oder FIPS auf gleichwertiger Stufe [31].
- Bereitstellung (Beschaffung oder eigene Produktion) eines elektronischen Identifizierungsmittels (eID) mit mindestens zwei Authentifizierungsfaktoren und akkreditierten standardisierten Protokollen; zum Beispiel FIDO ready Label [32].
- Bereitstellung der operativen eID-Infrastruktur und des Webportals und einer Test eID für eine Funktionsprüfung (Testkit)
- Erklärung des IdP, dass durch ihn alle gesetzlichen Vorgaben (z.B. Haftung) und Richtlinien sowie alle Verpflichtungen gegenüber dem SID eingehalten werden.
- Einreichung der gesamten Unterlagen an den Lizenzierungsdienst des SID in einer standardisierten Antragsform; gleichzeitig wird vom IdP das Testkit zur Verfügung gestellt.

Das Antragsdossier wird vom Lizenzierungsdienst geprüft und aufgrund der eingereichten Unterlagen bewertet. Das Testkit wird vom Lizenzierungsdienst benutzt um alle Funktionalitäten, die den

SID betreffen zu überprüfen. Fallen beide Prüfungen positiv aus, wird dem IdP eine Lizenz für den Betrieb des nun staatlich anerkannten eID-Systems ausgestellt. Die Lizenz besteht aus einer Lizenznummer, die vom SID signiert ist und den Sicherheitsparametern für den sicheren Kanal zu den SID Diensten. Die Lizenznummer identifiziert den IdP. Der IdP wird unter seiner Lizenznummer als Betreiber eines staatlich anerkannten eID-Systems publiziert. Der IdP erhält ein zeitlich limitiertes Zertifikat für seine Lizenznummer und sein Lizenzschlüsselzertifikat, das er für die Signaturen bei den Attributbestätigungen brauchen muss. Die Lizenz ist mit einer kostendeckenden Gebühr verbunden und ist jährlich zu erneuern. Das Erneuerungsdossier ist eine vereinfachte Form des Antragsdossiers. Alle drei Jahre muss erneut ein vollständiges Antragsdossier eingereicht werden.

Die Details dieses Akkreditierungsprozesses werden in Zusammenarbeit mit potenziellen IdP ausgearbeitet. Der Anerkennungsprozess soll für die Sicherheit, die einfache Nutzbarkeit und die Integration und Interoperabilität der staatlich anerkannten eID sorgen. Der Prozess soll möglichst einfach sein und keine prohibitive ökonomische Schwelle darstellen. Zumindest in Form einer Übergangsregelung wird dafür gesorgt, dass heutige marktgängige eID-Systeme, die für die Authentifizierung das Sicherheitsniveau „substanziell“ (eIDAS Definition) erreichen, die staatliche Anerkennung erhalten können.

6.3.9 (D.2) Validierung einer IdP Lizenz durch einen vertrauenden Beteiligten

Das Lizenzzertifikat ist Teil der Attributbestätigungen eines IdP und kann von jedem vertrauenden Beteiligten beim SID Validierungsdienst überprüft werden. Der Validierungsdienst bestätigt einem Anfragenden vBt, ob der IdP zum Zeitpunkt der Anfrage eine gültige Lizenz hat oder nicht.

6.3.10 (D.3) Revokation einer Lizenz für die Ausgabe staatlich anerkannter eID

Die Lizenz eines IdP kann vom SID vorzeitig annulliert werden, wenn der IdP die gesetzlichen Vorgaben nicht mehr erfüllt oder fällige Gebühren nicht bezahlt. eID eines IdP, dessen Lizenz revoziert wurde, können nicht mehr neu für den Zugang zum ID-Konto registriert werden. Bereits registrierte eID behalten ihr Zugangsrecht während der normalen Laufzeit ihrer Gültigkeit, sofern kein Sicherheitsrisiko besteht.

6.4 Übergreifende Lösungselemente

6.4.1 Rechtsetzung

Für staatlich anerkannte und notifizierbare eID-Systeme wird ein Rechtsrahmen geschaffen. Die gesetzlichen Regelungen sollen sich auf ein Minimum beschränken und möglichst viele Bestimmungen in diesem dynamischen Umfeld auf Verordnungsstufe festgelegt werden. In Anbetracht der engen wirtschaftlichen Beziehungen der Schweiz zu den EU-Staaten und der globalen Natur von Online-Diensten im Internet, erachten wir es als sehr wichtig, ein vom Staat herausgegebenes elektronisches Identifikationsmittel so zu gestalten, dass es über die Grenzen hinaus auch im europäischen Raum eingesetzt werden kann. Das EJPD hat aus diesem Grund beschlossen, die Anforderungen für schweizerische eID so auszugestalten, dass sie vom Konzept her im Prinzip nach den Vorgaben der eIDAS-Verordnung der EU notifizierbar wären.

Weitere Ausführungen und Analysen zum Gesetzgebungsbedarf finden sich in Kapitel 7. Dieses Kapitel gibt einen ersten Überblick über die Problemstellung und Lösungsansätze. Zugleich dient es als eine Grundlage für ein künftiges Normkonzept zur eID-Gesetzgebung.

6.4.2 Standardisierung

Für eine möglichst einfache und rasche Integration der Lösung in bestehende und kommende Systeme soll für die technischen Schnittstellen zu den staatlichen Lösungskomponenten wenn immer möglich auf bestehende Standards zurückgegriffen werden. Wo diese fehlen, müssen diese geschaffen werden oder bestenfalls bestehende angepasst werden. Technische Standards in diesem Kontext sind z.B. die anwendbaren ISO/IEC/ITU-Normen [33], eCH-Richtlinien [7] [34] [35] oder auch Industrie-Standards wie FIDO [25]. Im Rahmen der Erarbeitung des Detailkonzepts werden die betroffenen Standards genauer zu identifizieren sein.

Für die rasche Verbreitung von schweizerischen eID bei vertrauenden Beteiligten ist auch die Interoperabilität der staatlich anerkannten eID untereinander eine wichtige Voraussetzung. Die Erfüllung der Interoperabilitätsanforderungen wird ebenfalls eine zwingende Voraussetzung für die staatliche Anerkennung eines eID-Systems sein.

6.4.3 Kommunikation

Kommunikation und Marketing spielen im Zusammenhang mit einer eID eine zentrale Rolle. Dies einerseits um eine einheitliche Begrifflichkeit innerhalb des eID-Ökosystems zu fördern, aber auch um aufklärende Ausbildung zu betreiben. Deshalb muss im Rahmen der Einführung von staatlich anerkannten eID auch eine einheitliche Kommunikationsstrategie für aktuelle und umfassende Information der eID-Nutzer entwickelt und umgesetzt werden. Wir sind der Meinung, dass sowohl die Definition als auch Umsetzung einschliesslich Finanzierung der Strategie von der Privatwirtschaft und dem Staat gemeinsam erfolgen muss.

6.4.4 Notifizierung

Die Anforderungen, welche an ein schweizerisches eID-System zu stellen sind, wenn dieses konform mit der eIDAS-Verordnung sein soll, damit es später gegebenenfalls nach den Vorgaben dieser Verordnung in der EU notifizierbar wäre, werden auf Grund ihrer Bedeutung in Kapitel 7 ausführlicher behandelt.

Neben der Erfüllung der rechtlichen Voraussetzungen müssen die technischen Voraussetzungen geschaffen werden, damit die eID-Systeme der beteiligten Länder gegenseitig kommunizieren können. Dazu muss ein Netzwerk (Proxy Dienst) für die grenzüberschreitende Nutzung von elektronischen Identitäten aufgebaut werden, welches zusätzliche Investitionen ausserhalb des vorliegenden Projekts notwendig macht (vgl. STORK [5]). Dieser Proxy Dienst muss alle notifizierten eID-Systeme der beteiligten Länder verstehen und alle grenzüberschreitenden Identitätsanfragen und Bestätigungen korrekt weiterleiten können (Identity Broker). Gleichzeitig könnte er das auch im Inland tun, so dass z.B. staatliche inländische vertrauende Beteiligte nur noch ein föderiertes Authentifizierungsprotokoll unterstützen müssten. Als Praxisbeispiel sei hier noch das in Deutschland kürzlich lancierte Produkt „SkIDentity [36] erwähnt. Der Aufbau dieser nationalen und internationalen Föderierungsdienste ist Teil des Vorhabens Identitätsverbund Schweiz (IDV-Schweiz) des Programms E-Government Schweiz in der Verantwortung des SECO.

6.4.5 eID-Ökosystem

Um die in Kapitel 2.3 geschilderten Prozesse alle elektronisch abwickeln zu können, braucht es neben staatlich anerkannten eID zahlreiche weitere Vertrauensdienste, wie z.B. elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste und Webseiten-Zertifikate. Ein attraktives und sinnvolles Angebot von Online-Diensten ist für die Entwicklung des eID-Ökosystems essentiell. Ein solches aufzubauen, liegt in der Verantwortung der Protagonisten des eID-Ökosystems; vorliegendes Projekt kann nur seinen eigenen Teil dazu beitragen.

Zum Beispiel stellt sich bei Vote électronique zusätzlich die Frage, ob kommerzielle Endgeräte (PCs, Tablets, Mobiltelefone, Kartenleser) über das erforderliche Vertrauensniveau verfügen. Vote électronique benötigt für die sichere und medienbruchfreie Stimmabgabe ein besonders vertrauenswürdiges Endgerät, das Manipulationsversuche erkennbar macht. Zwar bieten die Anbieter von mobilen Endgeräten mittlerweile geschützte Laufzeitumgebungen (TEE) auf ihren Geräten an, die sie als besonders sicher beschreiben. Falls aber die vertrauenden Beteiligten - wie im Fall von Vote électronique - zum Schluss kämen, dass sich die gewünschte Vertrauenswürdigkeit ohne staatliche Einflussnahme nicht erreichen lässt, müssten sich die betroffenen Stakeholder zu einer Interessengemeinschaft zusammenschliessen und für die Standardisierung, Entwicklung und Finanzierung eines sicheren Endgerätes besorgt sein. Das Endgerät könnte als Garant für die vertrauenswürdige Abwicklung von Geschäften gelten und die Abgabe eines solchen Endgerätes könnte möglicherweise dazu führen, dass sich deutlich mehr Personen für die elektronische Abwicklung von Geschäften entscheiden. In diesem Fall wäre das Gerät als entscheidender Bestandteil des schweizerischen eID-Ökosystems zu betrachten.

Allerdings muss ein solches Endgerät mit den jeweiligen Anwendungen interagieren können, was entsprechende technische Schnittstellen voraussetzt, was wiederum zu einem nicht zu vernachlässigenden Supportaufwand führen wird, wie vergleichbare Lösungen zeigen. Die Herstellung, die Verbreitung und der Support wären mit zusätzlichen Kosten verbunden, für die nicht der SID aufkommen würde. Eine Pflicht zur Verwendung dieses sicheren Endgerätes oder eine Verlagerung der Haftung bei einzelnen Geschäftsfällen müsste in den jeweiligen spezialgesetzlichen Ausführungsbestimmungen resp. AGB verankert werden. Ein solches sicheres Endgerät könnte voraussichtlich im Rahmen der persönlichen Vorsprache einer Person bei der Beantragung eines ID-Kontos ohne grossen Mehraufwand abgegeben werden.

An dieser Stelle wird angeregt, eine Analyse der möglichen Stakeholder bei Behörden und Wirtschaft durchzuführen und in Zusammenarbeit mit ihnen die Chancen und Risiken, die mit einem vertrauenswürdigen Endgerät einhergehen würden, weiter zu erörtern. Dies soll unabhängig vom vorliegenden Projekt erfolgen und könnte zum Beispiel ein Teil des Programms E-Government Schweiz werden. Die Umsetzung und die Sicherheit des vorliegenden eID-Konzepts ist jedoch unabhängig davon, ob ein solch staatlich abgegebenes Endgerät eingeführt wird oder nicht.

6.5 Datensicherheit und Datenschutz

Die Nutzung der staatlich anerkannten eID wird durch den Einbezug von marktnahen IdP-Diensten flexibler. Gleichzeitig muss aber sichergestellt werden, dass die Flexibilität und die Öffnung für privatwirtschaftlich organisierte IdP die Sicherheit und den Schutz der persönlichen Daten nicht gefährdet. Es müssen deshalb hinreichende Sicherheitsmassnahmen im System implementiert sein, um möglichen Bedrohungen zu begegnen. Wichtig ist jedoch, und das zeigen verschiedene Beispiele aus anderen Ländern, dass die Benutzerfreundlichkeit unter den Sicherheitsmassnahmen nicht leidet.

6.5.1 Bedrohungen

Durch die Einführung von staatlich anerkannten eID-Systemen sollen für die nutzenden Personen keine von den staatlichen Diensten direkt verursachten Schwachstellen erzeugt werden, die zu neuen Bedrohungen für die persönlichen Daten führen. Der Staat kann aber in keinem Fall für Handlungen der Personen verantwortlich gemacht werden, die nicht in direktem Zusammenhang mit dem Gebrauch der eID stehen und die Personenidentifizierungsdaten Bedrohungen durch potenzielle Angreifer aussetzen. Die zu diskutierenden Bedrohungen beschränken sich deshalb auf Situationen, bei denen der Staat oder staatlich anerkannte IdP Personenidentifizierungsdaten verarbeiten oder aufbewahren. Hauptsächlich folgende Bedrohungen sind denkbar:

- (B1) Unberechtigter Zugang zum ID-Konto;
- (B2a) Attributbeglaubigungen durch den Siegeldienst für eine eID einer nicht berechtigten Person (Identitätsdiebstahl);
- (B2b) Attributbestätigungen durch einen staatlich anerkannten IdP für eine eID einer nicht berechtigten Person (Identitätsdiebstahl);
- (B3) Manipulation von Identitätsattributen im ID-Konto;
- (B4) Falsche Identifizierung einer Person im Registrierungsdienst;
- (B5a) Datenverlust oder -korruption im SID;
- (B5b) Datenverlust oder -korruption bei einem staatlich anerkannten IdP
- (B6) Bildung eines privaten Identifizierungsmonopols.

Es gibt natürlich weitere Bedrohungen, die direkt im IT Umfeld eines eID Nutzers (Person oder vBt) wirksam sein können. Insbesondere betrifft dies die Sicherheit des Endgeräts, in das die eID-Funktionen integriert sind oder mit dem Transaktionen abgewickelt werden. Es ist Aufgabe der IdP in Zusammenarbeit mit Herstellern und Betriebssystementwicklern sichere Lösungen bereitzustellen. Von der Industrie werden in diesem Bereich grosse Anstrengungen unternommen und die aktuelle Entwicklung in Richtung abgesichertes Kompartiment mit HW-Verankerung in mobilen Geräten (Trusted Execution Environment [15]) verbindet Sicherheit mit Benutzerfreundlichkeit. Dieses Konzept hat das Potenzial in nützlicher Frist zu einem de facto Standard zu werden. Aber auch die Nutzer müssen in die Pflicht genommen werden, ihre Systeme zu pflegen und Sorgfalt walten zu lassen. Daneben bestehen auch Bedrohungen für IAM Systeme von vBt, die aber ausserhalb des Wirkungsbereichs der staatlichen Instanzen des eID-Systems sind. Sie werden hier deshalb nicht weiter analysiert oder diskutiert.

