Beilage 01

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidg. Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Konzeptstudie elektronischer Identitätsnachweis

Klassifizierung *	Nicht klassifiziert
Status **	In Prüfung
Projektname	Erneuerung Pass und Identitätskarte
Projektabkürzung	EPI
Projektnummer	7876
Projektleiter	M. Waldner
Auftraggeber	Th. Kräuchi
Autor	fedpol
Bearbeitende	Wdm, Gka, Bue
Prüfende	Teilnehmer Workshop
Genehmigende	Projektauftraggeber
Verteiler	öffentlich
Doc_ID	7876-063

* Nicht klassifiziert, Intern, Vertraulich

** In Arbeit, In Prüfung, Abgeschlossen

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle
0.2	17.05.2013	Nach eID-Workshop und Präferenzen	Div.
0.5	30.06.2013	Entwurf für Versand an PA	Bue, Wdm, Gka
0.7	10.07.2013	Für Übersetzung und WS-Teilnehmer	Div.
1.0a	12.08.2013	Version für informelle Konsultation	fedpol

Inhaltsverzeichnis

1 Einführung

1.1 Zweck des Dokuments

Die vorliegende Konzeptstudie fasst die bisherigen Überlegungen und Ergebnissen zur Konzeption der künftigen Schweizerischen elektronischen Identität (eID) gemäss Auftrag des Bundesrates vom 19. Dezember 2012 zusammen. Sie ermöglicht eine übergreifende Sicht auf die Ziele und Anforderungen sowie auf mögliche Realisierungs-Varianten für ein elektronisches Identifikationsmittel, das zusammen mit der neuen Identitätskarte oder anderen staatlichen Ausweisen bezogen werden kann.

Das Dokument soll zuerst im Rahmen einer informellen Konsultation den interessierten Stellen in Wirtschaft und Verwaltung für eine Meinungsbildung und Stellungnahme dienen, später - zusammen mit einem weiter ausgearbeiteten Lösungsvorschlag und einem Entwurf für die notwendige Gesetzgebung - Teil eines Antrag an den Bundesrat bilden und schliesslich als Basis für die weitere Realisierung bzw. Beschaffung dienen.

Das Dokument basiert auf dem Hermes-Dokument 'Bericht Konzept', wurde aber für diesen Zweck angepasst.

1.2 Zusammenfassung

Wieder einmal steht die Konzeption und Beschaffung einer neuen Identitätskarte (IDK) an. Da stellt sich die Frage, ob zusammen mit diesem verbreiteten Ausweis für die physische Welt künftig auch ein Ausweis für die Online-Welt angeboten werden soll. Der Bundesrat hat den Auftrag gegeben, diese Frage zu prüfen und ihm bis Mitte 2014 ein Konzept und einen Rechtsetzungs-Vorschlag für ein zusammen mit der IDK angebotenes, elektronisches Identifikationsmittel (eIdM) vorzulegen.

Mit einem solchen 'Online-Ausweis' kann man seine Identität oder gewisse Eigenschaften, wie z.B. die Staatsangehörigkeit oder das Alter überall dort, wo das erforderlich ist, auch über das Internet nachweisen. Einige Anwendungsbeispiele von vielen sind hier die Online-Bestellung eines Handy-Abonnements, der Bezug von Waren mit Altersbeschränkung, die Eröffnung eines Bankkontos oder der Bezug eines Geburtsscheins. Dabei muss dieses elektronische Identifikationsmittel in die bestehende wie auch in die künftige elektronische Infrastruktur passen, mit verschiedenen weiteren Komponenten beim Benutzer, im Netz und beim Dienstanbieter zusammenwirken und vom Benutzer einfach angewendet werden können. Wenn man bedenkt, dass eine IDK-Technologie typischerweise über 25 Jahre Bestand haben muss, ist das keine einfache Anforderung.

Eine weitere Frage ist, welches der optimale Beitrag des Staates ist, um einen starken elektronischen Identitätsnachweis zu fördern, und wie diese Funktion mit der bisherigen Identitätskarte verknüpft werden soll. Im Minimum soll der aufwendigste Teil für die Herausgabe eines Ausweises, nämlich das Vorsprechen bei der Behörde und die Überprüfung und Feststellung der Identität gleichzeitig auch für den Bezug einer elektronischen Identität mitbenutzt werden können, sofern diese Option gewünscht wird. Ob dann das elektronische Identifikationsmittel gleich auch in die Identitätskarte integriert werden soll und wie es genau aufgebaut ist, dafür gibt es verschiedene Lösungsansätze mit unterschiedlichen Vor- und Nachteilen, die hier in der Form von vier Lösungsvarianten vorgestellt werden:

Variante 1: Private eID mit staatlicher Identifikation und Regulierung

Variante 2: Identitätsnachweis mit der ePass-Funktion

Variante 3: Klassische staatliche Mainstream-eID

Variante 4: eID à la Deutschland.

