eID-Ökosystem Modell

Projektabschlussbericht

Version 1.1, Juni 2015

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Staatssekretariat für Wirtschaft SECO
Direktion für Standortförderung

Impressum

Herausgeber

Berner Fachhochschule im Auftrag von:

Staatssekretariat für Wirtschaft SECO, Direktion für Standortförderung, Ressort KMU-Politik

Projektleitung SECO

Christian Weber

Mitwirkende Berner Fachhochschule

Ronny Bernold
Oliver Brian (Projektleiter)
Jérome Brugger
Angelina Dungga Winterleitner
Marianne Fraefel
Roman Hosang
Prof. Dr. Reinhard Riedl (Projektverantwortlicher)
Thomas Selzam (Stv. Projektleiter)
Prof. Dr. Konrad Walser
Katinka Weissenfeld

Adresse

Berner Fachhochschule
Fachbereich Wirtschaft
E-Government-Institut
Brückenstrasse 73
CH-3005 Bern
Tel. +41 31 848 34 00
Fax +41 31 848 34 01
wirtschaft@bfh.ch
www.wirtschaft.bfh.ch

Berner
Fachhochschule

Inhaltsverzeichnis

Management Summary

Ein soziotechnisches Ökosystem rund um die nationale eID ist vielfältig und voller komplexer Abhängigkeiten zwischen seinen Elementen. Der Erfolg in Form von tatsächlicher Nutzung der nationalen eID oder davon abgeleiteter eIDs hängt vom Zusammenspiel vieler verschiedener Instanzen und Akteure ab. Der Vergleich mit dem Ausland zeigt: Einige Staaten waren mit der Lancierung ihrer eID erfolgreich, weil sie eine dafür günstige Ausgangssituation vorfanden und ziemlich viel richtig machten. Andere Staaten waren erfolglos. In beiden Fällen erwiesen sich der organisatorische Aufbau und die konkrete Gestaltung der Vertrauensdienste als wesentlich entscheidender, als das rein technische Design. Das technische Design und das Design der Ausgabeprozesse können anhand existierender bzw. gerade in Finalisierung befindlicher Qualitätsstandards beurteilt werden. Für den grösseren organisatorischen Aufbau gibt es bislang keine Evaluationswerkzeuge. Der einzige, internationale Referenzrahmen ist das eIDAS (EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) zugrundeliegende Begriffssystem für die Vertrauensdienste.

Im Rahmen dieses Projektes hat das E-Government-Institut der Berner Fachhochschule deshalb ein Modell für das eID-Ökosystem entwickelt, das die Zusammenhänge zwischen seinen Bereichen und Elementen abbildet und die Diskussion über Fördermassnahmen und über die Zusammenarbeit zwischen Staat und Wirtschaft erleichtert. Das Modell ist eine geeignete Referenz-Basis für sachlich differenzierte Strategie- und Einführungs-Diskussionen. Es ist darauf ausgerichtet, sowohl von Fachexperten für das Thema eID als auch von Geschäftsverantwortlichen in der Wirtschaft, Entscheidungsträgern in der Verwaltung und Entscheidungsträgern in der Politik genutzt zu werden. Eine besondere Qualität des Modells ist, dass es nicht die Darstellung eines IST- und SOLL-Zustands präsentiert, sondern alle sinnvoll möglichen Elemente umfasst. Daraus können konkrete SOLL-Zustände abgeleitet und miteinander verglichen werden.

Die Validierung des Modells in zwei Dutzend Interviews und in zwei Halbtagesworkshops ergab, dass es tatsächlich die Fachdiskussionen gut zu strukturieren vermag, dass es hilft, die Präzision in den Diskussionen zu erhöhen und Missverständnisse zu verringern und dass es auch in grösseren Gruppen eine Konsensfindung fördert. Sowohl Auslegeordnung als auch Ausgestaltung des Modells wurden von den Experten als sehr geeignet beurteilt. Kleine Verbesserungsvorschläge sind in der hier vorgelegten endgültigen Version bereits berücksichtigt.

In den beiden Halbtagesworkshops wurde basierend auf der Public Value Theorie insbesondere der Stakeholder-spezifische Nutzen zweier Instanziierungen des Modells identifiziert. Die Ergebnisse wurden dazu verwendet, konkrete Empfehlungen für die Förderung der Entwicklung des eID-Ökosystems abzuleiten. Führt man diese Empfehlungen mit den in den Validierungsinterviews herausgearbeiteten Perspektiven zusammen, und reflektiert das resultierende Meinungsbild, so sind es vor allem zwei Dinge, die über den Erfolg einer nationalen eID entscheiden werden: Viel mehr und viel bessere Kommunikation und eine gegenüber dem heutigen Zustand stark verbesserte Zusammenarbeit der wichtigen Akteure.

Bei der Validierung des Modells zeigte sich teilweise sehr drastisch, dass die Perspektiven auf das Thema sehr divergieren – sowohl bezüglich der relativen Wichtigkeit der einzelnen Vertrauensdienste und ihres Designs als auch bezüglich der relativen Wichtigkeit der Gestaltungsmöglichkeiten und der Nutzenarten. In der bisherigen Diskussion führte das meist dazu, dass jeder Versuch einer Strategiediskussion durch entstehende, häufig disparate Detaildiskussionen blockiert wurde. Selbst wenn scheinbar alle vom Gleichen sprechen, sind die oft unausgesprochenen Einschätzungen diametral entgegengesetzt, weil das Gleiche meist nicht Dasselbe ist. Mit dem hier vorgelegten eID-Ökosystem Modell verbessert sich die Situation grundlegend. Damit es seine Wirkung entfalten kann, muss es aber auch aktiv für die Kommunikation der Zusammenhänge und Abhängigkeiten im eID-Ökosystem genutzt werden.

1. Einleitung

1.1 Kontext

Die Ausgangslage für den vorliegenden Bericht stellt der Auftrag des Bundesrates zur Anpassung des Schweizerischen Pass und der Identitätskarte (IDK) bis Ende 2016 an das Eidgenössische Justiz- und Polizeidepartement (EJPD) dar [1]. Mit der IDK soll auch die Möglichkeit angeboten werden, auf einem Chip elektronisch gespeicherte biometrische Daten und eID-Funktionalitäten zu integrieren. Diese neuen Funktionen erfordern, neben einer umsichtigen technischen Umsetzung, auch die Konzeption eines umfassenden „Identitäts-Ökosystems". Die eID in der IDK ist nur eine Komponente im gesamten Ökosystem und muss für eine erfolgreiche Einführung durch weitere Infrastrukturen und entsprechende Dienste ergänzt werden. Die eID kann nur dann nutzenbringend eingesetzt werden, wenn auch entsprechende Umsysteme zur Verfügung stehen. Dies kann teilweise der Privatwirtschaft überlassen werden, jedoch braucht es eine starke Rolle des Staates, insbesondere in der übergeordneten Koordination und Kommunikation.

Neben diesem Bundesratsauftrag basiert das Projekt auf Workshops, die Ende 2013 und Anfang 2014 vom Bundesamt für Polizei fedpol organisiert wurden. Erste Erkenntnisse wurden in einem Bericht[1] von der Berner Fachhochschule (BFH) an das SECO festgehalten. Aussagen aus diesen Workshops dienten als Grundlage im Projekt und wurden in unabhängigen Interviews und Workshops bekräftigt.

Das Projekt eID-Ökosystem Modell, dessen Abschlussbericht hiermit vorliegt, startete im Oktober 2014 und endete im Mai 2015. Parallel zu diesem Projekt hat der Bundesrat das EJPD beauftragt, ein Konzept und einen Entwurf für die rechtliche Ausgestaltung des künftigen staatlichen elektronischen Identifikationsmittels (eID), das zusammen mit der neuen Identitätskarte angeboten wird, auszuarbeiten. Es fand ein Austausch zwischen den beiden Projekten statt, jedoch lag das Konzept des fedpol erst nach den Public Value Workshops und kurz vor Projektende vor und konnte somit nicht abgestimmt werden. Zurzeit läuft die Informelle Konsultation des Konzeptes des EJPD[2].

Internationale Aspekte wurden aufgrund der verfügbaren Informationen in die Entwicklung des Modells miteinbezogen. Aufgrund der unterschiedlichen Ausgangslage anderer eID Entwicklungen und politischer und struktureller Gegebenheiten können die Modelle aus dem Ausland nicht direkt übernommen werden. Die ausländischen Ökosysteme, die innerhalb des Projekts betrachtet wurden, sind im Kapitel 2.2 beschrieben. In diesem Kontext wurde ein eID-Ökosystem Modell entwickelt, Interviews geführt und zwei Public Value Workshops durchgeführt.

[1] eID Schweiz – Anforderungen an die Ökosystem Modellierung und erste System-Sichten [6]

[2] Informelle Konsultation: http://www.schweizerpass.admin.ch/pass/de/home/aktuell/konsultation.html

1.2 Ziele und Anforderungen

Das Ziel dieses Projekts ist es ein umfassendes eID-Ökosystem Modell für das Eidgenössische Departement für Wirtschaft, Bildung und Forschung WBF und darin insbesondere für das Staatssekretariat für Wirtschaft SECO zu entwickeln. Dieses Modell soll eine strategische Planung für ein eID-Ökosystem ermöglichen und mögliche Ausgestaltungen der eID vergleichbar machen.

Zu Beginn des Projekts wurden, in Absprache mit dem Auftraggeber, die Nutzung und die Nutzer des Ökosystem Modells sowie vier Nutzungsszenarien definiert.

Nutzung

Innerhalb eines BFH-internen Workshops wurde im Zusammenhang mit dem eID-Ökosystem Modell folgende Nutzung identifiziert.

Das eID-Ökosystem:

- Gibt eine Gesamtübersicht, die Abhängigkeiten aufzeigt: Daraus resultiert eine Diskussionsgrundlage, um Aktivitäten von Stakeholdern aufzuzeigen,
- ermöglicht Impact Assessment (Wirkungsanalyse),
- zeigt langfristige Entwicklungsperspektive (Modellierung) auf,
- bildet die Design Grundlage für die Schweizer eID und eIDK und ermöglicht diese national und international interoperabel zu gestalten,
- ermöglicht allen Stakeholdern sich und ihre bestehenden wie künftigen Lösungen im Kontext eID Schweiz einzuordnen und
- erleichtert Wirkungszusammenhänge zu erkennen und Massnahmen abzuleiten.

Dabei wurde konkret von der Nutzung des Ökosystems Modells ausgegangen und nicht vom Nutzen eines möglichen Produkts, das sich im Ökosystem befindet.

Nutzungsszenarien

Aus der obigen Nutzung wurden anschliessend die vier Nutzungsszenarien ableitet:

- **Fachexperten** aus dem Bereich eID
- Vertreter von **Lösungsprovidern** im Bereich IAM, die Dienste und Lösungen mit grossem Impact im Scope des eID-Ökosystems potentiell anbieten können oder bereits anbieten
- **Bundesämter,** welche Identity und Access Management (IAM) im Kerngeschäft betreiben oder zentrale Interessen darin haben; alle weiteren Bundesämter in einer erweiterten Runde
- **Politische Akteure** im politischen Prozess
    - Bundesrat
    - Beratende Stellen im Mitberichtsverfahren
    - Adressaten der Vernehmlassung
    - Parlament, insbesondere die Opinion Leader in den Fraktionen (u.a. die Mitglieder der e-Power-Initiative) und Lobbyisten im Themenfeld

- Medienvertreter, die im Rahmen der Parlamentsdebatte über das Thema berichten.

Die detaillierte Beschreibung dieser vier Nutzungsszenarien des eID-Ökosystem Modells ist im Anhang 2 zu finden.

Als weitere Anforderung im Projekt galt es, das Modell mit den relevanten Stakeholdern abzustimmen. Um das eID-Ökosystem erfolgreich aufzubauen, ist eine breite Akzeptanz zwingend notwendig.

1.3 Begriffsdefinition

In diesem Dokument werden folgende Begriffe mit folgender Bedeutung verwendet:

Begriff	**Definition**
Anwendungsfall	Dies ist eine Beschreibung von Anwendungsfällen der eID, die eine Nutzung der eID und damit von entsprechenden eID-Funktionen voraussetzen. Anwendungsfälle werden im Modell (Vgl. dazu die Abbildung 4: eID-Ökosystem Modell Grundbereiche) auf der linken Seite exemplarisch beschrieben.
eHealth	Unter dem Begriff «eHealth» werden elektronische Gesundheitsdienste zusammengefasst: Mit elektronischen Mitteln werden im Gesundheitswesen die Abläufe verbessert und die Beteiligten vernetzt. [2]
eID-Ökosystem	Das Schweizer eID-Ökosystem ist eine schematische Darstellung der Vernetzung von Entitäten (Stakeholdern und Elementen). Es beschreibt Interaktionen und Interdependenzen (politisch, rechtlich, institutionell, organisatorisch, semantisch, technisch), aus denen mögliche Entscheidungspunkte und Entwicklungsrichtungen abgeleitet werden können.
eID-Ökosystem Modell	Dabei handelt es sich um ein abstraktes Modell des Schweizer eID-Ökosystems, das vom E-Government-Institut (EGI) der BFH entwickelt wurde.
Identitätskarte (IDK)	Ausweise dienen der Inhaberin oder dem Inhaber zum Nachweis der Schweizer Staatsangehörigkeit und der eigenen Identität. Alle Schweizer Staatsangehörigen haben gemäss Ausweisgesetz Anspruch auf einen Ausweis je Ausweisart, also auf einen Pass (Pass 10 oder provisorischer Pass) und eine Identitätskarte. [1]
Instanziierung	Eine Instanziierung stellt eine mögliche Ausprägung des Modells dar.
Modell	Ein Modell ist ein abstrahiertes Abbild einer existierenden oder noch zu schaffenden Realität [3]

Nutzungsszenario	Ein Nutzungsszenario stellt die Nutzung des eID -Ökosystem Modells als Werkzeug für unterschiedliche Akteure dar.
Relying Party (RP)	Die Relying Party vertritt die Interessen der Ressource, auf die elektronisch zugegriffen werden soll. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von IAM-Dienstanbietern für den Schutz seiner Ressourcen. Sie braucht zur Beurteilung der Berechtigung eines (elektronischen) Ressourcenzugriffs nähere Informationen zu einem Subjekt. [4]
Qualitätsstufe	Qualitätsstufen aus dem eID-Qualitätsmodell (QM) dienen der Bewertung und Einstufung elektronischer Identitäten. [5]

Tabelle 1: Begriffsdefinitionen

2. Projektgrundlagen

2.1 Methodisches Vorgehen im Projekt

Aus Sicht des methodischen Vorgehens baut die vorliegende Entwicklung und Validierung eines eID-Ökosystems auf diversen Vorarbeiten, Workshops und Erkenntnissen aus der Literatur auf. Unter der Leitung der BFH fanden zwei Workshops zum Thema „eID Schweiz – Anforderungen an die Ökosystem Modellierung und erste Systemsichten“ [6] statt.

Zudem war das EGI der BFH mit der eCH-Fachgruppe IAM und im Priorisierten Vorhaben *B2.06 E-Government Schweiz* in die Entwicklung diverser eCH-Standards für eine föderierte IAM-Lösung für den breiten Einsatz in der E-Society involviert. Das Konzept trägt die Bezeichnung SuisseTrustIAM (STIAM).[3]

Grundsätzlich wurde ein qualitatives und iteratives Vorgehen gewählt, theoriebasiert und deduktiv. Das Vorhaben lässt sich in die oben geschilderte langfristige Entwicklung von Standards innerhalb von eCH und die Arbeit im priorisierten Vorhaben B2.06 einordnen und stellt in dieser Entwicklungslinie einen weiteren zentralen Meilenstein für die Implementierung einer erfolgreich nutzbaren elektronischen Identität dar. Aktuell läuft beim SECO das Projekt Identitätsverbund Schweiz Dessen Ziel ist es, einen schweizweiten Verbund von Identitäts- und Authentisierungsdiensten aufzubauen[4].

Konkret erfolgte zunächst eine Literaturstudie, im Rahmen derer Begriffsdefinitionen zum eID-Ökosystem erarbeitet wurden. Danach erfolgte, u.a. auf Basis der Arbeiten an den eCH-Standards Modellentwicklung. Anschliessend wurde dieses Modell für eine qualitative Umfrage bei knapp zwei Dutzend unterschiedlichen Stakeholdern aus allen Bereichen der E-Society in einen Interview-Fragebogen gefasst (Vgl. hierzu Anhang 2).

Die Entwicklung des eID-Ökosystems erfolgte von der Idee bis zum abschliessenden eID-Ökosystem Modell über iterative Zwischenschritte auch zur Verifizierung und zur Fokussierung des Modells. Dies hatte auch Konsequenzen für den in Anhang 2 aufgeführten Fragebogen. Die Befragung erfolgte durch unterschiedliche Personen des Projektteams (EGI-intern) und die Interviews wurden elektronisch aufgezeichnet und protokolliert. Die Analyse der Transkripte erfolgte durch andere Personen als die Durchführung der Interviews und deren Transkriptionen. Dadurch konnte eine Triangulation sichergestellt werden, was zur Validität und Reliabilität der Untersuchung beitrug. Das thematische „Taging“ der Transkripte auf Basis des Inhaltsanalyse-Werkzeugs Atlas-TI erfolgte wiederum durch andere Personen als die Auswertung zuhanden des

[3] Vgl. dazu auf www.ech.ch die Standards wie folgt: eCH-0107, eCH-0167, eCH-0168, eCH-0169, eCH-0170, eCH-0171, eCH-0172 sowie eCH-0174.

[4] Vgl. http://www.egovernment.ch/b206/index.html?lang=de

vorliegenden Schlussberichts. Dies sorgte für eine weitere Triangulation und verleiht den daraus resultierenden Schlussfolgerungen damit noch weitergehende Objektivität.

Ausgehend von den derart erarbeiteten Resultaten zum Modell wurde in zwei Szenarien je eine vierstufige Workshop-Runde unter Zuhilfenahme der Public-Value-Theorie[5] durchgeführt. Teilnehmer der Workshops waren neben dem Auftraggeber einige der zuvor im Rahmen der Interviews befragten Personen, aber auch weitere Rollenträger innerhalb der E-Society. Dies führte zu einer weiteren Validierung des eID-Ökosystems sowie zu weiteren Konkretisierungen insbesondere zu den Instanziierungen einer eID im eID-Ökosystem. Aufgrund des geschilderten Vorgehens konnten valide Ergebnisse zur Berücksichtigung im eID-Verbund Schweiz erarbeitet werden.

Insgesamt gingen in die Entwicklung des eID-Ökosystems, anhand dessen die erfolgreiche Einführung einer eID in der Schweiz evaluiert werden soll, die Einarbeitung der verschiedenen Vorprojekterfahrungen und Standardisierungserfahrungen ein. Zentral war aber die Entwicklung von Fördermassnahmen für eine erfolgreiche Einführung einer eID im Identitätsraum Schweiz.

Innerhalb des Forschungsfeldes Virtuelle Identität am EGI der BFH wurde das Projekt auf Basis eines stark diskursiven Verfahrens in internen Workshops vorangetrieben. Basierend darauf wurden auch die Erfolgsfaktoren und die Erarbeitung der Public Value Bereiche sowie die Instanziierungen des eID-Ökosystems entwickelt.

2.2 Stand des Wissens und Literaturstudie

Der von Herbert Kubicek herausgegebene Sammelband [7] bietet einerseits theoretische Grundlagen und andererseits Fallstudien zu eID Einführungen in ausgewählten EU-Ländern an. Letztere zeigen, wie dort eIDs lanciert und genutzt wurden. Dies scheint wesentlich, da über die Fallstudien ganz unterschiedliche Arten von Implementierungen präsentiert werden, die in Teilen oder insgesamt für die Schweiz eine wesentliche Rolle spielen können. Es werden die Fallstudien Spanien, Österreich, Belgien, Deutschland, Dänemark, Finnland, Schweden sowie Estland präsentiert. Die Studie arbeitet grosse Unterschiede insbesondere bei der Realisierung von eIDs heraus. Ebenfalls sehr unterschiedlich fiel die Sicht auf das Angebot der eID aus, staatlich versus privat. Kubicek präsentiert zum besseren Verständnis ein magisches Dreieck für eID-Systeme (vgl. hierzu die folgende Abbildung). Die darin gezeigten Ziele sind teilweise konfliktär und dominieren heute die Diskussion rund um das Angebot von eIDs.

[5] Vgl. zum Public Value Konzept [26] [27].

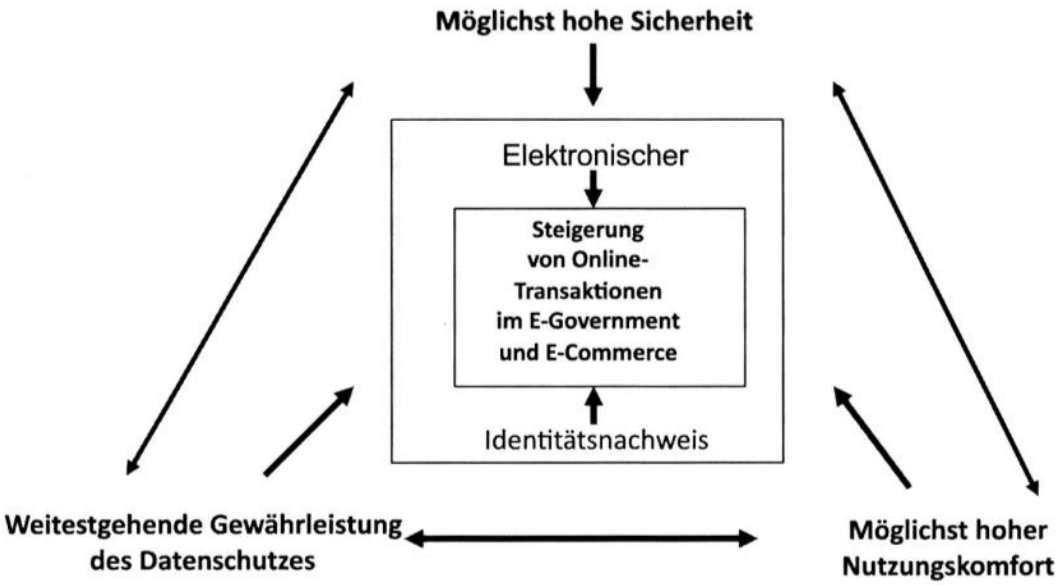


Abbildung 1: Das magische Dreieck zu elektronischen Identitäten [8]

Dies sind zentrale Bedingungen für die Akzeptanz einer eID bei Nutzern und Anwendern. Die bisherigen Ansätze, Online-Transaktionen technisch sicherer zu gestalten, sind überwiegend mit einer Verringerung des Nutzerkomforts im Sinne möglichst einfacher Nutzung verbunden (Beispiel: Die geringe Akzeptanz qualifizierter elektronischer Signaturen).

Stevens et al. [9] beschäftigten sich mit der Modellierung eines eID-Ökosystems. Dieses ist eher Stakeholder-orientiert. Dennoch bietet es eine interessante Ausgangslage für den vorliegenden Bericht, insbesondere weil wertschöpfungsorientiert in unterschiedlichen Kontexten Stakeholder und deren Zusammenspiel in Grossbritannien thematisiert werden. Eine mögliche Differenzierung der Stakeholder geht u.a. den Dimensionen Policy, Regulation, Exploitation, Infrastructure, Technologies, Support einher. Diese Dimensionen gingen in die Entwicklung des vorliegenden eID-Ökosystems ein. Auch der Support im Sinne einer (eID-)Serviceorganisation wird thematisiert. Auch dies scheint für eine erfolgreiche Implementierung einer eID ein wesentlicher Faktor zu sein. Im Rahmen u.a. erster Geschäftsmodelle für den eID-Betrieb wird die Nutzengenerierung innerhalb der verschiedenen Dimensionen diskutiert.

Ein weiterer wesentlicher Beitrag, der eID-Ökosystem-Charakter hat, ist der Beitrag von Lusoli und Compañó [10]. Miteinbezogen in diese Studie des eID-Marktes werden soziale, technische und regulatorische Sichten. Überdies werden die daraus sich ergebenden Opportunitäten und Herausforderungen für Policy Maker im eID-Umfeld analysiert und präsentiert. So stellt sich die Frage, ob ein einziger Europäischer Markt für eine eID realistisch ist. Dies ist ja die Vision wie sie z.B. STORK 2.0 zu realisieren versucht. Dies wird nicht einfach sein. Das zeigen ja schon die in Kubicek's Sammelband herausgearbeiteten Unterschiede über die acht EU-Länder hinweg. Gleiches in leicht anderer Lesart lässt sich für die stark föderale Schweiz diskutieren. Die Autoren kommen zum Schluss, dass die Nutzenvorstellungen zwischen Anbietern und Nutzern unterschiedlich sind. Das macht den Erfolg einer eID so schwer erreichbar. Der Beitrag zeigt auch die

Barrieren des Privacy-by-Design-Ansatzes auf. In der Studie wird ein Marktsystem mit den Ebenen Regulation, Applikationen, Infrastrukturen und Technologien propagiert (Vgl. Abbildung 2), über welches diverse Policy-Herausforderungen für eID-Ökosysteme adressierbar sind.

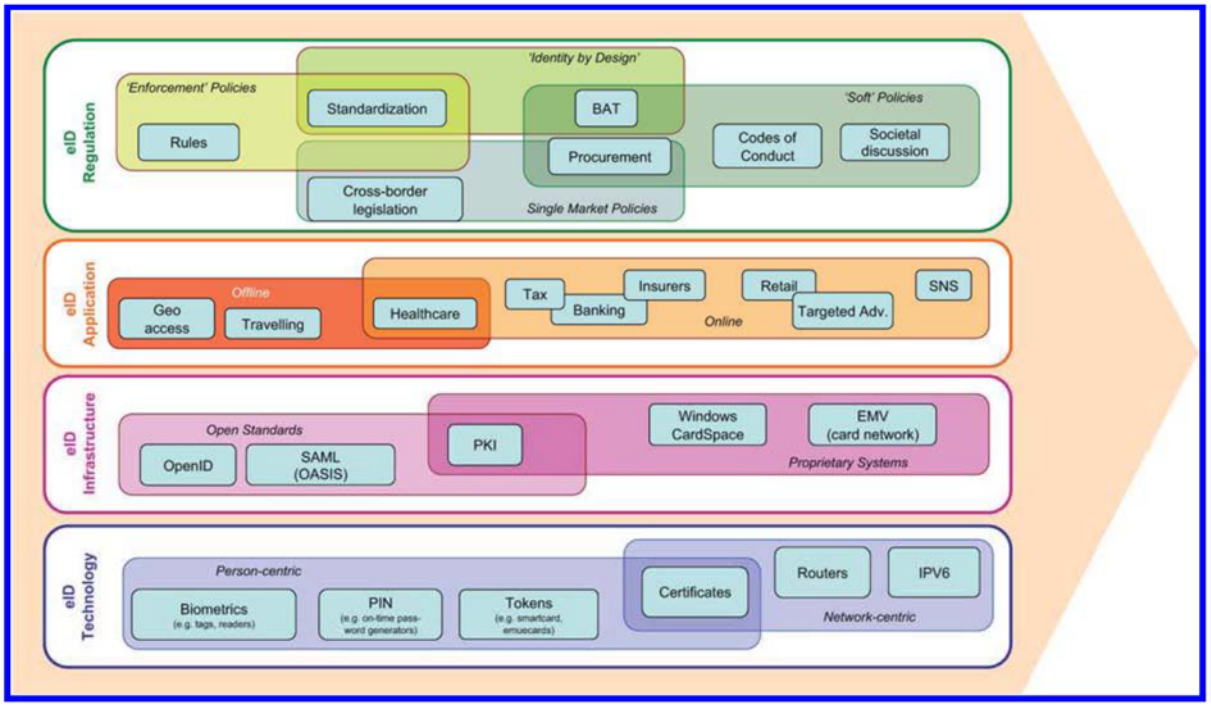


Abbildung 2: eID-Ökosystem für das Design von eID-Policies nach Lusoli/Compañó [10]

Eine gute Zusammenfassung der deutschen Diskussion zur Elektronischen Identität gibt das entsprechende White Papier von ISPRAT zum Identity Management wieder [11]. Der Themenbereich Elektronisches Identitätsmanagement – Nutzen und Notwendigkeit wird durch acht Thesen zu den folgenden Themen illustriert: Neue Infrastruktur, Einfachheit und Vertrauen, Sicherheit und Anonymität, Abgestimmte Instrumente, Privatwirtschaftliche Geschäftsmodelle, Interoperabilität, Institutionalisierung der Zusammenarbeit sowie Engagement, Leuchtturmanwendungen und Kommunikation. Die wesentlichsten Erkenntnisse aus der Diskussion der acht Thesen lauten wie folgt: Welche Instrumente und Infrastrukturen für das elektronische Identitätsmanagement letztlich auch ausgewählt werden ist von weniger hoher Bedeutung, wichtiger ist, dass die Bürger und Verbraucher ihnen vertrauen, sonst wird ihre weite Verbreitung an der mangelnden Akzeptanz scheitern. Instrumente und Infrastrukturen müssen sicher und ihre Nutzung muss einfach sein. Essenziell ist zudem, dass sie eine breite Palette von Anwendungen abdecken. Serviceanbietern müssen sie zudem attraktive Geschäftsmodelle ermöglichen. Wo sich privatwirtschaftliche Investitionen nicht lohnen wird sich die Privatwirtschaft nicht engagieren.

Der elektronische Personalausweis kann, muss aber nicht, eine zentrale Rolle im Identitätsmanagement übernehmen. Er könnte als Vertrauensanker für die Bürger und Konsumenten fungieren, dafür muss er aber die im erstgenannten Punkt enthaltenen Anforderungen erfüllen.

Die entstehende Infrastruktur für das Identitätsmanagement muss im Zielzustand grenzüberschreitend funktionieren, damit sie den erwünschten grösstmöglichen Nutzen erzielt. Nischenlösungen oder isolierte Lösungen, die sich an rein nationalen Anforderungen orientieren, helfen mittel- bis langfristig nicht weiter und werden auch nicht erfolgreich sein.

Alle Beteiligten (u.a. Regulatoren, Datenschützer, die Industrie, Endnutzer und Nichtregierungs-Organisationen) müssen bei der Einführung eines einheitlichen Identitätsmanagements an *einem* Strang ziehen und in institutionalisierter Form zusammenarbeiten. Erfolgskritisch für die Einführung ist ausserdem der absolute Wille von Staat und Privatwirtschaft, das Projekt zum Erfolg zu führen, sowie "Leuchtturmanwendungen" zu propagieren, anhand derer der Nutzen des elektronischen Identitätsmanagements verifiziert und kommuniziert werden kann. Die eID-Einführung muss in jedem Fall von einer (massiven) Informationskampagne begleitet werden.

Zur Zusammenarbeit von Staat und Wirtschaft gibt das ISPRAT-Paper [11] die folgenden Empfehlungen ab: Eine der wichtigsten zu schlagenden Brücken ist die zwischen öffentlichem Sektor und Privatwirtschaft. Nur durch ein Zusammenwirken können für alle Teilnehmer (öffentlicher Sektor, Privatwirtschaft und Bürger/Verbraucher) auf den elektronischen Transaktionsmärkten Verbundeffekte (economies of scope) realisiert werden. Das setzt einen Dialog auf allen Ebenen voraus: Auf technologischer Seite muss sichergestellt werden, dass die wichtigsten Nutzungsszenarien unterstützt werden. Für den wirtschaftlichen Betrieb der Infrastruktur kann es geboten sein, dass rechtliche Regelungen den Betrieb der entsprechenden Netzwerke und Rechenzentren durch die Privatwirtschaft bzw. durch Public-Private-Partnerships zulassen. Zur Sicherung der Qualität, z.B. des Grades der Systemverfügbarkeit, der Güte der Kundenbetreuung, der Vertraulichkeit von Daten und des Niveaus der garantierten Sicherheit ist eine unabhängige Instanz vorteilhaft, die die Steuerung übernimmt.