Obschon die Sicherheit aller Komponenten und Beteiligter im eID-Ökosystem wichtig ist, kann es aber nicht Aufgabe des Staates sein, Sicherheitsmassnahmen gegen alle Bedrohungen im gesamten eID-Ökosystem zu implementieren. Der Staat muss lediglich geeignete Sicherheitsmassnahmen für die von ihm betriebenen Komponenten implementieren und Sicherheitsstandards als Auflage für die staatliche Anerkennung von eID-Systemen und die Anerkennung von IdP definieren. Ziel muss sein, durch geeignete Auflagen die vom Staat beeinflussbaren Schwachstellen der staatlich anerkannten eID-Systeme unter der oben genannten Bedrohungslage auf ein akzeptables Restrisiko zu reduzieren.

6.5.2 Risiken

Das Risiko ist die Wahrscheinlichkeit, dass ein erfolgreicher Angriff eine der obgenannten Bedrohungen realisiert, multipliziert mit dem Schadenspotenzial. Die folgende Tabelle qualifiziert die Risiken nach einer ersten noch vorläufigen Analyse. Eine vertiefte Risikobetrachtung nach dem „Handbuch Risikomanagement Bund vom 29. April 2013“ kann erst im Rahmen der Erarbeitung des Detailkonzepts durchgeführt werden:

Tabelle 8 – Bedrohungen und Risiken

Bedrohung	Wahrscheinlichkeit	Schadenspotential	Risiko
B1	Mittel-Hoch	Verlust der Geheimhaltung der Personenidentifizierungsdaten: kleiner Schaden	Klein
B2a / B2b	Niedrig-Mittel	Verlust der Identität bei vertrauenden Beteiligten: mittlerer bis hoher Schaden	Mittel

Bedrohung	Wahrscheinlichkeit	Schadenspotential	Risiko
B3	Marginal	Partieller Identitätsdiebstahl und Identitäts-verleugnung: hoher Schaden	Klein-Mittel
B4	Niedrig	Vollständiger Identitätsdiebstahl: sehr hoher Schaden	Mittel-Hoch
B5a / B5b	Marginal (SID)-Niedrig (IdP)	Verlust privater Daten von vielen Personen: mittlerer bis hoher Schaden	Klein-Mittel

Das Konzept für staatlich anerkannte eID-Systeme sorgt bereits durch die Architektur dafür, dass die vom Staat oder von staatlich anerkannten IdP ausgehenden Risiken beschränkt sind. Insbesondere sind mit der eID, verglichen mit den Risiken, welche mit der Ausstellung von Pässen und IDK einhergehen, keine neuen höheren Risiken verbunden.

6.5.3 Sicherheitsmassnahmen

Die Protokolle für die Nutzung der Personenidentifizierungsdaten sollen immer die folgenden drei Absicherungsfunktionen erfüllen:

- Sicherstellen, dass nur die berechtigte Person die eID nutzt: Authentifikation der Person mit der staatlich registrierten eID auf dem Sicherheitsniveau „Substanziell“, das heisst, mit der Verifikation von zwei Authentifizierungsfaktoren.
- Sicherstellen, dass für eine eID nur beglaubigte Attribute bestätigt werden und dass Attributbestätigungen mit der richtigen eID verbunden sind. Integrität der Daten ist durch die staatliche Beglaubigung der Attribute beim IdP gewährleistet. Die vom IdP an einen vertrauenden Beteiligten direkt oder indirekt gelieferte Attributbestätigung kann vom vertrauenden Beteiligten einerseits durch eine erfolgreiche Authentifikation der Person mit ihrer eID und andererseits durch Überprüfung der Zertifikate überprüft werden.
- Sicherstellen, dass die eID von einem IdP nur in einer Form herausgegeben wird, die es einem vertrauenden Beteiligten immer erlaubt zu wissen, wer die Attribute einer Person bestätigt hat: Einbezug der Lizenz des IdP in die Bestätigung und Bindung der Bestätigung an einen eindeutigen Identifikator der eID

Die Absicherung der Integrität der eID-Daten und die Offenlegung der IdP-Lizenzen für vertrauende Beteiligte sind spezifische Aufgaben, welche von den staatlich anerkannten IdP übernommen und deren Erfüllung durch die staatliche Aufsichtsstelle (SID) periodisch überprüft wird.

Der IdP-Dienst kann weitere Attribute über andere Quellen erfassen und verwalten. Er übernimmt abschliessend die Garantie für alle von ihm verteilten oder bestätigten Attribute. 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 Siegeldienst garantiert dabei nur die Integrität der von ihm gelieferten Attributbeglaubigungen und die Authentizität der berechtigten Person bei der Auslieferung der Attributbeglaubigung an den IdP. Die Identifizierung der Person, die Authentifizierung für den Zugang zum ID-Konto und die Registrierung einer eID für den Zugang zum ID-Konto liegt hingegen voll in der Verantwortung des Staates (Registrierungsdienst). Die Verantwortung für die Erfüllung der Sicherheitsanforderungen ist für die verschiedenen Instanzen in Abbildung 12 dargestellt.

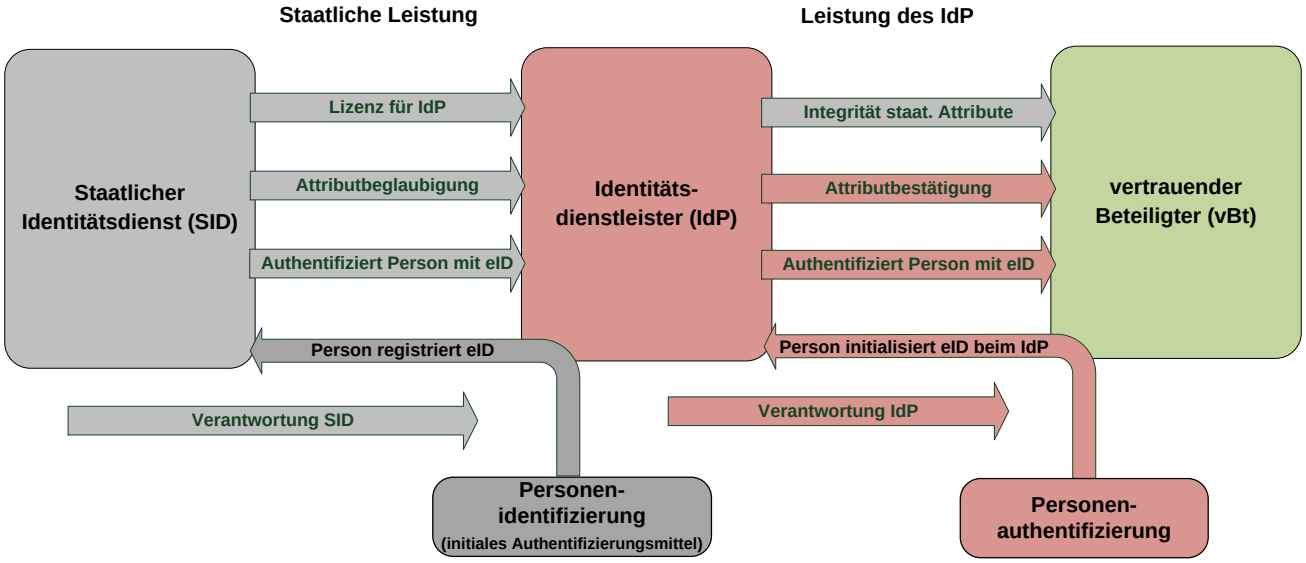

Abbildung 12 – Verantwortlichkeitsbereiche eines staatlich anerkannten eID-Systems

Selbstverständlich müssen auch die einschlägigen Vorgaben des Datenschutzgesetzes eingehalten werden.

- Es braucht eine gesetzliche Basis für die Verwaltung und Aufbewahrung von persönlichen Daten im SID mit Datenschutzvorschriften, geforderten Integritätsgarantien, Aufbewahrungsfristen und Zuständigkeiten von staatlichen Aufsichtsstellen.
- Die Information der betroffenen Personen über die Erhebung, Weitergabe und Aufbewahrung ihrer Personenidentifizierungsdaten sowie der Möglichkeiten zur Kontrolle dieser Daten ist durch das Einsichtsrecht in das persönliche ID-Konto realisiert.
- Der Staat liefert die Attributbeglaubigungen nur in einer Form, welche es ausschliesslich dem empfangenden IdP erlaubt diejenigen Attributwerte zu erfassen und auf Richtigkeit zu überprüfen, die ihm von der berechtigten Person zur Verfügung gestellt werden. Damit ist sichergestellt, dass der Staat keine personenbezogenen Daten an unautorisierte Dritte offen legt.

Unter dem Aspekt des Datenschutzes sind die beiden oben bereits erwähnten unterschiedlichen eID mit und ohne eindeutigen überall bekannten Identifikator zu unterscheiden:

- Eine eID mit einer Authentifizierungslösung mit einem verbindungsabhängigen Identifikator, zum Beispiel nach den Spezifikationen eines FIDO-Authentifikators (siehe [25] und Kapitel 10.3 Anhang), bietet einen hohen Schutz gegenüber Profilierungen.
- Eine eID mit einem überall gleichen Identifikator ermöglicht weniger aufwändige Lösungsansätze, kann aber von einem Profilierungsdienst einfacher verfolgt werden. Unter dem Aspekt des Datenschutzes sind solche eID-Lösungen eher zu vermeiden.

7 Rechtliche Voraussetzungen einer Notifizierung

7.1 Die eID-Regulierung der EU gemäss eIDAS-Verordnung

7.1.1 Überblick über die eIDAS-Verordnung

Am 23. Juli 2014 wurde in der EU die eIDAS-Verordnung verabschiedet und ist am 17. September 2014 in Kraft getreten.

Nebst der Regelung und Zertifizierung der Anbieter der elektronischen Signatur und weiterer Vertrauensdienste in der Art der bisherigen Signatur-Richtlinie[10] enthält die neue Verordnung in den Artikeln 6 ff. als besonderes und neues Thema die Notifizierung und damit gegenseitige Anerkennung von staatlichen Systemen für die elektronische Identifizierung (eID bzw. Authentifizierung). Die eIDAS-Verordnung bildet somit die rechtliche Grundlage für den länderübergreifenden eID-Einsatz, der seit einigen Jahren mit den Projekten STORK und STORK2 [5] pilotiert wird.

Die eIDAS-Verordnung gilt grundsätzlich ab 1. Juli 2016, zusammen mit umfangreicher Umsetzungs-Gesetzgebung auf tieferer Stufe (sogenannte Durchführungsrechtsakte). Im Gegensatz zur abgelösten Signatur-Richtlinie ist die neue eIDAS-Verordnung für alle Mitgliedstaaten direkt anwendbar.

7.1.2 Der Grundsatz der gegenseitigen Anerkennung

Im Kern werden alle Mitgliedstaaten verpflichtet, überall dort, wo sie für den Zugang zu Behördendiensten eine eID verlangen, auch jede ausländische eID jedes notifizierten eID-Systems zu akzeptieren (Art. 6 eIDAS-Verordnung). Dies trifft selbst für einen Mitgliedstaat zu, der selbst kein bei der EU notifiziertes eID-System hat. Aus Sicht einer Person, welche die Staatsangehörigkeit eines EU-Mitgliedstaates besitzt, bedeutet das, dass sie ihre nationale eID sofort EU-weit für elektronisch zugängliche, öffentliche Dienste verwenden kann.

Damit ein nationales eID-System notifiziert werden kann, muss es die in der eIDAS-Verordnung in Artikel 7 aufgeführten Bedingungen erfüllen (siehe Details unter Ziff. 7.3.2 und 7.3.3). Anerkannte, bzw. notifizierte elektronische Identifikationsmittel werden in einer von der EU-Kommission geführten Liste veröffentlicht.

Der Grundsatz der obligatorischen Anerkennung ist sehr stark und wirkt sich auf Bereiche aus, an die man prima Vista nicht denken würde. So müssen auch sämtliche E-Government-Dienste auf nachgelagerten Ebenen, bis hin zur kommunalen Ebene, jede notifizierte ausländische eID akzeptieren. Bei einer Integration der Schweiz in dieses System der gegenseitigen Anerkennung würde das heissen, dass sämtliche Kantone und Gemeinden sofort verpflichtet wären, solche ausländische eID mit ihren Authentifizierungen zu akzeptieren.

7.1.3 Das Verfahren der Notifizierung

Das Verfahren der Notifizierung ist in Artikel 9 eIDAS-Verordnung geregelt. Danach muss der notifizierende Mitgliedstaat der Kommission diverse Informationen bekanntgeben, wie beispielsweise eine Beschreibung des elektronischen Identifizierungssystems, das geltende Aufsichtssystem und Informationen über die Haftungsregelung sowie die für das elektronische Identifizierungssystem

[10] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1.2000, S. 12

zuständige(n) Behörde(n). Allfällige Änderungen dieser Informationen müssen stets unverzüglich gemeldet werden (die Details sind im Anhang aufgeführt).

7.2 Teilnahme der Schweiz am eIDAS-System der EU

Für die Teilnahme am EU-eID-System würde die Schweiz mindestens einen, eher aber mehrere eID-Anbieter nicht nur normal zulassen, sondern als eIDAS-konforme eID-Anbieter (für ein bestimmtes Sicherheitsniveau nach Art. 8 eIDAS-Verordnung) zertifizieren (Lizenz) und durch den SID beaufsichtigen.

Sobald die staatsvertraglichen Grundlagen gegeben wären (vgl. diesbezüglich Ausführungen unter Ziff. 7.2.2 nachstehend), würde die Schweiz das komplette eID-System, bestehend aus den eIDAS-zertifizierten eID-Anbietern und der eigenen Zertifizierung und Beaufsichtigung bei der EU notifizieren lassen.

7.2.1 Interesse für Teilnahme an gegenseitiger Anerkennung

Wie bereits ausgeführt (vgl. Ziff. 2.2), ist die eIDAS-Verordnung für die Schweiz als Nichtmitglied der EU nicht verbindlich; zudem ist die Schweiz im Rahmen der bestehenden bilateralen Abkommen mit der EU auch nicht zur Übernahme dieser EU-Verordnung verpflichtet. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern wird aber in den bisherigen eID-Konzepten 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. Dies würde es ermöglichen, dass Inhaber einer schweizerischen eID mit ausländischen Behörden, und im Gegenzug ausländische Personen mit ihrer nationalen eID sicher mit Schweizer Behörden verkehren können. Auch wenn vorläufig offen ist, ob, wann und wie die Schweiz sich staatsvertraglich in dieses System einbinden wird (vgl. diesbezüglich Ausführungen unter Ziff. 7.2.2 nachstehend), soll das schweizerische eID-System von Beginn an so konzipiert werden, dass es grundsätzlich notifiziert werden könnte („notifizierbar“).

7.2.2 Abkommen mit der EU

Damit die Schweiz (als Drittstaat) am eIDAS-System teilnehmen kann, müsste sie ein Abkommen mit der EU aushandeln, welches die Grundlage für diese Beteiligung am System der gegenseitigen Anerkennung bildet und die Bedingungen einer solchen Beteiligung klärt. Es wird davon ausgegangen, dass die Schweiz mit den gleichen Rechten und Pflichten, wie sie gemäss der EU-Verordnung für die EU-Mitgliedstaaten gelten, am eIDAS-System teilnehmen wird. Wie schon in Kapitel 7.1.2 angetönt, hätte ein solcher Beitritt umgehend Auswirkungen auf alle Verwaltungsebenen bis hin zu den Gemeinden.

7.3 Gesetzgebungsanalyse

7.3.1 Annahmen

Für die nachstehende Gesetzgebungsanalyse wird von den folgenden zwei Annahmen ausgegangen:

- Die Schweiz wird mit der EU ein irgendwie gestaltetes Abkommen zur Teilnahme am System der gegenseitigen Anerkennung nach eIDAS abschliessen (siehe Kapitel 7.2). Der Abschluss dieser Vereinbarung bildet nicht Inhalt der vorliegenden Erörterungen;

- Das nationale schweizerische eID-System wird mehrere private, aber staatlich zertifizierte Anbieter von 'offiziellen' elektronischen Identifikationsmitteln umfassen, wie das aktuell geplant ist (siehe Kapitel 6). In der eIDAS-Verordnung wären das also Anbieter gemäss Artikel 7 Buchstabe a Ziffer iii.

7.3.2 Voraussetzungen für die Notifizierung nach Artikel 7 im Überblick

Ein elektronisches Identifizierungssystem kann notifiziert werden, wenn sämtliche in Artikel 7 der eIDAS-Verordnung aufgelisteten Voraussetzungen erfüllt sind (siehe Anhang). Wie vorstehend erwähnt, gehen wir davon aus, dass wir in der Schweiz ein notifizierbares eID-System gemäss Buchstabe a Ziffer iii eIDAS-Verordnung mit staatlich anerkannten Anbietern haben werden.

Aus dem Rest der Voraussetzungen (Art. 7 eIDAS-Verordnung) scheinen uns nachstehende **vier** für die eID-Gesetzgebung in der Schweiz besonders wichtig:

V1 eID-System und eID halten die technischen Anforderungen ein
Gemäss Artikel 7 Buchstabe c eIDAS-Verordnung müssen sowohl das gesamte eID-System wie auch die elektronischen Identifizierungsmittel (eID) die technischen Anforderungen von mindestens einem Sicherheitsniveau erfüllen.

V2 Staat stellt die Personenidentifizierung sicher
Der notifizierende Staat stellt nach Artikel 7 Buchstabe d eIDAS-Verordnung sicher, dass - zum Zeitpunkt der Ausstellung - der eID die richtigen Personenidentifizierungsdaten zugeordnet sind. Er haftet dafür auch im Schadensfall nach Artikel 11 Absatz 1 eIDAS-Verordnung.

V3 eID-Aussteller stellt Zuordnung der eID zur Person sicher
Die Aussteller der eID stellt nach Artikel 7 Buchstabe e eIDAS-Verordnung sicher, dass die eID gemäss den technischen Spezifikationen stark der richtigen Person zugewiesen wird. Im Schadensfall haftet er dafür nach Artikel 11 Absatz 2 eIDAS-Verordnung.

V4 Staat garantiert dauernd verfügbare Online-Authentifizierung
Der notifizierende Staat stellt nach Artikel 7 Buchstabe f eIDAS-Verordnung sicher, dass jedem der 'vertrauenden Dienste' EU-weit jederzeit eine Online-Authentifizierung der eID zur Verfügung steht. Für öffentliche Dienste muss diese gratis sein, für Private dürfen keine prohibitiven Gebühren oder andere Bedingungen gelten. Im Schadensfall haftet er wiederum nach Artikel 11 Absatz 1 eIDAS-Verordnung.

Artikel 7 der eIDAS-Verordnung nennt noch weitere Voraussetzungen, die im Zusammenhang mit der Notifizierung zu beachten sind, die aber unseres Erachtens entweder keinen wesentlichen Einfluss auf die Ausgestaltung des schweizerischen Systems haben oder erst bei die spätere Notifizierung eingehalten werden müssen. Aus diesem Grund werden nachstehend nur die vier oben aufgeführten Voraussetzungen näher bezüglich des Rechtsetzungsbedarfs überprüft.

7.3.3 Allgemeine Bemerkungen zur eIDAS-Umsetzung in der Schweiz

Im Unterschied zu den EU-Mitgliedstaaten, für welche die Verordnung mit den entsprechenden 'Durchführungsrechtsakten' (~Ausführungs-Gesetzgebung) unmittelbar gelten wird, müsste die EU-Verordnung in der Schweiz im nationalen Recht umgesetzt werden. Der Aufbau könnte ähnlich sein wie bei der bisherigen Umsetzung der Signatur-Richtlinie im schweizerischen Recht:

- Bestimmungen auf Gesetzesstufe (wahrscheinlich im eID-Gesetz, das ja schon einmal entworfen war), welche die Zuständigkeiten und Verantwortlichkeiten regeln und insbesondere dem Bundesrat die Kompetenz geben, die Materie zu regeln.
- eine kurze Verordnung, die primär auf die Bestimmungen für die Zertifizierung und die von der EU erlassenen Durchführungsrechtsakte und Standards verweist.

- Standards für die Zertifizierung(en) der IdP in formeller und inhaltlicher Hinsicht.

7.3.4 V1: eID-System und eID halten die technischen Anforderungen ein

Gemäss Artikel 7 Buchstabe c eIDAS-Verordnung müssen sowohl das gesamte eID-System wie auch das elektronische Identifizierungsmittel (eID) die technischen Anforderungen von mindestens einem Sicherheitsniveau erfüllen, wie es nach Artikel 8 eIDAS-Verordnung und dem zugehörigen 'Durchführungsrechtsakt' vorgeschrieben ist bzw. nach Fertigstellung der Ausführungs-Gesetzgebung inklusive der technischen Standards spezifiziert sein wird.

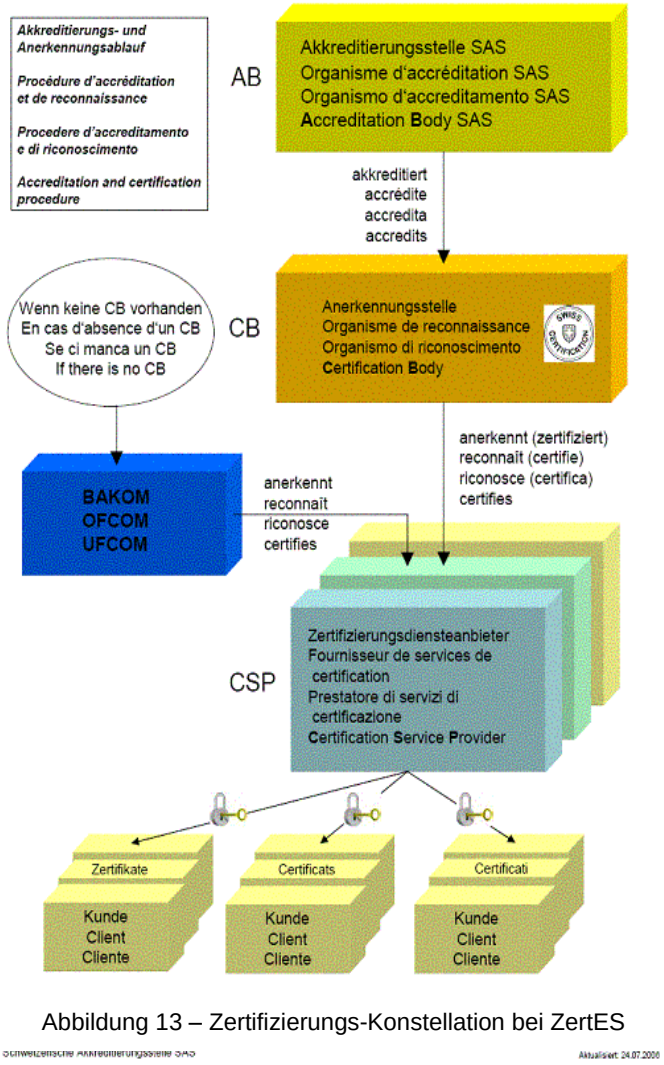

Abbildung 13 – Zertifizierungs-Konstellation bei ZertES

Diese Anforderungen müssen innerhalb des schweizerischen eID-Systems irgendwie an die Herausgeber von staatlich anerkannten eID weitergereicht werden. Rein rechtlich lässt sich das innerhalb des vorgesehenen eID-Systems inklusive der Haftung relativ leicht bewerkstelligen. Um die Einhaltung jedoch für eine Notifizierung nachweisen zu können, braucht es wohl eine Zertifizierung der Anbieter und der Produkte mit dem dazu notwendigen Überbau, bis hin zu periodischen Audits, vergleichbar mit der ZertES-Zertifizierung [6] gemäss Abbildung 13.

Einzig bei den anwendbaren technischen Spezifikationen wird man einfach und direkt auf die entsprechenden europäischen und internationalen Normen verweisen können.

Für den Zugriff auf das staatliche ID-Konto sind von den drei Sicherheitsniveaus in Artikel 8 eIDAS-Verordnung nur die beiden höheren, nämlich 'substanziell' und 'hoch' vorgesehen. Somit können sich auch nur Herausgeber von eID, welche diese Sicherheitsniveaus unterstützen, zertifizieren und staatlich anerkennen lassen. Eine solche Einschränkung für schweizerische eID sollte staatsvertraglich regeln lassen, dies muss aber sicher noch weiter abgeklärt werden.

7.3.5 V2: Staat stellt die Personenidentifizierung sicher

Der notifizierende Staat stellt nach Artikel 7 Buchstabe d eIDAS-Verordnung sicher, dass - zum Zeitpunkt der Ausstellung - der eID die richtigen Personenidentifizierungsdaten zugeordnet sind. Er haftet dafür auch im Schadensfall nach Artikel 11 Absatz 1 eIDAS-Verordnung.

Da nach aktuellem eID-Konzept der Staat die eID nicht selbst herausgibt, muss er diese Zuordnung durch entsprechende Ablauf-Schritte bei der Registrierung der eID auf das ID-Konto sicherstellen. In der aktuellen, vorstehend beschriebenen Konstellation ist das sichergestellt. Mit der anlässlich der persönlichen Vorsprache auf das ID-Konto registrierten eID kann diese Verknüpfung bei richtiger bzw. sicherer Ausgestaltung sichergestellt werden. Es würde allerdings genügen, wenn mit dieser

eID einmalig die Personenidentifizierungsdaten an den eID-Herausgeber übergeben bzw. beglaubigt würden (oder wenn das direkt schon auf der Passstelle geschehen würde). Vorgesehen ist aktuell, dass mit der registrierten eID der staatlichen Vertrauensstelle die Berechtigung gegeben wird, diese Daten später auf Initiative des Nutzers dem anfragenden eID-Herausgeber wiederholt beglaubigen zu können.

Auf jeden Fall muss der schliesslich gewählte Mechanismus wohl auf Gesetzesstufe angesprochen und seine korrekte Durchführung wohl auch zertifiziert werden; letzteres wiederum nicht primär aus juristischen Gründen, sondern um die Einhaltung bei der Notifizierung gegenüber der EU belegen zu können.

Zusätzlich braucht es wohl eine Haftungs-Norm, damit EU-weit ein beliebiger Geschädigter aufgrund der Verletzung dieser Anforderungen die Schweiz belangen könnte (Art. 11 Abs. 1 eIDAS-Verordnung). Diese Frage der Haftung muss jedoch im allfälligen Staatsvertrag geregelt sein.

7.3.6 V3: eID-Aussteller stellt Zuordnung der eID zur Person sicher

Artikel 7 Buchstabe e eIDAS-Verordnung stellt sicher, dass das vom Beteiligten ausgestellte elektronische Identifizierungsmittel der entsprechenden Person (Bst. d) – unter Berücksichtigung der technischen Spezifikationen und Sicherheitsniveaus – zugewiesen wird. Bei allfälligen Haftungsfragen, die in Zusammenhang mit Artikel 7 Buchstabe e eIDAS-Verordnung stehen, findet Artikel 11 Absatz 2 eIDAS-Verordnung Anwendung. Danach haftet der Austeller des elektronischen Identifizierungsmittels für Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugeführt werden. Darunter fallen auch Pflichtverletzungen, die auf eine grenzüberschreitende Transaktion zurückzuführen sind.

Gemäss unserer aktuellen eID-Konzeption trifft diese Pflicht den privaten Anbieter der eID, also den herausgebenden IdP. Es kommen die gleichen Überlegungen wie bei den beiden vorangegangenen Kapiteln kombiniert zur Anwendung. Es braucht eine Definition der Rolle im (eID-)Gesetz, eine Zertifizierung des Anbieters bzw. des Produkts - basierend auf den entsprechenden Vorschriften der EU - und eine Haftungszuweisung an den Aussteller, wiederum im eID-Gesetz.

7.3.7 V4: Staat garantiert dauernd verfügbare Online-Authentifizierung

Der notifizierende Staat stellt nach Artikel 7 Buchstabe f eIDAS-Verordnung sicher, dass jedem 'vertrauenden Dienst' EU-weit jederzeit eine Online-Authentifizierung der eID zur Verfügung steht. Für öffentliche Dienste muss diese gratis sein. Die technischen Anforderungen für den Zugriff dürfen nicht unverhältnismässig sein. Im Schadensfall haftet nach Artikel 11 Absatz 1 eIDAS-Verordnung wiederum der Staat.

Hier müssen - sehr ähnlich wie bei Artikel 11 ZertES [6]- die eID-Anbieter im Gesetz verpflichtet werden, diesen Dienst permanent, für öffentliche Dienste gratis und für alle anderen nach bestimmten Regeln anzubieten. Für ausländische eID erfolgt dieser Dienst nach STORK über einen vom Staat betriebenen Proxy-Server (PEPS).

Die Haftung würde wohl im Gesetz dem Anbieter überbunden, ultimativ müsste aber wiederum die Schweiz haften, was – wie vorstehend unter Ziffer 7.3.6 bereits ausgeführt – im entsprechenden Staatsvertrag zu regeln ist.