Castro [12] fasst die Sachverhalte zum Stand der eID-Implementierung in der EU und ansonsten auf der Welt im Hinblick auf US-Anforderungen wie folgt zusammen. Viele Länder der EU (analog zu Ländern des Mittleren Ostens und Asiens) haben in die eID investiert. Jedoch hat die eID nirgendwo zu einem integrierten Anwendungsumfang gefunden. Allerdings gibt es Länder, die mehr Erfolg hatten als andere: Estland ist aktuell der klare Führer in dieser Beziehung. 1.2 Mio. Smartcards wurden dort ausgegeben. Bis 2011 erfolgten damit 52 Mio. elektronische Signaturen. Zudem wurden über 88 Mio. elektronische Transaktionen mit der eID Estlands authentifiziert. Die eID dient auch für das E-Voting. Als Gegenstück führt der Autor die USA ins Feld, wo bis 2011 keine eID lanciert wurde. Trotzdem wurde in den USA die National Strategy for Trusted Identities im Cyberspace (NSTIC) [13] lanciert.

NSTIC hat das Ziel ein eID-Ökosystem für die USA zu schaffen (Vgl. dazu Kapitel 4.3.2 Ansätze von eID-Ökosystem Modellierungen). Interessant sind die Empfehlungen, welche Castro zuhanden den USA bezüglich Policy Making im eID-Umfeld abgibt. „Therefore, to promote e-ID adoption and use in the United States, policymakers should do the following:

- "[…] Create an e-ID implementation plan with broad input from all stakeholders, including the private sector."
- "[…] Build an e-ID framework that supports both current and emerging technologies."
- "[…] Use government to increase both supply and demand for e-IDs."
- "[…] Design an e-ID solution that maximizes utility for both users and service providers."
- "[…] Ensure that privacy does not come at the expense of eliminating useful information from the information economy."
- "[…] Strive for disruptive innovation, not just incremental innovation."
- "[…] Ensure that e-ID solutions are accessible and available to all individuals."
- "[…] Design an e-ID system for the global digital economy."

Fazit aus der Literaturstudie

Die geschilderten Ansätze bieten Hinweise auf die Dimensionen des eID-Ökosystems, die für die Entwicklung des eID-Ökosystems Modells verwertbar sind.

- Der Nutzen der Endnutzer muss explizit in den Vordergrund gestellt werden, wenn ein eID-Ökosystem Erfolg haben soll.
- Zentral ist die Bereitstellung von Mehrwertdiensten, über welche die Nutzung von eIDs gefördert werden kann.
- Der zu starke Fokus auf die Technik ist der Nutzung von eIDs hinderlich und schädlich.
- Im Dreieck zwischen Datenschutz, Sicherheit und Nutzungskomfort gilt es die goldene Mitte zu finden, über welche kontextspezifisch möglicherweise unterschiedliche Lösungen resultieren, die jedoch trotzdem interoperabel sind.
- Das eID-Ökosystem (und die Nutzung der eID) endet an nationalen Grenzen nicht und muss grenzüberschreitend interoperabel sein, wenn das Ökosystem respektive die eID wirklichen Nutzen entfalten soll.
- Nur das Zusammenwirken von Privaten und Öffentlichem Sektor kann eine nationale eID erfolgreich machen. Ein Denken in einzelnen Domänen wie E-Government, E-Health, E-Education oder E-Business ist hinderlich und für den eID-Erfolg schädlich.

3. Stakeholder-Analyse

Im Verlauf der Projektarbeit wurde eine Zusammenstellung aller relevanten Stakeholdern erstellt und konkretisiert. Initial hat hierzu ein BFH-interner Workshop stattgefunden, bei dem mögliche Stakeholder des eID-Ökosystems identifiziert wurden. Diese Stakeholder-Landkarte dient zum einen als Grundlage für die Konkretisierung des eID-Ökosystems und zum andern wurde sie für die Identifizierung der Interviewpartner und Workshop-Teilnehmer verwendet.

Bei einigen Interviews und den Public Value Workshops wurde zusätzlicher Input für weitere potentieller Stakeholder geliefert, der laufend in die Stakeholder-Landkarte aufgenommen wurde (iteratives Vorgehen).

Die Ausgangslage der Stakeholder-Analyse war eine Auflistung der Stakeholder wie sie im Folgenden kategorisiert präsentiert wird:

Politisches Umfeld:

- Politische Entscheidungsträger auf allen föderalen Ebenen
    - insbesondere: Kommissionsmitglieder in den relevanten Kommission des nationalen Parlamentes
- Lobbyisten für oder gegen eine eID
- Kommissionen, die sich mit dem Thema eID beschäftigen
- Stimmberechtigte bei eventueller Abstimmung zu eID (Bevölkerung)
- Öffentlichkeit
- Kantone, Gemeinde, Städte.

Organisatorisches Umfeld:

- eID Anbieter
- IAM Anbieter
- Fachapplikationsbetreiber oder Verantwortliche, die ein IAM System einsetzen
- IAM Spezialisten mit generellem Interesse
- Registeranbieter.

Technisches Umfeld – Das eID-Ökosystem Modell selbst zeigt keine technischen Details auf:

- Systemintegrator (technischer Architekt)
- IT-Architekt.

Anschliessend wurde methodisch auf Basis einer Mind Map eine Stakeholder-Analyse durchgeführt. Daraus ergab sich die folgende Stakeholder-Landkarte:

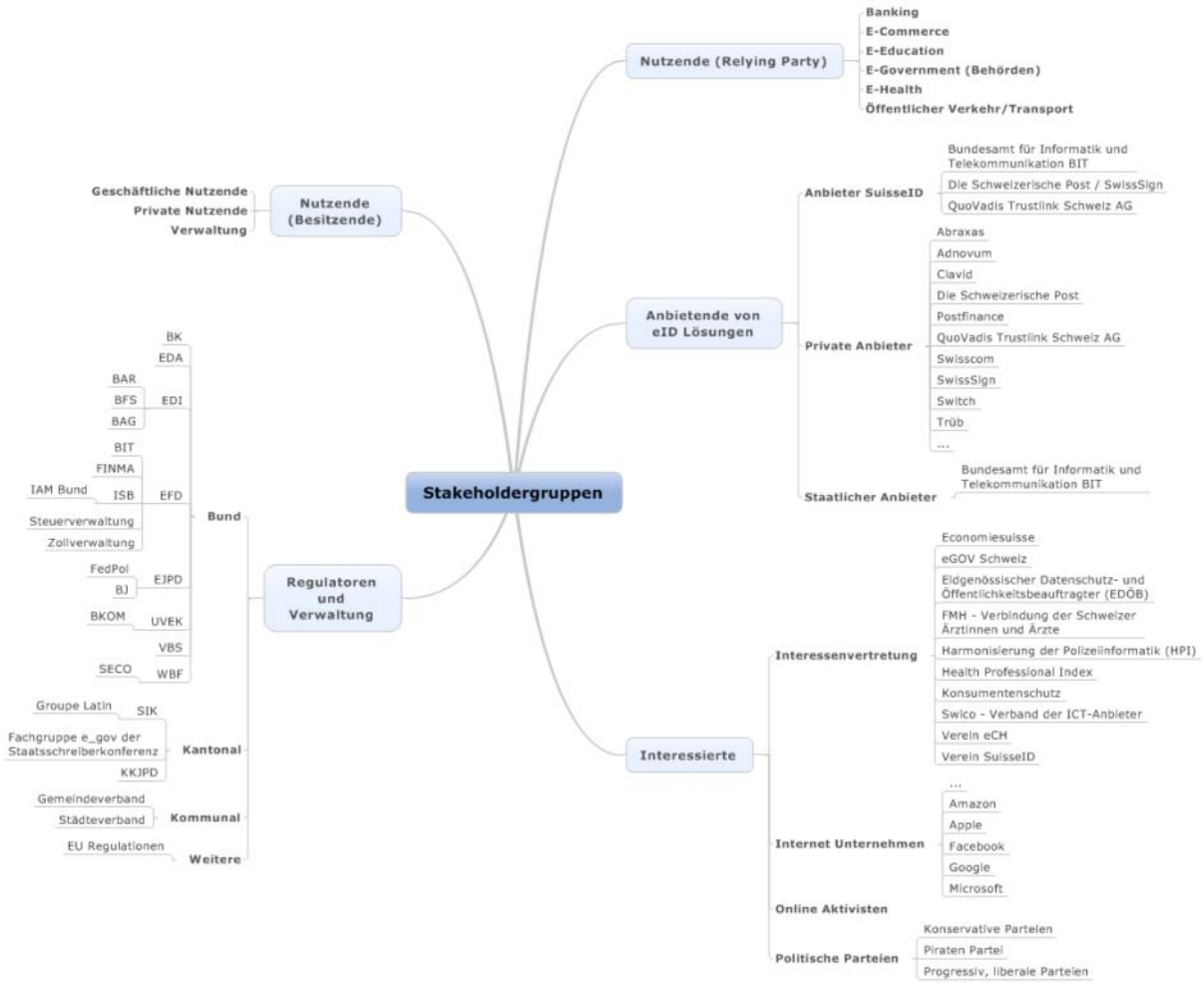


Abbildung 3: Stakeholder Landkarte

Auf einer obersten Ebene in der Abbildung 3 können die Stakeholder-Gruppen *Nutzende (Besitzende)*, *Nutzende (Relying Party)*, *Interessierte*, *Anbietende von eID Lösungen* und *Regulatoren und Verwaltung* unterschieden werden. Dies erfolgt aufgrund der Rolle im Ökosystem Modell. Auf einer darunter liegenden Ebene werden diese Stakeholder-Gruppen differenziert. Eine nächst tiefere Ebene, sowie wo vorhanden auf der tiefsten Ebene werden Beispiele zu den Stakeholder-Gruppen präsentiert.

Bei der Stakeholder-Gruppe *Nutzende* ist kein Beispiel genannt, da hier keine Konkretisierung vorhanden ist oder keine konkreteren nennbar sind.

Im Folgenden werden die für das eID-Ökosystem relevanten Stakeholder-Gruppen im Detail beschrieben:

Nutzende (Besitzende)

Diese Gruppe beinhaltet Nutzer respektive Besitzer der eID. Sie nutzen die eID mit ihren Funktionen um sich zu authentifizieren, Eigenschaften elektronisch nachzuweisen oder Dokumente zu

verschlüsseln oder zu signieren. Die Nutzenden können auch Organisationen vertreten, indem sie beispielsweise ein Organisationssiegel verwenden.

Nutzende (Relying Party)

Die Nutzenden als Relying Party (RP) bauen ihre Dienste aufgrund des Vertrauensraums basierend auf der nationalen eID auf. Die RP vertraut darauf, dass ihr Geschäftspartner richtig und sicher identifiziert wurden. Die RP muss dies nicht selber tun. Im Weiteren können sich Kunden an Systemen digital authentifizieren oder Dokumente elektronisch signiert einreichen.

Interessierte

Diese Gruppe umfasste Stakeholder, die ein Interesse an der Einführung einer eID oder eine Präferenz gegen eine entsprechende Einführung haben. In dieser Gruppe sind auch Organisationen, die bestimmte Interessen vertreten, angesiedelt (Lobbyisten).

Anbietende von eID Lösungen

Diese Stakeholdergruppe umfasst Anbieter von Identifikationslösungen, die auch potentielle Anbieter einer nationale eID sein können.

Regulatoren und Verwaltung

Regulatoren und Verwaltung sind für die Entwicklung, Einführung und Umsetzung notwendiger, regulatorischer Rahmenbedingungen für eine eID zuständig. Die Stakeholder Gruppe beinhaltet die drei föderalen Ebenen Bund, Kantone und Kommunen sowie weitere ausserhalb des staatlichen Umfelds regulierende Stakeholder.

4. eID-Ökosystem Modell

In den folgenden Abschnitten werden das eID-Ökosystem Modell und die ihm zugrunde liegenden Überlegungen erläutert. Es ist wichtig zu verstehen, dass es sich zunächst nicht um die Darstellung generischer oder konkreter Instanziierungen des Ökosystems handelt. Zwei generische Instanziierungen werden in Kapitel 4.4 behandelt.

4.1 Beschreibung des Modells

Das eID-Ökosystem Modell ist das abstrahierte Abbild einer möglichen Realität. Es basiert auf Reduktionen. Ihm ist infolgedessen eine gewisse Unschärfe eigen. Reduktionen sind notwendig, um die Komplexität der realen Zusammenhänge auf ein brauchbares Mass zu reduzieren. Dadurch werden Design-Entscheide für eine nationale eID sowie Massnahmen zur Förderung einer solchen erleichtert und überhaupt erst ermöglicht.

Das vorliegende eID-Ökosystem Modell fokussiert gezielt nicht auf spezifische Stakeholder-Gruppen, sondern auf die möglichen Elemente der Nutzung sowie der Bereitstellung einer nationalen eID. Hintergrund dazu ist, dass das Modell allen potentiellen Stakeholdern ermöglichen soll, die Zusammenhänge der Elemente zu verstehen und sich bzw. die eigene Organisation in den jeweils möglichen Rollen bei Nutzung und Bereitstellung verorten zu können. Die in Kapitel 2 diskutierten Stakeholder dienten dabei als Ausgangspunkt, um realistische Anwendungsfälle zu definieren, von denen ausgehend das Modell entwickelt wurde.

Das Modell wird in zwei unterschiedlichen Auflösungen visualisiert. Die obere Auflösung, dargestellt in Abbildung 4, schafft den Überblick über den Ordnungsrahmen und die darin existierenden Zusammenhänge zwischen den Grundbereichen des eID-Ökosystems.

Weitere Details liefert Abbildung 5: eID-Ökosystem Modell Elemente. Die Grundbereiche werden hier in ihre einzelnen Komponenten oder Elemente aufgelöst. Dies ist relevant für die Diskussion der Instanziierungen, denn nur auf der Detailebene lassen sich Auswirkungen von Design-Entscheiden einer eID auf das Ökosystem erkennen und nur so können entsprechende Fördermassnahmen entwickelt werden.

Das eID-Ökosystem Modell liest sich von links nach rechts: Ausgehend von den Nutzenden lassen sich Anwendungsfälle für den Einsatz einer eID definieren, die für Erstere einen Nutzen generieren. Die Anwendungsfälle lassen sich wiederum in einzelne Nutzungen abstrahieren, die in ihrer Gesamtheit oder Menge den nutzenstiftenden Kern einer eID bilden. Jede Nutzung basiert auf mindestens einer eID-Funktion, der grundlegenden Grösse auf der Bereitstellungsseite einer eID. Die eID-Funktionen werden ermöglicht durch die Definition von Vertrauensdiensten und deren Implementierung auf Basis der technischen Infrastruktur. Die Vertrauensdienste orientieren sich eng an der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung) [14]. Aus Gründen der Ver-

ständlichkeit wurden diese im eID-Ökosystem Modell auf Ebene der Elemente angepasst wiedergegeben (z.B. Einführung und Aufteilung der Identifikatoren). Vertrauensdienste wie auch die technische Infrastruktur erfordern, dass die entsprechenden institutionell-rechtlichen Rahmenbedingungen passend gestaltet werden. Überdies machen sie einen passenden organisatorischen Unterbau notwendig, der sich um alle Aspekte kümmert, von der Entwicklung der Lösungen, über das Management, bis hin zur Durchsetzung der Governance im eID-Ökosystem. Sowohl die Nutzung wie auch Bereitstellung einer eID erfolgen innerhalb eines politischen Rahmens, der über verschiedene Handlungen zur Gestaltung des Ganzen beiträgt und so in erheblichem Masse zum Erfolg einer nationalen eID in der Schweiz beiträgt.

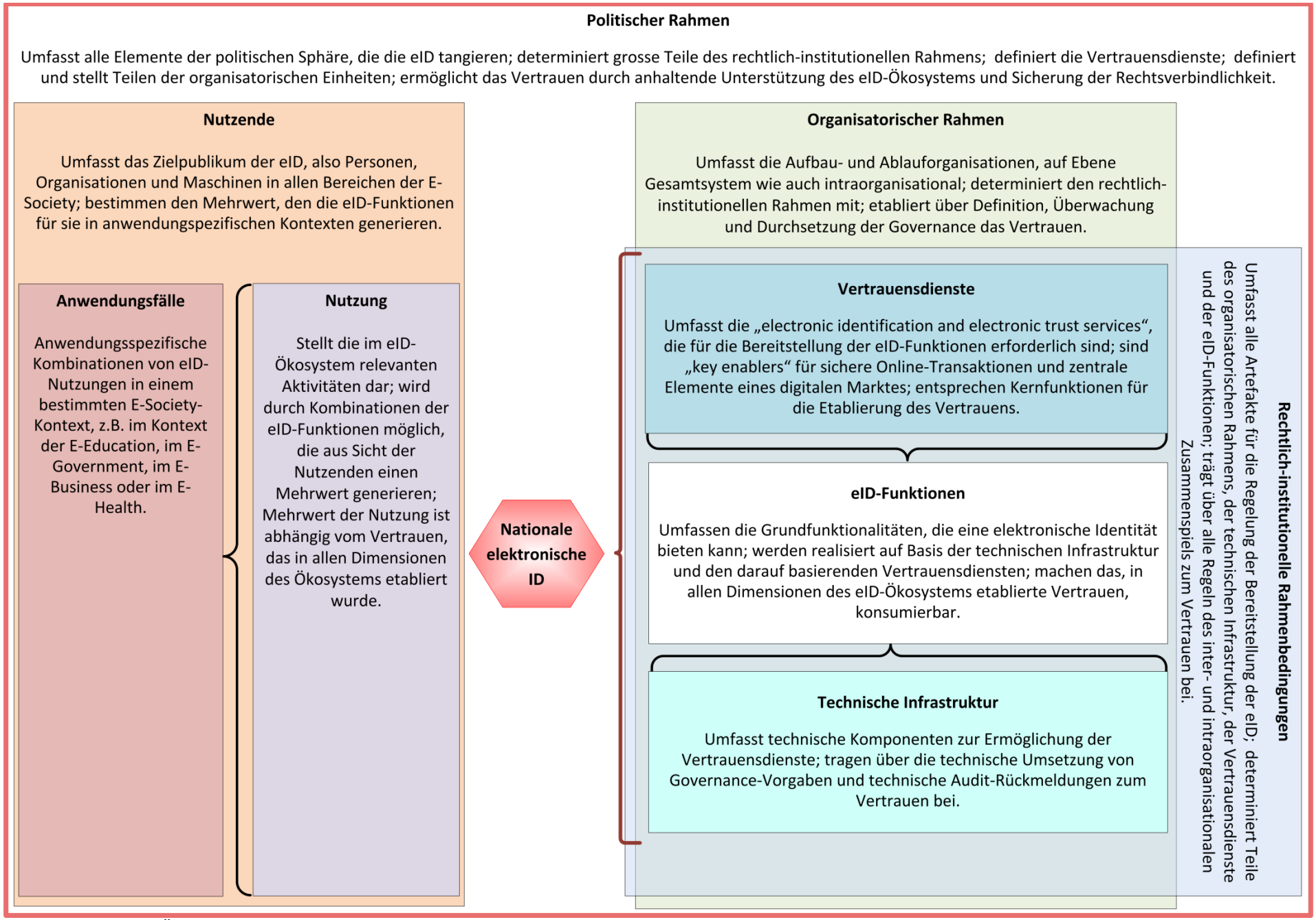


Abbildung 4: eID-Ökosystem Modell Grundbereiche

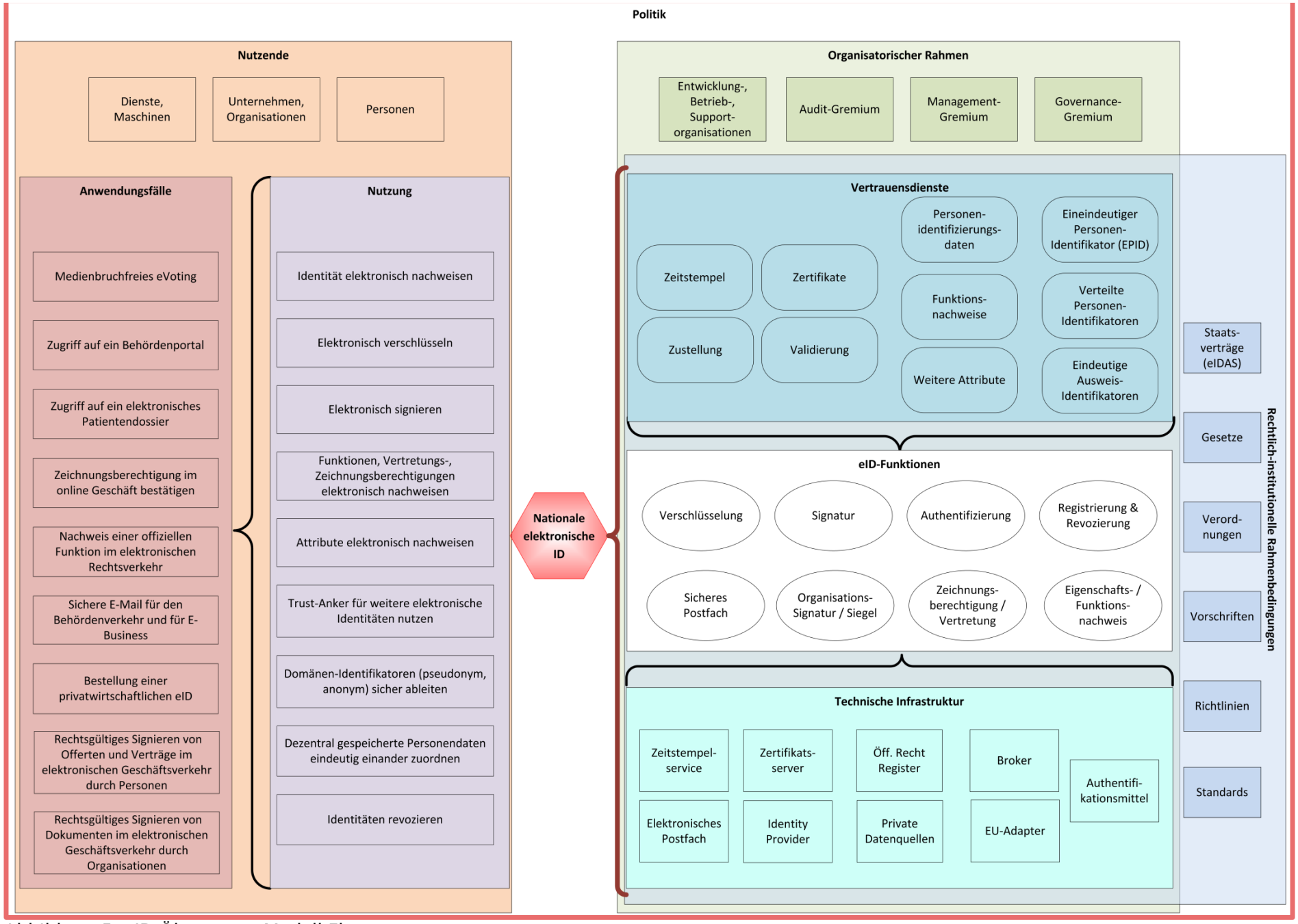


Abbildung 5: eID-Ökosystem Modell Elemente

4.2 Beschreibung der Grundbereiche und Elemente

4.2.1 Grundbereiche Nutzung

Die linke Seite der Darstellung stellt den relevanten Kern, die Perspektive der Nutzung einer nationalen eID dar. Ausgehend von den Nutzenden lassen sich Anwendungsfälle im Kontext der E-Society definieren. Diese lassen sich wiederum in Nutzungen zerlegen, die von einer eID angeboten werden können.

Nutzende

Die Nutzenden umfassen das Zielpublikum der eID, also Personen, Organisationen und Maschinen in allen Bereichen der E-Society. Die Nutzenden bestimmen den Mehrwert, den die eID-Funktionen für sie in anwendungsspezifischen Kontexten generieren.

Nutzung

Die Nutzung stellt die im eID-Ökosystem relevanten Aktivitäten dar. Sie wird durch Kombinationen der eID-Funktionen möglich, die aus Sicht der Nutzenden einen Mehrwert generieren. Der Mehrwert der Nutzung ist u.a. abhängig vom Vertrauen, das in allen Dimensionen des Ökosystems etabliert wird.

Anwendungsfälle

Die Anwendungsfälle stellen anwendungsspezifische Kombinationen von eID-Nutzungen in einem bestimmten E-Society-Kontext dar, also von E-Education, E-Government, E-Business und E-Health.

4.2.2 Grundbereiche Bereitstellung

Auf der rechten Seite der Visualisierung finden sich die Grundbereiche der Bereitstellung einer nationalen eID. Um die Nutzungen zu realisieren, sind gewisse eID-Funktionen notwendig. Diese basieren sowohl auf definierten Vertrauensdiensten wie auch auf der technischen Infrastruktur, welche die eID-Funktionen ermöglicht. All das ist eingebettet in einen rechtlich-institutionellen und einen organisatorischen Rahmen. Der politische Rahmen umfasst als Basis die gesamte Bereitstellung, aber auch die Nutzung.

Politischer Rahmen

Der politische Rahmen umfasst alle Elemente der politischen Sphäre, welche die eID tangieren. Er determiniert weiter grosse Teile des rechtlich-institutionellen Rahmens, definiert die Vertrauensdienste, definiert und stellt Teile der organisatorischen Einheiten zur Verfügung, ermöglicht das Vertrauen durch anhaltende Unterstützung des eID-Ökosystems und die Sicherung der Rechtsverbindlichkeit.

Rechtlich-institutioneller Rahmen

Der rechtlich-institutionelle Rahmen umfasst alle Artefakte für die Regelung der Bereitstellung der eID. Er determiniert Teile des organisatorischen Rahmens. Er determiniert weiter die technische Infrastruktur, die Vertrauensdienste und die eID-Funktionen. Der rechtlich-institutionelle Rahmen trägt über alle Regeln des inter- und intraorganisationalen Zusammenspiels zum Vertrauen bei.

Organisatorischer Rahmen

Der organisatorische Rahmen umfasst die Aufbau-und Ablauforganisationen auf Ebene Gesamtsystem wie auch intraorganisational. Er determiniert weiter den rechtlich-institutionellen Rahmen mit. Er etabliert das Vertrauen im eID-Ökosystem über die Definition, Überwachung und Durchsetzung der entsprechenden Governance.

Vertrauensdienste

Die Vertrauensdienste umfassen die in Europa definierten Elemente, die für die Bereitstellung von Identifizierung und elektronischen Vertrauensdiensten erforderlich sind. Die Vertrauensdienste sind „key enabler" für sichere Online-Transaktionen und zentrale Elemente eines digitalen Marktes. Sie entsprechen den Kernfunktionen für die Etablierung des Vertrauens.[6]

eID-Funktionen

Die eID-Funktionen umfassen die Grundfunktionalitäten, die eine elektronische Identität bieten kann. Sie werden realisiert auf Basis der technischen Infrastruktur und den darauf basierenden Vertrauensdiensten. Sie machen das in allen Dimensionen des eID-Ökosystems etablierte Vertrauen konsumierbar.

Technische Infrastruktur

Die technische Infrastruktur umfasst die Komponenten zur Ermöglichung der Vertrauensdienste. Die technische Infrastruktur trägt über die technische Umsetzung von Governance-Vorgaben und technischen Audit-Rückmeldungen zum Vertrauen bei.

4.2.3 Elemente Nutzung

Anwendungsfälle

Die auf der linken Seite des Modells aufgeführten Anwendungsfälle sind nur beispielhaft und keinesfalls als abschliessende Auflistung zu verstehen. Ausgangspunkt für die Diskussion der Anwendungsfälle waren die Resultate aus den beiden weiter oben erwähnten externen Workshops von Dezember 2013 und Januar 2014 sowie der Aufbereitung der Resultate. Die hier aufgeführten Anwendungsfälle decken den potentiellen Nutzen, den eine eID innerhalb der E-Society generieren kann, breit ab.

[6] Die Begrifflichkeiten sind in Artikel 3 der eIDAS-Verordnung spezifiziert [21]

In den Anwendungsfällen lässt sich die eigentliche Generierung von Nutzen für die Nutzenden verorten. Sie sind die konkreten Ausprägungen des Konsums des Vertrauens im eID-Ökosystem. Jeder Anwendungsfall lässt sich in Kombinationen von Nutzungen dekomponieren. So dürften für medienfreies E-Voting zum Beispiel „Identität elektronisch nachweisen“, „Elektronisch verschlüsseln“, „Elektronisch signieren“ und „Domänen-Identifikatoren (pseudonym, anonym) sicher ableiten“ in Kombination genutzt werden. Um etwa eine „Zeichnungsberechtigung im online Geschäft bestätigen“ zu können, wird wiederum die Kombination von „Identität elektronisch nachweisen“ und „Funktionen, Vertretungs-, Zeichnungsberechtigungen elektronisch nachweisen“ benötigt.

Auf die Beschreibung sämtlicher Anwendungsfälle wird hier verzichtet, zumal diese ohnehin als nicht abschliessend zu verstehen sind. Wichtig ist, dass in Diskussionen über die Ausprägung der Schweizer eID und des zugehörigen Ökosystems von Anwendungsfällen ausgegangen wird. Davon werden Nutzungen dekomponiert und daraus die richtigen Schlüsse für die Bereitstellung der notwendigen Elemente gezogen.

eID-Ökosystem-Bereich	eID-Ökosystem-Element	Beschrieb
Nutzende	Person	Mit Person sind natürliche Personen gemeint.
Nutzende	Unternehmen, Organisation	Dies umfasst alle juristischen Personen.
Nutzende	Dienste, Maschinen	Ein Dienst ist eine technische, autarke Einheit, die zusammenhängende Funktionalitäten zu einem Themenkomplex bündelt und über eine klar definierte Schnittstelle zur Verfügung stellt.
Nutzung	Identität elektronisch nachweisen	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Authentifizierung.
Nutzung	Elektronisch verschlüsseln	Dies setzt sich zusammen aus den eID-Funktionen Registrierung und Revozierung, Verschlüsselung.
Nutzung	Elektronisch signieren	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Signatur.
Nutzung	Funktionen, Vertretungs-, Zeichnungsberechtigungen elektronisch nachweisen	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Authentifizierung, Zeichnungsberechtigung / Vertretung, Eigenschafts- / Funktionsnachweis.
Nutzung	Attribute elektronisch nachweisen	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Authentifizierung, Eigenschafts- / Funktionsnachweis.
Nutzung	Trust-Anker für weitere elektronische Identitäten nutzen	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Authentifizierung; erfordert eineindeutigen Personen-Identifikator (EPID), verteilte Personen-Identifikatoren.
Nutzung	Domänen-Identifikatoren (pseudonym, anonym) sicher ableiten	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung, Authentifizierung; erfordert verteilte Personen-Identifikatoren.

Nutzung	Dezentral gespeicherte Personendaten eindeutig einander zuordnen	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung; erfordert eineindeutigen Personen-Identifikator (EPID)
Nutzung	Identitäten revozieren	Dies setzt sich zusammen aus den eID-Funktionen Registrierung & Revozierung.