8 Umsetzung

8.1 Planung und Organisation

Frühere Lösungsansätze hatten die Eigenheit, dass die Erneuerung der Identitätskarte und die Bereitstellung eines staatlichen elektronischen Identifizierungsmittels sehr eng verknüpft waren. In der hier vorgeschlagenen Lösung besteht dieser enge Konnex nicht mehr. Die Projekte zur Erneuerung der Identitätskarte und das Projekt zur Umsetzung der nun vorgeschlagenen Lösung können weitgehend entkoppelt und getrennt weiterverfolgt werden. Dies reduziert die Projektrisiken und erlaubt unterschiedliche Terminpläne und Verantwortlichkeiten.

Der Grobterminplan für die Umsetzung hängt stark mit der politischen Meinungsfindung zum Thema staatlich anerkannte elektronische Identität und den Beratungen des geplanten eID-Gesetzes ab:

2015 Konzept genehmigt, notwendige gesetzliche Regelungen vorbereitet

2016 Vernehmlassung abgeschlossen, gesetzliche Regelungen im Parlament

2018 WTO-Pflichtenheft für die Beschaffung der SID Infrastruktur publiziert

2019 Zuschlag erteilt, Aufnahme Testbetrieb

2020 Lösung eingeführt

Die Gesamtverantwortung für alle im vorliegenden Kontext notwendigen Prozesse, IKT-Systeme und Anwendungen soll im EJDP (fedpol) liegen, da zwischen der Beantragung der Schweizer Ausweise und einem ID-Konto grosse Synergien bestehen. Es bestehen aber enge Beziehungen zum priorisierten E-Government-Vorhaben IDV-Schweiz, so dass die Aufteilung der Verantwortlichkeiten in der kommenden Rechtsetzungsphase genau geprüft werden sollen. So liegt z.B. die Verantwortung für den Aufbau des Föderierungsdienstes und damit der EU-Schnittstelle beim Vorhaben IDV-Schweiz im SECO. Zudem muss weiterhin eine enge Abstimmung mit den bereits laufenden Arbeiten im Bereich eHealth erfolgen.

Bereits geprüft wurde die Variante, ob die Verantwortung für die mit der staatlich anerkannte eID verbundenen ID-Konten nicht auch im Umfeld des Zivilstandsregisters Infostar anzusiedeln wäre. Dies aus dem Grund, dass Infostar die wichtigste Quelle von Identitätsattributen ist und über einen umfassenden Personenstamm verfügt. Diese Variante stellt gemäss Einschätzung des BJ aber einen massiven Eingriff in die bestehende Systemstruktur dar und hätte eine umfassende Reorganisation des gesamten „Einwohnerwesen“ zur Folge. Die historisch gewachsenen und jeweils selbständigen Ausländer-, Ausweisschriften-, Einwohnerkontroll- resp. Zivilstandswesen würden zu einem „Einwohnerwesen“ fusioniert. Es müsste eine komplexe Neukonzeption erarbeitet werden, was wiederum mit einem unverhältnismässig hohen Aufwand und hohen Kosten verbunden wäre. Aus den oben aufgeführten Gründen ist diese Variante zu verwerfen.

Das EFD (BIT) und/oder das ISC-EJPD sollen die Leistungserbringer für die IKT-Lösungen sein, welche für die Lösungselemente „Registrierung“, „Lizenzierung“ und „Siegelung“ notwendig sind. Die Umsetzung der notwendigen Anpassungen am Informationssystem Ausweisschriften (ISA) fällt in die Verantwortung des EJPD (ISC-EJPD). Leistungsbezüger ist jeweils das EJPD, es sei denn im Rahmen des Finanzierungskonzepts wird eine andere Lösung favorisiert. Der Versand der notwendigen Briefe mit den Benutzernamen und PIN soll durch das Bundesamt für Bauten und Logistik (Passproduzent) erfolgen. In der Verantwortung des EJPD (BJ) liegt die Schaffung der notwendigen gesetzlichen Grundlagen. Die periodische Überprüfung der Legal Compliance der im IAD registrierten eID-Herausgeber soll durch noch zu bestimmende und vom SECO (SAS) akkreditierte Konformitätsbewertungsstellen der Privatwirtschaft erfolgen.

8.2 Kosten und Aufwand

Grundsätzlich überlässt es die gewählte Lösung dem Markt, die staatlich anerkannten eID-Systeme aufzubauen und die Online-Dienstleistungen, Geschäftsfälle und Anwendungsszenarien zu definieren. Die Marktteilnehmer bestimmen und decken alle diesbezüglichen Aufwände und Erträge.

Für die Realisierung der notwendigen bundeseigenen Lösungskomponenten fallen voraussichtlich nachfolgende Kosten und Stellenprozente für die rund dreijährige Umsetzungsphase und den Betrieb an, wobei die Angaben für die IT-Systeme teilweise in einer sehr frühen Projektphase seitens ISC-EJPD abgeschätzt worden sind. Die Kostenangaben sind deshalb mit einer Streuung belegt und sie müssen im Detailkonzept weiter präzisiert werden.

Tabelle 9 – Kostenübersicht

Pos.	Komponente	Umsetzung	Betrieb p.a. (ab 2019)
1	Fachapplikation SID - Staatlicher Registrierungsdienst - Identitätsattribut Siegeldienst - Identitätsdienstleister Lizenzierungsdienst - ID-Konto Web Front End	CHF 3‘900‘000	CHF 1’500‘000
2	Adaption bestehender Applikationen - Fachapplikation ISA - Internetantrag	CHF 600‘000	CHF 0 (keine Mehrkosten da keine neuen Komponenten)
3	Projektumsetzung über 3 Jahre - Personelle Ressourcen (zusätzliche 200%) - Dienstleistungen, Kommunikation, Sonstiges	CHF 1‘800‘000	-
4	Betrieb Staatlicher Identitätsdienst - personelle Ressourcen (zusätzliche 300%) - Dienstleistungen und sonstiger Aufwand	-	CHF 600‘000 (inkl. 300 Stellenprozente)
5	Aktuelle Schätzung der Gesamtkosten	CHF 6‘300‘000	CHF 2‘100‘000

Hinweis: In diesen Angaben sind die Kosten für die nationalen und internationalen Föderationsdienste, welche auch die „Notifizierung“ des nationalen eID-Schemas gegenüber der EU, den Aufbau und den Betrieb der EU-Schnittstelle (vgl. Kapitel 6.4.4) einschliessen, nicht enthalten, da diese in die Verantwortung des separaten Vorhabens IDV-Schweiz fallen. Die notwendige Informationsstrategie soll in enger Zusammenarbeit mit dem Programm E-Government Schweiz erarbeitet und finanziert werden.

Die Finanzierung ist durch den mit dem Bundesratsbeschluss vom 16.12.2011 bewilligten Verpflichtungskredit nur teilweise abgedeckt. Im Rahmen der geplanten Vernehmlassung soll dem Bundesrat deshalb mit dem Gesetzesentwurf im Herbst 2015 ein revidiertes Finanzierungskonzept vorgelegt werden. Bedingt durch die neuen Aufgaben sind im EJPD (fedpol) für den Staatlichen Identitätsdienst neu geschätzt zusätzliche 300 (statt 200) Stellenprozente notwendig, welche im Rahmen der Gesamtschau Ressourcen dem BR beantragt werden müssen. Alle Aussagen zu Ressourcen und Finanzen gelten ausdrücklich vorbehältlich der Resultate der noch ausstehenden politischen Meinungsfindung im Rahmen der Vernehmlassung.

In den Registrierungsstellen bei den Kantonen und den Schweizer Auslandvertretungen fallen aus heutiger Sicht keine zusätzlichen Investitionskosten an. Es muss jedoch mit einem gewissen zusätz-

lichen (Beratungs-) Aufwand für die eID Registrierung gerechnet werden, welcher noch genauer bestimmt werden muss. Dieser kann Auswirkungen auf den Personalbedarf der Registrierungsstellen und die Gebühren haben (vgl. Kapitel 9.4.3).

8.3 Projektrisiken

Als die Hauptrisiken im Bereich eID werden die Unsicherheiten bezüglich des tatsächlichen Bedarfs für eine eID mit staatlich bestätigten Identitätsattributen einerseits und der Akzeptanz einer konkreten staatlichen eID-Lösung andererseits angesehen. Zahlreiche Staaten und Private haben schon verschiedentlich eID-Systeme entwickelt und lanciert. Die jeweiligen eID-Ökosysteme haben die eID aber eher widerwillig bis gar nicht aufgenommen. Umso wichtiger scheint es uns, dass die Lösung gut skalierbar und jederzeit – auch nach der Einführung - an neue Bedürfnisse des eID-Ökosystems anpassbar ist. Nur so können die finanziellen Mittel gezielt und ökonomisch eingesetzt werden.

Aus diesen Gründen begnügt sich der Staat bei der vorgeschlagenen Lösung mit der elektronischen Beglaubigung von Identitätsattributen, nutzt aber gleichzeitig die Stärken des Marktes für innovative eID-Lösungen. So kann der Staat seinen Beitrag an die Entwicklung des eID-Ökosystems im Bereich der gesicherten und interoperablen Authentifizierung und Identifizierung leisten. Wichtig ist, dass die Einführung von privatwirtschaftlich getragenen staatlich anerkannten eID-Systemen nicht durch zu hohe Regulierungsanforderungen behindert wird, da der Markt der potenziellen Nutzer nicht bereit ist, für eine staatliche Anerkennung überhöhte Kosten zu tragen. Ein nicht gänzlich auszuschliessendes Risiko in diesem Bereich ist, dass sich ein Anbieter im Markt eine Monopolstellung erkämpft und mit seiner Marktmacht die Preise diktieren könnte. Für eine einzelne Person wäre dies ein kleiner Schaden – das dem Konzept zugrunde liegende Prinzip des marktwirtschaftlichen Wettbewerbs wäre so jedoch ausgehebelt.

Der Gesamterfolg hängt auch ganz wesentlich von den übrigen Akteuren im eID-Ökosystem ab – denn sollte kein wirklicher Bedarf an vertrauenswürdigen Online-Diensten bestehen, bringt auch die Einführung einer staatlich anerkannten eID nichts. Aus diesem Grund ist eine enge Abstimmung mit dem Programm E-Government Schweiz sowie den möglichen staatlich anerkannten IdP während der Projektumsetzung wichtig. Wie in Kapitel 2.4 ausgeführt, sind die Umsetzung eines nationalen Föderierungsdienstes und einer durchgängigen Informationsstrategie weitere unabdingbare Bausteine für den Erfolg des Gesamtsystems. Die Informationsstrategie soll in enger Zusammenarbeit mit dem Programm E-Government Schweiz erarbeitet und finanziert werden.

9 Auswirkungen

9.1 Personen mit Schweizer Staatbürgerschaft

Für Personen mit Schweizer Staatsbürgerschaft wird mit dem Vorhaben die Möglichkeit geschaffen, sich auch im Internet mit einem staatlich anerkannten Ausweis auszuweisen. Dies umfasst eine sichere, staatlich anerkannte Authentifizierung gegenüber vertrauenden Beteiligten, aber auch den Nachweis von staatlich beglaubigten Personenidentifizierungsdaten, wie Name oder Staatsbürgerschaft. Unter der Voraussetzung, dass das eID-Ökosystem attraktive Online-Dienstleistungen anbietet, wird ein messbarer Nutzen geschaffen (vgl. auch Kapitel 4.2.1). Sollte in der Schweiz ein Bürgerkonto oder Bürgerdossier als Single Sign On Portal geschaffen werden (wie etwa in [37] angedacht), wäre das ID-Konto darin zu integrieren. Durch eine am Datenschutz und an der Datensicherheit orientierte staatliche eID-Regulierung und Umsetzung wird insgesamt die Sicherheit und der Persönlichkeitsschutz bei Transaktionen im Internet verbessert, so etwa in den wichtigen Berei-

chen Handel und Bezahlen. Sollte die Schweiz ihre eID-Systeme zudem der EU notifizieren, dann werden damit auch die Barrieren („der Medienbruch“) der Landesgrenzen durchbrochen. Eine sichere und breit akzeptierte eID fördert, wie vom Bundesrat gewünscht, ganz allgemein die Entwicklung der Schweiz zur Informationsgesellschaft.

9.2 Personen mit ausländischer Staatsbürgerschaft

Die Beglaubigung von Personenidentifizierungsdaten ist im vorliegenden Konzept auf Personen mit Schweizer Staatbürgerschaft eingeschränkt, da die Schweiz nur für diese hoheitlich die Identität beglaubigen kann. Auch die entsprechende Verordnung der EU geht davon aus, dass jeder Mitgliedsstaat ein nationales eID-System für seine Bürger aufbaut und dieses dann notifizieren kann. Mit einer Notifikation wird es im EU-Raum anerkannt, so dass die einzelnen Länder für andere EU-Bürger keine eigene eID herausgeben müssen. Für die Schweiz gilt das Gesagte nur dann, wenn sie ihr eID-System über einen mit der EU zu schliessenden Staatsvertrag notifiziert. Keine Lösung bietet die Notifikation dagegen für Drittstaatsangehörige.

Das vorliegende Konzept könnte in der Verantwortung des Staatssekretariats für Migration auch auf die ausländische Wohnbevölkerung ausgedehnt werden, falls dies dem mehrheitlichen politischen Willen entsprechen würde. Die Daten für das ID-Konto würden entsprechend aus ZEMIS kommen und die persönliche Vorsprache müsste auf den Migrationsämtern erfolgen. Zudem müssten die Attribute im ID-Konto mit einer Qualitätsstufe (z.B. gemäss eCH-Richtlinie eCH0171 [35]) versehen werden, da nicht alle mit der gleichen Qualität festgestellt werden können. Ausserdem müssten vorab einerseits rechtliche Abklärungen getroffen und andererseits die ausführenden Stellen konsultiert werden. Es ist daher zum heutigen Zeitpunkt noch unklar, ob und wann diese Erweiterung überhaupt umgesetzt werden könnte.

Diese Einschränkung schliesst ausländische Personen aber nicht grundsätzlich vom Gebrauch von staatlich anerkannten eID aus, denn auch diese Personen können eine solche eID bei einem IdP beziehen und als Authentifizierungsmittel nutzen. Sie können lediglich keine Attributbestätigungen mit beglaubigten Identitätsattributen an vertrauende Beteiligte liefern. Die IdP und vertrauenden Beteiligten können jedoch - wie schon heute - selbst zusätzliche nicht staatlich beglaubigte Identitätsattribute erheben.