Tabelle 2: Übersicht Elemente Nutzende und Nutzung

4.2.4 Elemente Bereitstellung

eID-Ökosystem-Bereich	eID-Ökosystem-Element	Beschrieb
Rechtlich-institutionelle Rahmenbedingungen	Staatsverträge (eIDAS)	Für die Notifizierbarkeit einer nationalen eID bzw. die Beteiligung am über eIDAS intendierten Vertrauensrahmen und -raum ist ein Staatsvertrag der Schweiz mit der EU erforderlich. eIDAS repräsentiert die EU-Regulierung (EU) N910/2014 zur elektronischen Identifikation und zu Vertrauensdiensten für elektronische Transaktionen im internen Markt (eIDAS-Regulierung).
Rechtlich-institutionelle Rahmenbedingungen	Gesetze	Der gesetzliche Bezug zum eID-Ökosystem lautet wie folgt: Gewisse Dinge sind nur über Gesetz regelbar. Dies kann ZERTES oder ein neu zu definierendes eID-Gesetz sein.
Rechtlich-institutionelle Rahmenbedingungen	Verordnungen	Dies umfasst den oben genannten Gesetzen untergeordnete Umsetzungsbestimmungen.
Rechtlich-institutionelle Rahmenbedingungen	TAV	Dies bezeichnet „Technische und administrative Vorschriften“
Rechtlich-institutionelle Rahmenbedingungen	Richtlinien	Als Richtlinie wird eine Handlungs- oder Ausführungsvorschrift einer Institution oder Instanz bezeichnet.
Organisatorischer Rahmen	Governance-Gremium	Dies ist das Gremium, das gebildet wird, das Führungs- und Governance-Aufgaben im eID-Ökosystem übernimmt.
Organisatorischer Rahmen	Management-Gremium	Dies ist das Gremium, das gebildet wird, das Umsetzungsaufgaben im eID-Ökosystem zwischen den verschiedenen Beteiligten koordiniert.

Organisatorischer Rahmen	Audit-Gremium	Dies ist das Gremium, das gebildet wird, das Audits im eID-Ökosystem übernimmt, durchführt oder in Auftrag gibt.
Organisatorischer Rahmen	Entwicklungs-, Betriebs- sowie Supportorganisationen	Dies beinhaltet Organisationseinheiten, welche Entwicklung und Betrieb der eID und der erforderlichen Infrastruktur dazu sicherstellen. Dazu gehören u.a. Marketing, Verkauf, Support und generische Unterstützungsdienstleistungen sowohl für Nutzende und Bereitstellende im eID-Ökosystem.
Vertrauensdienste	Zeitstempel	Dies ist ein überprüfbarer bestätigter (Gültigkeits-)Zeitpunkt einer Signatur oder eines Siegels auf einem Dokument oder definierter Daten.
Vertrauensdienste	Zustellung	Dies ist ein Dienst, der die eingeschriebene Zustellung von elektronischen Dokumenten anbietet, die durch die Identifikation von Absender und Empfänger, Signatur oder Siegel und Zeitstempel bestätigt wird.
Vertrauensdienste	Zertifikate	Dies sind die elektronischen Bescheinigungen, die eine Signatur, ein Siegel oder eine Webseite mit einer natürlichen oder juristischen Person verknüpfen.
Vertrauensdienste	Validierung	Dies ist ein Dienst, der die Gültigkeit von Signaturen, Siegeln, Zeitstempeln, Zertifikaten und Dienste für sichere Zustellung überprüft.
Vertrauensdienste	Personenidentifizierungs-daten	Dies ist ein Datensatz, über den die Identität einer natürlichen oder juristischen Person festgestellt werden kann.
Vertrauensdienste	Attribute	Dies sind fakultative, zusätzliche Informationen, die in einer Signatur oder einem Siegel enthalten sein können. Innerhalb der Schweiz können sie auch für die Authentifizierung benutzt werden.[7]

[7] Gemäss eIDAS ist die Authentifizierung im grenzüberschreitenden Kontext ausschliesslich basierende auf den Personenidentifizierungsdaten möglich.

Vertrauensdienste	Funktionsnachweis	Dies sind weitergehende Attribute, deren Kontext-spezifische Informationen in einer Domäne eindeutig definiert und bekannt sind. Sie weisen einer Person bestimmte institutionelle Eigenschaften zu.
Vertrauensdienste	Eineindeutiger Personen-Identifikator (EPID)	Dies ist eine Zeichenkette, welche eine eID und damit eine Person innerhalb eines Namensraums elektronisch eineindeutig identifizierbar macht. Jede Person verfügt innerhalb eines Namensraums über maximal einen EPID.
Vertrauensdienste	Verteilte Personenidentifikatoren	Dies ist eine Zeichenkette, welche eine eID und damit eine Person innerhalb eines Namensraums elektronisch eindeutig identifizierbar macht. Jeder Person können innerhalb eines Namensraums 1-n verteilte Personenidentifikatoren zugewiesen werden.
Vertrauensdienste	Eindeutige Ausweis-Identifikatoren	Eine Zeichenkette, welche einen physischen oder elektronischen Ausweis innerhalb eines Namensraums eindeutig identifizierbar macht.
eID-Funktionen	Registrierung & Revozierung	Die Registrierung umfasst den Prozess einer Registrierungsstelle, bei dem eine Person eine eID mit dazu gehörigem Identitätsnachweis erlangt. Die Revozierung umfasst den Prozess einer Registrierungsstelle, bei dem einer Person ein Identitätsnachweis entzogen wird oder dessen Verbindung zur eID für ungültig erklärt wird.
eID-Funktionen	Authentifizierung	Dies ist der Nachweis der eigenen eID einer Person.
eID-Funktionen	Signatur	Diese beinhaltet Daten in elektronischer Form, die anderen elektronischen Daten beigefügt sind oder mit diesen verknüpft sind und die der Unterzeichner zum Unterzeichnen verwendet.

eID-Funktionen	Verschlüsselung	Als Verschlüsselung wird der Vorgang bezeichnet, bei dem ein klar lesbarer Text (Klartext; Informationen anderer Art wie Ton- oder Bildaufzeichnungen) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine „unleserliche“, das heisst nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird. Als entscheidend wichtige Parameter der Verschlüsselung werden hierbei ein oder auch mehrere Schlüssel verwendet.
eID-Funktionen	Organisations-Signatur / Siegel	Dies umfasst Daten in elektronischer Form, die anderen elektronischen Daten beigefügt sind oder mit diesen verknüpft sind, um deren Ursprung und Unversehrtheit sicherzustellen.
eID-Funktionen	Eigenschaftsnachweis	Dieser beinhaltet den Nachweis einer Eigenschaft, die ein Subjekt hat (Attribut).
eID-Funktionen	Zeichnungsberechtigung / Vertretung	Diese beinhaltet den Nachweis, dass eine Person berechtigt ist, im Namen einer juristischen oder natürlichen Person zu handeln.
Technische Infrastruktur	Token	Dies ist ein (physischer) Träger für ein Zertifikat.
Technische Infrastruktur	Broker	Ein Broker stellt eine Plattform dar, über die Daten zwischen Subjekten, Ressourcen und Services zur Ausführungszeit vermittelt werden.
Technische Infrastruktur	EU-Adapter	Dies ist eine Schnittstelle zum Austausch von IAM-Daten mit Ländern im Europäischen Identitäts-Raum (Pan-European Proxy Server (PEPS)).
Technische Infrastruktur	Öffentlich-rechtliche Register	Dies sind Verzeichnisse von öffentlich-rechtlichem Charakter (eingerichtet basierend auf einem Gesetz).
Technische Infrastruktur	Private Datenquellen	Dies sind Datenbanken, welche von Privaten betrieben werden, welche Identitätsdaten oder Attribute enthalten können.

Technische Infrastruktur	Zertifikats-Server	Dies ist die technische Infrastruktur um Zertifikate auszugeben sowie zu verwalten.
Technische Infrastruktur	Identity Provider	Dies ist die Entität, welche die eID verwaltet und ausgibt.
Technische Infrastruktur	Zeitstempelservice	Dies ist ein Service, über welchen einem Ereignis ein eindeutiger Zeitpunkt zugeordnet werden kann.
Technische Infrastruktur	Elektronisches Postfach	Ein elektronisches Postfach ist ein virtueller Ablageort einer Person für Dokumente und Informationen.

Tabelle 3: Beschreibung der Elemente Bereitstellung.

4.3 Vorgehen und Überlegungen zur Modellentwicklung

In den folgenden Kapiteln werden die Grundlagen für die Modellentwicklung sowie der Modellierungsprozess im Projektverlauf dargelegt.

4.3.1 Vorarbeiten und Grundüberlegungen zu eID-Ökosystem Modellen

Die Vorarbeiten zum hier vorliegenden eID-Ökosystem Modell wurden von der BFH im Rahmen der Untersuchungen zur Schweizerischen eID, im Auftrag des fedpol Ende 2013 und im Auftrag des SECO anfangs 2014 getätigt. Der Fokus lag dabei noch auf allgemeinen Betrachtungen zu einem eID-Ökosystem, jedoch bereits mit dem Hintergrund der Nutzenperspektive. Der Auslöser dafür war das im Sommer 2013 vom fedpol zur öffentlichen Vernehmlassung publizierte (und anschliessend zurückgezogene) erste Vorkonzept zu einem elektronischen Identitätsnachweis [15]. Dieses orientierte sich kaum an Nutzenaspekten oder Aspekten eines eID-Ökosystems als Gesamtsystem, sondern fokussierte stark auf die technischen Aspekte einer möglichen Implementierung.

Die Resultate der Arbeiten aus zwei externen Workshops mit Vertretern des Bundesamtes für Polizei fedpol, des Staatssekretariates für Migration SEM (ehemals BfM), des Bundesamtes für Informatik und Telekommunikation BIT, des Bundesamtes für Justiz BJ, des Informatiksteuerungsorgans des Bundes ISB, des Staatssekretariats für Wirtschaft SECO, Bürge Consulting und der BFH zeigten auf, dass bis dato kein generisches Modell eines eID-Ökosystems bekannt war[8]. Existierende Modellierungen konnten weder den Ansprüchen einer gesamtheitlichen Abbildung noch der Tauglichkeit sowohl für SOLL als auch IST Darstellung genügen. Um ein vertieftes Verständnis des Gesamtsystems „eID“ zu erlangen und den Entscheidungsträgern darauf aufbauend zu ermöglichen, eine auf den Nutzen ausgerichtete Lösung zu gestalten, brauchte es daher ein generisches Modell eines eID-Ökosystems. Für ein solches wurden drei übergeordnete Ziele identifiziert:

1. Schaffung von Vertrauen und Planungssicherheit für alle: Bereitstellung einer verständlichen Zukunftsperspektive, Verringerung der Unsicherheiten in Bezug auf zukünftige Entwicklungen und Erhöhung der Planungssicherheit für Staat und Wirtschaft.
2. Schaffung einer Basis für den Sachdiskurs: Etablierung einer Sprache, um sachliche Diskussionen unter Akteuren mit unterschiedlichem Hintergrund zu ermöglichen.
3. Ermöglichung eines offenen Systems mit optimaler Wertschöpfung: Vereinfachung der Integration privater eIDs und der Entwicklung neuer Anwendungsfälle.

[8] Nicht publiziert, internes Dokument zuhanden SECO.

Das bedeutet für das eID-Ökosystem-Modell, dass:

- eine einheitliche Ontologie zu definieren und anzuwenden ist
- ein Stakeholder- oder Akteursbild als Vorleistung benötigt wird[9]
- die Darstellung ein Zoom-Flat (auf disziplinäre Fachsichten wie Recht, Organisation, Technik) und ein Zoom-In (auf Teilsysteme, Schnittstellen, Rollen etc.) ermöglicht.

Ausgehend davon erarbeitete die BFH im Rahmen des Projekts verschiedene Versionen eines Modells, die teils wieder verworfen sowie teils weiterentwickelt wurden. Im folgenden Unterkapitel wird kurz auf einige der Arbeitsversionen eingegangen, um den Prozess der Entwicklung bis hin zum abschliessenden Modell intersubjektiv nachvollziehbar zu machen.

4.3.2 Ansätze von eID-Ökosystem Modellierungen

In den Arbeiten 2013/2014 wurden bestehende theoretische wie praktische Ansätze zu eID-Ökosystemen und -Modellen aus anderen Ländern recherchiert[10]. Diese Vorkenntnisse wurden bei der Erarbeitung berücksichtigt. Im Folgenden wird kurz auf die bereits erwähnten Arbeiten aus den USA eingegangen. Diese waren aus der Sicht der Autoren im Gesamtkontext von Ökosystem und Modellierung zum Projektzeitpunkt am Weitesten fortgeschritten.

Die National Strategy for Trusted Identities in Cyberspace [13] der US Regierung fokussiert auf die Etablierung eines Identitäts-Ökosystems, das Interoperabilität in Policies, Prozessen und Technologie zwischen verschiedenen Nutzergruppen ermöglichen soll. Komponenten davon sind:

- Ein Rahmenwerk: Mit übergreifenden Standards, Risikomodellen, Datenschutz- und Haftungsrichtlinien
- Eine Steuerungsgruppe: Zur Verwaltung und Durchsetzung von Standards, Policies und Akkreditierung
- Je ein Vertrauens-Rahmenwerk pro Nutzergruppe: Mit Definitionen zu Rechten und Pflichten der Teilnehmer, spezifischen Standards, Policies und Prozesen für die Nutzergruppe
- Sogenannte Trustmark Schemata: Zur Sicherstellung der Service Provider Compliance
- Akkreditierungs-Autoritäten: Zur Sicherstellung, dass Identity Provider, Attribute Authorities, Relying Parties und Authentifizierungsmittel dem Trustmark entsprechen.

Der Fokus liegt klar auf der Etablierung von Vertrauen zwischen den Stakeholdern.

[9] Die hierin gewählte Ontologie beruht hybrid auf eCH Standards (primär eCH-0107, eCH-0170 und eCH-0167) und eIDAS. Es ist absehbar, dass die eCH IAM Standards im Zuge der Finalisierung von eIDAS entsprechenden Überarbeitungen erfahren werden.

[10] Nicht publiziert, internes Dokument zuhanden fedpol.

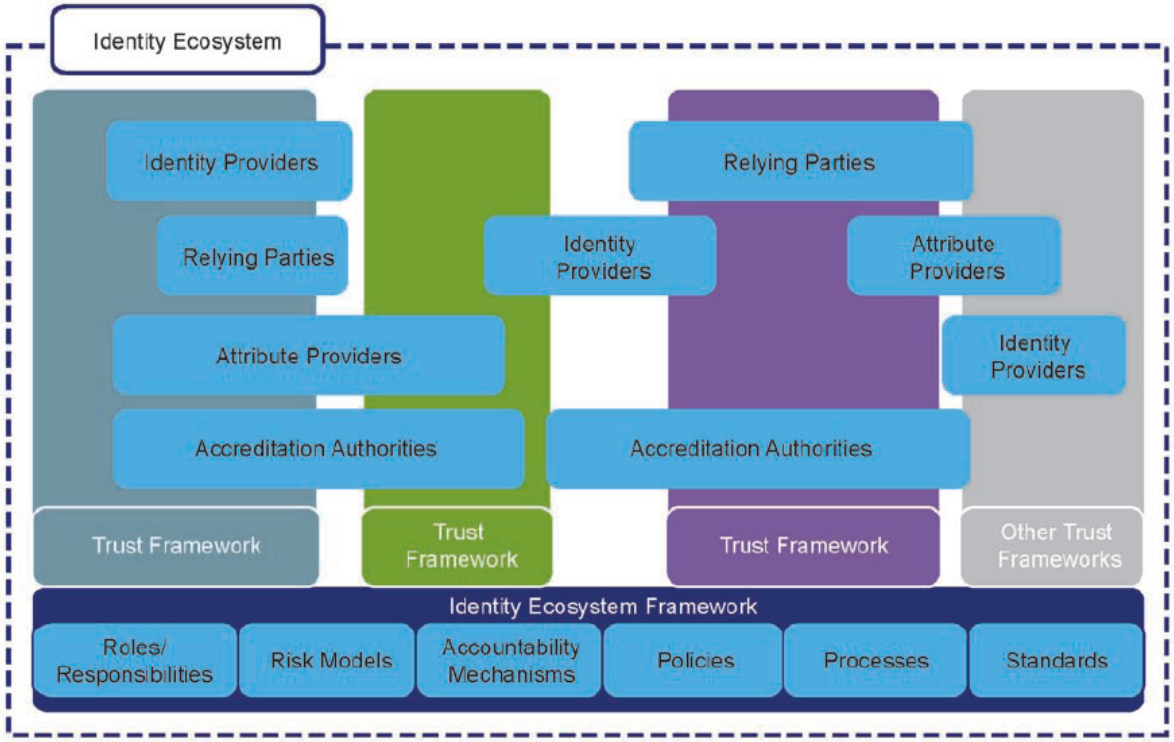


Abbildung 6: "The Identity Ecosystem", Quelle: NSTIC [13]

Während die Bildung eines Vertrauensraums zwischen allen Teilnehmenden bzw. Stakeholdern im eID-Ökosystem die Basis bildet, ist die Perspektive dennoch umzudrehen: Die Grundfrage nach dem zu schaffenden Nutzen muss für alle Stakeholder gestellt werden. Vertrauen ist im Ökosystem das, aus dessen Konsum die Nutzenden Nutzen ziehen. Vertrauen ist daher das, was auf möglichst nutzenbringende Weise bereitgestellt werden muss.

Es zeigte sich, dass die bis dato bekannten „eID-Ökosysteme“ und deren Modelle bestenfalls auf Teilaspekte des Gesamtsystems (Technik, Akteure, Rollen, Vertrauen etc.) fokussierten, was einer generischen Modellierung widerspricht. Dargestellt wurden üblicherweise entweder eine konkrete IST- oder eine angepeilte SOLL-Ausprägung dar. Von den existierenden Arbeiten folgte keine konsequent dem Grundsatz der Nutzenperspektiven. Den in den Vorarbeiten identifizierten Anforderungen an Ökosystem und Modellierung genügten deshalb die bis dahin bekannten Ansätze nicht.

Das vom Bundesamt für Polizei fedpol im Mai 2015 zur informellen Konsultation publizierte Konzept [16] erreichte das EGI der BFH erst kurz vor Projektabschluss.

Die Abbildung 7 stellt ein illustratives Beispiel daraus dar, wie einige Teile eines eID-Ökosystems zusammenhängen könnten (Vgl. dazu auch Abbildung 8). Dabei schafft das Konzept kein gesamtheitliches Systembild, was auch aus der unvollständigen Auflistung deutlich wird. Die Überlegungen des fedpol bewegen sich deutlich mehr in Richtung *technischer Systeme,* als dass sie das gesamte eID-Ökosystem berücksichtigen. Eine Modellierung basierend auf einem derart

eingeschränkten Betrachtungswinkel würde in der Folge den notwendigen Fachdiskurs kaum zu unterstützen vermögen.

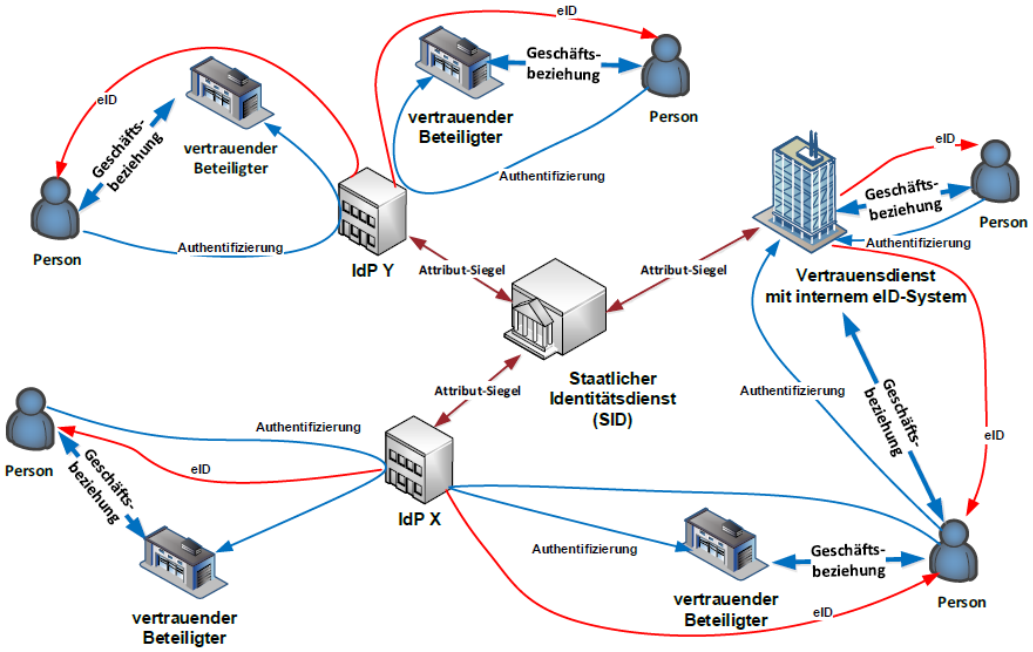


Abbildung 7: „Teilnehmer des eID-Ökosystems“, Quelle: Konzept fedpol 2015 [16]

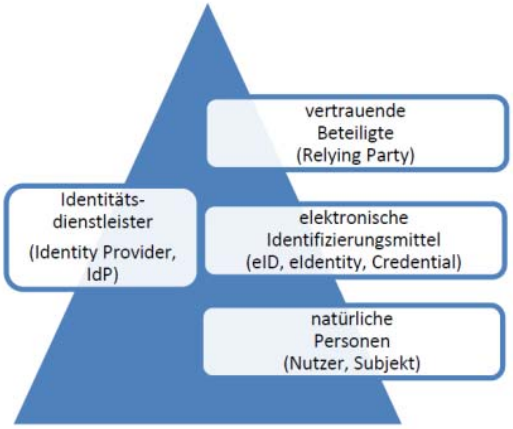


Abbildung 8: „Begriffe des eID-Ökosystems“, Quelle: Konzept fedpol 2015 [16]

4.3.3 Herleitung der eigenen Modellentwicklung

Die Beschäftigung mit möglichen Modellierungen und Visualisierungen von Identitäts- und Vertrauenssystemen starteten an der BFH bereits lange vor dem Auftrag zum eID-Ökosystem 2014. Als Vorbereitung auf einen ersten Austausch mit dem fedpol im Juni 2013 wurde das in Abbildung 9 dargestellte Modell entwickeltet, das ein System von abgeleiteten Vertrauensbeziehungen in einem eID-Ökosystem umfasst.

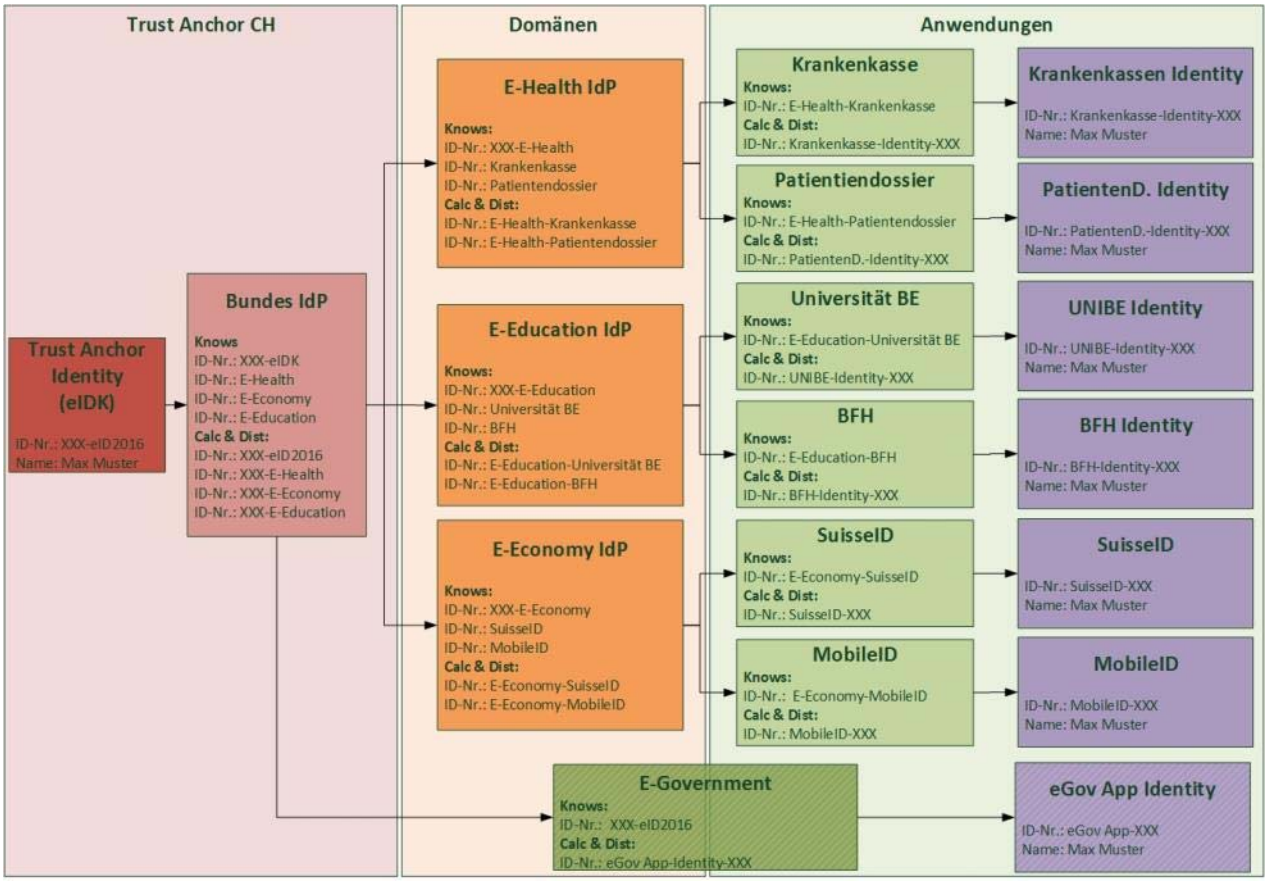


Abbildung 9: Draft Trust-Anker Ökosystem

Die gedankliche Ausgangslage dazu war eine nationale eID im Sinne eines Vertrauens-Ankers für abgeleitete Domänen-Identifikatoren. Von Letzteren können wiederum Identifikatoren für spezifische Anwendungsbereiche und schliesslich einzelne Anwendungen abgeleitet werden. Ein solches System kann mit überschaubarem Aufwand bereits einen deutlichen Beitrag zur Verbesserung der Online-Identifikation in der E-Society leisten, was einer realistischen Nutzenperspektive entspricht.

Die nachfolgenden Draft-Versionen wurden alle im Rahmen des Projekts 2014-15 erstellt und basieren auf den oben genannten Grundüberlegungen zur Modellentwicklung. Ein früher Entwurf ist dargestellt in Abbildung 10. Dieses Modell vereint bereits mehrere Grundüberlegungen, die sich auch in der finalen Version wiederfinden. Ausgehend von den Zoom-In Anforderungen, wurden hier drei Ebenen gewählt, zwischen denen sich Abhängigkeiten darstellen lassen sollten.

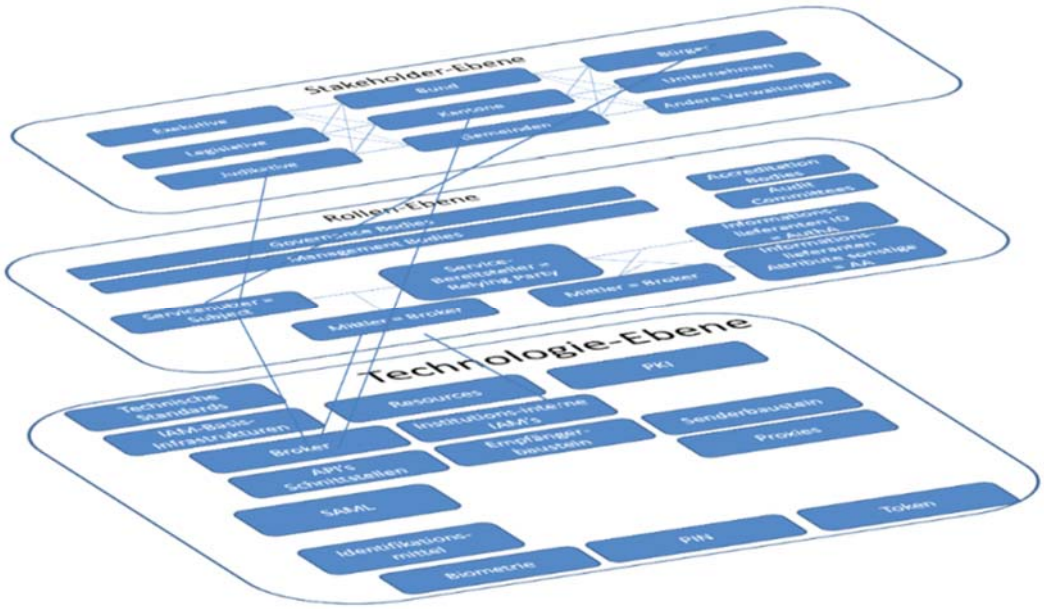


Abbildung 10: Modell Draft 1

Die Ebenen unterteilen sich in Grundbereiche, die mit Detailelementen angereichert sind. Beginnend mit Überlegungen, dass die Definition des Nutzens von den Stakeholdern auszugehen hat, stellen diese die oberste Ebene dar. Darunter liegend finden sich Rollen, die die Stakeholder innerhalb des Ökosystems wahrnehmen. Dem Ganzen zu Grunde liegt die Ebene der technischen Infrastruktur, die als Basis einer eID Implementierung dient.

Bei der weiteren Betrachtung wurde allerdings klar, dass aus der Visualisierung von Abhängigkeiten kein direkter Gewinn für das Verständnis des Ökosystems zu gewinnen ist. Hingegen reduziert dies in der Modellierung auf unnötige Weise die Übersichtlichkeit und lenkt von anderen, relevanteren Aspekten ab. Unter Hinzunahme des European Interoperability Framework (EIF) [17] (Vgl. Abbildung 11) wurden in der Folge die Überlegungen auf Vollständigkeit hin überprüft.

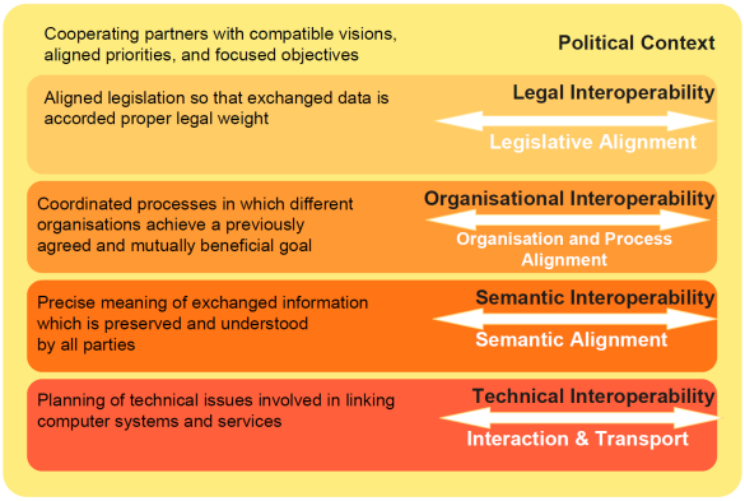


Abbildung 11: European Interoperability Framework [17]

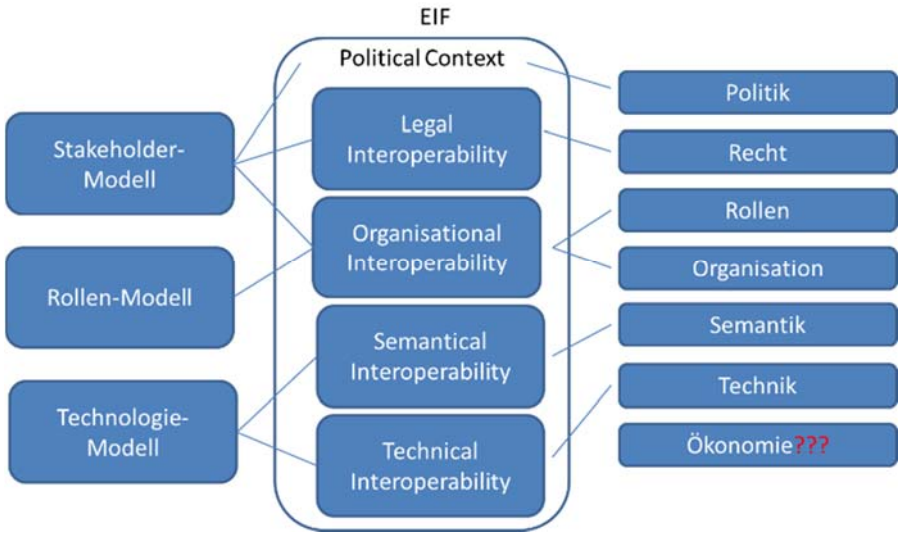


Abbildung 12: Modell Draft 2

Wie sich in Abbildung 12 zeigt, würden die drei Grundebenen eine adäquate Deckung ergeben. Hingegen bleibt ein Aspekt, der im EIF keine Erwähnung findet, aus Sicht der Autoren unberücksichtigt, der Aspekt der wirtschaftlichen Interoperabilität. Lösungen wie eine nationale eID müssen unbedingt schon vom Design weg Überlegungen zur langfristigen Wirtschaftlichkeit und Finanzierbarkeit miteinbeziehen (Business Case eines entsprechenden Projekts und des darauf folgenden Betriebs). Was der Abgleich mit dem EIF aber auch zeigt, ist, dass ein auf nur drei Grundbereichen basierendes Modell die sauber getrennten Analyseebenen des EIF verwischt.

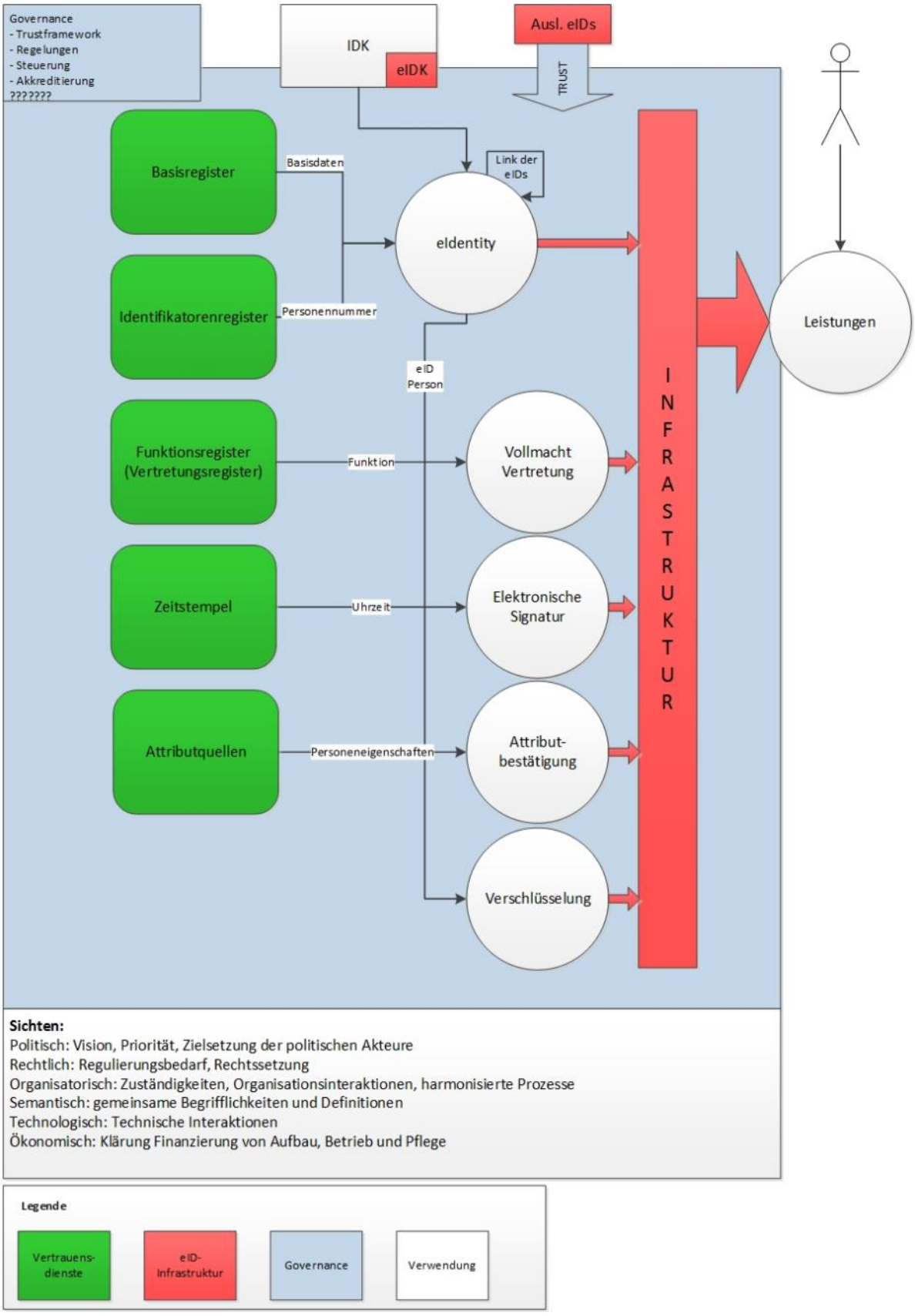


Abbildung 13: Modell Draft 3

Mit dem Modell Draft 3 (Abbildung 13) wurde in der Visualisierung ein deutlicher Wechsel vollzogen. Der Hintergrund dafür war die reifende Überzeugung, dass Bereitstellung und Nutzung im Modell die wesentlichen Grobstrukturen sein sollten. So findet sich hier eine Aufteilung auf Grundlagen der Bereitstellung: Governance (blau), Vertrauensdienste (grün), Infrastruktur (rot) und eID Funktionen (weiss). Die Nutzung, hier noch Leistungen genannt, ist visuell getrennt, ausserhalb des Bereiches der Bereitstellung und direkt bei den Nutzenden angeordnet. Der Einbezug des EIF als Analyseraster ist zumindest in Textform vorhanden, eine weitere Ausarbeitung im Sinne einer Visualisierung wurde angedacht. Selbiges gilt für den Teil der Leistungen, wobei dies in den damaligen Überlegungen als separate Grafik auf einer eigenen Seite Platz gefunden hätte.

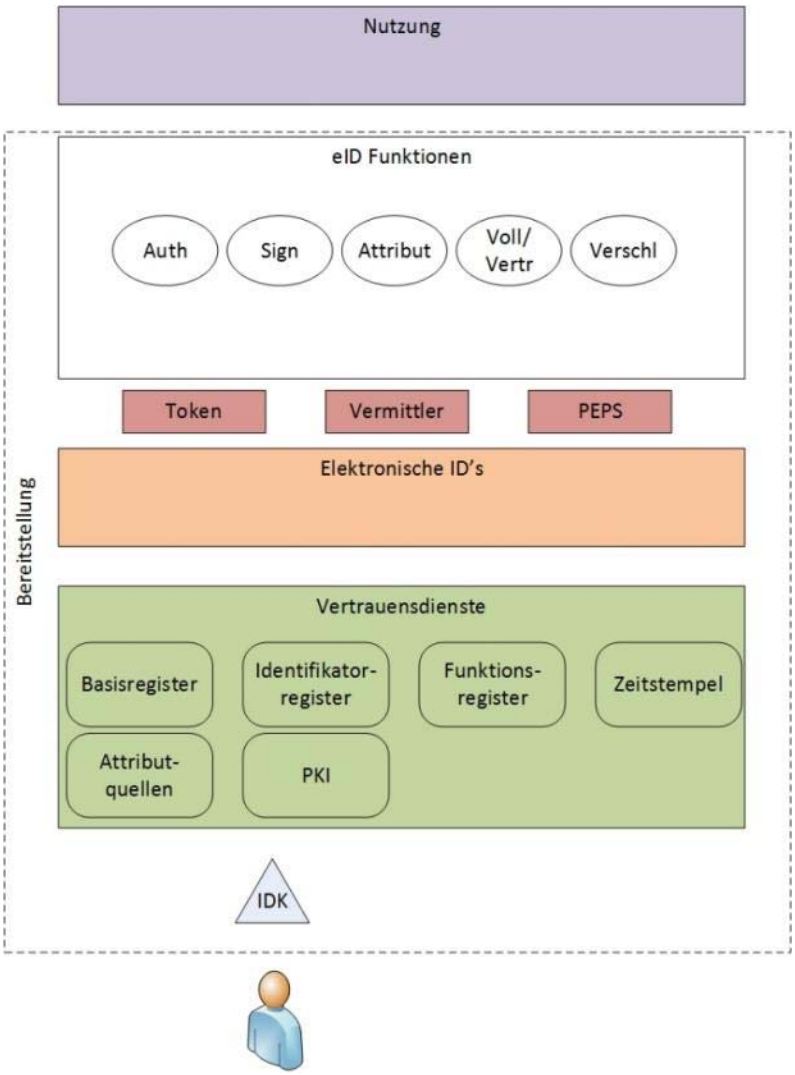


Abbildung 14: Modell Draft 4

Ausgehend davon wurde mit dem Draft Version 4 eine weitere Korrektur durchgeführt. Wie Abbildung 14 zeigt, nimmt die Nutzung hier (ebenfalls nicht weiter im Detail ausgearbeitet) eine symbolhafte, oberste Position ein. Sie ist visuell im Fokus. Wiederum deutlich getrennt davon wird der Teil der Bereitstellung präsentiert, der neu in die Grundbereiche der eID-Funktionen

Infrastruktur und Vertrauensdienste aufgeteilt ist. Als interessantes Detail taucht hier die Identitätskarte (IDK) selber auf, also das bereits heute im Umlauf befindliche Plastikdokument. Grund dafür ist, dass zu diesem Zeitpunkt noch nicht absehbar war, ob und wenn ja wie die Erneuerung der IDK direkt mit der eID zusammenhängen würde. In dieser Version noch nicht integriert waren der politische Rahmen sowie die rechtlich-institutionelle sowie die organisatorische Dimension.

Anzumerken bleibt, dass das abschliessende Modell (Vgl. Abbildung 15) gewisse Unterschiede zur Version aufweist, die in den Experteninterviews zum Einsatz kam. Die Änderungen ergaben sich hauptsächlich durch die Auswertungen der Interviews.

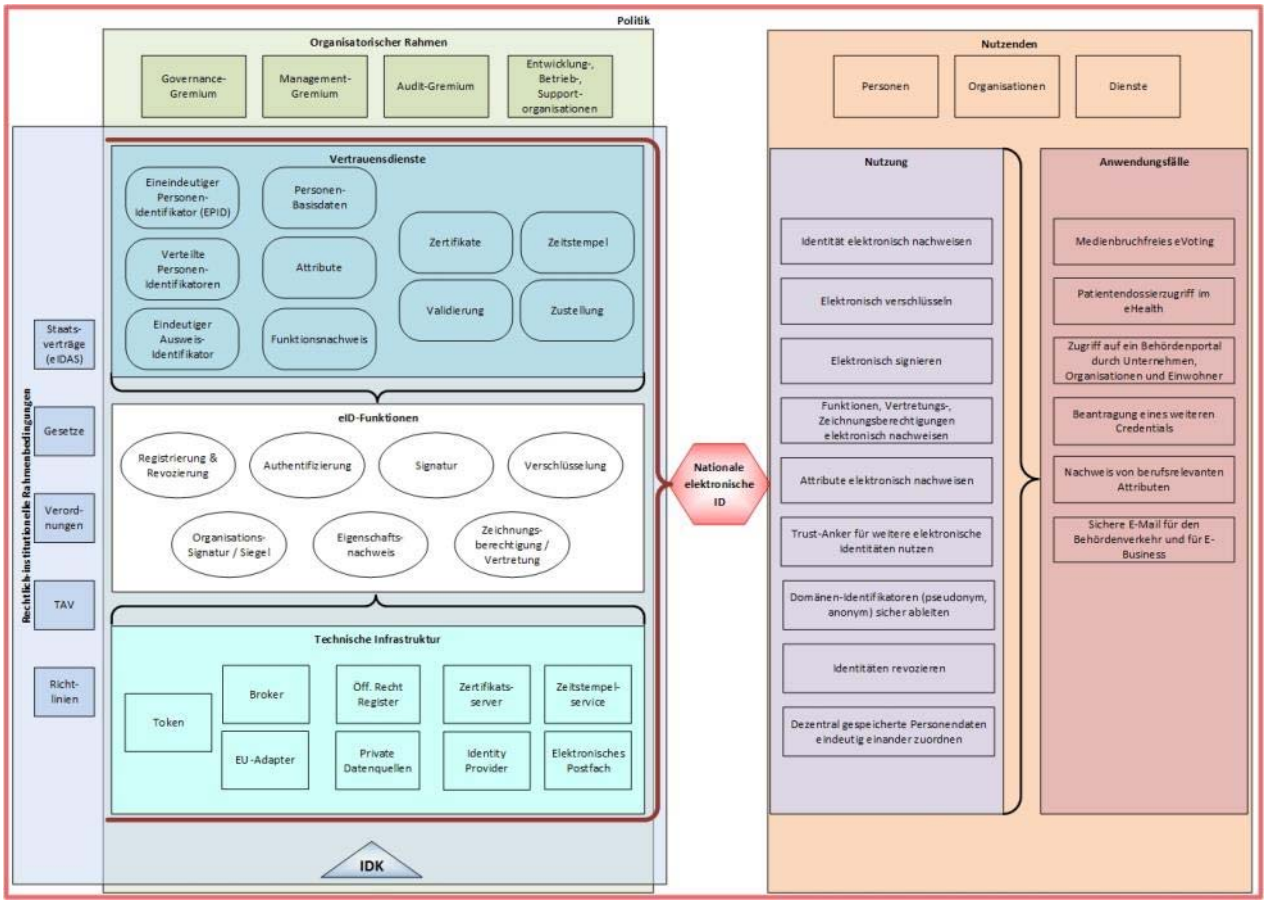


Abbildung 15: Modell Draft Interview Version

Nicht abschliessend aufgezählt waren dies:

- Bereitstellung und Nutzung haben die Seiten gewechselt, was auf Grund der Leserichtung von links nach rechts die Interpretation des Modells erleichtert.
- Nachdem sich abzeichnete, dass eine „eID als Chip auf der IDK“ wohl kaum realistisch sein wird (zumindest in den Überlegungen des fedpol), wurde diese aus dem Modell entfernt.
- Die Anwendungsfälle wurden ergänzt, um eine bessere Abdeckung über die E-Society Bereiche zu erhalten.

- Diverse Anpassungen erfolgten bei den Begriffen, etwa die Vermeidung von Abkürzungen sowie Präzisierungen.

Aus den Interviews kamen teils aber auch Rückmeldungen, die für weiterführende Arbeiten als relevant erachtet wurden, jedoch in der Visualisierung des Modells nicht für praktikabel erachtet wurden oder aber kaum Nutzen-stiftend gewesen wären. Hierzu gehören: die Qualität der eID, die Häufigkeit der Nutzung, die Benutzerfreundlichkeit, die Sicherheit, der Datenschutz, die Transparenz für die eID-Nutzenden sowie die Kosten und deren Verteilung. Aus Sicht der Autoren müssten diese Aspekte als Bewertungskriterien beim Design einer nationalen eID hinzugezogen werden. Das BFH-Projektteam erachtet diese auf Ebene von generischen Instanziierungen als nicht Nutzen-stiftend einsetzbar. Um diese Bewertungen seriös vornehmen zu können, bedarf es einer generischen und davon abgeleitet einer konkreten Instanziierung. Dazu gehören wieterführende Überlegungen dazu, wie die zu bewertenden Aspekte ausgestaltet werden sollen. Ebenfalls für weiterführende Arbeiten müsste dazu eine eigentliche Bewertungsmethodik entwickelt werden, um z.B. „Qualität“ oder „Benutzerfreundlichkeit“ mittels standardisierter Messgrössen beurteilen zu können.

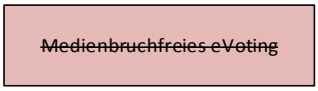
Das nunmehr vorliegende eID-Ökosystem Modell (Vgl. Abbildung 16 und Abbildung 17) stellt denn auch die organische Weiterentwicklung dar: Es erlaubt die Visualisierung der Nutzung getrennt von der Bereitstellung und umfasst alle relevanten Grundbereiche. Sinn der abschliessenden Darstellung ist auch die Ermöglichung von Zoom-In und Zoom-Flat bei gleichbleibender Grundform der Darstellung. Generische Instanziierungen (siehe Kapitel 4.4.0) wie spätere Konkretisierungen können als Visualisierungsebenen erstellt und aufeinander gelegt werden. Das eID-Ökosystem Modell kann so als Werkzeug zur Visualisierung einen sinnvollen Beitrag zu nachfolgenden Diskussionen leisten.

4.4 Ableiten von Instanziierungen des eID-Ökosystems

Nach den Experteninterviews und als Vorarbeiten für die externen Public Value Workshops wurden verschiedene Varianten generischer eID-Ökosystem-Instanziierungen erarbeitet. Weiterverfolgt und in die Workshops eingebracht wurden davon zwei eher ausgewogene Ausprägungen, die auf den folgenden Seiten dargestellt werden.

Erläuterung zum Signalement

Nutzung

	Gelb markierte Elemente der Nutzung sind aufgrund der durch den Staat bereitgestellten Elemente garantiert verfügbar.
	Durchgestrichene Elemente sind nicht garantiert verfügbar, da der Staat gewisse Elemente der Bereitstellung nicht garantiert.

Bereitstellung

	Gelb markierte Elemente der Bereitstellung werden durch den Staat selbst zwingend verfügbar gemacht.
	Grün markierte Elemente der Bereitstellung werden durch Private verfügbar gemacht. Der Staat ist jedoch für die Sicherstellung der Verfügbarkeit verantwortlich.
	Durchgestrichene Elemente sind nicht von staatlicher Seite garantiert verfügbar. Sie können jedoch von Privaten angeboten werden, wobei die Verknüpfung mit der Schweizer eID offen bleibt.

Tabelle 4: Erläuterung zum Signalement

Die gewählte Form der Visualisierung soll ermöglichen, Vor- und Nachteile der Instanziierungen schnell ersichtlich zu machen.

4.4.1 Vorüberlegungen zu möglichen Instanziierungen

Im Folgenden werden zunächst zwei nicht weiter verfolgte Versionen erläutert:

Maximalversion: Die Grundannahme hierzu wäre, dass die nationale eID in der E-Society für alle möglichen Online-Interaktionen eingesetzt wird, also nebst Identifikation und Unterschrift auch Funktionen wie die End-zu-End Verschlüsselung mitbringen. Verfügbar wäre die eID für alle natürlichen und juristischen Personen, die in der Schweiz tätig sind. Alle E-Government Dienstleistungen sind vorhanden und haben die eID integriert. Alle in der Schweiz angebotenen Online-Dienstleistungen, auch von Privaten angebotene, müssten die eID als Mittel zu Authentifikation und Signatur akzeptieren. Ebenfalls könnte mit der eID der Zugang zu Realwelt-Infrastrukturen geregelt werden. Die eID wäre ein elektronischer Hausschlüssel. Der Staat würde dafür entsprechende Rechtsgrundlagen schaffen und müsste die gesamte Bereitstellung übernehmen bzw. verantworten.

Eine solche Instanziierung ist alleine mit dem liberalen Grundverständnis der Schweiz kaum zu vereinbaren. Die Rechtsgrundlagen dazu zu schaffen wäre äusserst unrealistisch. Ausserdem würden Aufwand und generierter Nutzen in keinem akzeptablen Verhältnis zueinander stehen. Diese Maximalversion wurde deshalb nicht in die Diskussion innerhalb der externen Public Value Workshops übernommen.

Minimalversion: Hier wurde davon ausgegangen, dass die eID nur von Schweizer Staatsangehörigen bezogen werden kann und ausschliesslich für die kritischsten E-Government Anwendungen eingesetzt werden könnte, z.B. für E-Voting. Der Staat würde aber ausser Registrierung & Revozierung sowie Authentifizierung (und dazugehöriger Vertrauensdienste und technischer Infrastruktur) nichts selber liefern. Alles Weitere wäre der Privatwirtschaft überlassen.

Diese Variante würde im Kontext der E-Society kaum Nutzen generieren. Da seitens Staat keine an die eID gekoppelte Signatur garantiert würde, käme dies ausserdem einer Abkoppelung von ZertES nahe, was als unwahrscheinlich zu erachten ist. Entsprechend wurde auch diese Version nicht weiterverfolgt.

Ebenfalls diskutiert wurden konkrete Aspekte einer detaillierten Verteilung staatlicher und privatwirtschaftlicher Aufgaben. Dies wurde so nicht weiterverfolgt, da derartige Instanziierungen den Workshop Teilnehmenden zu wenig Raum für Diskussionen gelassen hätten. Ausserdem wären damit Design-Entscheide vorweg getroffen worden, die es erst noch zu diskutieren gilt, eben auf Basis der Resultate der vorliegenden Forschung.

Was am Ende für die Instanziierungen übrig blieb waren zwei eher ausgewogene Instanziierungen, die in der Folge erarbeitet wurden und in den Public Value Workshops als Diskussionsgrundlage eingesetzt wurden.

4.4.2 Instanziierungen des eID-Ökosystem

Instanziierung 1

Die Abbildung 16 (im Public Value Workshop genannt „Szenario Mönch“) stellt eine reduzierte Ausprägung als Instanziierung 1 dar. Der staatliche Bereitstellungsteil beschränkt sich auf all jene Elemente, die für die eID-Funktionen „Registrierung Revozierung“ sowie „Authentifizierung“ benötigt werden. Dabei ist jedoch dafür zu sorgen, dass von privater Seite die eID-Funktion „Signatur“ mit Koppelung an die eID auf dem Markt angeboten wird.

Folgende Grundannahmen gelten für die Instanziierung 1:

- Eine eID ist nur für Privatpersonen verfügbar: Personen mit Schweizer Staatsbürgerschaft können eine Schweizer eID beziehen. Personen aus EU-Staaten können die eID ihres jeweiligen EU-Mitgliedslands einsetzen.
- Die eID wird von Personen in der E-Society eingesetzt für Authentifikation und Signatur.
- Die Schweizer eID ist im E-Government (zumindest bei Bund, Kantonen und den zehn grössten Städten) breit integriert und akzeptiert sowie mit den wichtigsten E-Government Dienstleistungen verfügbar.
- In der Privatwirtschaft wird die elektronische Signatur infolge einfacher Durchführbarkeit und Überprüfbarkeit breit eingesetzt.
- Der Staat stellt sicher, dass Private unterschiedliche Signaturen auf dem Markt anbieten, die an die Schweizer eID angebunden sind.
- Die Usability der Schweizer eID muss sehr hoch sein.
- Die Integration der Schweizer eID in Lösungen Dritter muss sehr einfach sein.

Obschon eine solche Instanziierung 1 bei den Nutzungen nur zwei Einschränkungen mit sich bringt, sind die Auswirkungen davon bei den noch möglichen Anwendungsfällen wesentlich ausgeprägter: Ohne eine an die eID gebundene Verschlüsselung dürfte medienbruchfreies E-Voting kaum realisierbar sein. Das Fehlen von Zeichnungsberechtigung / Vertretung macht einen entsprechenden Nachweis im Online-Geschäft unmöglich. Analoges gilt für den Nachweis einer offiziellen Funktion. Da eine eID in dieser Ökosystem-Instanziierung ausschliesslich für natürliche Personen verfügbar ist, fällt auch das rechtsgültige Signieren durch Organisationen und Unternehmen weg. Ein sicheres Postfach für den Behördenverkehr und für E-Business wird zumindest von staatlicher Seite ebenfalls nicht bereitgestellt.

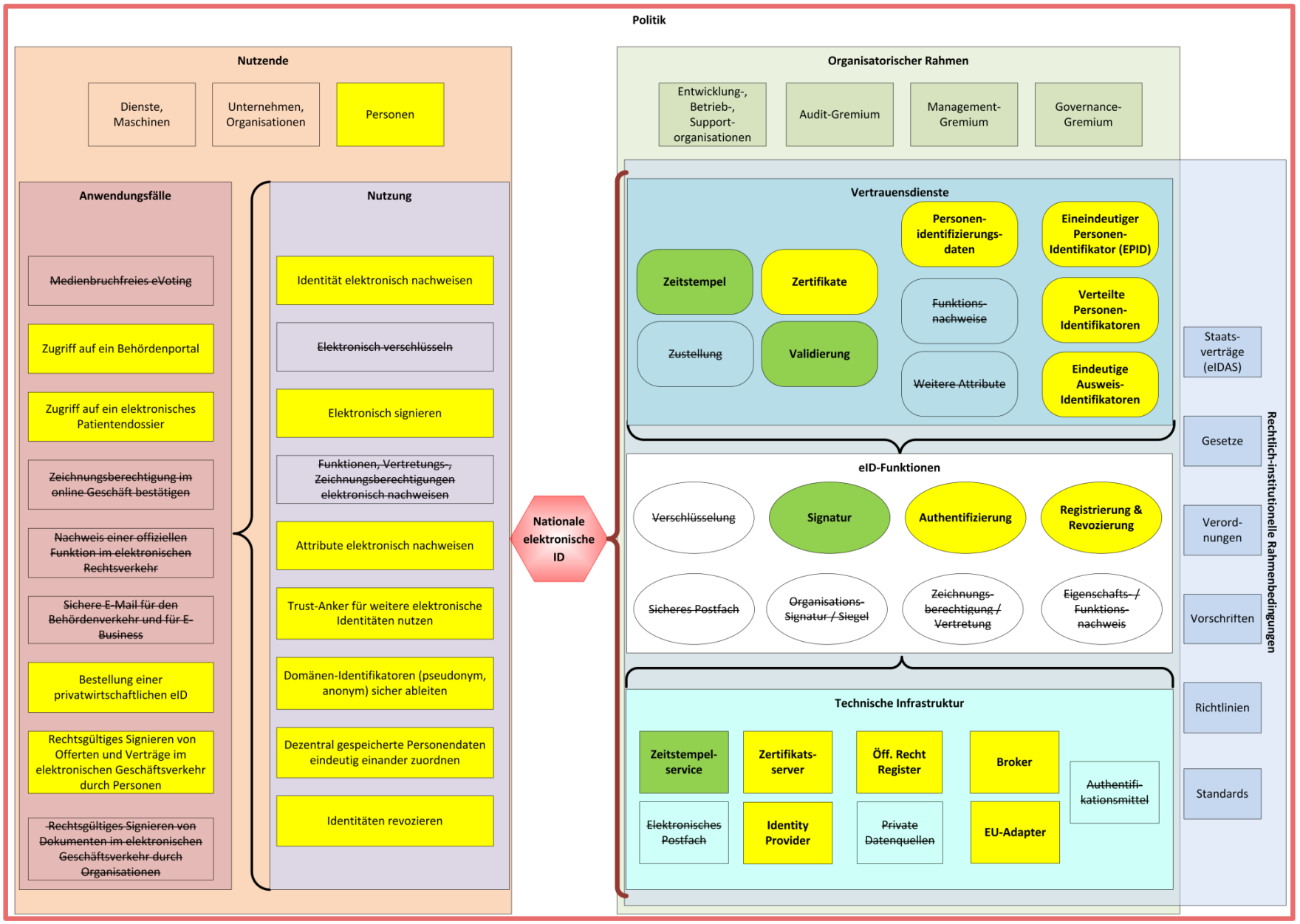


Abbildung 16: eID-Ökosystem Instanziierung 1

Instanziierung 2

Deutlich ausgeprägter ist die Rolle des Staates in Abbildung 17 (im Public Value Workshop genannt „Szenario Jungfrau“) und damit der Instanziierung 2. Der staatliche Bereitstellungsteil umfasst hier fast alle modellierten Elemente. Einzig auf die Bereitstellung einer an die Schweizer eID gebundenen Verschlüsselung und ein sicheres Postfach wird verzichtet.

Folgende Grundannahmen gelten für die Instanziierung 2:

- Die Schweizer eID ist für Personen und Organisationen mit Schweizer Niederlassung erhältlich.
- Die Schweizer eID wird – wo sinnvoll – für alle elektronischen Interaktionen in der E-Society eingesetzt.
- Alle E-Government Dienstleistungen werden auf allen föderalen Ebenen angeboten und haben die Schweizer eID integriert.
- Die Schweizer eID ist ein rechtlich anerkanntes Mittel für Authentifizierung und elektronische Signatur in E-Health und E-Education.
- Die Schweizer eID umfasst digitale Signaturen für Dokumente, Mails, etc.
- Alle privaten Schweizer Online-Geschäfte haben die eID integriert.

Diese sehr breite Ausprägung und darin das starke In-die-Pflicht-nehmen der öffentlichen Hand, auf allen föderalen Ebenen, garantiert eine entsprechend weite Abdeckung der garantiert möglichen Anwendungsfälle. Das medienbruchfreie E-Voting und sichere Email-Dienste werden jedoch auch weiterhin nicht angeboten.