9.3 Privatwirtschaft

Durch die elektronische Bereitstellung von staatlich beglaubigten Identitätsattributen können diejenigen Abläufe vereinfacht werden, welche heute zur Identifikation eine persönliche Vorsprache verlangen. Die Privatwirtschaft kann Dienstleistungen attraktiver anbieten, da Zeit- und Kostenaufwand sowohl der Anbieter als auch der Kunden eingespart werden können. Gerne verweisen wir in diesem Zusammenhang auf die Ausführungen in Kapitel 4.2.

9.4 Behörden

9.4.1 Allgemein

Die „E-Government-Strategie Schweiz“ [2] hat zum Ziel, dass sowohl die Wirtschaft als auch die Bevölkerung die wichtigen Geschäfte mit den Behörden elektronisch abwickeln können. Die Behörden ihrerseits sollen ihre Geschäftsprozesse modernisieren und untereinander elektronisch verkehren. Die E-Government-Strategie Schweiz ist als Teilstrategie in der „Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz" [10] enthalten. Das priorisierte Vorhaben „B2.15 Nati-

onal und im EU-Raum barrierefrei anerkannte elektronische Identität“ (Verantwortung fedpol) ist einer der Bausteine zur Umsetzung dieser Strategien des Bundesrates.

Das Vorhaben hat zahlreiche Berührungspunkte zu den priorisierten Voraussetzungen [4] „B1.06 - E-Government-Architektur Schweiz“ (Verantwortung ISB), „B2.06 - Dienst für die Identifikation und Berechtigungsverwaltung“ (SECO) und zu „B1.16 Wissensmanagement E-Government-Recht“ (Verantwortung BJ) im Bereich Rechtsetzung. Zudem bestehen Beziehungen zu zahlreichen priorisierten Leistungen wie „A1.13 Vote électronique“ (Verantwortung BK), „A1.07 a-h Bestellung und Bezug von beglaubigten Registerauszügen, Ausweisen des Zivilstandswesens, Kopien von wichtigen öffentlichen Urkunden und Verfahrensentscheiden“ (Verantwortung BJ) oder auch „A2.04 Dienstleistungen der Strassenverkehrsämter“ (Verantwortung Vereinigung der Strassenverkehrsämter). Sehr wichtig ist auch die enge Abstimmung mit eHealth Schweiz.

9.4.2 Bund

Der Bund muss mit der Umsetzung des Vorhabens neue Aufgaben übernehmen und den rechtlichen Rahmen für die Erbringung und Nutzung dieser Dienstleistungen in Form eines „eID-Gesetzes“ schaffen (vgl. Kapitel 6.4.1).

Nach den provisorischen Aufwandschätzungen (vgl. Kapitel 8.2) sind zur Umsetzung CHF 6.3 Mio. und für den Betrieb jährlich CHF 2.1 Mio. notwendig, darin eingeschlossen die Kosten für 300 Stellenprozente für neue Aufgaben beim aufzubauenden Staatlichen Identitätsdienst. Die Umsetzung und der Betrieb kann nur unvollständig mit dem bewilligten Verpflichtungskredit für die Erneuerung von Pass und Identitätskarte finanziert werden. Im Rahmen der geplanten Vernehmlassung soll dem Bundesrat deshalb ein revidiertes Finanzierungskonzept vorgelegt werden. Alle Aussagen zu Ressourcen und Finanzen gelten ausdrücklich vorbehältlich der Resultate der noch ausstehenden politischen Meinungsfindung im Rahmen der Vernehmlassung. Auch sei hier nochmals ausdrücklich auf die in Kapitel 8.3 genannten Projektrisiken hingewiesen. Wichtig für den Erfolg ist der Aufbau eines Föderierungsdienstes zwischen den verschiedenen eID-Lösungen parallel zur Lancierung von staatlich anerkannten eID. Dies ist das Ziel des vom SECO geführten Vorhabens Identitätsverbund Schweiz (IDV-Schweiz). Die vom ISB erarbeitete Lösung IAM-Bund könnte als staatlich anerkanntes eID-System in das vorliegende eID-Konzept eingebunden werden.

9.4.3 Kantone

Die kantonalen Passstellen müssen einen neuen Geschäftsfall abdecken, nämlich den „Antrag für ein ID-Konto“ (Registrierung). Ein Grossteil der Tätigkeiten ist beinahe 1:1 mit denjenigen für die Beantragung eines Passes identisch und viele Personen werden wohl ein preislich vorteilhaftes Kombiangebot „Pass + ID-Konto“ wählen. Neu müssen zusätzlich die Nummer des mitgebrachen Mobiltelefons registriert respektive validiert werden. Eventuell ist zusätzlich eine kurze Beratung der Personen zum Thema eID notwendig. Diese Aufgaben könnten, abhängig von der noch genauer zu bestimmenden Dauer und Häufigkeit einer Registrierung, zu einem personellen Mehraufwand in den Registrierungsstellen führen. Für eine Überschlagsrechnung der Gebühren geht das Konzept von einem Mehraufwand von durchschnittlich fünf Minuten aus.

9.5 Gebühren

Die Investitionen und Betriebsausgaben müssen mittelfristig durch kostendeckende Gebühreneinnahmen egalisiert werden. Ob in der Anfangsphase auch eine Anschubfinanzierung[11] durch den Bund möglich und politisch gewünscht ist, bleibt im Rahmen des Finanzierungskonzepts abzuklären. Wie hoch diese Gebühren tatsächlich ausfallen, kann verständlicherweise noch nicht definitiv abgeschätzt werden. Eine informative Überschlagsrechnung hat die Zahlen in Tabelle 10 ergeben (ohne Amortisation der Projektkosten).

Tabelle 10 – Abschätzung der Gebühren

Pos.	Komponente	Kosten für die Registrierung ohne Kombi mit Pass	Kosten für die Registrierung bei Kombi mit Pass
1	Identifikation und Eröffnung ID-Konto (Passstellen)	CHF 60	CHF 10
2	Zentrale Dienste (Bund)	CHF 20	CHF 20
3	Gesamtkosten (Gebühren)	CHF 80	CHF 30

Registrierungsgebühren: Davon ausgehend, dass der Zusatzaufwand für die Registrierung und die Beratung der Person in den Kantonen bei einem Kombiangebot „Pass und ID-Konto“ fünf Minuten beträgt, müssten die Kantone mit rund CHF 10 entschädigt werden. Die jährlichen Zusatzkosten der zentralen Dienste des Bundes in der Grössenordnung von CHF 2.1 Mio. müssen auf die Anzahl der jährlichen Registrierungen abgewälzt werden. Bei einer an den Zahlen von Österreich [18] orientierten Schätzung von durchschnittlich 100‘000 Stück (ca. 20% aller Personen) müsste der Bund mit CHF 20 pro Registrierung entschädigt werden (gerundet auf ganze CHF 5). Zusammen mit den Kosten der Kantone betragen die Gebühren also rund CHF 30, sofern das ID-Konto als Kombi-Angebot beantragt wird. Diese Registrierungsgebühren fallen alle 5 oder 10 Jahre pro Registrierung an (keine Jahresgebühr). Darin nicht enthalten sind die Kosten für die durch die Personen selbst zu beschaffenden staatlich anerkannten eID, welche durch den Markt bestimmt werden. Hier gibt es aktuell Preismodelle auf dem Markt, bei welchen der Person keine zusätzlichen direkten Kosten für ihre eID erwachsen (z.B. Mobile ID).

Lizenzierungsgebühren: Die Einnahmen aus den Lizenzen der staatlich anerkannten IdP sollen einen Beitrag an die Kosten für die Verwaltung der Lizenzen, den Betrieb des Validierungsservers für die Lizenzen und den Fachsupport leisten. Diese Kosten belaufen sich jährlich auf schätzungsweise CHF 500‘000. Die Lizenzierungskosten fallen jährlich an (Jahresgebühr). In welchem Umfang die Kosten tatsächlich auf die IdP abgewälzt werden sollen, unterliegt der anstehenden politischen Diskussion. Durch die Kostenübernahme reduzieren sich die im Abschnitt „Registrierungsgebühren“ genannten Anteile, was wohl der Akzeptanz zuträglich wäre.

[11] Aufgrund der angespannten Finanzlage der Bundesverwaltung ist gemäss einer Stellungnahme der eidgenössischen Finanzverwaltung von einer Anschubfinanzierung durch den Bund abzusehen. Es müssen im Rahmen der Folgearbeiten also auch noch andere Finanzierungsmodelle geprüft werden.

10 Anhang

Die nachfolgenden Ausführen dienen der vertieften Erläuterung einzelner Aspekte und Prinzipien der vorgeschlagenen Lösung.

10.1 Auszug aus der eIDAS-Verordnung

Die Artikel 7 - 12 in der eIDAS-Verordnung definieren die Auflagen und Rahmenbedingungen für gegenseitige Anerkennung von eID-Systemen innerhalb der EU. Ein elektronisches Identifizierungssystem kann gemäss Artikel 7 der eIDAS-Verordnung notifiziert werden, wenn sämtliche folgenden Bedingungen erfüllt sind:

a) Die elektronischen Identifizierungsmittel im Rahmen des betreffenden Systems werden ausgestellt i) vom notifizierenden Mitgliedstaat, ii) im Auftrag des notifizierenden Mitgliedstaats oder iii) unabhängig vom notifizierenden Mitgliedstaat und von diesem anerkannt;

b) die elektronischen Identifizierungsmittel im Rahmen dieses Systems können im notifizierenden Mitgliedstaat für den Zugang zu mindestens einem von einer öffentlichen Stelle bereitgestellten Dienst, für den eine elektronische Identifizierung erforderlich ist, verwendet werden;

c) dieses System und die im Rahmen dieses Systems ausgestellten elektronischen Identifizierungsmittel erfüllen die Anforderungen zumindest eines der Sicherheitsniveaus, die in dem in Artikel 8 genannten Durchführungsrechtsakt aufgeführt sind;

d) der notifizierende Mitgliedstaat stellt sicher, dass zum Zeitpunkt der Ausstellung des elektronischen Identifizierungsmittels im Rahmen des betreffenden Systems entsprechend den technischen Spezifikationen, Normen und Verfahren für das einschlägige Sicherheitsniveau, die in dem in Artikel 8 genannten Durchführungsrechtsakt aufgeführt sind, die Personenidentifizierungsdaten, die die betreffende Person eindeutig repräsentieren , der in Artikel 3 Nummer 1 genannten natürlichen oder juristischen Person zugewiesen werden;

e) der Beteiligte, der das elektronische Identifizierungsmittel im Rahmen des betreffenden Systems ausstellt, stellt sicher, dass das elektronische Identifizierungsmittel der in Buchstabe d genannten Person entsprechend den technischen Spezifikationen, Normen und Verfahren für das betreffende Sicherheitsniveau, die in dem in Artikel 8 genannten Durchführungsrechtsakt aufgeführt sind, zugewiesen wird;

f) der notifizierende Mitgliedstaat stellt sicher, dass eine Online-Authentifizierung zur Verfügung steht, so dass jeder im Hoheitsgebiet eines anderen Mitgliedstaats niedergelassene vertrauende Beteiligte die in elektronischer Form empfangenen Personenidentifizierungsdaten bestätigen kann. Für vertrauende Beteiligte, die keine öffentlichen Stellen sind, kann der notifizierende Mitgliedstaat Bedingungen für den Zugang zu dieser Authentifizierung festlegen. Die grenzübergreifende Authentifizierung sollte gebührenfrei erbracht werden, wenn sie in Bezug auf einen Online-Dienst erfolgt, der von einer öffentlichen Stelle erbracht wird. Die Mitgliedstaaten machen vertrauenden Beteiligten, die eine solche Authentifizierung durchfuhren mochten, keine spezifischen unverhältnismäßigen technischen Vorgaben, wenn derartige Vorgaben die Interoperabilität der notifizierten elektronischen Identifizierungssysteme verhindern oder erheblich beeinträchtigen;

g) der notifizierende Mitgliedstaat stellt den anderen Mitgliedstaaten für die Zwecke der Verpflichtung nach Artikel 12 Absatz 5 mindestens sechs Monate vor einer Notifizierung gemäß Artikel 9

Absatz 1 nach den in Artikel 12 Absatz 6 genannten Verfahrensmodalitäten eine Beschreibung dieses Systems zur Verfügung;

h) das System erfüllt die Anforderungen des in Artikel 12 Absatz 8 genannten Durchführungsrechtsakts.

Betreffend Haftung der beteiligten Stellen regelt Artikel 11 der eIDAS-Verordnung Folgendes:

1. Der notifizierende Mitgliedstaat haftet für die natürlichen oder juristischen Personen absichtlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in Artikel 7 Buchstaben d und f festgelegten Pflichten bei einer grenzübergreifenden Transaktion zurückzuführen sind.
2. Der das elektronische Identifizierungsmittel ausstellende Beteiligte haftet für die natürlichen oder juristischen Personen absichtlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in Artikel 7 Buchstabe e festgelegten Pflichten bei einer grenzübergreifenden Transaktion zurückzuführen sind.
3. Der das Authentifizierungsverfahren durchführende Beteiligte haftet für die natürlichen oder juristischen Personen absichtlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in Artikel 7 Buchstabe f festgelegten Pflichten bei einer grenzübergreifenden Transaktion zurückzuführen sind.
4. Die Absätze 1, 2 und 3 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet.
5. Die Absätze 1, 2 und 3 berühren nicht die unter das nationale Recht fallende Haftung der Beteiligten an einer Transaktion, bei der dem notifizierten System unterliegende elektronische Identifizierungsmittel verwendet wurden.

Weiter definiert die eIDAS-Verordnung in Art 8 in Anlehnung an die Sicherheitsniveaus 2-4 (Medium, High, Very High) des ISO Standards 29115:2011 die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ für elektronische Identifizierungsmittel. Sie legt in Artikel 12 auch noch fest, dass die notifizierten nationalen elektronischen Identifizierungssysteme interoperabel sein müssen und für diesen Zweck ein Interoperabilitätsrahmen geschaffen werden soll, wie er zum Beispiel im EU-projekt STORK vorbereitet wird.