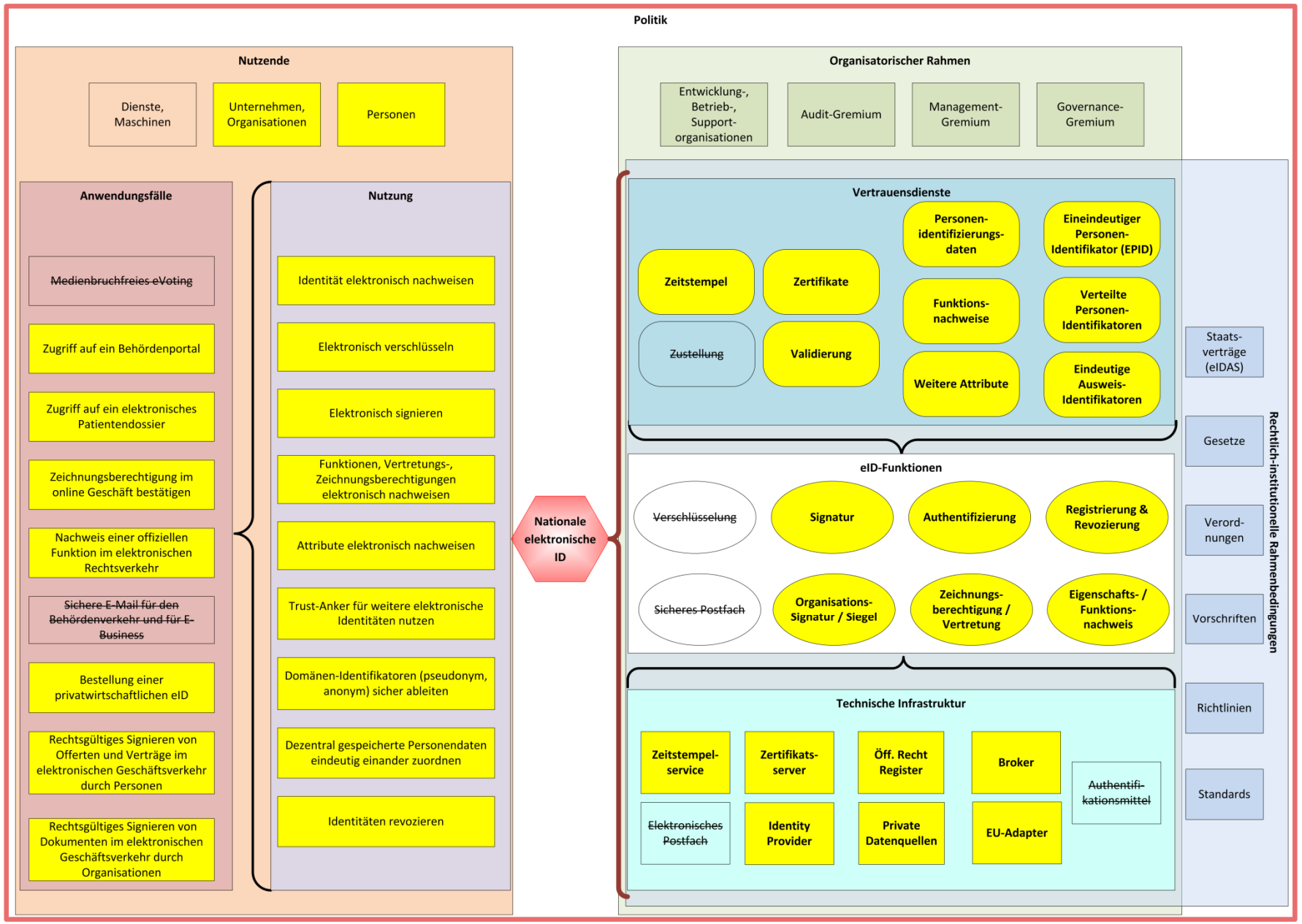


Abbildung 17: eID-Ökosystem Instanziierung 2

4.4.3 Anforderungen an konkrete Instanziierungen

Einige der ursprünglich identifizierten Anforderungen an ein eID-Ökosystem Modell mussten im Laufe der weiteren Arbeiten neu beurteilt werden, die wie folgt lauten:

- Darstellung des eID-, Register- und Vertrauensdienste-Universums: Abbildung des Zusammenspiels der staatlichen eIDs ab Level 2 nach eIDAS , bzw. Level 2 nach STORK und eCH-170, wichtiger kommerzieller eIDs ab Level 2, der staatlichen Register, der Attributzertifikatanbieter, der Anbieter von Zeitstempeldiensten, Signaturdienste und weiterer Vertrauensdienste.
- Darstellung des rechtlichen Kontexts: Unterstützung der Diskussion der Rechtssetzung und insbesondere der Schaffung von Transparenz bezüglich den konkreten Handlungsbedarf bei der Rechtssetzung sowie bei den Auswirkungen internationaler Regulierungen. Hier ist zwischen der Diskussion der Rechtsetzung zur eID (hierfür werden klare Anforderungen benötigt), den Anforderungen an die Rechtssetzung zur Ermöglichung eines bilateralen Vertrags mit der EU und der Unterstützung einer breiteren politischen Diskussion über weitergehende Rechtsetzungsaufträge im Kontext wichtiger Anwendungsfälle zu unterscheiden.
- Beschreibung von Aufgaben, Rollen sowie Zuständigkeiten: Identifikation der Aufgaben und der Rollen im Gesamtsystem und Klärung der Zuständigkeiten. Hierbei sollte insbesondere die Abgrenzung staatlicher und privatwirtschaftlicher Aufgaben (d.h. die Identifikation der jeweiligen Systemgrenzen) möglich sein, um Planungssicherheit zu schaffen und die Entwicklung eines (eID-)Markts zu fördern.
- Beschreibung von Schnittstellen und Abhängigkeiten: Identifikation aller Arten von Schnittstellen und aller Abhängigkeiten. Dies sollte entlang der Strukturierung europäischer Interoperabilitätsframeworks geschehen, wobei prioritär organisatorisch und technische Schnittstellen und Abhängigkeiten dargestellt werden sollten.

Diesen Anforderungen kann eine generische Modellierung nicht gerecht werden. Sie sind jedoch für weitere Arbeiten zur nationalen eID und deren Ökosystem zwingend zu berücksichtigen, sobald auf Stufe der Entscheidungsträger ein Entscheid für eine SOLL-Instanziierung gefällt wurde. Dann können konkrete Ausprägungen des eID-Ökosystems erarbeitet werden. Sobald die generischen Elemente durch realweltliche Instanziierungen abgebildet sind, lassen sich oben genannte Anforderungen ausarbeiten und entsprechende Massnahmen für eID und Ökosystem ableiten.

4.5 eID-Ökosystem Modell als Instrument zur Massnahmenerarbeitung

Die generische Tauglichkeit des vorliegenden Modells als Instrument wurde über Experteninterviews (siehe Kapitel 5) und über die Diskussion von zwei Instanziierungen (siehe Kapitel 1.1) in zwei halbtägigen Public Value Workshops (siehe Kapitel 6) geprüft und für gut befunden.

Für die weiteren Arbeiten rund um die nationale eID und das eID-Ökosystem empfiehlt sich das folgende Vorgehen. Ausgehend von einer generischen Instanziierung, die für tauglich befunden wird, ist je eine konkrete IST- und eine SOLL-Ausprägung zu erarbeiten. Dabei sind wiederum, von nunmehr spezifischen Nutzenden ausgehend, passende Anwendungsfälle zu definieren und die dazu notwendigen Nutzungen abzuleiten.

In der Folge ist dann zu diskutieren:

1. Welche konkreten Akteure bzw. Stakeholder welche Teile der Bereitstellung zu leisten haben bzw. zu leisten bereit sind
2. Wie der organisatorische Rahmen zu implementieren ist.
3. Was diese konkrete Instanziierung an rechtlich-institutionellen Anpassungen erfordert.
4. Welche Rollen, Aufgaben und Verantwortungen die konkreten Akteure innerhalb des politischen Rahmens wahrzunehmen haben.

Ausgehend von der Nutzungsseite ergeben sich diverse Abhängigkeiten auf Seite der Bereitstellung. Diese lassen sich aber nur anhand konkreter Ausprägungen des Ökosystems verlässlich identifizieren. Aus dem Delta von SOLL-und IST-Ausprägungen können Massnahmen zur Förderung des eID-Ökosystems und der nationalen eID erarbeitet werden.

5. Experteninterviews

5.1 Aufbau und Ziele der Interviews

Als Vorbereitung auf die Interviews wurde ein Interviewleitfaden erstellt, der Leitfragen für die Interviews beinhaltet. Darüber hinaus wurden im Rahmen der Vorbereitungen Ziele definiert, die durch die Interviews verfolgt werden sollen. Dabei handelt es sich um die folgenden Ziele:

- Verifikation des eID-Ökosystem-Modells
- Identifikation von möglichen Instanziierungen des eID-Ökosystem-Modells
    - Welche Elemente braucht es?
    - Wer bietet diese an?
    - Wer ist für die Elemente verantwortlich?
- Wie sollte die Bereitstellung von Diensten/Elementen erfolgen?
- Identifikation von kritischen Erfolgsfaktoren – bezogen auf alle Stakeholder (Relying Parties, Bürger)
- Auskünfte hinsichtlich der Nutzung
    - Was muss gegeben sein, dass eine eID verwendet wird?
    - Rolle des eindeutigen Personenidentifikator
    - Welche Qualität wird gefordert?
- Beziehungsmanagement in der Verwaltung und Privatwirtschaft (Akzeptanz vom Ökosystem und einer eID).

Eine technische Spezifikation und eine abschliessende Validierung des Modells waren nicht Ziele der Interviews.

Die Interviews wurden wie in der folgenden Tabelle dargestellt strukturiert und hatten eine Dauer von ca. 1 Stunde.

Nr.	Phase	Dauer	Frage / Tasks
1	Einführung	5 Min	• Information zu Gegenstand und Ziel des Projekts • Interviewstruktur aufzeigen • Rahmenbedingungen zu Interview klären
2	Modell-Erläuterung	15 Min	• Kurze Beschreibung des Modells auf oberster Ebene
3	Hauptteil	45 Min	• Fragen
4	Abschluss	5 Min	• Zusammenfassung und Ausblick • Nachfrage zu nicht angesprochenen Aspekten im Modell • Weiteres Vorgehen

Tabelle 5: Interviewstruktur

Insgesamt wurden 23 Interviews durchgeführt. Dabei wurden 14 Personen aus unterschiedlichen föderalen Verwaltungsebenen und 9 Personen aus der Privatwirtschaft (u.a. eID-Lösungsanbieter und Nutzer) interviewt.

Bei der Auswahl der Interviewpartner wurden somit alle zentralen Stakeholder-Gruppen berücksichtigt. Dies wird auch deutlich in der folgenden Grafik, in der die interviewten Stakeholder rot markiert sind.

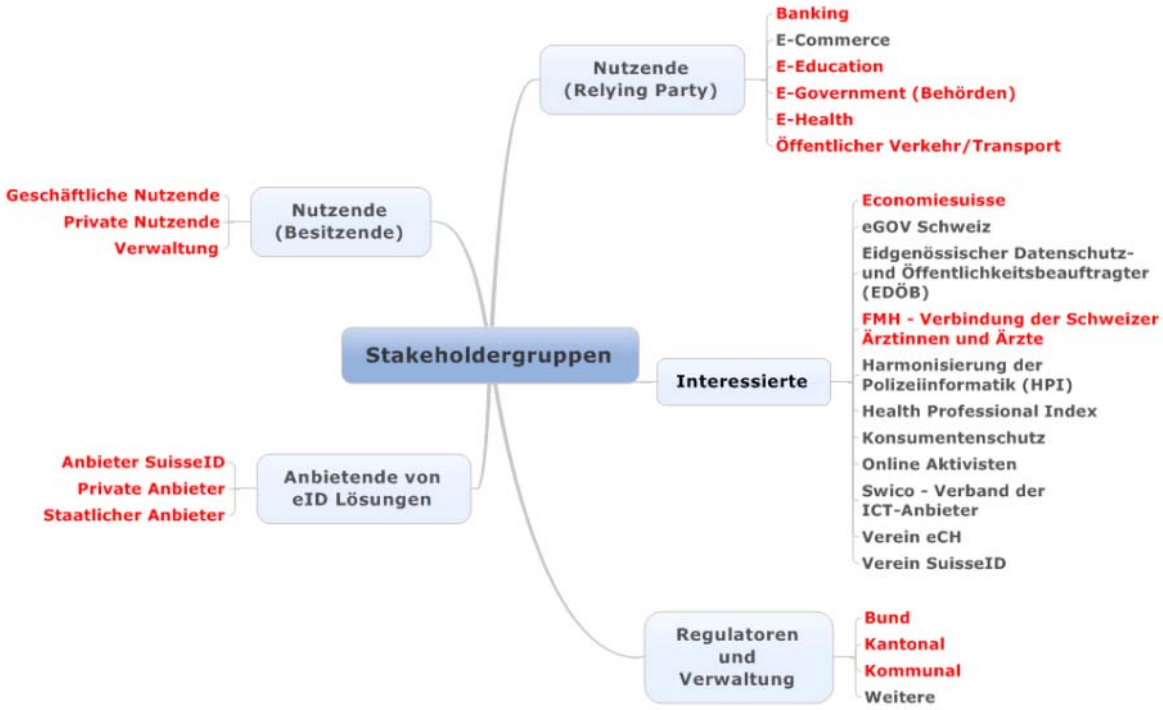


Abbildung 18: Übersicht der interviewten Personen

Alle interviewten Personen sind auf Ebene Geschäftsleitung resp. Direktionsebene tätig.

5.2 Vorgehen bei der Auswertung der Interviews

Für die Auswertung der Interviews wurden die während der Interviews erstellten Protokolle nach den folgenden Begriffen im Analysewerkzeug Atlas-TI „getagt“:

Tags	Bereiche
1. Ausgestaltung eID-Lösung	Anwendungsfälle und Nutzung
2. Einführung staatlicher eID	Nutzen
3. Funktionalitäten eID-Lösung	Anwendungsfälle und Nutzung
4. Nutzung eID-Lösung	Anwendungsfälle und Nutzung
5. Verantwortlichkeiten / Governance bezüglich eID-Lösung	Bereitstellung
6. eID-Ökosystem Modell	Modellverständnis und -validierung
7. Interaktion Akteure mit eID Systemkomponenten	Anwendungsfälle und Nutzung
8. eID-Lösungsbewertung	Anwendungsfälle und Nutzung
9. Unterstützende Massnahmen zur eID	Erfolgsfaktoren
10. Organisationsperspektive auf eID-Lösung (Persp. Interviewte) auf Nutzung	Anwendungsfälle und Nutzung
11. Organisationsperspektive auf eID-Lösung (Persp. Interviewte) auf Nutzen	Nutzen
12. Modell-Verständlichkeit Überblick	Modellverständnis und –validierung
13. Modell-Verständlichkeit Elemente	Modellverständnis und –validierung
14. Situierbarkeit der Interviewten im Modell	Nutzen
15. Verständlichkeit der Modellkategorien	Modellverständnis und -validierung
16. Nutzung/Mehrwert/Aufwände eID-Lösung	Nutzen
17. Erfolgsfaktoren	Erfolgsfaktoren
18. Hinderungsfaktoren	Hindernisfaktoren
19. Die fünf wichtigsten Erfolgsfaktoren	Erfolgsfaktoren
20. Bedeutung des eindeutigen Personenidentifikators zwingend	Modellverständnis und -validierung
21. Bedeutung des eindeutigen Personenidentifikators nice to have	Modellverständnis und -validierung
22. Bedeutung des eindeutigen Personenidentifikators Risiko	Modellverständnis und -validierung
23. Bereitstellung Staat Elemente	Bereitstellung
24. Bereitstellung Staat Leitbehoerde	Bereitstellung
25. Bereitstellung Private Elemente	Bereitstellung
26. Bereitstellung Private Voraussetzungen	Bereitstellung
27. Persönliche Einstellung zu eID	Nutzen
28. Verbesserungspotenzial bezüglich eID-Ökosystem-Modell	Modellverständnis und -validierung

Tabelle 6: Übersicht von Tags und Bereichen

Die daraus resultierenden Aussagen wurden anschliessend auf die sechs Bereiche Modellverständnis und -validierung, Anwendungsfälle und Nutzung, Nutzen, Erfolgsfaktoren, Hindernisfaktoren und Bereitstellung aufgeteilt.

Die nachfolgende Auswertung der Interviews basiert auf dieser Aufteilung und beinhaltet somit alle zentralen Aussagen der geführten Interviews.

5.3 Auswertung der Interviews

5.3.1 Modellverständnis und –validierung

5.3.1.1 Aussagen zum Gesamtmodell

Als Grundlage für die Interviews wurde eine erste Version des Modells verwendet. Dieses wurde als verständlich und vollständig betrachtet, wobei die Komplexität des Modells als hoch bewertet wurde.

Einige Interviewteilnehmer wiesen auf den hohen Abstraktionsgrad des Modells hin oder es wurde als sehr generisch eingestuft. Während das Modell insgesamt als hilfreich betrachtet wurde, scheint die Zugänglichkeit nicht intuitiv gegeben zu sein. Um die Modellverständlichkeit und die Zugänglichkeit zu erhöhen, haben die Befragten Vorschläge formuliert. Diese werden in Kapitel 4.3 behandelt.

5.3.1.2 Aussagen zu einzelnen Modellelementen

Eineindeutiger Personenidentifikator (EPID)

Dem EPID wird sowohl seitens Privatwirtschaft wie auch seitens Behörden ein hoher Wert zugesprochen. Circa die Hälfte der Befragten hat zu diesem Element eine Aussage gemacht und dessen Wichtigkeit bewertet. So setzt z.B. ein medienbruchfreies Personendossier den EPID voraus. In einer Aussage wird darauf verwiesen, dass die Einführung eines EPID dem Staat jährliche Kosten in Millionenhöhe einsparen würde, z.B. beim Nachvollziehen von Personen-(Daten) nach einem Umzug. Auch seitens Privatwirtschaft wäre ein EPID sehr willkommen. Ein solches Vorhaben bringe ein sehr hohes Vereinfachungspotenzial. Die Wirtschaft würde in die Einführung eines eineindeutigen Schlüssels investieren und Zahlungsbereitschaft zeigen. Allerdings wurde in einzelnen Voten die Schwierigkeit vermerkt, schon nur die rechtlichen Grundlagen für einen EPID zu erarbeiten. Bereits das Gelingen dieses Schritts wäre ein sehr grosser Erfolg.

Weitere Voten weisen darauf hin, dass heute in vielen Systemen bereits die AHVN13 als Personenidentifikator verwendet wird. Wird ein EPID eingeführt, ist unbedingt zu bedenken, welche Kosten ein Systemwechsel von der AHVN13 zu einer „neuen Nummer“ generieren würde.

Personenidentifizierungsdaten

Ein Votum betont die Wichtigkeit der Pflege von Basisdaten. Es ist wichtig, die Zuständigkeit für diese Aufgabe im Voraus zu regeln. Die Prozesse müssen in die Prozesse der Datenpflege im Zentralen Migrationsinformationssystem ZEMIS und in den Zivilstandsregistern eingebunden werden.

Attribute

Die Interviewten sind sich einig, dass Attribute nicht zentral zu führen sind. Sie sollten aus verschiedenen Applikationen abrufbar sein. Die Prozesse der Datennachführung müssen jedoch klar geregelt sein.

eID-Funktion – Authentifizierung / Registrierung und Revozierung

Diese Funktionen werden als wesentliche Funktionen betrachtet. Eine Aussage untermauert deren Bedeutung, indem sie 95% der Anwendungsfälle diesen Funktionen zuschreibt. Diese Funktionen sind von besonderer und zentraler Bedeutung in der Verhinderung von Missbrauchsfällen. Ein Votum bezeichnet diese Funktionen gar als Kernfunktionen der eID. Die eID soll als Pass für die digitale Welt fungieren und das „Reisen in der digitalen Welt" ermöglichen. Die bestehenden Prozesse um den physischen Pass haben sich bisher bewährt. Weil in diesem Prozess – weniger noch als der Business Case – Vertrauen ein zentrales Element darstellt, sind dies Funktionen, die vom Staat bereitzustellen sind.

eID-Funktion – Signatur

Zu dieser Funktion wurden in den Interviews unterschiedliche Meinungen geäussert. Die einen sehen die Signatur-Funktion als gekoppeltes aber nicht mit der eID verbundenes Phänomen. Es wird auch darauf hingewiesen, dass diese Funktion bereits angeboten wird. Andere sehen die Funktionen Signatur sowie Organisations-Signatur/Siegel, ähnlich wie die Funktionen Registrierung und Revozierung/Authentifizierung, als hoheitliche Aufgabe, weil hierbei das Vertrauen eine grössere Rolle spielt als der Business Case. Wieder andere verweisen auf eine Abnahme der Bedeutung dieser Funktion bei Transaktionen, die im Voraus bezahlt werden. Letztlich sind in den Aussagen zu dieser Funktion nicht nur gegenteilige Meinungen, sondern auch eine ambivalente Haltung festzustellen. Während die Funktion grundsätzlich als wichtig eingestuft wird, soll bei der Einführung einer eID darauf verzichtet werden, falls es den Erfolg der eID verhindern sollte. Diese Ambivalenz steht in Zusammenhang mit der Auffassung, die eID solle möglichst einfach ausgestaltet sein, um eine breite Nutzung zu ermöglichen (siehe auch Kapitel 5.3.6).

eID-Funktion – Verschlüsselung

Das Verschlüsseln ist wichtig oder wird in den kommenden Jahren immer wichtiger werden. Ähnlich der Signatur-Funktion lässt sich auch hier eine ambivalente Haltung feststellen. Entsprechend der oben erläuterten Logik, die eID möglichst einfach auszugestalten, besteht die Meinung, dass die Bereitstellung dieser Funktion wünschenswert wäre, aber nicht zwingend ist.

eID-Funktion – Organisations-Signatur/Siegel

Auch hierzu wurden kontroverse Meinungen geäussert. Während einzelne Interviewte diese Funktion als unbedingt vom Staat anzubietendes Element betrachten, finden andere, dass die Anbindung dieser Funktion an eine eID die Komplexität des Produkts zu stark erhöhen würde und damit den Erfolg der eID gefährden könne. Andere empfanden diese Funktion als unnötig oder nicht umsetzbar.

5.3.2 Mögliche Anwendungsfälle und Nutzung

Im Rahmen der Interviews wurde gefragt, welche Nutzungen und Anwendungsfälle die Interviewten für ihre Organisation, aber auch im Allgemeinen sähen. Den Interviews ist zu entnehmen, dass die Liste der Anwendungsfälle beliebig erweiterbar ist. Für fast alle im Modell aufgelisteten Nutzungen sind Anwendungsfälle vorstellbar. In den Aussagen wird jedoch bereits eine Priorisierung der von der eID anzubietenden Nutzungen vorgenommen. Dabei wurde klar zum Ausdruck gebracht, dass die Nutzung der eID für den *elektronischen Nachweis der Identität* von allen Befragten als wesentlich eingestuft wird. Als weitere wichtige Nutzung der eID wird der *elektronische Nachweis von Attributen oder Funktionen* betrachtet. Die anderen Nutzungen werden grösstenteils als nice-to-have bewertet.

Die Liste der Anwendungsfälle aus dem Modell kann nach Abschluss der Interviewrunde mit weiteren Anwendungsfällen ergänzt werden. Zu nennen sind hier alle E-Government-Dienstleistungen, z.B. im Steuerbereich, aber auch auf Gemeindeportalen, für B2B-Transaktionen, E-Education, E-Health, aber auch für die Realwelt-Authentifizierung für den Infrastrukturzugang sowie für ein medienbruchfreies Personendossier.

Nachfolgend sind diejenigen Anwendungsfälle aufgelistet, für welche die Befragten konkrete Anwendungsfälle für ihre Organisation sehen. Sie sind nach ihrer primären eID-Nutzung gruppiert.

Identität elektronisch nachweisen

Für das elektronische Nachweisen der Identität konnten fast alle Befragten mindestens einen konkreten Anwendungsfall nennen. So sind z.B. Anwendungen im Bereich meldepflichtige Gesundheitsdaten, für die Nachvollziehbarkeit von Mutationen in Informationssystemen, für Zutrittskontrollen (etwa in Online-Lesesälen), für die auf Identifizierung basierende Einsicht auf Datenbestände, bei Kontoeröffnungen, bei Tumorboards per Videokonferenz, bei Erhebungen oder für Online-Transaktionen auf Behördenportalen vorstellbar. Nicht relevant ist diese Nutzung bei Transaktionen, die durch sofortige Zahlung quittiert werden. In diesem Fall spielt die Identität des Zahlenden keine Rolle. Der Identifikationsnachweis kommt hierbei erst ins Spiel, wenn Kunden für eine Dienstleistung nicht sofort bezahlen.

Attribute / Funktionen elektronisch nachweisen

Diese Nutzung findet seinen Anwendungsfall z.B. in Dienstleistungen, die an Altersbeschränkungen gebunden sind, oder beim Ausstellen von Rezepten für Medikamente sowie bei der Gesuchstellung für Einsicht auf Datenbestände basierend auf einen Funktionsnachweis.

Elektronisch verschlüsseln

Die elektronische Verschlüsselung ist eine Nutzung, die vor allem im Gesundheitsbereich wichtig ist. Es geht darum, einen gesicherten Kommunikationskanal zwischen Patient und Anbieter bereitzustellen. Vorstellbar wären auch das Verfassen von Versicherungsberichten, die Meldung bei Spitalportalen, etc. Aber auch im Behördenverkehr, z.B. im Rahmen von internen Vernehmlassungen, wäre eine solche Nutzung vorstellbar.

Elektronisch signieren

Anwendungsfälle für das elektronische Signieren sind in allen Bereichen zu finden: Bei Vertragsabschlüssen oder z.B. auch im Kontext einer Organspende wäre das elektronische Signieren einsetzbar.

Trust-Anker für weitere elektronische Identitäten

Die eID könnte die verschiedenen elektronischen Identitäten im E-Health-Bereich zusammenführen. Diese Nutzung ist auch für den E-Education Bereich interessant. In der Privatwirtschaft könnte sie mit bestehenden Online-Identitäten verlinkt werden, wie z.B. mit der Mobile-ID. Sie könnte aber auch als Trust Anchor für die Bezahlfunktion genutzt werden.

Identitäten revozieren

Diese Nutzung ist stark mit dem elektronischen Identitätsnachweis verknüpft und wird entsprechend als wichtig empfunden.

Dezentral gespeicherte Personendaten eindeutig einander zuordnen

Diese Nutzung ist stark mit dem elektronischen Identitätsnachweis verknüpft und wird entsprechend als wichtig empfunden.

5.3.3 Nutzen einer eID

E-Health

Ein zentraler Nutzen einer nationalen eID wird von den interviewten Personen im Gesundheitswesen gesehen. Wenn über eine sichere Identifikation und einen verschlüsselten Kanal zwischen Patienten und Anbietern kommuniziert werden kann, bringt dies einen grossen Nutzen im Bereich E-Health. Aktuell hat das elektronische Signieren im E-Health-Bereich noch keine zentrale Bedeutung, allerdings wird sich dies voraussichtlich in weniger als zehn Jahren ändern (z. B. hinsichtlich der Einführung des elektronischen Patientendossiers, von elektronischen Archivierungen, elektronischen Rezepten, Organspenden, etc.).

Geschäftsprozesse

Die Interviewpartner sehen betriebswirtschaftliche Vorteile im Rahmen von Zertifikaten in Workflows, die Medien- und Prozessunterbrüche eliminieren und damit Kosten reduzieren.

Ebenfalls wird in der eID ein grosser Nutzen gesehen, um das Ziel von papier- bzw. medienbruchfreien Prozessen verfolgen zu können.

Im Rahmen des Behördenverkehrs würde durch die eID eine notwendige Rechtssicherheit entstehen. Heutzutage werden sehr häufig Dokumente unverschlüsselt per E-Mail verschickt, z.B. Vernehmlassungsanfragen und entsprechende Antworten, was durch die Einführung einer eID unter erhöhten Sicherheitsaspekten erfolgen könnte.

Hinsichtlich grenzüberschreitender Geschäfte wird insbesondere in der Privatwirtschaft ein erhöhter Nutzen beim Einsatz von eIDs gesehen.

Die Server-Signatur ist ebenfalls eine immer stärker gewünschte Funktion, d. h. Privatpersonen können Browser-basiert, ohne Chip, ohne Token, ohne PIN, etc. signieren. Auch hier würde eine eID einen grossen Mehrwert bringen.

Auch die Tatsache, dass das Signieren im Rahmen der Online-Kommunikation eine immer grössere Rolle spielt, wird von den interviewten Personen als ein Grund angesehen, der eID einen entsprechenden Mehrwert zuzuschreiben.

Strategischer Nutzen

Die Meinung einiger interviewter Personen ist, dass die eID ein Element ist, das in der Schweiz bis jetzt fehlt und aus diesem Grund im Rahmen der digitalen Agenda als Schwerpunkt zu berücksichtigen ist. Ebenfalls wird in der eID ein Werkzeug gesehen, das zum Aufbau einer Informationsgesellschaft beiträgt.

Die nationale eID oder eine abgeleitete eID ist darüber hinaus aus Sicht einiger Interviewpartner sehr zentral, um weitergehende Ziele beispielsweise in den Bereichen Justiz und Polizei zu verfolgen.

Abschliessend lässt sich den Interviewaussagen entnehmen, dass überall dort, wo Dienstleistungen bezogen werden und die Identität gesichert bewiesen werden muss, die eID einen grossen Mehrwert für die Nutzer bringen kann.

5.3.4 Erfolgsfaktoren der eID und daraus resultierende Fördermassnahmen

Durchgehend werden von allen interviewten Personen die Usability und das Vertrauen in die eID durch die Bürger als absolut zentrale Erfolgsfaktoren herausgestellt. Damit einhergehend werden als weitere Erfolgsfaktoren eine aktive Kommunikation und die Aufklärung der Bürger hinsichtlich der eID genannt.

Des Weiteren wird von den meisten Interviewpartnern eine flexible Lösung für die eID gefordert, ebenso wie breite Anwendungsmöglichkeiten. Auch der Kostenaspekt wird von vielen interviewten Personen als Erfolgsfaktor betrachtet, jedoch wird ihm keine so zentrale Rolle zugeschrieben wie etwa den zuvor genannten Erfolgsfaktoren.

Im Folgenden werden die Aussagen zu den zentralen Erfolgsfaktoren aus den Interviews im Detail geschildert.

Usability

In allen Interviews werden ein einfacher Beschaffungsprozess und eine einfach Anwendung im Zusammenhang mit der eID als absolut zentrale Erfolgsfaktoren angesehen. Im Rahmen der Beschaffung einer eID wird beispielsweise die Reduktion von persönlicher Anwesenheit an einer Ausgabestelle auf ein absolutes Minimum gefordert. Neben einem einfachen Beschaffungsprozess und einer einfachen Nutzung der eID, z. B. durch einen einfach gestalteten Identifikationsprozess, werden auch einfache Anwendungsfälle als notwendig erachtet, um eine hohe Akzeptanz und eine umfangreiche Nutzung der eID zu fördern. So wird dem Einsatz der eID bei einfachen Dienstleistungen von einigen interviewten Personen ein hoher Nutzen zugeschrieben. Hingegen wird bei komplexen Anwendungsfällen, wie beispielsweise einer erklärungsbedürftigen Ablehnung eines Baugesuchs, nach wie vor eine physische Präsenz als wichtig erachtet.

Im Rahmen der Interviews kam der Vorschlag auf, einen Anwendungsfall im Rahmen des Ökosystems zu erstellen, der eine hohe Usability hat und der möglichst viele Bürger betrifft. Von vielen interviewten Personen werden Anwendungsfälle, die eine hohe Nutzerzahl und -häufigkeit aufweisen, als wesentlicher Erfolgsfaktor gesehen, um eine eID etablieren zu können.

Einen weiteren Aspekt, der in Bezug auf Usability der eID zu berücksichtigen ist, sieht ein Interviewpartner darin, dass im Gesundheitsbereich, in dem eine eID auch zum Einsatz kommen könnte, vermehrt ältere Personen und damit Nutzer existieren (Demografischer Wandel). Beim Design der Lösung sind deshalb die Bedürfnisse dieser Usergruppe entsprechend zu berücksichtigen.

Ebenfalls wird eine zuverlässige und kompetente Unterstützung für die Nutzer der eID – beispielsweise im Rahmen eines Supports durch Relying Parties oder Dritte (Help Desk) – für die Usability als sehr wichtig betrachtet. Für die im Hochschulbereich verbreitete SWITCH-AAI-Lösung (Authentication and Authorization Infrastructure) wird dieser Aspekt rückblickend als ein zentraler Erfolgsfaktor betrachtet.

Von einigen Interviewpartnern wird auch für die Prozesse im Umsystem einer eID (beispielsweise einer Re-Zertifzierung) eine einfache Gestaltung gefordert, um den Erfolg einer eID zu erhöhen.

Um den Anforderungen an Sicherheit und eine gleichzeitig einfache Handhabung der eID gerecht zu werden, wird in den Interviews teilweise der Vorschlag gemacht, die Usability von der erforderlichen Sicherheitsstufe abhängig zu machen. Ebenfalls wurde in den Interviews mehrfach angeregt, zunächst mit einer einfachen Lösung und einer entsprechenden tiefen Qualitätsstufe zu starten und die eID dann später mit zusätzlichen Zertifikaten (höherer Qualitätsstufen) auszustatten.

Die Unabhängigkeit von einem Medium und spezifischen Plattformen wurde in einigen Interviews als Erfolgsfaktor gesehen. Als Beispiel für mögliche Probleme bei einer starren Anbindung an ein Medium wurde ein Arzt erwähnt, der seine Karte am Morgen möglicherweise vergessen könnte und ohne diese Karte seine eID nicht nutzen kann.

Sicherheit und Vertrauen

Sicherheit und Vertrauen in die eID sind für fast alle interviewten Personen ganz entscheidende Erfolgsfaktoren.

Das Vertrauen der Bürger in die eID-Lösung wird im Rahmen der Interviews als absolut zentral angesehen. Dazu muss gemäss den interviewten Personen zunächst das Vertrauen in die Lösung gewonnen werden. Je umfangreiche die Nutzungsmöglichkeiten sind, desto wichtiger erscheint die Vertrauensgewinnung in die Lösung.

Ein Vertrauen in die Lösung benötigt Standards denen die Nutzer vertrauen. Es muss ein Weg gefunden werden, über den gesteuert werden kann, dass der Bürger der eID vertraut. Wichtig ist auch, dass Datenschützer hinter einer eID stehen und keine Befürchtungen verbreiten.

Der Schutz der Identität und das Verhindern von Identitätsdiebstahl ist ebenfalls ein sehr häufig genannter Erfolgsfaktor im Zusammenhang mit einer eID in der Schweiz. Dem Datenschutz und dem Persönlichkeitsschutz müssen demnach grosse Aufmerksamkeit gewidmet werden.

Als Möglichkeit ein entsprechendes Vertrauen in eine eID sicherzustellen, wird eine Nachvollziehbarkeit des eID-Einsatzes (Nachvollziehbarkeit, von wem Identitätsdaten abgerufen wurden) gefordert. Ebenso ist es für viele Interviewpartner zwingend notwendig, dass beim Einsatz einer eID der Mensch bzw. Nutzer bestimmen kann, welche seiner Daten (z. B. Krankenkassen- und Patientendaten) sichtbar respektive nicht sichtbar sind.

Es muss somit ein Paradigmenwechsel vollzogen werden, der auch eine gewisse Zeit braucht. Ein neues Verständnis von Datenschutz entsteht und muss sich etablieren. Es ist der Nutzer, der die Datenweitergabe kontrolliert und nicht mehr das Gesetz, das die Datenweitergabe verhindert. Somit würde den Nutzern mehr Verantwortung zugesprochen werden.

Kommunikation

Als ein weiterer zentraler Erfolgsfaktor für eine erfolgreiche eID(-Einführung) wird von den Interviewpartnern in der umfangreichen und frühen Aufklärung der Nutzer gesehen.

Dabei ist es wichtig, sowohl auf mögliche Gefahren wie auch auf den Nutzen hinzuweisen. Statt Gefahren kann gemäss einiger interviewter Personen auch auf mögliche Erfolge im Ausland hingewiesen werden. Wichtig ist allerdings, dass bei der Kommunikation der Nutzen ehrlich transportiert wird, um Enttäuschungen vorzubeugen. Diese Kommunikation erscheint ausgehend von den beispielsweise in der Bevölkerung existierenden Ängsten und den Befürchtungen der Konsumentenschützer als absolut wesentlich.

Darüber hinaus wird von einigen interviewten Personen das frühe Einbinden aller kritischen Stakeholder-Gruppen innerhalb des Projekts als sehr zentral angesehen. Hierbei wird innerhalb der Verwaltung und der Gesellschaft eine aktive Kommunikation zum Projektfortschritt und der geplanten Roadmap gefordert. Als Beispiele für eine solche Kommunikation wurden im Rahmen der Interviews ein Newsletter oder ein jährlicher Beitrag im SECO-Magazin genannt. Die interviewten Personen würden darin ein Commitment des Staats sowie ein Signal, dass etwas im Rahmen einer eID entsteht, sehen. Dieses wiederum würde gemäss einiger Interviewpartner zu einem stärkeren Vertrauen in das Ökosystem führen. Ebenso wurde eine vorgängige Analyse hinsichtlich der Akzeptanz der eID durch die einzelnen Stakeholder-Gruppen im Rahmen der Interviews als Erfolgsfaktor herausgestellt.

Auch bei der Einführung einer eID sehen viele interviewte Personen einen enorm wichtigen Erfolgsfaktor in Marketing- und PR-Aktionen für die eID-Lösung, um Behörden und Bürger von der Nutzung einer eID zu überzeugen.

Ein weiterer wichtiger Aspekt hinsichtlich der Kommunikation im Rahmen der eID wird in der Sensibilisierung auf Behördenseite gesehen. So fehlt aktuell bei Behördenmitarbeitenden häufig die Sensibilisierung beispielsweise in Bezug auf E-Mails mit oder ohne Verschlüsselung oder Identifikation des Versenders. Diese Sensibilisierung könnte Vertrauen für eine eID schaffen, allerdings sehen die interviewten Personen auch viel Arbeit in einer solchen Sensibilisierung.

Integrierbarkeit und Flexibilität

Gemäss der Meinung einiger interviewter Personen ist für die eID eine Fokussierung auf die Identität und eine gleichzeitige Reduktion von Zusatzfunktionen sinnvoll. Die Integrierbarkeit der eID ist allerdings stark abhängig von ihrer Komplexität. Im Rahmen der Interviews wird u.a. die Integrierbarkeit mit der SuisseID als notwendig herausgestellt.

Wichtig ist, dass im Rahmen der eID Offenheit und Flexibilität gewahrt wird, sodass unterschiedliche Anforderungen beispielsweise hinsichtlich der Qualität mit der eID abgedeckt werden können.

Die nationale eID muss auch nach ihrer Einführung noch erweiterbar sein. Ein häufig geäusserter Vorschlag der Interviewpartner ist, dass eine eID zunächst auf einer tiefen Qualitätsstufe eingeführt wird und erst zu einem späteren Zeitpunkt auf eine höhere Stufe angehoben wird.

Die Kompatibilität über Ländergrenzen hinweg wird von den interviewten Personen als sehr wichtig betrachtet. Die EU sollte die eID analog zu bestehenden ID akzeptieren. Eine europäische Akzeptanz und eine damit verbundene grosse Verbreitung der eID wird von den interviewten Personen als Erfolgsfaktor gesehen.

Als weiterer Aspekt zur Integrierbarkeit wurde der rechtlich-institutionelle Rahmen genannt, der in jedem Fall vor Umsetzung im Detail definiert und sichergestellt werden muss.

Anwendung und Positionierung

In allen Interviews wurde erwähnt, dass die Anwendungsfälle und der Druck für eine nationale eID vorhanden sein müssen, damit die eID erfolgreich wird. Des Weiteren wird von einigen der interviewten Personen ein Anreizsystem für die Nutzung einer eID gefordert.

Ein absolut zentraler Aspekt für den Erfolg einer eID wird darin gesehen, dass die eID für Anwendungen zum Einsatz kommt, die eine breite Nutzung haben werden (z. B. e-Banking, Hochschulbetrieb, E-Commerce). Auch der Einbezug von möglichst vielen Akteuren ist ein sehr zentraler Erfolgsfaktor. Die Bürger müssen bei der eID-Lösung im Zentrum stehen und es muss eine Lösung für alle sein. Wenn für einen Teil der Bevölkerung eine separate Lösung gebaut werden muss, kann eine eID flächendeckend nicht erfolgreich werden. Somit sollte das Ziel einer eID eine möglichst flächendeckende Versorgung sein, damit keine alternativen Prozesse angeboten werden müssen.

Der Einsatz der eID bei den Relying Parties ist für die interviewten Personen ebenfalls sehr wichtig. Wenn die eID in der Verwaltung eingeführt wird, muss deren Verwendung für alle Mitarbeitenden verpflichtend sein. Die Verwaltung muss bei der Verwendung eine Vorbildfunktion einnehmen. Gemeinden sind aufgrund ihrer Anzahl ein wichtiger Faktor für den Erfolg und müssen spezifisch angesprochen werden.

Darüber hinaus wurden von den interviewten Personen das Zusammenspiel von Öffentlicher Verwaltung und Privatwirtschaft als zentral angesehen. Sollte die Privatwirtschaft im Rahmen der eID keine Rolle spielen, würde ein zentraler und grosser Teil an Anwendungen entfallen. Wenn die wichtigsten Akteure aus der Privatwirtschaft eine eID nutzen, werden die Erfolgschancen von den interviewten Personen als deutlich höher eingeschätzt.

Von einigen Interviewpartnern wurde eine flächendeckende eID-Verbreitung gefordert, unabhängig davon ob sie auch von allen genutzt wird. Des Weiteren wurde als Erfolgsfaktor eine eID für alle in der Schweiz lebenden Personen genannt, unabhängig von deren Nationalität.

Kosten

Hinsichtlich der Kosten gibt es bei den interviewten Personen klare Tendenzen zur Forderung einer kostenlosen eID, die vom Staat ausgegeben und verwaltet wird. Der Bund sollte eine eID finanzieren, um damit seine Bereitschaft zu investieren erkennbar machen. Im Rahmen der Interviews gab es auch Meinungen, die das Kosten-Nutzen-Verhältnis hinterfragen und eine kostenlose eID solange befürworten, bis vielfältige Nutzungsmöglichkeiten vorhanden sind. Dies würde bedeuten, dass die eID während der Einführungsphase staatlich finanziert wird und zu einem späteren Zeitpunkt, wenn sich die eID etabliert hat, auch die Nutzer etwas kosten wird.

5.3.5 Grenzen und mögliche Hinderungsfaktoren

Im Grossen und Ganzen sind die Grenzen und Hinderungsfaktoren konsistent zu den zuvor erwähnten Erfolgsfaktoren. Insbesondere bei Usability, Sicherheit und Vertrauen und den Kosten für eine eID werden von allen interviewten Personen Hinderungsgründe gesehen, sollten die zuvor genannten Erfolgsfaktoren nicht berücksichtigt werden.

Im Folgenden werden die wichtigsten Hinderungsfaktoren im Detail erläutert.

Usability

Hinsichtlich der Usability werden in vielen Interviews auch Hinderungsfaktoren gesehen, da eine Befürchtung vor zu komplexen Prozessen und möglichweise ausbleibenden einfachen und häufig auftretenden Anwendungsfällen besteht. Beispielsweise wurde auch im Rahmen der Interviews angemerkt, dass eine Dienstleistung, die einfacher auf dem Papierweg bezogen werden kann als mit einer eID, auch nach Einführung einer eID auf dem gewohnten Papierweg bezogen werden wird. Des Weiteren wurden angemerkt, dass E-Government-Prozesse sich nur bedingt für zentrale Anwendungsfälle eignen, da sie eine zu geringe Nutzungshäufigkeiten für durchschnittliche Nutzer bieten könnten.

Auch die Angst vor zu hohen Einstiegshürden (z. B. persönliches Erscheinen in einer Behörde) ist ein Hinderungsfaktor für einige interviewte Personen, da hierdurch eine Verbreitung der eID und damit die eID-Nutzer ausbleiben würden.

Sicherheit und Vertrauen

In den Bereichen Sicherheit und Vertrauen werden von den Interviewten die meisten Hinderungsgründe für eine flächendeckende und erfolgreiche eID gesehen.

Bei einer allumfassenden eID-Lösung besteht die Befürchtung von Daten-Matching, z. B. der Abgleich von Gesundheitsdaten mit Krankenkassendaten. Will man also das Vertrauen in zahlreichen Anwendungsbereichen der eID steigern, muss dabei systematisch das Risiko und die Angst vor Profil-Bildung, Überwachung und Missbrauch bekämpft werden. Das Vertrauen in eine eID besteht gemäss einigen Interviewpartnern solange, bis ein (erster grösserer) Missbrauchsfall bekannt wird. In den Interviews wurden eine Bundesinfrastruktur mit etablierten Prozessen (z. B. Anzeige bei der Polizei) und Gesetze als vorbeugende Massnahmen gegen Missbrauchsfälle

gefordert. Hinsichtlich der gesetzlichen Grundlage wurde die Problematik aufgebracht, dass die Entwicklungen im IKT-Bereich so schnell vorangehen, dass die rechtlichen Grundlagen teilweise noch gar nicht existieren. Somit sind die rechtlichen Folgen schwer abzuschätzen.

Des Weiteren wurde in einem Interview angemerkt, dass zwingend die emotionale Hürde des individuellen Datenschutzes berücksichtigt werden muss und die Grundrechte nicht gefährdet werden dürfen.

Als Widerspruch und Herausforderung wurde in den Interviews das Zusammenbringen der zwei Seiten gesehen bestehend aus Angst vor Datenmissbrauch und der gleichzeitigen Bestrebung Datenfreigaben und –weitergaben zu erleichtern.

Kosten

Eine teure eID wurde von den interviewten Personen klar als Hinderungsfaktor für die eID genannt. Als Negativbeispiel wurde an dieser Stelle teilweise die SuisseID genannt, die im Vergleich zu ihrem Nutzen als eher teuer eingeschätzt wird.

5.3.6 Bereitstellung

Bei den Interviews ging es auch um die Frage, was der Staat bereitstellen müsste, um eine nationale eID zu einer breiten Akzeptanz und Nutzung zu führen, aber auch welche Rolle die Privatwirtschaft in diesem Ökosystem übernehmen könnte.

Grundsätzlich geht es um die Frage, welche Dienstleistungen dem Markt überlassen werden können und welche Dienstleistungen unabhängig von Angebot und Nachfrage vom Staat garantiert werden müssen. Bei den staatlich garantierten Leistungen wird zwischen Dienstleistungen, die unmittelbar vom Staat bereitgestellt werden und solchen, die zwar privatwirtschaftlich angeboten, aber staatlich reguliert oder beaufsichtigt werden, differenziert.

Rechtlich-institutionelle Rahmenbedingungen

Die meisten Interviewten vertraten die Meinung, der Staat solle sich auf das Setzen von Rahmenbedingungen konzentrieren und darauf achten, keine Konkurrenz zur Privatwirtschaft darzustellen. Die Forderungen an den Staat belaufen sich auf das Anbieten einer Infrastruktur, in die sich weitere Services einfach einbinden lassen. Einzelne Voten weisen auch auf die Notwendigkeit eines Bundesgesetzes hin.

Organisatorischer Rahmen

Die Aufgaben Governance, Management, Audit sowie Entwicklung, Betrieb und Support werden grundsätzlich von allen Befragten als Aufgabe des Staates gesehen. Einzelne Stimmen räumen die Möglichkeit ein, die Entwicklung und den Betrieb an die Privatwirtschaft abzugeben. Die Wichtigkeit von Kommunikation, Transparenz und Support vom Staat wird durch ein Votum besonders hervorgehoben. Ein stabiler Dialog zwischen Anwender und Amtsstellen ist stark zu gewichten.

Vertrauensdienste

Die Rolle des Staates bei der Bereitstellung von Vertrauensdiensten kann in drei Kategorien eingeteilt werden.

- *Bereitstellung durch Staat (a)*

Kategorie a) enthält die Bereitstellung eines eineindeutigen Personenidentifikators (EPID), von verteilten Personenidentifikatoren (PID), eines Ausweisidentifikators (Ausweis-ID) sowie von Personenidentifizierungsdaten.

Die Bereitstellung eines EPID sowie eines Ausweis-IDs betrachten alle Befragten als staatliche Aufgabe. Die Bereitstellung von verteilten Personenidentifikatoren wird grundsätzlich als staatliche Aufgabe aufgefasst. Lediglich ein Votum räumt die Möglichkeit ein, verteilte Personenidentifikatoren auch als staatlich regulierte Aufgabe zu gestalten.

Die Bereitstellung von Personenidentifizierungsdaten ist eng verknüpft mit der Forderung nach einer klaren Identifikation von Personen. Die Bereitstellung wird einstimmig als staatliche Aufgabe verstanden.

Das Verlinken (Pairing) des EPID mit der Ausweis-ID oder mit der PID wird explizit als staatliche Aufgabe gesehen. In diesem Zusammenhang wird explizit auf die Pflicht des Staates hingewiesen, die Anonymität von Personen zu gewährleisten.

Ein Votum spricht sich dafür aus, dass der Staat sämtliche Vertrauensdienste bereitstellt.

- *Bereitstellung durch Privatwirtschaft mit staatlicher Regulierung / Aufsicht (b)*

Zur Kategorie b) zählen die Vertrauensdienste Zeitstempel, Zertifikate, Validierung und Zustellung. Das Anbieten von privaten Services unter staatlicher Aufsicht und Regulierung wird hier als Modell gesehen.

- *Bereitstellung durch Staat und Privatwirtschaft (c)*

Die Kategorie c) enthält die Bereitstellung von Attributen und Funktionsnachweisen. Aussagen dazu beschreiben die Sicht, dass staatlich vergebene Attribute und Funktionsnachweise durch den Staat vergeben werden, während alle weiteren Attribute und Funktionsnachweise durchaus von der Privatwirtschaft geliefert werden können. Es gab kein Votum, das sich für eine zentrale Führung der Attribute aussprach. Hingegen wurde mehrmals die Meinung vertreten, dass Attribute aus verschiedenen Applikationen einholbar sein sollten, wobei eine staatliche Regulierung der Prozesse als notwendig erachtet wird.

Funktionen der eID

Die Ausstellung und Bestätigung von Identitäten wird generell als hoheitliche Aufgabe betrachtet. Der Staat muss eindeutig sicherstellen, wer die Person ist. Die Analogie zum physischen Pass wird von mehreren Interviewpartnern explizit genannt. Einzelne sehen dies gar als die einzige eID-Funktion an, die vom Staat bereitgestellt werden sollte.

In diesem Zusammenhang wurde in einzelnen Fällen auf die Wichtigkeit der Interoperabilität der eID-Nutzung mit dem Ausland – insbesondere mit dem EU-Raum – hingewiesen. Dies stehe aber nicht im Vordergrund und habe keine zeitliche Priorität.

Die Meinungen zu den Funktionen Signatur und Verschlüsselung sind nicht eindeutig (siehe auch Kapitel 5.3.1.2.). Einerseits wird auf die Wichtigkeit dieser Funktionen verwiesen. Andererseits scheint die Sicht vorzuherrschen, dass die Bereitstellung dieser Funktionen im Rahmen einer nationalen eID die Komplexität so stark erhöhen würde, dass der Erfolg der eID damit gefährdet wäre. Einzelne Interviewte sehen darin kein Problem, da diese Funktion heute bereits angeboten wird, oder sie betrachten diese Funktion als eine von der eID-abgekoppelte Funktion. Zusammenfassend scheint Einigkeit über die Wichtigkeit der Funktion zu bestehen. Wer diese Funktion, wie und wann zur Verfügung stellt ist noch sehr unklar.

Nutzende

Weitere Aussagen geben zu bedenken, dass die Wirtschafts- und Wohnpopulation in der Schweiz nicht nur aus Schweizer Bürgerinnen und Bürger besteht. Wird ein Teil der Wirtschaftsteilnehmenden oder der Wohnbevölkerung ausgeschlossen, müssten einige der befragten Organisationen für diesen Teil der Population Parallellösungen entwickeln. Ob sich dann die Nutzung der eID für die einzelne Organisation noch lohnen würde, hängt vom jeweiligen Anwendungsfall ab.

5.4 Zusammenfassung der Interview-Ergebnisse

Die Besprechung des Modells und der Modellelemente zeigte, dass der Einführung eines EPID eine hohe Bedeutung zugesprochen wird. Anhand der nicht eindeutigen Haltungen in Bezug auf die Funktionen Signatur und Verschlüsselung lässt sich erkennen, dass die Diskussion um die definitive Ausgestaltung der eID erst begonnen hat und es weitere Dialoge braucht.

Was die Anwendungsfälle und Nutzungen einer eID betrifft, so sind sehr viele Anwendungsfälle vorstellbar. Diese sind abhängig davon, welche Nutzungsmöglichkeiten für die eID gegeben sind. Diese Erkenntnis steht im Gegensatz zu Aussagen, die den Erfolg einer eID gerade an einem prominenten Anwendungsfall aufhängen möchten. Auch hier lässt sich erkennen, dass der Diskurs noch am Anfang steht und dass für den Erfolg der eID ein Dialog zwischen Nutzenden und Bereitstellern anzustreben ist.

Aus Sicht der Befragten spielt der Staat eine zentrale Rolle bei der Bereitstellung, wobei die Übernahme von regulatorischen Aufgaben im Zentrum steht.

Die interviewten Personen sehen in der eID ein wichtiges Werkzeug, das zum Aufbau einer Informationsgesellschaft beiträgt.

Die Top 5 Faktoren für die erfolgreiche Einführung der eID werden in den folgenden Punkten gesehen:

- Hohe Usability
- Vertrauen in die eID, Sicherheitsaspekte
- Nutzer kontrolliert Weitergabe von persönlicher Daten (user-centric)
- Ehrliche Kommunikation
- Ausbaufähigkeit der eID.

Hinsichtlich der Kosten für eine eID wurde von vielen interviewten Personen das Kosten-Nutzen-Verhältnis hinterfragt und eine kostenlose eID solange befürwortet, bis deutliche Nutzungsmöglichkeiten erkennbar sind.

6. Public Value Workshop

Im Rahmen des Projekts wurden zwei halbtägige Workshops zum Thema Public Value des eID-Ökosystem Modells durchgeführt. Unter den zwölf Teilnehmern der Workshops waren neben dem Auftraggeber einige der zuvor im Rahmen der Interviews befragten Personen, aber auch weitere Schlüsselpersonen innerhalb der E-Society. Dieses Kapitel beschreibt sowohl die Gründe für die Verwendung der Public Value-Methode sowie den Aufbau, die Ziele und die Resultate der Workshops.

6.1 Gründe für die Verwendung der Public Value Methode

Es gibt mindestens drei gute Gründe für den Staat, ein eID-Ökosystem zu fördern: erstens Aufgaben im Polizei- und Justizbereich, zweitens ein Nichtfunktionieren des Markts aufgrund nicht internalisierter Externalitäten und drittens ein möglicher Monopolcharakter.

Dem potentiellen Nutzen für die Polizei- und Justizaufgaben entspricht, dass der Bundesratsauftrag für den Entwurf eines Konzepts für die nationale eID an das fedpol vergeben wurde. Letztlich ist das aber nur ein Anwendungssektor unter vielen, innerhalb welcher auch Sektor-spezifische Lösungen grundsätzlich Sinn machen können.

Bedeutender ist, dass die Vertrauensdienstleistungen im eID-Ökosystem Externalitäten schaffen, die nicht oder nur eingeschränkt durch die Marktteilnehmer internalisiert werden können. Viele geplante Innovationen setzen beispielsweise die Existenz einer vertrauenswürdigen und breit genutzten nationalen eID voraus. Dies ergibt sich aus vertraulichen Gesprächen mit der Wirtschaft. Der Aufbau einer eigenen eID-Lösung ist nicht nur teuer, sondern potentiell auch nicht sehr nachhaltig, weil neue sich am Markt durchsetzende Lösungen möglicherweise übernommen werden müssen. Eine nationale Schweizer eID, die überdies eIDAS kompatibel ist, reduziert die Kosten und stärkt die Nachhaltigkeit der Investitionen. Es entstehen also durch die Vertrauensdienste Realoptionen für verschiedene Stakeholder-Gruppen aus der Wirtschaft. Zusätzlich entsteht Nutzen für weitere Stakeholder in der Gesellschaft, insbesondere auch für die breite Bevölkerung, die eine eID erwerben und einsetzen kann. Nicht zuletzt werden gute eID-Lösungen auch im öffentlichen Sektor, beispielsweise im E-Government und im E-Health, benötigt.

Problematisch ist, dass dieser Nutzen von den Anbietern von Vertrauensdiensten nur unzureichend internalisiert werden kann. Lange ROI-Dauern mit entsprechend hohen Risiken stehen einem signifikanten langfristigen Nutzen für die Gesellschaft gegenüber. Es ist deshalb mehr als sinnvoll, dass der Staat entweder die Dienstleistungen selber anbietet oder den Anbietern von Vertrauensdienstleistungen über entsprechende Fördermassnahmen eine Internalisierung ermöglicht.

Auch der potentielle Monopol-Charakter mancher Vertrauensdienstleistungen spricht für ein energisches Engagement des Staats, sei es durch ein eigenes Angebot, sei es durch klare Einschränkungen oder sei es durch Förderungen, die an die Einhaltung gewisser Standards und

Good Practices (beispielsweise dem Verzicht auf Lockangebote mit verstecktem oder offenem Lock-In) gebunden sind. Doch das Hauptthema ist aus heutiger Sicht die unzureichend internalisierbaren Externalitäten.

Um diese Problematik anzugehen, eignet sich die Public Value Theorie von Mark Moore [18] sehr gut, welche dieser als Pendant des öffentlichen Sektors zur privatwirtschaftlichen Shareholder Value Theorie entwickelte. Die Public Value Theorie beschäftigt sich mit dem Zusammenspiel (bzw. Beziehungsdreieck) der drei kritischen Steuerungsfaktoren öffentliches Handeln und Nutzen für die Gesellschaft (Public Value), demokratische Legitimation sowie Umsetzungsressourcen. Public Value ist dabei der Nutzen, den ein Projekt oder eine Geschäftstätigkeit (des öffentlichen Sektors) für die unterschiedlichen Stakeholder-Gruppen der Gesellschaft schafft. Dieser Wert fällt in der Regel für die unterschiedlichen Stakeholder-Gruppen recht unterschiedlich aus, sowohl in Bezug auf die Art als auch auf die Grösse des Werts.

Indem man eine Matrix aus Stakeholdern und Wertedimensionen aufspannt, kann man die Wirkung einer nationalen eID gut verständlich positionieren – und zwar sowohl den direkten Nutzen für die Kunden der Vertrauensdienstleister als auch den indirekten Nutzen für Dritte, insbesondere die gesellschaftlich relevanten Externalitäten. Bei der Identifizierung der Wertperspektiven kann man sich unter anderem an Gomez/Meynhart orientieren. [19, p. 136]

Im Zentrum des zu veranstaltenden Workshops stand die Bestimmung der Public-Value-Matrix. Deren Spalten entsprechen den Stakeholder-Gruppen. Deren Zeilen entsprechen den Wertarten. Die Matrix wird verwendet, um zu positionieren, worauf u.a.bei einem Nicht-Gelingen der eID-Einführung verzichtet werden muss. Eine solche Analyse macht nur Sinn, wenn man den Nutzen für konkrete Instanziierungen des eID-Ökosystem Modells betrachtet. Eine generische Betrachtung hingegen wäre sinnlos, weil der Nutzen stark davon abhängt, wie viele Nutzer für wie viele Vertrauensdienstleistungen in welchen Anwendungsfällen zu gewinnen sind.

In vorangegangenen Projekten wurde oft der Fehler gemacht, über den finanziellen Nutzen einer nationalen eID zu diskutieren. Dabei wurde ausgeblendet, dass es unterschiedliche Stakeholder-Perspektiven und unterschiedliche, auch nicht-finanzielle, Arten an Nutzen gibt und dass der Nutzen stark von der Vielfalt an Vertrauensdienstleistungen und der Zahl der Nutzenden – d.h. der eID-Besitzenden und der Relying Parties – abhängt. Eine Instanziierungs-spezifische Public-Value-Matrix vermeidet diese Probleme und liefert wesentlich klarere Aussagen als die konventionellen Nutzenanalysen.

6.2 Aufbau und Ziel des Public Value Workshops

Das Ziel der Public Value Workshops war es, ein differenziertes Bild des Nutzens einer eID zu erarbeiten und die wichtigsten Fördermassnahmen zu identifizieren. Die Workshops unterteilten sich in vier Abschnitte, die jeweils in Gruppen erarbeitet wurden.

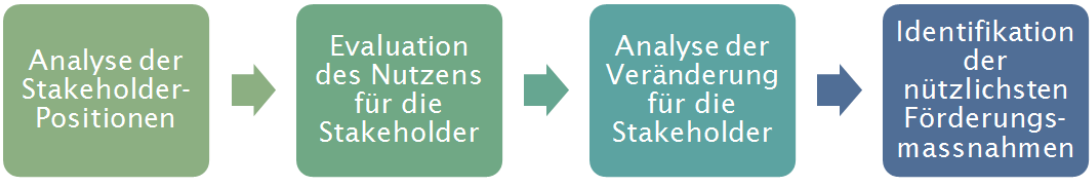


Abbildung 19: Die vier Abschnitte und Arbeitsphasen der Public Value Workshops

Dazu wurden die Teilnehmer in zwei Gruppen aufgeteilt. Jeder der Gruppen wurde eine Instanziierung des eID-Ökosystem Modells (Mönch oder Jungfrau; Vgl. hierzu Kapitel 4.4.2) zugeteilt. Bei den Instanziierungen handelte es sich zum einen um eine gut und zum anderen um eine sehr gut ausgebaute Version des eID-Ökosystems. Die bearbeiteten Instanziierungen sind im Kapitel 1.1.1 beschrieben.

Teil 1 – Analyse der Stakeholder Positionen

Nach einer kurzen Einführung ordneten die Workshop-Teilnehmenden die Stakeholder in Bezug auf ihre Relevanz ein. Dabei wurden die Stakeholder hinsichtlich der Kriterien "Einfluss auf die Einführung der eID" und "Interesse an der Einführung einer eID" bewertet.

Ziel dabei war es die relevanten Stakeholder zu identifizieren und zu clustern.

Teil 2 – Evaluation des Nutzens für die Stakeholder

Im zweiten Teil wurde für die pro Instanziierung wichtigsten Stakeholder eine Public-Value-Matrix erstellt. Dabei wurde von den Teilnehmenden der Public Value für die ausgewählten Stakeholder hinsichtlich der der folgenden Dimensionen ermittelt und bewertet:

- Finanziell – Finanzieller-ökonomischer Nutzen, z. B. Kosteneinsparpotenziale oder zusätzliche Einnahmen
- Politisch – Nutzen für den Einfluss auf die Politik
- Sozial – Nutzen in sozialer und zwischenmenschlicher Hinsicht
- Strategisch – Nutzen für die Verfolgung der strategischen Ziele
- Ideologisch – Nutzen für die Erfüllung moralischer oder ethischer Verpflichtungen
- Lebensqualität – Nutzen für die individuelle Sicherheit und Zufriedenheit
- Vertrauen und Reputation – Nutzen hinsichtlich öffentlichem Vertrauen, Integrität und Legitimität.

Ziel war es, den Public Value für die ausgewählten Stakeholder zu identifizieren.

Teil 3 – Analyse der Veränderungen für die Stakeholder

Für ausgewählte Stakeholder wurden anschliessend die potentiellen Veränderungen durch die Einführung einer eID ermittelt. Dabei wurden die folgenden Aspekte berücksichtigt:

- Effizienz
  Wie verändert sich die Wirtschaftlichkeit (Kosten-Nutzen-Relation) für den jeweiligen Stakeholder?
- Effektivität
  Wie verändert sich die Qualität der Zielerreichung für den jeweiligen Stakeholder?
- Interne Organisation
  Gibt es organisatorische, prozessuale oder kulturelle Veränderungen für den Stakeholder?
- Umweltfaktoren
  Welchen Einfluss haben Veränderungen von Umweltfaktoren auf den Stakeholder?
- Beziehungen zu Stakeholdern
  Wie verändern sich für den Stakeholder die Beziehungen zu anderen Stakeholdern?
- Sicherheit (Daten, System und Identität)
  Wie verändert sich die Sicherheit für den Stakeholder?