10.2 Authentifizierung und Identifizierung

10.2.1 Authentifizierung

Die Authentifizierung ist der Basisprozess im eID-Ökosystem, der die Gewissheit liefert, dass ein vertrauender Beteiligter mit einer identifizierten Person kommuniziert – und umgekehrt[12]. Wie in der physischen Welt haben Geschäftspartner auch in der Online-Welt je nach Tragweite eines Geschäfts unterschiedliche Sicherheitsansprüche. Darauf muss bei der Systemgestaltung Rücksicht genommen werden. Die Authentifizierung wird bei jedem Geschäftskontakt durchgeführt und muss deshalb besonders einfach, effizient und flexibel an die Sicherheitsbedürfnisse anpassbar sein. Sie beinhaltet immer einen Messprozess (z.B. Erfassung einer biometrischen Eigenschaft, Nachprüfung eines Wissens der Person, Kontrolle der Präsenz eines physischen Gegenstandes) und stellt damit die Verbindung zwischen der physischen Person und ihrer digitalen Repräsentation (Identifikator)

[12] In der eIDAS-Verordnung der EU wird der Begriff „Authentifikation“ auch für juristische Personen und Daten verwendet(Zitat: „Authentifizierung“ ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit elektronischer Daten ermöglicht.).

her, mit der die Authentifikation gegenüber einem vertrauenden Beteiligten bestätigt wird. Eine erfolgreiche Authentifizierung legt per se nebst dem Identifikator, der nur in einem spezifischen Kontext eine Bedeutung hat (zum Beispiel ein Benutzername), noch keine weiteren Identitätsattribute der zugeordneten Person offen. Sie kann also anonym oder pseudonym sein - die vertrauenden Beteiligten wissen einzig, dass sie es immer mit derselben Person zu tun haben. Die Authentifizierung ist aber Vorbedingung für weitere Prozesse, wie zum Beispiel die Erfassung von zusätzlichen Identitätsattributen, die Absicherung von Transaktionen wie dem Altersnachweis oder auch weitere komplexe Kombinationen solcher Prozesse wie die qualifizierte elektronische Signatur oder Vote électronique. Beim Einsatz einer eID für die Authentifizierung wird lediglich die elektronische Authentifizierungsfunktion der eID (Authentifikator) gebraucht.

Zweck der Authentifizierung ist der elektronische Nachweis, dass es sich immer um die physische Person handelt, der der Identifikator zugeordnet ist, implizit wird dadurch auch die physische Präsenz der Person überprüft. Der Prozess wird sehr häufig beansprucht und erfolgt mit Hilfe der Authentifizierungsfunktion von elektronischen Identifizierungsmitteln (eID).

10.2.2 Identifizierung

Die Identifizierung mit zusätzlichen Personenidentifizierungsdaten ist eine Erweiterung der Authentifizierung und umfasst zusätzlich die Erfassung resp. den Nachweis von weiteren Identitätsattributen der Person. Eine Identifizierung mit staatlichen Identitätsattributen erfolgt in der Regel nur bei der Neuaufnahme eines Geschäftskontaktes, damit der vertrauende Beteiligte die Person in ihrem System einordnen und allenfalls die richtigen Rechte und Rollen zuordnen kann. Die staatlichen Personenidentifizierungsdaten der eID werden nur in diesem deutlich selteneren Kontext gebraucht, sollten dann aber aktuell und verlässlich sein. Die der eID zugeordneten Identitätsattribute einer Person werden in einem solchen Kontext also für die Abdeckung zusätzlicher Identifizierungsanforderungen und punktuell auch für die Absicherung einer Transaktion gebraucht, falls letztere auf gewisse Identitätsattribute wie zum Beispiel das Alter angewiesen ist. Die Vertrauenswürdigkeit der Identitätsattribute muss für gewisse Geschäfte besonders hoch – eben staatlich – sein. Dies ist zum Beispiel immer dann der Fall, wenn in der physischen Welt vor Ort die Identitätskarte vorgewiesen werden muss, wie beim Eröffnen einer neuen Bankbeziehung oder beim Bezug einer SIM-Karte.

Zweck der Identifizierung ist die Authentifizierung und der Nachweis von Identitätsattributen einer Person. Der Prozess wird meist nur bei der Aufnahme einer neuen Geschäftsbeziehung beansprucht und erfolgt mit Hilfe von zusätzlichen Identitätsattributen, die mit der eID verbunden sind und durch diese bestätigt werden.

10.3 Authentifikationsfunktion in einer eID

Das heute von fast allen relevanten Instanzen (eIDAS, FICAM, FIDO, GSMA, IDESG, NIST, GlobalPlatform etc.) propagierte und von den wichtigsten Anwendern (z.B. Banken) bereits übernommene Modell für die umfassende Absicherung einer End-To-End Kommunikation geht von einer nutzerzentrierten Authentifizierung aus.

In der Referenzarchitektur, schematisch dargestellt in Abbildung 14, hat die Person ein Endgerät, auf dem eine abgesicherte Funktion (oft auch als Authentifikator bezeichnet) realisiert ist, die einem vertrauenden Beteiligten einen Nachweis für die korrekte Durchführung der Authentifizierung liefert. Damit der Beteiligte einem solchen Nachweis vertrauen kann, muss er sicher sein, dass dieser von einem ihm bekannten und als sicher akzeptierten Endgerät stammt. Das Endgerät identifiziert sich durch seinen Identifikator, der damit gleichzeitig zu einem Identitätsattribut der Person wird. Zusätzlich hat der Authentifikator eine Komponente, die feststellt, ob eine bestimmte Person, im Normalfall

der Besitzer und Nutzer des Endgeräts, sich mit den verlangten Authentifizierungsfaktoren[13] ausweisen kann (Verifikation). In Zukunft wird der aktive Beweis, den die Person noch heute oft mit einem Passwort oder einer Einbindung in ein Challenge-Response-Protokoll leisten muss, immer mehr durch intelligente Sensorik im Nutzergerät ersetzt, welche die berechtigte Person mittels mehrerer Merkmale sicher erkennt [12]. Der Verifikationsmechanismus wird vom Nutzer jedes Mal gebraucht, wenn er sich bei einem Zugangsportal eines vertrauenden Beteiligten, also zum Beispiel beim IdP oder beim ID-Konto authentifizieren muss. Zusätzliche Identitätsattribute sind für diesen sich oft wiederholenden Authentifizierungsprozess im Normalfall nicht nötig.

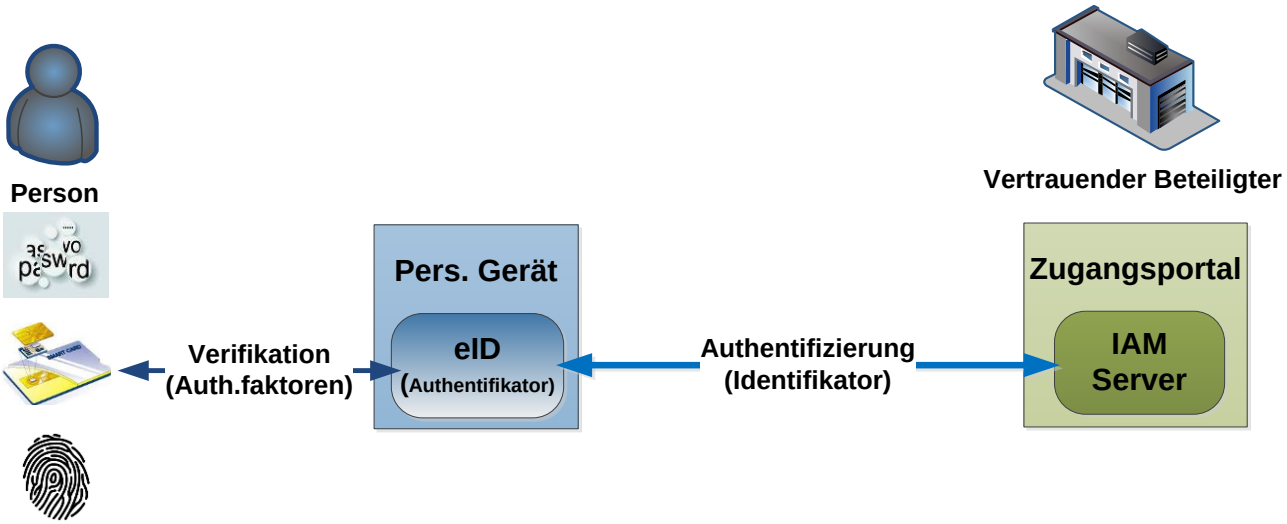

Abbildung 14 – Authentifikationsfunktion einer eID

Fundament für die nutzerzentrierte Authentifizierung ist ein Initialisierungs- und ein Registrierungsprozess. Im Initialisierungsprozess wird die eineindeutige Verbindung zwischen Person und eID hergestellt. Für die Initialisierung muss auf dem Gerät ein geeignet abgesicherter Authentifikator installiert sein. Es müssen, in Abhängigkeit des verlangten Sicherheitsniveaus der Authentifizierung, die möglichen Authentifizierungsfaktoren nebst dem Besitz des Gerätes (Biometrie, Passwort, PIN, Smartcard etc.) bestimmt werden, die das Nutzergerät vertrauenswürdig erfassen kann. Die Initialisierung wird mit der Erfassung der Authentifizierungsfaktoren der Person abgeschlossen, die für spätere Authentifizierungen als Referenz dienen. Für die Registrierung des Geräts als eID bei einem vertrauenden Beteiligten muss zwischen der eID und dem vertrauenden Beteiligten ein sicherer Kommunikationskanal definiert werden, der es jeweils erlaubt, die beiden Kommunikationspartner zu identifizieren und eine erfolgreiche Authentifizierung durch einen digitalen Ausweis zu bestätigen. Die Identifikation einer eID erfolgt durch den eindeutigen Identifikator, der entweder für alle Beteiligten gleich ist, oder verbindungsabhängig für jeden vertrauenden Beteiligten neu definiert wird; zum Beispiel in Form eines Schlüssels, der jeweils nur dem vertrauenden Beteiligten bekannt ist.

10.3.1 Methoden und Technologien für die Authentifizierung

Das nutzerzentrierte Authentifizierungsmodell impliziert, dass die ausgetauschten authentifizierenden Ausweise nur von den beiden involvierten Parteien ausgewertet und überprüft werden können (Schutz der Privatsphäre) und dass anstelle von personenbezogenen Merkmalen nur noch kryptographische Tokens ausgetauscht werden, die für eine erfolgreiche Verifikation der Authentifikationsfaktoren der Person stehen (Datenschutz). Eine konsequente Umsetzung dieser Anforderung führte

[13] Als authentifizierende Faktoren dienen Kenntnis eines Geheimnisses, biometrische Eigenschaften oder Besitz eines bestimmten Gegenstandes

bisher meist dazu, dass jede Organisation ein eigenes Authentifizierungssystem ausgerollt hat und unterhalten musste [22]. Daraus ergibt sich die heutige recht unbefriedigende Situation, dass ein Nutzer von Onlinediensten multiple Authentifizierungsprotokolle und -verfahren beherrschen und eine Vielzahl von Authentifikationsfaktoren verwalten muss. Sehr oft ist die Verifikation der Authentifizierungsfaktoren noch ganz oder teilweise mittels Passwörtern realisiert, was nicht nur zunehmend unsicher sondern für die Person und den Systembetreiber auch unpraktisch beziehungsweise kostentreibend ist [38].

Die unbefriedigende Situation hat dazu geführt, dass sich verschiedene Organisationen und Allianzen mit dem Problem der Vereinfachung und mehrfachen Nutzung einer Authentifizierung auseinandergesetzt haben. Daraus sind vorerst Föderationsdienste und dazugehörige Architekturen und Standards entstanden. In einer solchen Architektur authentifiziert ein IdP die Person und verteilt dann Authentifizierungs- und Identitätsnachweise an unterschiedliche vertrauende Beteiligte [39]. Die industriegetriebene Initiative *Fast Identity Online Alliance* (FIDO) geht noch einen Schritt weiter und propagiert ein vereinfachendes Modell (Abbildung 15) einer nutzerzentrierten Authentifizierung. In diesem Modell wird die Authentifizierung direkt auf dem Nutzergerät als standardisiertes und sicherheitstechnisch akkreditiertes Modul (FIDO-Authentifikator) implementiert, das im Verbund mit einer standardisierten Authentifizierungsanwendung mit entsprechend standardisierten Authentifizierungsdiensten direkt einen privaten sicheren Kanal erstellen und so von einer Vielzahl von vertrauenden Beteiligten direkt genutzt werden kann [25].

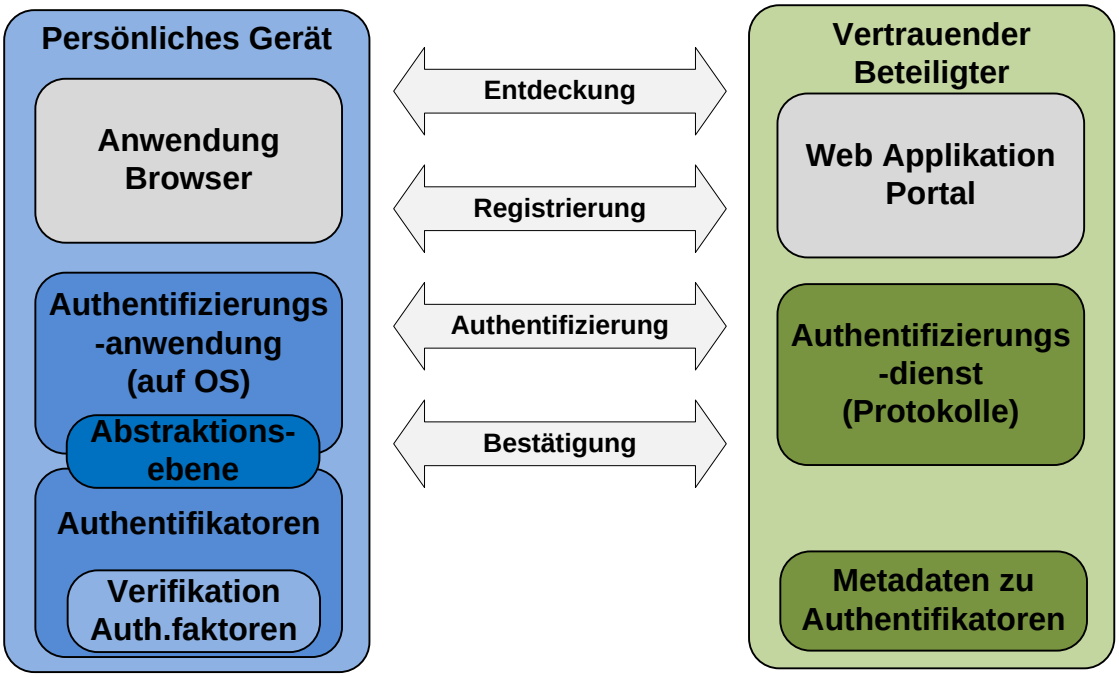

Abbildung 15 – Authentifikation nach FIDO

Ein FIDO-Authentifizierungsdienst eines beliebigen vertrauenden Beteiligten kann mit jedem Gerät mit der installierten FIDO-Authentifizierungsanwendung im Feld die gleichen FIDO-Authentifizierungsprotokolle abwickeln, ohne dass er die genauen Details der Personenverifikation (Überprüfung der erfassten Authentifizierungsfaktoren) auf dem Gerät kennen muss. Bei der Registrierung stellt der Authentifizierungsdienst mit Hilfe der Metadaten zu den Authentifikatoren lediglich fest, auf welchem Sicherheitsniveau die eID eine Authentifikation durchführen kann (Entdeckungsprozess).