Ziel war es, die Veränderungen, die durch die Einführung einer eID bei den ausgewählten Stakeholder resultieren, zu identifizieren.

Teil 4 - Identifikation von Erfolgs-versprechenden Fördermassnahmen

In einem letzten Schritt wurden jene Fördermassnahmen identifiziert, durch welche potentiell besonders grosser positiver Nutzen oder allenfalls klar negativer Nutzen geschaffen wird. Es ging darum, vor allem jene Massnahmen zu identifizieren, die entweder negative und deshalb blockierende Externalitäten aufheben oder positive Externalitäten noch weiter verstärken, und so das Potential besitzen, die Selbstorganisation des Markts zu fördern.

6.3 Auswertung des Workshops

6.3.1 Relevante Stakeholder

In der ersten Gruppenarbeit wurden die relevanten Stakeholder identifiziert und kategorisiert. Dabei stand den Teilnehmern eine vereinfachte Stakeholder-Landkarte zur Verfügung, die ergänzt werden konnte.

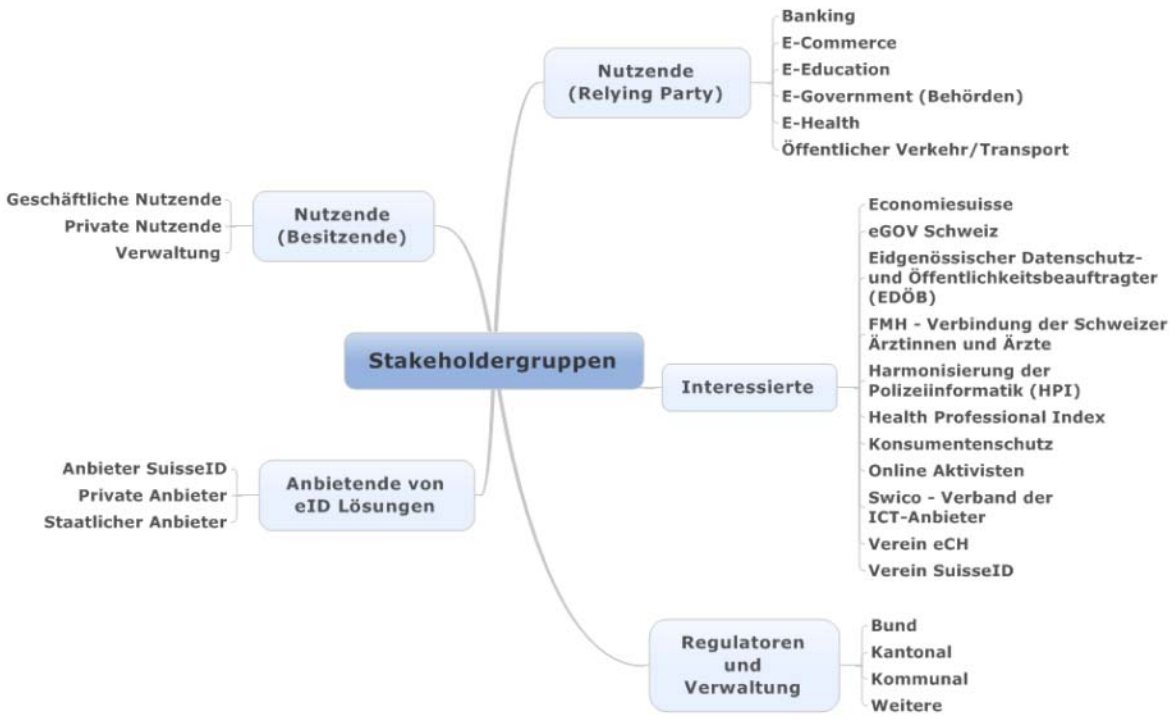


Abbildung 20: Vereinfachte Stakeholder Landkarte

Die Stakeholder Landkarte wurde anschliessend von den Teilnehmenden um die folgenden weiteren relevanten Stakeholder ergänzt:

- Politische Parteien
    - Progressiv, liberale Parteien
    - Konservative Parteien
- Internet-Unternehmen
    - Google
    - Facebook
    - Amazon.

Die Stakeholder-Gruppen wurden in eine zweidimensionale Matrix eingeordnet. Die horizontale Dimension beschreibt den Einfluss auf die Einführung der eID. Die vertikale Dimension entspricht dem Interesse an einer Einführung einer eID. Das darauf abgebildete Kontinuum reicht von einem hohen Interesse über eine neutrale Haltung bis hin zu einer Präferenz gegen die Einführung einer eID.

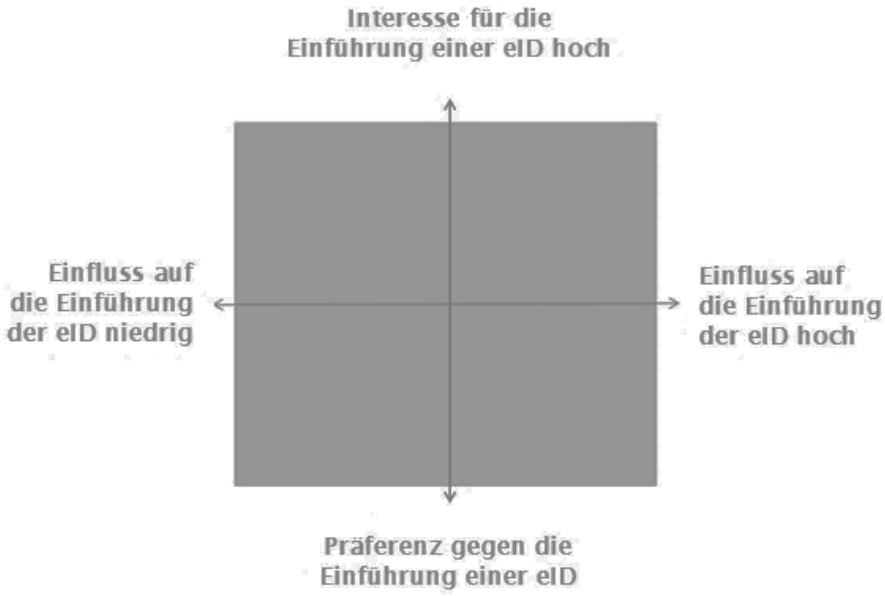


Abbildung 21: Stakeholder-Matrix

Für das eID-Ökosystem werden als relevante Stakeholder Anspruchsgruppen mit hohem Einfluss und einem hohen Interesse an einer Einführung oder einer Präferenz gegen die Einführung bezeichnet. Als weniger relevante Stakeholder werden Gruppen, Organisationen und Personen gesehen, die wenig Einfluss auf die Einführung der eID haben. Hieraus lässt sich zu einem späteren Zeitpunkt beispielsweise ein Kommunikationskonzept ableiten. Ein beispielsweise sehr einflussreicher Stakeholder muss stark in das eID-Projekt involviert werden. Stakeholder ohne grösseren Einfluss müssen entsprechend keine direkte Rolle in einem eID-Projekt haben und müssen beispielsweise nur informiert werden. Unabhängig von der Einordnung sollten aber alle identifizierten Stakeholder betrachtet werden.

Aufgrund der Grösse von einzelnen Stakeholder-Gruppen und auch deren interner Diversität war im Rahmen der Workshops eine klare Einteilung in die beiden Dimensionen teilweise sehr schwierig. So wird beispielsweise die Stakeholder-Gruppe E-Health mit sehr gegensätzlichen Interessen bezüglich eID bewertet. Unbestritten scheint, dass eine eID allen einen Mehrwert bieten könnte. Bei einigen Stakeholdern war den Workshop Teilnehmenden die Interessenslage nicht bekannt, sodass es sich um eine geschätzte Zuordnung handelt.

Im Generellen spielen für die Workshop-Teilnehmenden die folgenden Faktoren eine massgebliche Rolle bei der Einschätzung der einzelnen Stakeholder:

- Kosten für die Benutzer der eID
- Kosten für die Relying Parties, welche die eID einsetzen
- Usability
- Sicherheit
- Die Rolle im Ökosystem
- Technische Implementierung.

Besonders kontrovers wurde die Relevanz von bestehenden eID-Anbietern diskutiert. So besteht auf der einen Seite eine essentielle Gefahr für ihr Geschäftsmodell, anderseits könnte eine nationale eID auch ihren eID-Angeboten zum Durchbruch verhelfen. Dies könnte beispielsweise der Fall sein, wenn an eine bestehende eID staatlich signierte Attribute angehängt würden.

Unsicherheit unter den Workshop-Teilnehmern herrscht bezüglich der Frage, ob im Rahmen von E-Commerce und E-Government ein wirklich grösserer Nutzen durch eine eID entstehen würde. Bei E-Commerce sind bereits etablierte Systeme im Einsatz, welche die Identität der Kunden verwalten. Eine eindeutige und sichere Identifikation ist nur in den wenigsten Fällen umgesetzt. Der Einfluss von E-Commerce auf die Einführung einer nationalen eID wird jedoch als sehr gross eingestuft. Eine breite Verwendung der eID im E-Commerce deren Einführung zum Durchbruch verhelfen. Besonders die Initiale Anmeldung[11] ist im E-Commerce eine grosse Herausforderung, da unter Umständen ein direkter Kontakt zum Kunden notwendig ist.

Als „bedeutend" eingeschätzt werden die Rollen von grossen Internet-Unternehmen, die über eine eID in Form von Benutzer-Accounts verfügen. Die Macht dieser Konzerne ist gross und es ist anzunehmen, dass sie im Themenfeld eID viel bewegen könnten. Der Vorteil an deren Lösungen wäre, dass sie schnell und unkompliziert in unterschiedlichste Anwendungen integriert werden können.[12]

Für den Bereich E-Government wird ein grosser Nutzen identifiziert, da bei einigen Prozessen eine eindeutige und sichere Identifikation des Kunden (Bürger) notwendig ist. Zudem kann die Verwaltung mit einer Verpflichtung des Einsatzes einer nationalen eID als Vorbild vorangehen und dadurch deren Verbreitung fördern.

[11] Die Anmeldung oder Registrierung beim ersten Kundenkontakt kann ein sehr aufwändiger Prozess sein. Abhängig von den Regulationen muss der Kunde aufwändig identifiziert werden.

[12] In anderem Zusammenhang wurde auch Apple mit Apple Pay erwähnt, als möglicher Konkurrent von Finanzdienstleister Geschäftsmodellen.

Einordnung der Stakeholder

Bei den folgenden Stakeholdern werden bei den Workshop Teilnehmenden von einem grossen Interesse an einer Einführung der eID und einem hohem Einfluss auf die Einführung ausgegangen:

- **E-Health (Nutzende - Relying Parties)**
- **E-Government (Nutzende - Relying Parties)**
- **Private Nutzende (Nutzende - Besitzende)**
- **Private Anbieter (Anbietende von eID Lösungen)**[13]
- Staatliche Anbieter (Anbietende von eID Lösungen).

Eine neutrale Einstellung zur Einführung, jedoch einen grossen Einfluss haben gemäss den Workshop-Resultaten:

- **E-Commerce (Nutzende - Relying Party)**
- **Bund (Regulator und Verwaltung)**
- Banking (Nutzende - Relying Party).

Eine Präferenz gegen die Einführung und ein grosser Einfluss werden von den Workshop-Teilnehmenden bei den folgenden Stakeholdern gesehen:

- **Verwaltung (Nutzende - Besitzer)**
- **Private Anbieter (Anbietende von eID Lösungen)**[14]
- Politische Parteien (abhängig von der Instanziierung und der politischen Ausrichtung)
- Online Aktivisten.

Folgende Stakeholder haben laut den Workshop Teilnehmenden keinen grossen Einfluss auf die Einführung einer nationalen eID:

- Geschäftliche Nutzer (Nutzende - Besitzende)
- Private Nutzer (Nutzende - Besitzende)
- Verwaltung (Nutzende - Besitzende)
- Anbieter SuisseID (abhängig von der Instanziierung)
- Interessenverbände.

Die fett markierten Stakeholder wurden für die Fortführung des Public Value Workshops verwendet.

[13] Unter der Annahme, dass die Private Anbieter durch die Einführung einer eID einen Vorteil für ihr Geschäftsmodell erhalten.

[14] Unter der Annahme, dass wirtschaftlicher Nachteil entsteht oder eine Verschärfung der Konkurrenzsituation

Grundsätzlich ist festzuhalten, dass viele Akteure ein Interesse an der eID-Einführung haben. Vom Staat wird eine entsprechende Regulierung erwartet und eine erfolgreiche Einführung vorausgesetzt.

Die beiden Stakeholder-Gruppen Geschäftliche und Private Nutzende sind für die Einführung einer eID äusserst relevant. So sollen diese Stakeholder die eID künftig umfangreich und häufig einsetzen können. Nur der häufige und einfache Gebrauch einer eID kann das Interesse bei den Privaten erhöhen.

Die Schlussfolgerungen lauten damit wie folgt: Stakeholder mit hohem Interesse an einer Einführung oder einer starken Präferenz gegen die Einführung, die unabhängig davon einen grossen Einfluss auf die Einführung haben, sind als relevant zu betrachten. Diese Stakeholder müssen auch entsprechend im Projekt integriert sein. Abhängig von der gewählten Instanziierung kann sich die Einstellung auf die Einführung und den Einfluss der Stakeholder nochmals ändern.

6.3.2 Nutzen und Veränderungen für die Stakeholder

Dieses Kapitel enthält die Ergebnisse aus der Bewertung der Public Values und möglicher Veränderungen (Teile 2 und 3). Der Nutzen und die Veränderungen haben eine starke Abhängigkeit und werden deshalb hier zusammen beschrieben. Der Nutzen und die Veränderungen wurden anhand der Public Value Dimensionen (vgl Kapitel 6.2) erhoben. In diesem Kapitel werden die relevanten Ergebnisse erläutert.

Die Äusserungen in diesem Kapitel sind Aussagen und Wortmeldungen aus dem Workshop von einzelnen oder mehreren Teilnehmern und können nur bedingt als repräsentativ betrachtet werden.

6.3.2.1 Allgemeine Erkenntnisse

Innerhalb des Workshops war man sich einig, dass eine grosse Anfangsinvestition im Rahmen einer Bereitstellung einer nationalen eID notwendig ist. Diese Investition kommt aber erst wesentlich später als Nutzen bei den Benutzern an. Durch die eID wird ein schlanker Staat mit einem gesteigerten Image ermöglicht. Das Vertrauen in die Verwaltung steigt, erwünschte Konzepte wie Single Point of Contact (SPOC) oder Front Office werden durch oder dank der eID möglich. Politisch ist die eID-Einführung als neutral zu betrachten.

Aus privatwirtschaftlicher Perspektive wird von den Workshop-Teilnehmenden mehrfach eine Kosten-Nutzen-Abwägung als die relevante Entscheidungsgrundlage genannt. Zudem besteht ein hoher Anspruch an eine nationale eID, was Sicherheit und Qualität betrifft.

Im Workshop wurden weitere Eigenschaften wie Kosten, Nutzen, Qualität, Usability und Sicherheit einer eID diskutiert. Die Abhängigkeiten dieser Eigenschaften wurden wie im Folgenden dargestellt besprochen.

Kosten-Nutzen

Abhängig vom möglichen Nutzen einer eID ist auch die Bereitschaft vorhanden, gewisse Kosten für die eID zu übernehmen: Je höher der Nutzen ist, umso eher ist der Benutzer auch bereit dafür zu zahlen. Für die erfolgreiche und breite Verbreitung ist eine ökonomische Kosten-Nutzen Abwägung relevant. Die Aufteilung dazu, wer was und wie viel übernimmt, gilt es aber noch zu klären, respektive sind entsprechende Modelle zu definieren.

Kosten-Qualität

Analoges zu den Kosten-Nutzen Überlegungen gilt auch für die Kosten-Qualitätsperspektive. Für qualitativ gute Lösungen ist die Bereitschaft Kosten zu übernehmen höher. Zu tiefe Qualität führt zu einer Ablehnung und Misstrauen. Hohe Qualität kann zu einem hohen Vertrauen beitragen.

Usability und Sicherheit

Auch während des Workshops fanden Diskussionen um die scheinbar konträren Ziele von hoher Sicherheit und einfacher Usability (Gebrauchstauglichkeit) statt. Der Wunsch nach einer einfach zu nutzenden eID, die absolut sicher ist, scheint utopisch oder zumindest nicht finanzierbar zu sein. Eine absolute Sicherheit wird nicht erreichbar sein. Ebenso wird ein zu komplexes eID-System keinen Durchbruch erfahren.

Diese Abhängigkeiten zwischen den divergierenden Zielen Sicherheit, Gewährleistung des Datenschutzes und Nutzungskomfort wird in der Literatur (vgl. Kapitel 2.2) als magisches Dreieck zu elektronischen Identitäten beschrieben.

6.3.2.2 E-Health (Nutzende - Relying Party)

Der grösste Nutzen einer eID für E-Health besteht in der eindeutigen Identifikation der Akteure. Dies sind gemäss E-Health Suisse [20] der Patient selber, Leistungserbringer (z.B. ÄrztInnen, ApothekerInnen, Spitäler, Pflegende), Versicherer, Patienten- und Konsumentenorganisationen. Eine eindeutige Identifikation ist die Grundvoraussetzung für den benötigten Vertrauensraum und eine Basiskomponente im Architekturmodell von E-Health Suisse. Im Dokument „Standards und Architektur Empfehlungen II“ wird die Identifikation wie folgt erwähnt: „Die eindeutige Identifikation von Personen und deren Zuordnung zu elektronischen Identitäten erfolgt ausserhalb des Systems, z.B. im Rahmen des Identity and Access Managements (IAM) des nationalen Programms eGovernment.“ [21]

Im Workshop wurde E-Health als Katalysator für eine eID identifiziert, da eine grosse Verbreitung und häufige Verwendung gegeben ist. Dies setzt aber eine eID für die Gesamtbevölkerung voraus. Bereits vorhandene eIDs wie die Health Professional Card (HPC)[15] oder auch die Versichertenkarte [22] müssen im Ökosystem berücksichtigt werden.

[15] Die Health Professional Card (HPC) der FMH ist ein personalisierter Mitglieder- und Arztausweis mit praktischen elektronischen Zusatzfunktionen wie elektronische Authentifizierung und Signier-Funktion [29].

Erhöhte Transparenz aus der Patientensicht wurde als klarer Nutzen identifiziert. Transparenz für einen direkten Vergleich von Leistungserbringern wurde hingegen als Hemmnis für das gesamt System bewertet.

Obwohl die Identifikation bereits teilweise gelöst ist, ist eine positive Veränderung im Sinne der Effizienz und der Effektivität zu erwarten. Besonders organisationsübergreifende Prozesse können schneller und mit weniger Medienbrüchen durchgeführt werden.

6.3.2.3 E-Government (Nutzende - Relying Party)

Innerhalb des Workshops wurde für E-Government ein grosser Nutzen mit Einsparpotential (nach einer gewissen initialen Investition) und Qualitätsverbesserung identifiziert. Als strategischer Nutzen wurden Standortattraktivität, erhöhte Glaubwürdigkeit und gesteigerte Planungssicherheit erwähnt. Im Gegensatz zu E-Commerce wird davon ausgegangen, dass im E-Government mehr Prozesse eine sichere Identifikation voraussetzen. Die grosse Masse von Behördenkontakten ist aber nicht bei den Bürgern, sondern eher bei den Firmen und Organisationen zu finden.

Ein konsequenter Einsatz einer eID hat einen positiven Einfluss auf die Effizienz im E-Government. Die verlässliche Identifikation der Kunden (Bürger) ist nur teilweise gelöst. Einige E-Government Lösungen bieten ausgeklügelte IAM-Bausteine an, diese stossen aber bei behördenübergreifenden Prozessen an ihre Grenzen. Behördenprozesse könnten durch den eID-Einsatz effizienter ablaufen, da die Qualität von Personendaten aktueller und verlässlicher nachgewiesen werden kann.

Eine moderne Verwaltung wird im positiven Sinne als bürger-freundlicher und attraktiver wahrgenommen.

Für die interne Organisation einer Behörde könnte eine eID massive Veränderungen bringen. So fällt eine wiederholde Identitätsprüfung weg und Prozesse könnten vermehrt ganz elektronisch ablaufen. Dafür wäre es denkbar, dass ausgehend vom eID-Einsatz von Behörden neue Aufgaben übernommen werden könnten. Ein Beispiel hierzu wäre eine einmalige Identitätsprüfung für die Ausstellung oder Reaktivierung einer eID. Die Anforderungen an die Verfügbarkeit und Aktualität der von der Verwaltung gepflegten Register würde sicher steigen, da diese rund um die Uhr direkt online abgefragt werden könnten. Dies hat einen weiteren Einfluss auf die tägliche Arbeit innerhalb der Verwaltung (Effizienz- und Effektivitätsgewinne). Überdies werden dabei Unsicherheiten darüber, welche Information ein Behördenmitarbeiter an wen herausgegen darf, geregelt. Eine grosse Veränderung hat ein User-Centric[16] System auf die Eigenverantwortung der Bürger.

[16] User-Centric: Die von der Relying Party angeforderten Informationen (insb. Identitätsdaten) gehören dem Individuum. Das User-Centric Konzept geht davon aus, dass das Subjekt auch über die Weitergabe selbst entscheiden kann und die Kommunikation ausschliesslich benutzerzentriert erfolgt, z.B. über den Browser des Benutzers [22], [23], [24]

Diese würde gestärkt, da sie auf ihre Daten direkt Zugriff haben und die Verantwortung für deren Pflege und Aktualität tragen.

6.3.2.4 Verwaltung (Nutzende - Besitzende)

Für die Verwaltung als Nutzer der eID im Ökosystem ergibt sich ein langfristiger finanzieller Vorteil. Das Ziel ist es, verwaltungsintern die gleiche eID wie der Kunde (Bürger) zu verwenden. Durch diese Vorbildfunktion wird die eID gestärkt. Interne Prozesse können optimiert und transparent ausgeführt werden. Somit steht der ganzen Verwaltung, unabhängig von der föderalen Ebene, eine vertrauenswürde Identität für ihre Mitarbeiter zur Verfügung.

6.3.2.5 E-Commerce (Nutzende - Relying Party)

Die Stakeholder Gruppe E-Commerce wurde sehr konträr diskutiert. Zum einem werden Kunden (innerhalb der Organisation) in Systemen bereits ausreichend identifiziert. Dies wird bereitwillig vom Kunden zugelassen. Hingegen fehlen für ergänzende Attribute wie Altersangabe, Nachweis von Mitgliedschaften oder studentische Immatrikulation vertrauenswürdige Quellen. Hier wird mit pragmatischen Lösungen und administrativ aufwändigen Prozessen ausgekommen. Eine positive Veränderung auf die Stakeholder Gruppe hat eine eID nur, wenn sie einfach und günstig integriert und verwendet werden kann. Solange die eID nicht in den Business Case eines e-Commerce Anbieters passt oder nicht verpflichtend ist, wurde die Chance auf eine Akzeptanz der eID als niedrig eingestuft.

6.3.2.6 Private Nutzer (Nutzende - Besitzende)

Die privaten Nutzer verschieben ihre Nutzung von Konsumation von Produkten und Leistungen zunehmend ins Internet. Ein zeitgerechter Service wird erwartet oder sogar gefordert. Die Vorteile sind bekannt: Zeitlich und örtlich unabhängige Verfügbarkeit sowie Nachvollziehbarkeit und effiziente Prozessgestaltung. Aus der Perspektive des Nutzers ist dieser Umstand schon fast keine grössere Veränderung mehr, da Onlineservices bereits zum Standard gehören.

Als weiterer Vorteil für den privaten Nutzer wurde die zeitliche Flexibilität identifiziert. Die Prozesse sollen effizient ablaufen und dadurch dem privaten Nutzer einen Zeitgewinn verschaffen. Die Erwartungshaltungen sind entsprechend hoch.

Eine Beschränkung der eID auf den Anwendungsfall E-Government wurde als nicht ausreichende Nutzungsverbreitung eingestuft. Wenn die eID nur wenig eingesetzt wird, wird sie von den privaten Nutzern nicht akzeptiert.

6.3.2.7 Private Anbieter (Anbietende von eID Lösungen)

Der Nutzen und die Veränderung für die privaten Anbieter von eID Lösungen sind von der Ausprägung des Ökosystems abhängig. Wenn eine nationale eID ganz vom Staat angeboten wird und dadurch das bestehende Geschäftsmodell der privaten Anbieter ausgehebelt wird, ist eine Ablehnung nachvollziehbar. Wird die nationale eID jedoch so implementiert, dass die Anbieter ihr Geschäftsmodell beibehalten oder sogar erweitern können, ist mit einer Unterstützung seitens Lösungsanbieter zu rechnen.

Als eine grosse Herausforderung für die privaten Anbieter von eID Lösungen wurde das Onboarding identifiziert. Der Umstand, wie einfach die Integration in eine bestehende Infrastruktur erfolgen kann, ist massgebend. Als Argument wurden relativ hohe bereits getätigte Investitionen in bestehende eID Infrastrukturen erwähnt.

Aus der Perspektive der Lösungsanbieter wurde die eID nicht als Verbesserung der Wettbewerbsfähigkeit erkannt. In Anbetracht der Tatsache, dass vermehrt Anbieter in den Markt mit starken Sicherheitslösungen eintreten könnten, wurde mit Bedenken wahrgenommen.

6.3.2.8 Bund (Regulatoren und Verwaltung)

Der Bund in der Rolle eines Regulators wurde am Workshop als wichtig eingestuft. Erwartet werden entsprechende Rahmenbedingungen, aber kein zusätzlicher Nutzen für den Bund in dieser Rolle. Für den Bund als Regulator soll das Vorhaben kostenneutral aufgesetzt werden.

6.3.3 Fördermassnahmen

In der vierten Gruppenarbeit wurden mögliche Fördermassnahmen identifiziert, welche die erfolgreiche eID-Einführung unterstützen. Ausgehend von den beiden behandelten Instanziierungen wurden unterschiedliche Massnahmen genannt.

Arbeitsgruppe mit der Instanziierung 1

Hier lauteten die Massnahmen wie folgt:

- Werte Kommunizieren (auch als Behördenaufgabe)
- Die Verwaltung soll Vorbilder schaffen, analog der Verpflichtung von e-Rechnung für Lieferanten des Bundes[17].
- Konditionierung von Leistungen, analog den Banken mit Bankomaten oder Self-Scanning im Retailmarkt.
- Ängste nehmen
    - Transparenz über Nutzung der eID (vgl Estland[18])
    - Einfaches Auskunfts-/Klagerecht (Rechtlicher Rahmenbedingung schaffen)
    - Einfache Nutzung/Support versus Sicherheit
- Einfache Zugänglichkeit für Relying Parties
    - Etablieren von Standards für Prozesse und Schnittstellen
    - Ermöglichen von Services in unterschiedlichen Qualitätsstufen. Dies ermöglicht tiefere Einstiegshürden und Step-up[19] Möglichkeiten.

[17] http://www.e-rechnung.admin.ch/d/erechnungssteller/e_rechnung_2016.php

[18] http://www.id.ee/?lang=en

[19] Die Relying Party akzeptiert in einem ersten Schritt eine einfache Authentifikation vom Benutzer und bietet entsprechende Services an. Um auf erweiterte Dienste, mit höheren Authentifikations-Anforderungen, zugreifen zu können muss sich der Benutzer mit einer stärkeren Authentifikationsmethode (z.B. biometrisch oder zertifikatsbasiert) identifizieren. [25]

- Prozessdesign (Registrierungsprozess, Fehler-logs)
    - Integration in Passausgabe
    - Ohne Zusatzkosten
- Mehr E-Government Services anbieten
- Usability von E-Government Service verbessern und standardisieren.

Arbeitsgruppe mit der Instanziierung 2

Hier lauteten die Massnahmen wie folgt:

- Der Staat stellt jedem Bürger eine nationale eID zur Verfügung.
- Nur von der nationalen eID abgeleitete eIDs dürfen für E-Health genutzt werden.
- Kopplung von Ausgabe der nationalen eID mit Identitätskarte und/oder Pass.
- Marketing für Transparenz im E-Health (Good Government für Gesundheitswesen).
- Ausbildung und Schulung für die Leistungserbringer anbieten.
- Die nationale eID muss verpflichtend und nachhaltig in der Verwaltung eingesetzt werden.
- Übergreifende Finanzierungsmodelle müssen definiert werden.
- Hilfsmittel und Support für die Unterstützung bei der Einführung und Verwendung. Dies könnten beispielsweise Musterprozesse, Registraturpläne, Berechtigungskonzepte für DMS der Archivierungsmethoden sein.
- Definieren eines Prozesses für den Umgang mit Identitätsmissbrauch.
- Das System muss sicher gebaut werden.
- Transparenz und Nachvollziehbarkeit über die Verwendung der eID.
- Übergeordnete Strategie für den Standort Schweiz muss definiert sein.
- Unterstützung eines E-Government Service Providers und dessen Umfeld.
- Sanktionierung des Nicht-Einsetzens von eIDs.

6.3.3.1 Zusammenfassung der Fördermassnahmen

Aus den Massnahmen der beiden Gruppen lassen sich folgende Massnahmen vereinheitlichen und in drei Kategorien zusammenfassen.

Kommunikation

- Eine gute Kommunikation wurde als essentiell identifiziert.
- Durchführen von Marketingaktivitäten für Transparenz.
- Definition von klaren Supportprozessen.
- Damit die eID auch nachhaltig erfolgreich ist, ist eine strategische Grundlage notwendig.

Verwendungshäufigkeit und Verbreitung

- Der Staat stellt jedem Bürger eine nationale eID zur Verfügung.

- Für die Verbreitung und die Herausgabe soll der bestehende Prozess für die Ausgabe von Identitätskarte und Pass verwendet werden.
- Die eID soll für den Nutzer gratis oder zumindest günstig erhältlich sein. Der Nutzer ist bereit dafür etwas zu zahlen, wenn er für sich durch die eID-Nutzung einen Nutzen wahrnimmt.
- Vorbilder schaffen, durch die Verpflichtung innerhalb der Verwaltung und allenfalls dem Verwaltungsumfeld (beispielsweise Lieferanten oder andere Verwaltungen).
- Konditionierung des eID-Einsatzes durch Anreize bei der Verwendung derselben.

Usability und Sicherheit

- Das System muss grundsätzlich als sicher empfunden werden. Dies kann jedoch ein direkter Widerspruch zur Sicherheit sein. Hier gilt es ein vernünftiges Mittelmass zu finden.
- Einfache Zugänglichkeit für die RP durch einfache Integration, einfach implementierbare Standards und klar definierte Prozesse.
- eID Services in unterschiedlichen Qualitätsstufen zur Verfügung stellen. Dies ermöglicht tiefere Einstiegshürden und Step-up Möglichkeiten.

6.4 Zusammenfassung der Workshop-Ergebnisse

Dieses Kapitel fasst die Erkenntnisse aus den Public Value Workshops zusammen.

Grundsätzlich ist festzuhalten, dass sehr viele Akteure ein Interesse an der eID-Einführung haben. Stakeholder, welche eine Präferenz gegen eine Einführung und über einen grossen Einfluss auf die Einführung haben, wurden, nur wenige identifiziert.