Auf der anderen Seite kann die Person ihre Präsenz mit einem einzigen oder mit nur ganz wenigen unterschiedlichen Authentifikationsfaktoren gegenüber einer Vielzahl von unabhängigen vertrauenden Beteiligten ausweisen. Ein FIDO Authentifikator verbindet die Personenverifikation mit einem

Authentifizierungsschlüssel und bezeugt dessen Vertrauenswürdigkeit mit einem Bestätigungszertifikat, das nur ein FIDO akkreditierter Authentifikator haben kann. Eine FIDO Authentifikator liefert dann jedem vertrauenden Beteiligten einen eigenen, durch das Zertifikat bestätigten Schlüssel, der den Aufbau eines sicheren Kanals zwischen Authentifizierungsanwendung und –dienst ermöglicht, über den dann der Nachweis für eine erfolgreiche Verifikation der Authentifizierungsfaktoren der Person übermittelt werden kann. Da jede Verbindung einen neuen und unabhängigen Schlüssel erhält, sind die Kommunikationspartner auch gut gegen MITM Angriffe und Profilierung geschützt. Das Bestätigungszertifikat wird vom Hersteller der eID herausgegeben und enthält alle Angaben zur Stärke der Personenverifikation, der Absicherung im Gerät und der zertifizierenden Stelle (Metadaten).

FIDO ergänzt damit Initiativen (OATH, TCG) und Standards (PKCS#11, ISO 24727, ISO 29115 etc.), die hauptsächlich Eigenschaften von hardwarebasierten Authentifikatoren beschreiben. FIDO ist auch komplementär zu den bekannten Föderationsdiensten und -standards (OpenID, SAML, OAuth), die zum Ziel haben eine erfolgte Authentifizierung via gesicherte Mechanismen zu einer Single Sign On (SSO) Funktion für eine Vielzahl von vertrauenden Beteiligten zu erweitern. Es ist heute nicht klar, ob sich genau die von FIDO vorgeschlagenen Protokolle als Standard etablieren werden, die grundsätzliche Architektur der nutzerzentrierten und interoperablen Authentifizierung ist aber unbestritten [12] [38] [40] [22] [39] [41] und ist damit eine Prämisse für ein zeitgemässes eID Konzept.

10.3.2 Authentifikatoren nach FIDO Spezifikation

Ein FIDO-Authentifikator, schematisch dargestellt in Abbildung 16, ist ein sicheres Modul verankert in einem Nutzergerät, das für jeden vertrauenden Beteiligten unabhängige kryptographische Schlüssel erzeugen und verwalten kann. Die Schlüssel dienen als Ausweis für die Präsenz und korrekte Funktionsweise des Authentifikators. Der Authentifikator hat zudem eine interne Verifikationsfunktion, die feststellt, ob präsentierte Authentifizierungsfaktoren einer Person mit denjenigen übereinstimmen, die bei der Initialisierung abgegeben wurden (Geheimnis, Biometrie). Optional hat ein Authentifikator noch ein sicheres Display für die Anzeige von Transaktionsdaten.

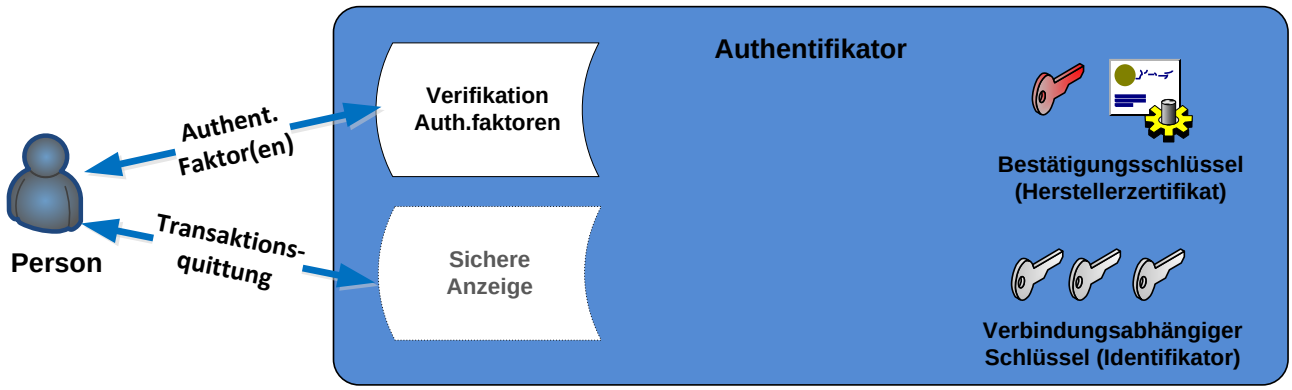

Abbildung 16 – FIDO Authentifikatoren

Die erzeugten Schlüssel erlauben eine sichere und private End-to-End Verbindung zwischen Authentifikator und dem Authentifizierungsdienst beim vertrauenden Beteiligten. Das Bestätigungszertifikat des Herstellers bestätigt dabei dem vertrauenden Beteiligten die Echtheit und den Typ des Authentifikators mit Angaben zur Verifikation der Authentifizierungsfaktoren und der Sicherheit des Authentifikators.

Diese Modellarchitektur für ein nutzerseitiges Authentifizierungsmittel ist heute in zahlreichen Endgeräten implementierbar oder ist in vielen Geräten sogar bereits installiert. Generell muss ein sicherer Authentifikator in der HW des Trägergeräts verankert sein. Beispiele für Geräte bereit für die

Installation eines Authentifikators sind Smartphones mit TEE (Samsung S4, S5, S6, iPhone 6 etc.), Secure Elements (Java Cards, Sticks) oder Computer mit TPM Chip. Authentifikatoren werden typisch direkt vom Hersteller solcher Geräte bereitgestellt und haben im FIDO Modell via einen *Authentifikator Abstraction Layer* standardisierte Schnittstellen, die von beliebigen vertrauenden Beteiligten je unabhängig voneinander angesprochen werden können.

Der wichtigste Unterschied zwischen einem FIDO-Authentifikator und den heute noch oft gebrauchten proprietären Authentifizierungstoken oder -anwendungen ist die Interoperabilität. Dank standardisierten Schnittstellen und Protokollen, kann ein- und derselbe FIDO-Authentifikator von beliebig vielen vertrauenden Beteiligten für die Authentifizierung einer Person gebraucht werden. Wenn sich dieses Konzept durchsetzt, und viele Indizien sprechen dafür [41], darf sich eine eID Lösung dem nicht verschliessen. Mit der Delegation der Herausgabe von eID an die IdP ist eine solche Entwicklung automatisch ins Konzept integriert.

10.3.3 Authentifizierungsniveau

Das Sicherheitsniveau einer Authentifizierung sind in der ISO/IEC Norm 29115:2013 definiert und werden in die vier Vertrauensstufen eingeteilt [33]:

Tabelle 11 – Vertrauensstufen nach ISO 29115

Vertrauensstufe	Beschreibung
1 – Low	Little or no confidence in the asserted identity
2 – Medium	Some confidence in the asserted identity
3 – High	High confidence in the asserted identity
4 – Very high	Very high confidence in the asserted identity

Die eIDAS-Verordnung übernimmt die drei stärkeren Stufen als mögliche Realisierungen für ein notifizierbares eID-System und nennt diese

- „Niedrig“ (entspricht Medium),
- „Substanziell“ (entspricht High),
- „Hoch“ (entspricht Very High).

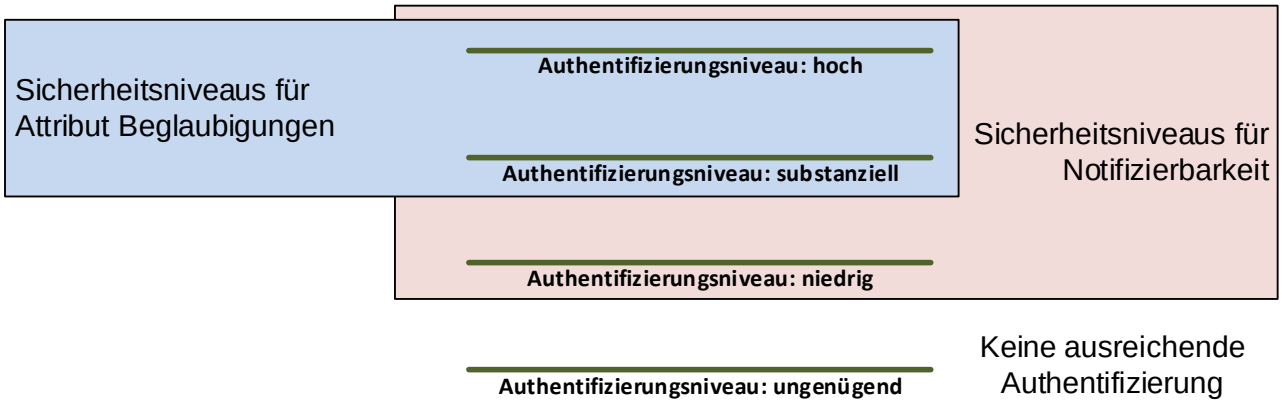

Abbildung 17 – Sicherheitsniveaus der Authentifizierung

Für die Stufen 3 und 4 ist in der ISO Norm zwingend eine Multi-Faktor Authentifizierung vorgeschrieben. Eine schweizerisch staatlich anerkannte eID muss eine Authentifizierung auf dem Si-

cherheitsniveau 3 – „Substanziell“ oder 4 – „Hoch“ ermöglichen. Dies heisst aber nicht, dass mit dem Einsatz der eID immer zwingend eine 2-Faktor Authentifizierung verbunden ist. Situationsabhängig kann ein vertrauender Beteiligter auch eine Authentifizierung auf dem Niveau „Niedrig“ akzeptieren. Für die Registrierung beim staatlichen Registrierungsdienst und für eine Attributbeglaubigung über das ID-Konto ist im schweizerischen eID-System zwingend eine Authentifizierung auf dem Niveau „Substanziell“ vorgeschrieben. Eine Authentifizierung mit PIN und OTP über einen zweiten Kanal, wie sie mit der initialen Authentifizierungsmethode für den Zugang zum ID-Konto definiert ist, entspricht einer starken 2-Faktor Authentifizierung auf dem Sicherheitsniveau „substanziell“. Die Sicherheitsniveaus und ihre Akzeptanzbereich ist in Abbildung 17 dargestellt.

10.4 Einsatz einer eID mit staatlich beglaubigten Identitätsattributen

Ein vertrauender Beteiligter definiert, welches Sicherheitsniveau einer eID für die Authentifikation und die Identifikation für den Zugang zu seinen Mehrwertdiensten akzeptabel ist. Er definiert auch die Art der Nutzung, den Einsatz der eID für die Identifikation bei der Erstregistrierung, den Einsatz als Authentifizierungsmittel bei jeder Anmeldung oder je nach technologischer Ausgestaltung der eID auch den Einsatz des Trägergeräts für weitere Absicherungsdienste. Er betreibt dazu ein Identitäts- und Access Management (IAM) System, das für die Akzeptanz der zugelassenen eID und der vorgesehenen Absicherungsfunktionen konfiguriert ist. In der Regel wird er für die Nutzung einer spezifischen eID eine vertragliche Abmachung mit dem herausgebenden IdP haben. Dies hängt aber von den Geschäftsmodellen der IdP ab und wird durch dieses Konzept nicht tangiert; denkbar sind auch IdP mit General Public License (GPL) Modellen.

Der wohl wichtigste Vorteil für einen vertrauenden Beteiligten ist, dass die technischen Schnittstellen aller staatlich anerkannten eID normiert werden. Somit wird einerseits der Integrationsaufwand für ihn reduziert, andererseits der Authentifikationsvorgang für die anmeldende Person vereinheitlicht. Dies bedeutet in letzter Konsequenz, dass alle staatlich anerkannten eID auf allen Portalen auf die gleiche Art und Weise funktionieren. Es ist also nicht einmal mehr notwendig, je nach eID auf dem Portal einen unterschiedlichen Anmeldebutton zu drücken.

10.4.1 Anwendungsbeispiel

Das oben skizzierte (Fall 1 in Kapitel 4.2.1) Einsatzszenario kann nun mit vorliegendem Konzept noch etwas konkretisiert werden (vergleiche auch Abbildung 18):

Heidi de Maienfeld ist überzeugt, dass eine eID ihre Online-Beziehungen vereinfacht und bestellt deshalb bei ihrem bevorzugten Identitätsdienstleister MyIdP eine eID für ihr neues Smartphone. Sie eröffnet beim MyIdP ein Konto, definiert einen Benutzernamen und gibt ihre Personalien mit Heimadresse und Zahlungsmittel und die Telefonnummer ihres Smartphones an. Sie erhält dann Zugang zum Webstore des MyIdP und kann eine eID Anwendung direkt in den sicheren Bereich des Smartphones herunterladen. MyIdP hat dazu die entsprechenden Sicherheitsmechanismen mit dem Hersteller des Smartphones vorbereitet, so dass die TEE des Smartphones die MyIdP-eID problemlos installiert.

Heidi wird nun aufgefordert in den sicheren Bereich des Smartphones zu wechseln, was sie mit einem Touch auf das Ikon in Form eines Schutzschildes macht. Sie startet die MyIdP-eID App und durchläuft den Initialisierungsprozess. Sie muss dazu nacheinander drei Finger auf den Fingerprintsensor halten und am Schluss zweimal eine selbstgewählte 4-stellige PIN eingeben. Damit ist ihre eID initialisiert.

Die eID Anwendung verbindet sich nun automatisch mit dem Authentifizierungsserver des MyIdP IAM Systems und installiert die Sicherheitsschlüssel für die geschützte Verbindung zwischen der

eID-App in Heidis Smartphone und dem IAM von MyIdP. Sie ist damit beim MyIdP mit ihrem Smartphone als eID Träger registriert.

Sie möchte nun für ihre eID bestätigte Identitätsattribute beziehen. MyIdP verbindet sie mit dem Anmeldeportal des lokalen staatlichen Registrierungsdienstes, wo sie einen Vorsprechtermin für die persönliche Vorsprache auswählen kann. Sie gibt dabei auch die Telefonnummer ihres Smartphones in die Anmeldemaske ein. Sie erhält auf der Seite gleich auch noch die Information, dass der Registrierungsdienst für sie ein ID-Konto beim SID eröffnen wird und dass sie zur Vorsprache ihr Smartphone mit der gemeldeten Telefonnummer mitbringen soll.

Zum vereinbarten Termin meldet sie sich im Empfangsraum der Registrierungsstelle und kann gleich in die Aufnahmekabine gehen, wo sie ihre Unterschrift auf einem Eingabepad malt und ihr Gesichtsbild aufgenommen wird. Anschliessend bekommt sie vom SID ein SMS mit einem Test-OTP. Sie tippt das OTP auf dem dafür vorgesehenen Keypad ein und bestätigt damit, dass die früher angegebene Nummer richtig ist und zu ihrem Smartphone gehört.