Die Rolle des Staates wird in der Verantwortung eines Regulators gesehen, der die notwendigen Rahmenbedingungen vorgibt. Des Weiteren könnte der Staat staatliche Register für entsprechende Attributnachweise anbieten. Modelle, in welchen der Staat als eID Anbieter mit sämtlichen Funktionalitäten auftritt, wurden mehrheitlich als nicht realistisch eingestuft. Eine Instanziierung ohne eine Unternehmensvertretung im Sinne eines Siegels wurde ebenfalls als nicht zielführend eingeschätzt.

Der grösste Nutzen einer eID wird bei organisationsübergreifenden Prozessen gesehen, bei welchen die eindeutige und sichere Identität einer Person relevant ist. Als weitere Kerneigenschaften der eID wurden immer wieder die grosse Verbreitung und die breite Nutzung identifiziert. Weiter wurde das Optimum zwischen Sicherheit und Einfachheit der Nutzung als zentrale Erfolgsparameter genannt.

Für die genannten Hindernisse wurden auch mögliche Lösungsvorschläge gemacht. Damit die eID den unterschiedlichen Qualitätsanforderungen der Relying Parties gerecht wird, soll sie unterschiedliche Qualitätsstufen unterstützten. Durch diese Funktionalität wird eine grössere Verbreitung erreicht, dies mit der Begründung, dass die eID nicht nur für hoch-sichere Anwendungen eingesetzt wird.

Die zu erwartende grosse Anfangsinvestition wird sich erst mittelfristig durch effizientere Prozesse auszahlen. Die späteren Nutzer der möglichen Kosteneinsparungen sind nicht zwingend diejenigen, welche die Investition tragen. Hier gilt es entsprechende Finanzierungs- oder Geschäftsmodelle zu finden.

Neben den gewonnen Erkenntnissen wurden die Diskussionen während des Workshops von den Teilnehmenden sehr geschätzt. Divergente Resultate konnten im Verlauf des Workshops teilweise geklärt werden. Eine erste Konsolidierung der Meinungen und ein Schritt hin zu einem gemeinsamen Verständnis haben stattgefunden. Hier besteht aber noch weiterer Handlungsbedarf.

7. Schlussfolgerungen und Ergebnisse

Die Ergebnisse der Interviews wie auch der Public Value Workshops zeigen auf, dass der Mehrwert einer eID von deren Ausgestaltung abhängig ist. Um einen Mehrwert zu erzielen, ist bei der Einführung auf folgende Punkte zu achten:

- Eine aktive und ehrliche Kommunikation der Aktivitäten bereits von Beginn an und die Definition von Supportprozessen werden für eine erfolgreiche Einführung als essentiell eingestuft. Dazu gehört auch die Sensibilisierung der Bevölkerung hinsichtlich der Unzulänglichkeiten der heutigen Praxis.
- Eine häufige Verwendung und weite Verbreitung der eID trägt wesentlich zum Gelingen bei. Hierfür sind die Ausbau- und Integrierbarkeit der eID massgebend, sowie die Gewinnung von Anwendungsfällen mit einfachen Prozessen und mit hohen Nutzerzahlen.
- Usability und Sicherheit müssen sich die Waage halten. Um die Einbindung unterschiedlicher Services zu erlauben, könnten unterschiedliche Qualitätsstufen angeboten werden. Dies ermöglicht tiefere Einstiegshürden und Step-up Möglichkeiten. Um die Integration einfach zu halten, ist es wichtig Standards und Prozesse zu definieren.

Daraus ergeben sich folgende Nutzen

- Mehr Qualität: Die Möglichkeit Identitäten auf elektronischem Wege eindeutig nachzuweisen erbringt einen deutlichen Nutzen an sich. Dieser Mehrwert wurde sowohl bei den Interview- wie auch bei den Workshop-Ergebnissen identifiziert.
- Mehr Geld: Das damit verbundene Einsparpotenzial und der Effizienzgewinn werden als separater Nutzen betrachtet.
- Mehr Effizienz: Die eID vereinfacht die organisationsübergreifende Zusammenarbeit.
- Mehr Transparenz: Die eID erlaubt eine benutzerzentrierte Datenverwaltung. Dieses neue Paradigma verschiebt die Verantwortung von Datenfreigaben auf den Benutzer. Dadurch, dass der Benutzer künftig die Weitergabe seiner Daten kontrolliert, wird die Transparenz in der Verwendung persönlicher Daten erhöht.
- Mehr Rechtssicherheit: Die eID ermöglicht die klare Identifizierung von Sender und Empfänger von Nachrichten sowie deren Verschlüsselung.

Der Staat nimmt bei der Bereitstellung eine zentrale Rolle ein, indem er den institutionell-rechtlichen und organisatorischen Rahmen festlegt und indem er die Identitätsvergabe als hoheitliche Aufgabe versteht. Für das Gelingen ist eine hohe Anfangsinvestition seitens des Staates vorzusehen.

Insbesondere aus den Interviews kommt die Erkenntnis, dass als Nutzende nicht einzig Schweizer Bürgerinnen und Bürger zu verstehen sind, sondern alle potenziellen eID-Nutzer berücksichtigt werden müssen. Konkret ist bei der Definition der Nutzenden vom Nationalitätskonzept wegzukommen, hin zu allen potenziellen Kunden einer E-Commerce-, E-Health, E-Education- oder E-Government- Transaktion.

Die Erfahrungen aus den Interviews und den Public Value Workshops zeigen, dass das eID-Ökosystem Modell sich gut als Grundlage für den fachlichen Austausch zwischen verschiedenen Teilnehmern des eID-Ökosystems eignet. Trotz dem hohen Abstraktionsgrad und der Komplexität des systemischen Sachverhalts ist es Personen bzw. Organisationen möglich, sich selbst im Modell einzuordnen. Die Stakeholder sind in der Lage, ihren potenziellen Beitrag als Bereitsteller, Nutzer oder beides präzise zu benennen. Das Modell hat eine gemeinsame Sprache für die weitere, sich erst am Anfang befinliche Diskussion zur Ausgestaltung der nationalen eID in der Schweiz geschaffen. Es bietet damit eine gute Basis, um den Dialog zwischen den verschiedenen Stakeholdern im eID-Ökosystem zu stärken.

8. Empfehlungen

Gestützt auf die Ergebnisse aus den Interviews wie auch aus dem Public Value Workshop wurden im Projekt folgende Empfehlungen im Hinblick auf die Weiterentwicklung des eID-Ökosystems und die Einführung einer nationalen eID ausgearbeitet.

Anwendung des eID-Ökosystem Modells

Das eID-Ökosystem Modell und die abstrakten Instanziierungen lassen nur generische Diskussionen rund um die eID zu. Um die Diskussionen weiter zu führen und Faktoren wie Kosten, Qualität, Sicherheit und Usability zu diskutieren, braucht es eine realistische und konkrete Ausprägung einer eID-Umsetzung.

Konkrete Anwendungsfälle unterstützen Diskussionen und vereinfachen die Sichtweise der an der Diskussion Beteiligten. Dies kann unter Anderem helfen, die konkreten Anforderungen zu formulieren. Eine Fokussierung auf nur einen (oder einzelne) Anwendungsfall/-fälle verhilft der eID nicht zum Durchbruch und ist für eine erfolgreiche Implementierung hinderlich.

Die generische Tauglichkeit des vorliegenden Modells wurde über Experteninterviews (siehe Kapitel 5) und über die Diskussion von zwei Instanziierungen (siehe Kapitel 1.1) in zwei halbtägigen Public Value Workshops (siehe Kapitel 6) geprüft und für gut befunden. Für die weiteren Arbeiten rund um die nationale eID und das eID-Ökosystem empfiehlt sich folgendes Vorgehen.

Ausgehend von einer generischen Instanziierung, die für tauglich befunden wird, ist je eine konkrete IST- und eine SOLL-Ausprägung zu erarbeiten. Dabei sind, von spezifischen Nutzenden ausgehend, passende Anwendungsfälle zu definieren und die dazu notwendigen Nutzungen abzuleiten. In der Folge ist zu diskutieren: Erstens - welche Stakeholder welche Teile der Bereitstellung zu leisten haben; zweitens – welche Stakeholder bereit sind mitzutun; überdies ist drittens zu klären, was die Implementierung der eID an institutionellen bzw. rechtlichen Anpassungen erfordert; viertens ist zu klären, wie der organisatorische Rahmen zu implementieren ist und welche Rollen, Aufgaben und Verantwortungen die konkreten Akteure innerhalb des politischen Rahmens wahrzunehmen haben. Ausgehend von der Nutzungsseite ergeben sich diverse Abhängigkeiten in Relation zur Bereitstellungsseite, die sich aber nur anhand konkreter Ausprägungen des Ökosystems verlässlich identifizieren lassen. Aus dem Delta von SOLL- und IST-Ausprägungen, können dann Massnahmen zur Förderung des Ökosystems und der nationalen eID erarbeitet werden.

Einbezug von Stakeholdern

Von zentraler Bedeutung bezüglich Abstützung des eID-Ökosystems und der Implementierung der eID ist es, alle relevanten Stakeholder miteinzubeziehen. Eine entsprechende Stakeholder-Analyse, auf welcher aufgebaut werden kann, ist in diesem Bericht vorhanden. Frühzeitig sollen auch Nutzer/Bürger involviert werden. Hier wäre eine Akzeptanzbefragung eine mögliche Methode. In Anbetracht der vielen Stakeholder mit unterschiedlichen Interessen ist ein regelmässiger Austausch von Information ratsam. Dies könnte unter anderem in Workshops rund um das Thema eID erfolgen. Hieraus ergibt sich ein grosses Potential, relevante Entscheidungsträger abzuholen.

Empfehlungen für das Ökosystem

Weitere Empfehlungen aus den Interviews und den Public Value Workshops betreffen die Umsetzung des eID-Ökosystems. Als Ziel sollte eine Gesamtlösung angestrebt werden. Isolierte Teillösungen werden aufgrund eines geringen Umfangs und geringer Funktionalitäten keinen Durchbruch der eID ermöglichen. Das System soll offen gebaut und für spätere Anwendungsfälle (z.B. Integration mit der EU) ausbaufähig sein. Modulare Lösungen sind zu bevorzugen und sollen den Anforderungen nach verschiedenen Qualitätsstufen gerecht werden. Dadurch sollen unterschiedliche Anwendungen und eine weite Verbreitung ermöglicht werden.

Finanzierungs- und allenfalls Geschäftsmodelle, welche die anfallenden Kosten aufzeigen und sie möglichen Nutzen gegenüberstellen, aber auch die Aufteilung von Kosten und Nutzen zwischen den Stakeholdern sind zu erarbeiten, abzustimmen und Ungleichgewichte gezielt zu eliminieren.

Der Markt im Bereich eID entwickelt sich rasant. Bei Nichtvorhandensein einer staatlichen eID könnten private eIDs in die Lücke springen und auch ohne staatliche Vertrauensgrundlage für sichere Nutzung verwendet werden. Dies würde Abstriche beim Datenschutz und der Verwendbarkeit für staatliche Services bedeuten. Es besteht aktuell die Chance, die Grundlage für eine staatliche, sichere und akzeptierte Lösung zu schaffen.

9. Fazit und Ausblick

Nebst den materiellen Resultaten, die im vorliegenden Bericht präsentiert sind, generierten die Arbeiten rund um das Schweizer eID-Ökosystem auch nicht verschriftliche Resultate. Die Interviews mit Schlüsselakteuren aus allen Bereichen der E-Society, der öffentlichen Verwaltung auf allen föderalen Ebenen wie auch der Privatwirtschaft haben deutlich dazu beigetragen, die Aufmerksamkeit auf die Thematik einer Schweizer eID zu lenken. Die Arbeiten haben somit Information und Sensibilisierung der unterschiedlichen Stakeholder, aber auch deren aktiven Einbezug und Beteiligung am Diskurs bewirkt. Dies wurde von verschiedenster Seite begrüsst. Der vertiefte Diskurs hat dabei auch gezeigt, dass deutliche Unterschiede in Kenntnisstand, Interpretation und Verständnis der Faktenlage, aber auch im bekannten und verwendeten Vokabular vorhanden sind. Das erarbeitete und verwendete Modell vermochte zur Konsolidierung der Sichten und Meinungen beizutragen und den zuvor eher emotional geprägten Diskurs in fachliche Richtung zu lenken. Im Verlaufe der Arbeiten wurde aber auch wiederholt klar, dass die Entwicklungen rund um eine Schweizer eID nur dann zum Erfolg führen, wenn die involvierten Entscheidungsträger und Fachexperten zur Kooperation über Departemente, Organisationen und Fachbereiche hinweg bereit sind.

Während die erfolgten Arbeiten also sicher einen Beitrag zur Konsolidierung von Wissen, Sprache und Verständnis leisten konnten, darf die gesamtgesellschaftliche Wirkung einer eID nicht unter- aber auch nicht überschätzt werden. Die bis dato involvierten Kreise sind nach wie vor überschaubar. Es werden weiterhin Investitionen notwendig sein, um den Fachdiskurs auszuweiten und die Konsolidierung der Sichten weiterzutreiben. Mit dem vorliegenden eID-Ökosystem Modell liegt ein Instrument vor, das nun in der weiteren Kommunikation eingesetzt werden kann. Eine solche Massnahme wurde vom Projektteam bereits in die Wege geleitet: Nach erfolgter Publikation der Botschaft des Bundesrates zur Schweizer eID ist die Durchführung eines Informationsanlasses zusammen mit der Parlamentarischen Gruppe ePower geplant.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Schweizerische Eidgenossenschaft, «Schweizerpass,» 16 12 2011. [Online]. Available: http://www.schweizerpass.admin.ch/pass/de/home/aktuell/news/2011/ref_2011-12-16.html.

[2] eHealth suisse, «Was ist eHealth?,» [Online]. Available: http://www.Was ist eHealth?.ch/. [Zugriff am 05 2015].

[3] Stachowiak, Allgemeine Modelltheorie, Wie: Springer-Verlag, 1973.

[4] eCH Fachgruppe IAM, «eCH-0107: Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM),» 04 12 2013. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0. [Zugriff am 05 2015].

[5] eCH Fachgruppe IAM, «eCH-0170: eID Qualitätsmodell,» 06 06 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=1.0. [Zugriff am 05 2015].

[6] R. Riedl, «Anforderungen an die Ökosystem Modellierung und erste System-Sichten,» Berner Fachhochschule, Bern, 2014.

[7] H. Kubicek, Special Issue: The Diversity of National E-IDs in Europe: Lessons from Comparative Research. In: Identity in the E-Society 3, 2010.

[8] H. Kubicek und T. Noack, Mehr Sicherheit im Internet durch elektronischen Idenitätsnachweis - Der neue Personalausweis im europäischen Vergleich, Berlin: Lit Verlag, 2011.

[9] T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros und W. Lusoli, «The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies.,» 2010. [Online]. [Zugriff am 26 05 2015].

[10] W. Lusoli und R. Compañó, «From security versus privacy to identity: an emerging concept for policy design?,» *info 12,* pp. 80-94, 2010.

[11] Graudenz et al., «Elektronisches Identitätsmanagement - Mehr Einfachheit, Datenhoheit und Datensicherheit in unserer virtualisierten Welt. ISPRAT Whitepaper.,» [Online]. Available: http://epub.sub.uni-hamburg.de/epub/volltexte/2010/4681/pdf/ISPRAT_Whitepaper_Elektronische_Identitaeten.pdf. [Zugriff am 26 05 2015].

[12] D. Castro, «Explaining International Leadership: Electronic Identification Systems,» ITIF, The Information Technology & Innovation Foundation., 2011.

[13] T. W. House, «National Strategy for Trusted Identities in Cyberspace,» 2011. [Online]. Available: https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. [Zugriff am 27 05 2015].

[14] Europäisches Parlament und Rat der Europäischen Union, «VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Regulierung),» 23 06 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=EN. [Zugriff am 05 26 2015].

[15] Bundesamt für Polizei fedpol, «Konzeptstudie elektronischer Identitätsnachweis,» Bern, 2013.

[16] L. Müller und M. Walser, «Konzept für schweizerische staatlich anerkannte eID-Systeme,» Bundesamt für Polizei fedpol, Bern, 2015.

[17] E. Kommission, «European Interoperability Framework (EIF) for European public services,» 16 12 2010. [Online]. Available: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf. [Zugriff am 26 05 2015].

[18] M. Moore, Creating Public Value - Strategic Management in Government, New York: Harvard University Press, 1995.

[19] P. Gomez und T. Meynhardt, «Gesellschaftliche Wertschöpfung im Fokus der Führung,» 2010. [Online]. Available: http://schweizerdialog.ch/wp-content/uploads/2010/05/PublicValue_Ges.Wertschoepfung_im_Fokus_der_Fuehrung.pdf. [Zugriff am 05 2015].

[20] Bundesamt für Gesundheit BAG, «eHealth – Fragen und Antworten,» 2007. [Online]. Available: http://www.e-health-suisse.ch/. [Zugriff am 05 2015].

[21] eHealth Suisse, «Standards und Architektur,» 04 05 2015. [Online]. Available: http://www.e-health-suisse.ch/. [Zugriff am 05 2015].

[22] Bundesamt für Gesundheit BAG, «Versichertenkarte,» 16 09 2011. [Online]. Available: http://www.bag.admin.ch/themen/krankenversicherung/07060/. [Zugriff am 05 2015].

[23] E. P. u. Rat, «VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische

Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Regulierung),» 23 06 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=EN. [Zugriff am 05 26 2015].

[24] eCH Fachgruppe IAM, «eCH-0167 SuisseTrustIAM Rahmenkonzept,» 06 06 2014. [Online]. Available: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0167&documentVersion=1.0. [Zugriff am 05 2015].

[25] S. Rieger, «User-centric Identity Management in heterogeneous Federations,» 2009. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5072572&tag=1 . [Zugriff am 05 2015].

[26] A. Jøsang und S. Pope, «User Centric Identity Management,» 2005. [Online]. Available: http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf. [Zugriff am 05 2015].

[27] Microsoft Corporation, «Step-Up Authentication Scenario,» 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee517290.aspx. [Zugriff am 05 2015].

[28] A. M. Cresswell, G. B. Burke und T. A. Pardo, «Advancing Return on Investment Analysis for Government IT: A Public Value Framework,» 2006. [Online]. Available: http://www.ctg.albany.edu/publications/reports/advancing_roi?chapter=&PrintVersion=2. [Zugriff am 05 2015].

[29] Verbindung der Schweizer Ärztinnen und Ärzte FMH, «FMH-HPC – Ärzteausweis mit Mehrwert,» 2015. [Online]. Available: http://www.fmh.ch/services/fuer_die_mitglieder/hpc.html. [Zugriff am 05 2015].

Anhang

Anhang 1: Interview Fragebogen

Die Experteninterviews wurden auf der Grundlage des folgenden Fragebogens durchgeführt. Je nach Interviewverlauf konnten nicht alle Fragen abschliessend beantwortet werden.

1. **Verständlichkeit**
    a. Gibt es grundsätzliche Fragen zum Modell?
    b. Sehen Sie sich in diesem Modell? Wo und in welcher Rolle?
    c. Ist dieses Modell verständlich?
    d. Ist die Kategorisierung sinnvoll?
    e. Sind alle relevanten Kategorien integriert?

2. **Mögliche Nutzungen**
    [zu formulieren: Erläuterung der einzelnen Nutzungen in allgemeiner Form, inkl. Beispielen]

    a. Nutzen für die eigene Organisation
        i. Ausgehend von den abgebildeten Nutzungen: Welche könnten in Ihrer Organisation hauptsächlich genutzt werden?
        ii. Was für einen Mehrwert bringen diese Nutzungen aus Ihrer Sicht für Ihre Organisation (aus Innensicht, aus Leistungserbringungssicht, aus Sicht der Kunden, aus Sicht der Mitarbeiter)?
        iii. Welche Aufwände stehen dem Nutzen Ihrer Verwaltung aus der eID-Nutzung gegenüber?
    b. Nutzen in übergreifender Perspektive
        i. Ausgehend von den abgebildeten Nutzungen: Welche sind Ihrer Meinung nach die wichtigsten für die Nutzung durch Verwaltung, Wirtschaft und Gesellschaft?

3. **Erfolgsfaktoren**
    a. Welches sind die kritischen Erfolgsfaktoren einer nationalen eID Lösung?
        i. offene Antwort
    b. Wir haben eine Liste von möglichen kritischen Erfolgsfaktoren zusammengestellt, können Sie aus dieser Auswahl nochmal die fünf wichtigsten nennen? [Anm. aufgrund der knappen Zeit wurden hier nur die kritischen Erfolgsfaktoren abgefragt]
        i. Europäische Akzeptanz der eID-Lösung
        ii. Europäische Notifizierung der eID
        iii. Nutzungshäufigkeit der eID
        iv. Einsatz der eID bei den Relying Parties
        v. Anwendungsbereich der eID (Key- oder Killerapplikationen)
        vi. Zusammenspiel von Öffentlicher Verwaltung und Privatwirtschaft
        vii. Einfachheit der Ableitung von Identitäten
        viii. Anerkennung von abgeleiteten Identitäten
        ix. Haftungsfragen im Zusammenhang mit der eID seitens Verwaltung und Privatwirtschaft

x. User-Zentrizität der eID-Lösung
xi. Qualität (im Sinne von QAA) der eID
xii. Attributebereitstellung in Zusammenhang mit eID
xiii. Nachvollziehbarkeit des eID-Einsatzes (Nachvollziehbarkeit wer sich ausgewiesen hat)
xiv. Integration der eID-Lösung bei den Relying Parties
xv. Unterstützung der Nutzung der eID (Support) z.B. durch Relying Parties oder Dritte (Help Desk).
xvi. Vertrauen der Bürger in die Lösung
xvii. Akkreditierung der eID-Lösung bei den Relying Parties
xviii. Marketing und PR für die eID-Lösung
xix. Kosten der eID-Lösung für die Bürger
xx. Kosten der eID-Lösung für die Privatwirtschaft

c. Je nach Ausgestaltung der gesamten Lösung ist eine durchgehende Identifikation eines Nutzers über einen einheitlichen Personenidentifikator möglich oder wird durch Neuzuteilung einer Nummer bei jeder Erneuerung/jedem zusätzlichen Identitätstoken verhindert. Welche Bedeutung hat für Sie ein eindeutiger Personenidentifikator im Kontext der eID?
    i. zwingend für Nutzen/Nice-to-have/Risiko für Akzeptanz/…

d. Was sind zwingende Erfolgsfaktoren für den Erfolg des eID-Ökosystem und was die grössten Hinderungsfaktoren?

4. Bereitstellung

Im Kontext des Ökosystems stellt sich die Frage nach einer optimalen Zusammenarbeit zwischen Staat und Privaten in der Bereitstellung.

a. Bereitstellung des Staates
    i. Welche Elemente müssen Ihrer Meinung nach zwingend durch den Staat bereitgestellt werden? Aus welchem Grund? (Rechtlich, Vertrauen, kein Business, …)
    ii. Welche bestehenden oder zu schaffenden Behörden sollen Ihrer Meinung nach eine wichtige Rolle im Betrieb der Schweizer eID übernehmen?

b. Bereitstellung durch die Privatwirtschaft
    i. Welche Elemente sollen vorzugsweise von privaten Anbietern betrieben werden?
    ii. Welche Voraussetzungen müssen für den Betrieb durch Private gegeben sein?
    iii. Welche Eigenschaften müssen Private dazu erfüllen?

5. Einstellung zu eID

a. Wie stehen Sie in einigen Sätzen dem Vorhaben eine nationale eID zu realisieren gegenüber?
    i. Gründe für Zustimmung/Ablehnung/Vorbehalte

6. Abschlussfrage

a. Wo sehen Sie Verbesserungspotential für das Modell?

Anhang 2: Die vier Nutzungsszenarien

Zur Fokussierung des Projektes wurden in einem internen Workshop des Projektteams drei prioritäre Nutzungsszenarien für das Ökosystem-Modell definiert und in der Diskussion mit dem Auftraggeber um ein weiteres ergänzt. Zusätzlich soll das Modell zur Entwicklung von Anwendungsfällen für eIDs mit einer Beschreibung des Nutzens angewendet werden.

Die Arbeiten sollen dazu dienen, sehr konkret die Anwendung und Nutzen von elektronischen Identitäten zu benennen. Diese Anforderung ist entscheidend und wird der methodischen und wissenschaftlichen Herleitung übergeordnet, gleichwohl stellt die methodische Korrektheit die Glaubwürdigkeit des Modelles sicher.

Die Reihenfolge der vier Nutzungsszenarien in diesem Dokument entspricht dem chronologischen Ablauf eines möglichen Gesetzgebungsprozesses. Aus der Experten-Perspektive wird ein funktionierendes Modell erstellt und unterstützende Massnahmen definiert. Im Dialog mit den privatwirtschaftlichen Akteuren wird das Modell überprüft und gegeben falls überarbeitet. Um das Modell in der Verwaltung zu etablieren wird eine Ämterkonsultation durchgeführt. Danach können die politischen Akteure die Umsetzung der Massnahmen auf politischer Ebene angehen.

Experten (BFH, SECO, Teilnehmer der Fedpol Workshops)

Wer	Fachexperten aus dem Bereich eID
Wozu	Instrument für die Herleitung und Begründung der Begleitmassnahmen Aufzeigen von Nutzen und Folgen für die Politik und Fachkontakte Aufzeigen der Funktionsweise des Ökosystems und der Interdependenzen zwischen Elementen
Form	Grafische Darstellung des Ökosystem-Modells mit Erläuterung Auflistung möglicher Massnahmen zur Förderung des eID-Ökosystems Kurzfassung des Modells (Grafik) für den Dialog mit verschiedenen Stakeholdern
Wie	Flughöhe: Überblick, organisatorisch detailliert / keine technische Details Auswirkung in den Dimensionen die für Politik und Fachkontakte relevant sind Bezugsrahmen: Relevante eCH-Standards, existierende nationale und privatwirtschaftliche Lösungen, wissenschaftliche Literatur, Bezugsrahmen der für Politik und Fachkontakte relevant ist
Erfolgskriterien	Erste Priorität: - Ableitung von Massnahmen, die an die Politik vermittelbar sowie umsetzbar und wirksam sind - Überzeugende Begründung der Massnahmen mit Hilfe des Modells - Akzeptanz durch Experten - Gründe für Widerstand abbauen Zweite Priorität: - Verallgemeinerung und Wiederverwendbarkeit des Modells herstellen - Adaption für wissenschaftliche Publikationen

Privatwirtschaftliche Akteure im Bereich IAM

Wer	Vertreter von Lösungsprovidern im Bereich IAM, die Dienste und Lösungen mit grossem Impact im Scope des eID-Ökosystems potentiell anbieten können oder bereits anbieten (Post, Swisscom, QuoVadis, SBB, …).
Wozu	Instrument zur Skizzierung der Businesschancen Wiedererkennung des eigenen Geschäftes im Ökosystemmodell Unterstützung durch Anbieter sichern
Form	Grafische Darstellung des Ökosystem-Modells mit Erläuterung Aufzeigen von Funktionsweise und Abhängigkeiten
Wie	Flughöhe: Überblick, organisatorisch detailliert / keine technische Details Fokus auf Elemente und Applikationen, die privatwirtschaftlich erbracht werden können/sollen, Darstellung möglicher Umsatzströme Bezugsrahmen: existierende nationale und privatwirtschaftliche Lösungen, wissenschaftliche Literatur, Public Value-Perspektive
Erfolgskriterien	Modell dient als Grundlage zur Darstellung von Businesschancen, die im Dialog mit den privatwirtschaftlichen Akteuren überprüft und überarbeitet werden. Ergänzend zu den Businesschancen hilft das Modell, mögliche Lücken zwischen Public Value der gesamten Lösung und wirtschaftlicher Rentabilität einzelner Elemente zu eruieren. Modell fördert Unterstützung durch privatwirtschaftliche Schlüsselakteure für die geplante Lösung
Einschränkung	Keine ausführliche technische Dokumentation

Fachkontakt mit Ämtern

Wer	In erster Priorität: Bundesämter welche IAM im Kerngeschäft betreiben oder zentrale Interessen darin haben (Bundesamt für Polizei fedpol, Bundesamt für Migration, Bundesamt für Informatik und Telekommunikation, Bundesamt für Justiz, Informatiksteuerungsorgan des Bundes, Staatssekretariat für Wirtschaft, Bundeskanzlei und die SIK für die Sicht der Kantone, Gemeinde- und Städteverband) In zweiter Priorität: alle weiteren Bundesämter Ansprechpersonen: Amtsdirektoren, CIOs der Ämter Zusätzliche Dokumentation für beurteilende Stellen z.B. IT-Architekten
Wozu	Wiedererkennung der Organisation im Ökosystemmodell Aufzeigen von Nutzen und Konsequenzen der Massnahmen für die Organisation Einschätzung und Bewertung der Veränderungen Rückmeldung zu Massnahmen aus Amtssicht, ggf. weitere Massnahmen anregen
Form	Akteur-orientierte grafische Darstellung des Ökosystem-Modells Massnahmenliste Aufzeigen von Funktionsweise und Abhängigkeiten
Wie	Flughöhe: organisatorisch detailliert / keine technischen Details Auswirkung aufzeigen in den Dimensionen: Eigene Organisation und Partner Bezugsrahmen: Gesetzlicher Auftrag, Organisations-Strategie, Projekte, Applikationen und Register des jeweiligen Amtes
Erfolgskriterien	Akzeptanz durch Bundesämter, Unterstützung in der Ämterkonsultation Potentielle Gründe für Widerstand abbauen Schlüsselanforderungen abholen
Einschränkung	Klare Priorität auf der Sicht der Leitung, keine ausführliche technische Dokumentation

Politische Akteure

Wer	Politische Akteure im politischen Prozess: Bundesrat, den BR beratende Stellen im Mitberichtsverfahren Adressaten der Vernehmlassung Parlament, insbesondere die Opinion Leaders in den Fraktionen (u.a. die Mitglieder der e-Power-Initiative) und Lobbyisten im Themenfeld Medienvertreter, die im Rahmen der Parlamentsdebatte über das Thema berichten
Wozu	Begründung für Gesamtkonzeption und vorgeschlagene Begleitmassnahmen Darstellung des Nutzens der Lösung, Adressierung von Sicherheits- und Datenschutzbedenken für die Interkation mit einem kritischen Gegenüber
Form	Einfache grafische Darstellung des eID-Ökosystems in welcher sich alle Beteiligten (Bund, Kantone, Gemeinden, Wirtschaft) wieder finden. Darstellung von Auswirkungen und Abhängigkeiten zu anderen Vorhaben/bestehenden Gesetzen
Wie	Flughöhe: hoch Überblick schaffen Fokus auf Auswirkungen bei Annahme oder Ablehnung. Auswirkung in den Dimensionen: Verwaltung, Wirtschaft und Gesellschaft Bezugsrahmen: Legislaturplanung, bestehende und geplante Gesetze (insb. Ausweissgesetz), Strategien (Informationsgesellschaft, E-Government, E-Health, …)
Erfolgskriterien	Annahme der Vorlage Überzeugende Argumentation, mögliche Kritikpunkte sind adressiert Modell wird als Grundlage für die Medienberichterstattung verwendet
Einschränkung	Keine inhaltliche Aufarbeitung der Abhängigkeiten zu bestehenden und geplanten Gesetzesvorhaben

Staatssekretariat für Wirtschaft SECO
Direktion für Standortförderung
KMU-Politik
Holzikofenweg 36, 3003 Bern
Tel. +41 58 462 28 71, Fax +41 58 463 12 11
www.seco.admin.ch, www.kmu.admin.ch