Sie erhält umgehend den Benutzernamen und die PIN in einem Brief zugestellt und kann sich danach in ihrem ID-Konto einloggen. Sie meldet sich auf dem SID Webportal bei ihrem ID-Konto mit der ID-Kontonummer an, authentifiziert sich mit der PIN und erhält auf ihrem Smartphone per SMS das OTP, das sie als zweiten Authentifizierungsfaktor ebenfalls eintippen muss.

Eingeloggt in ihrem ID-Konto kann sie die erfassten Attribute ansehen und ihre MyIdP-eID als zukünftiges Authentifizierungsmittel registrieren. Sie wird dazu automatisch mit dem MyIdP Portal verbunden und authentifiziert sich als MyIdP-eID Inhaberin. Im Hintergrund sendet danach der MyIdP Server alle notwendigen Informationen, damit die MyIdP-eID von Heidi registriert und in Zukunft für den Zugang zum ID-Konto gebraucht werden kann. Mit dieser Registration wird die MyIdP-eID zum primären Authentifizierungsmittel für ihr ID-Konto.

Heidi verlangt nun noch staatliche Beglaubigungen für ihren Namen, Nationalität, Geburtsdatum und die beiden Bilder (Gesichtsbild, Unterschriftsbild), die ihrem MyIdP gesendet werden sollen. Sie bekommt eine Meldung auf die Anzeige des MyIdP-eID auf ihrem Smartphone mit der Quittung für die gewählten Attribute zusammen mit einem OTP, das sie als Auftragsbestätigung im entsprechenden Antwortfeld des MyIdP-eID Client auf ihrem Smartphone eintippt.

Der SID Siegeldienst erstellt für jedes der gewählten Attribute eine Beglaubigung und schickt diese mit dem Beglaubigung Identifikator, der vom MyIdP vorgängig zusammen mit den Daten für die Registrierung der MyIdP-eID geschickt wurde, an den MyIdP zu. Der MyIdP registriert die Daten in seinem IAM und kann nun für Heidi Attributbestätigungen für die beglaubigten Attribute ausstellen.

Heidi geht dann auf die Webseite des Telecom Operators und bestellt eine weitere SIM Karte, da sie eine zweite Telefonnummer möchte. Sie registriert auf ihrem Konto beim Telecom Operator ihre MyIdP-eID und kann sich ab sofort über ihren MyIdP Föderationsdienst authentifizieren. Das lästige erinnern an Benutzernamen und Passwort entfällt. Sie beauftragt nun noch ihren MyIdP dem Telecom Operator die nötigen staatlich beglaubigten Attribute für den Bezug der SIM Karte zu senden und dieser übermittelt die entsprechende Bestätigungsdatei an den Telekom Operator. Aus Compliance Gründen verlangt dieser eine Verifikation der Bestätigung vom MyIdP und verbindet sich mit dem Validierungsdienst des MyIdP IAM-Systems. Dieses überprüft das Zertifikat und validiert die Bestätigung für den Telecom Operator. Nach erfolgter Validierung der Attributbestätigung erhält Heidi die SIM-Karte per Post zugestellt.

Der gesamte eben in Form eines Anwendungsfalls beschriebene Vorbereitungsprozess bis zur operativen Bereitschaft der eID für den wiederholten Zugang zu einem vBt ist in Abbildung 18 dargestellt. Heidi de Maienfeld möchte zusätzlich ein neues Bankkonto eröffnen. Die Bank muss dabei der Regulierung entsprechend die Identität und Staatsangehörigkeit des Neukunden prüfen. Heute muss sich ein Neukunde persönlich am Schalter melden und originale Identitätspapiere vorweisen, die dann in kopierter Form abgelegt werden. Es braucht dann weitere 1-7 Tage bis der Kunde das

Konto nutzen kann. Mit bestätigten Attributen wird dieser Prozess vereinfacht und beschleunigt. Heidi de Maienfeld meldet sich nun für die Kontoeröffnung über den Browser ihres Smartphones beim Onlineportal der Bank an und füllt ein Onlineformular mit den verlangten Angaben zur Eröffnung des Kontos aus. Das bankeigene IAM-System verlangt von ihr nun die staatlich garantierte Bestätigung der gemeldeten zivilen Identitätsattribute. Sie bestellt die verlangte Bestätigung direkt aus der Applikation bei ihrem MyIdP, wobei sie sich natürlich mit ihrer eID authentifizieren muss. Dieser sendet die Bestätigung dann an die Bank. Diese überprüft die Echtheit und Authentizität der Bestätigung in gleicher Weise wie der Telekom Operator (vergleiche auch Abbildung 19).

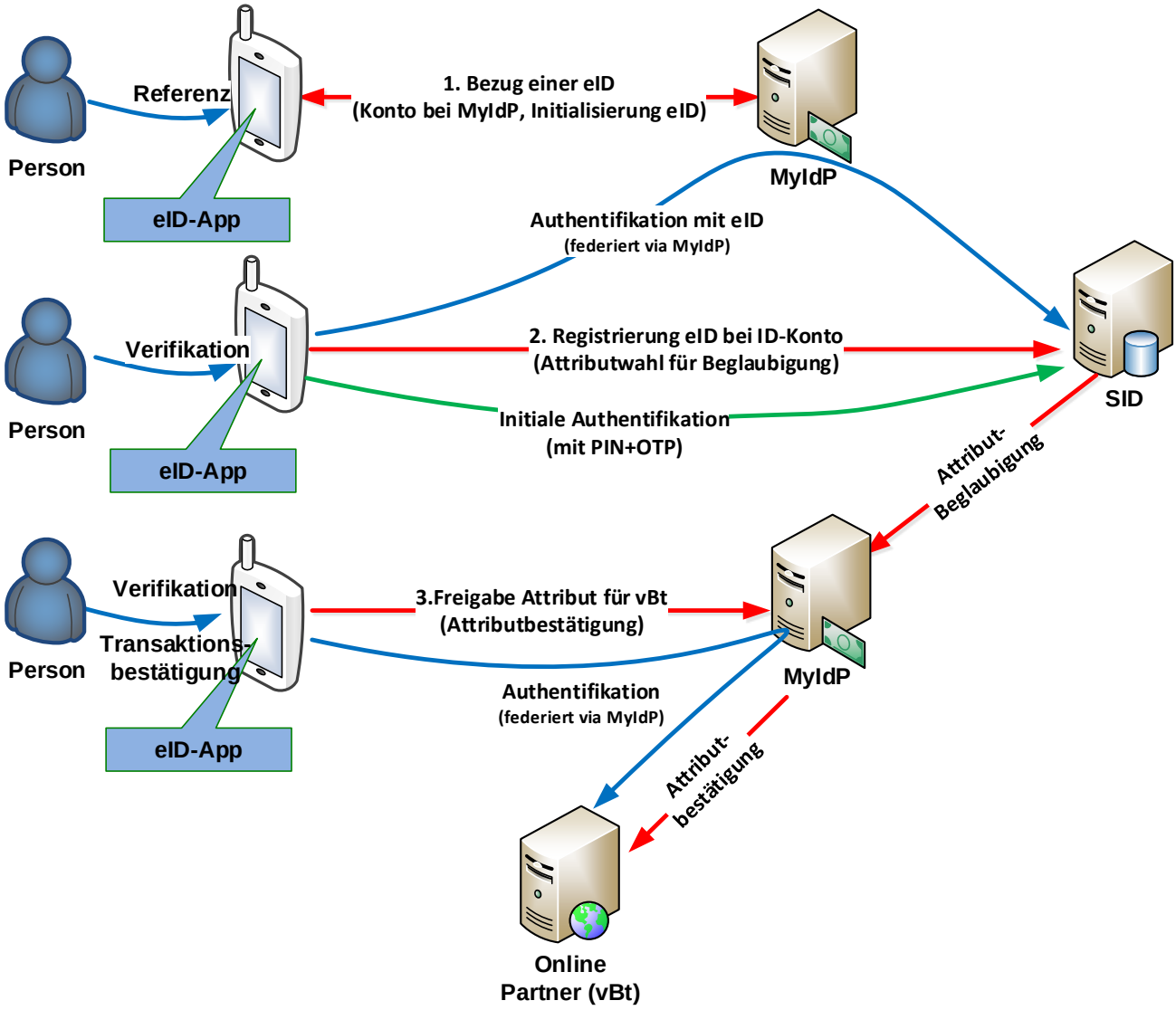

Abbildung 18 – Drei Schritte bis zur Einsatzbereitschaft der eID

Das Konto ist damit eröffnet und Transaktionen können sofort ausgeführt werden. Die Bank kann für das Online-Banking über dieses Konto sogar noch die MyIdP-eID als Authentifikationsmittel brauchen. Sie muss dazu lediglich eine Registrierung der eID auf ihrem Authentifikationsserver durchführen, wobei eigene Schlüssel und Credentials definiert werden können, da die MyIdP-eID die Interoperabilität gemäss den FIDO Spezifikationen erlaubt.

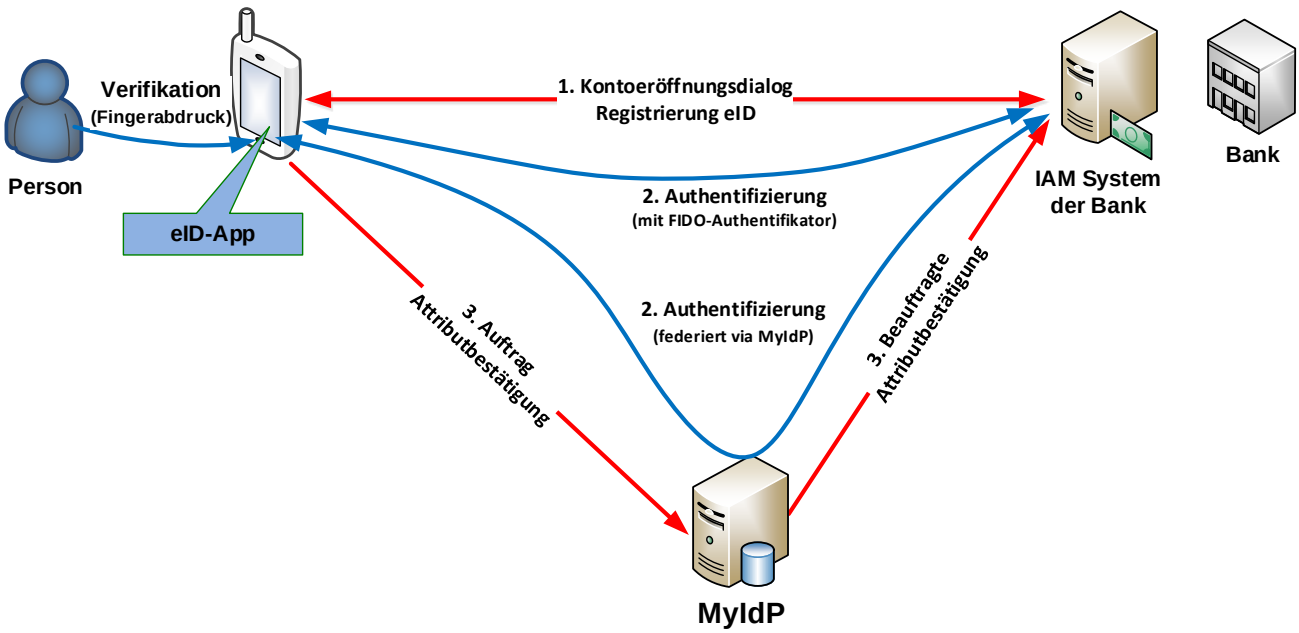

Abbildung 19 – Einsatz der eID bei vertrauendem Beteiligten (z.B. Bank)

Legende: Beispiel für Eröffnung eines Kontos für eine identitätsbasierte Dienstleistung bei einem vertrauenden Beteiligten wie zum Beispiel einer Bank (Abbildung 19).

1) Anmeldung beim Onlineportal des vBt (Bank) und Durchführung des Kontoeröffnungsdialogs. Teil dieses Dialogs ist die Registrierung der eID (Erfassung eines Identifikators für die eID und Festlegung der Authentifikationsmethode: direkte Nutzung der eID als Authentifikationsmittel oder föderierte Authentifikation durchgeführt vom MyIdP mit Authentifizierungsbestätigung des Authentifikationsservers von MyIdP)

2) Authentifizierung der Person mit der eID und der definierten Authentifikationsmethode;

3) Übermittlung von staatlich beglaubigten Attributen in einer vom MyIdP signierten Attributbestätigung; die Bestätigung kann von der Person direkt in Form einer Bestätigungsdatei (Voraussetzung: Bestätigung ist via eindeutigem Identifikator an eID gebunden) oder via Auftrag an den MyIdP geliefert werden.

11 Literaturverzeichnis

[1] EU Parlament, „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," 28. August 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&qid=1422521123960&from=EN. [Zugriff am 12. April 2015].

[2] 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].

[3] 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].

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

[5] EU, „STORK," 2015. [Online]. Available: https://www.eid-stork.eu/. [Zugriff am 12. April 2015].

[6] 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].

[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] 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].

[9] D. Hühnlein, „Identitätsmanagement-eine visualisierte Begriffsbestimmung," *Datenschutz und Datensicherheit, Heft 3,* p. 163, 2008.

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

[11] Schweizer Bundesrat, „Bundesratsbeschluss zur Ausarbeitung eines Gesetzgebungspaketes zur Förderung des elektronischen Geschäftsverkehrs," 19. Dezember 2012. [Online].

[12] 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].

[13] 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].

[14] SuisseID, „SuisseID," 2015. [Online]. Available: http://www.suisseid.ch/de. [Zugriff am 12. April 2015].

[15] „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].

[16] J. Fromm und et al., „3-Jahre Online Ausweisfunktion – Lessons Learned," *Fraunhofer Fokus,* Oktober 2013.

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

[18] 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].

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

[20] 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.

[21] 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].

[22] 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].

[23] 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].

[24] 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].

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

[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] 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].

[28] SkIDentity, „eID-Integration aus der Cloud," 2015. [Online]. Available: www.skidentity.de. [Zugriff am 09. Mai 2015].

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

[30] 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].

[31] I. 1. Standard, „Common Criteria for Information Technology Security Evaluation".

[32] R. Dholakia, „A question of Scale," NokNok Labs, 2012.

[33] 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].

[34] 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].

[35] 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].

[36] „eID-Integration aus der Cloud," 2015. [Online]. Available: www.skidentity.de. [Zugriff am 12. April 2015].

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

[38] 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].

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

[40] 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].

[41] D. O'Shea, „Fido U2F & UAF Tutorial," in *World e-ID Congress, Marseille 2014*, Marseille, 2014.

[42] 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].

[43] 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].

[44] 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].

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