Aus Sicht der Projektleitung sind alle vier Varianten sinnvolle, machbare Lösungen mit je eigenen Vor- und Nachteilen. Wichtige Bewertungs-Kriterien sind die Kosten für Investition und Betrieb (Support), die Risiken bei der Realisierung und bezüglich des Erfolgs in der Anwendung sowie der Komfort für die Benutzer und das Verhältnis zum Persönlichkeitsschutz. Eine Präferenz für die eine oder andere Variante kann sich aber auch daraus ergeben, wie man die Rolle des Staates in diesem Bereich sieht, welche Kosten und Risiken man zu tragen bereit ist und natürlich auch danach, wie man die künftige Entwicklung des gesamten eID-Gesamtsystems einschätzt. Aus diesem Grund hat das Bundesamt für Polizei (fedpol) entschieden, eine informelle Konsultation der interessierten Kreise vorzunehmen, bevor eine Lösung detaillierter ausgearbeitet wird.

Je nach Ergebnis der Konsultation und interner Entscheidfindung werden anschliessend eine bis zwei Lösungsvarianten detailliert geplant und inklusive detaillierter Kostenberechnung und Konzepten für die Anpassung der Prozesse und für die gesetzlichen Grundlagen dem Bundesrat vorgelegt.

2 Ausgangslage

2.1 Anlass und Begründung

Das EJPD – bzw. fedpol – ist daran, eine neuen Pass und eine neue Identitätskarte (IDK) zu beschaffen. Aufgrund erster Studien und eines Antrags des EJPD hat der Bundesrat die beiden Aufträge in seinem Beschluss vom 16. Dezember 2011 näher definiert. Bezüglich Identitätskarte wird das EJPD beauftragt, in Zusammenarbeit mit den betroffenen Stellen des Bundes und der Kantone ein Projekt zur Erneuerung der IDK umzusetzen.

Im BRB zu einem umfassenden Gesetzgebungspaket zur Förderung des elektronischen Geschäftsverkehrs vom 19. Dezember 2012 hat der Bundesrat den Auftrag bezüglich der eID und ihrer gesetzlichen Grundlage wie folgt weiter konkretisiert:

> *Das EJPD wird beauftragt, in Zusammenarbeit mit der BK, dem EVD, UVEK und EFD ein Konzept und einen Entwurf für die rechtliche Ausgestaltung des künftigen elektronischen staatlichen Identifikationsmittels (eID), das zusammen mit der neuen Identitätskarte angeboten wird, auszuarbeiten und dem Bundesrat bis Mitte 2014 vorzulegen.*

2.2 Elektronischer Identitätsnachweis - um was geht es

2.2.1 Was ist und was soll ein elektronischer Identitätsnachweis?

Über 5 Millionen Schweizerinnen und Schweiz nutzen heute die Identitätskarte (IDK). Nicht nur zum Identitätsnachweis gegenüber Behörden, sondern ebenso im geschäftlichen Umfeld, beispielsweise beim Eröffnen eines Bankkontos, beim Erwerb von Waren mit Altersbeschränkungen oder beim Abholen von Einschreiben bei der Post.

Immer mehr solcher Dienstleistungen werden heute elektronisch angeboten, zusammen mit neuen, ausschliesslich netzbasierten Dienstleistungen. In dieser elektronischen Welt ersetzt der **elektronische Identitätsnachweis** den konventionellen Nachweis mit der IDK. Durch ein zusammen mit der Identitätskarte erworbenes **elektronisches Identifikationsmittel** soll künftig der Online-Beweis der Identität gegenüber einer Behörde oder einem Anbieter im Netz genauso praktisch und einfach sein, wie es das Vorzeigen eines Ausweises heute ist.

Gleich wie bei den physischen Kontakten gibt es in der Online-Welt viele Fälle, wo man anonym bleiben möchte, was zu schützen ist. Gleichzeitig gibt es aber auch viele Anwendungen, wo es sehr wichtig oder unabdingbar ist, dass sich die Geschäftspartner identifizieren oder mindestens bestimmte Merkmale wie Staatsangehörigkeit oder Alter nachweisen können. Beispiele solcher Kontakte sind das E-Banking, der Zugriff auf ein Patientendossier, die Bestellung von Waren mit Altersnachweis oder eines Geburtsscheins.

Das eigentliche elektronische Identifikationsmittel kann sich auf einer Chipkarte, einem USB-Stick, einer SIM-Karte oder selbst im Prozessor eines Smartphones, Tablet-Computers oder PC befinden. Es besteht im Kern meist aus zwei zusammenhängenden Zahlen (‚Schlüsselpaar'), einer öffentlichen und einer geheimen. Mit der geheimen Zahl authentisiert sich der Besitzer in der virtuellen Welt, ohne diese selbst dabei preisgeben zu müssen. Der Kommunikationspartner wiederum kann mit der öffentlichen Zahl (im ‚Zertifikat' enthalten) die entsprechende elektronische Identität prüfen, ohne die geheime Zahl des Besitzers zu kennen.

Bis heute gibt es in der Schweiz kein staatliches oder weit verbreitetes elektronisches Identifikationsmittel. Mit der vom Staat unterstützten privatwirtschaftlichen SuisseID konnten zwar erste Erfahrungen in professionellen Nischenbereichen gemacht werden, eine grosse Verbreitung konnte aber aus verschiedenen Gründen nicht erreicht werden.

2.2.2 Elektronisches Identifikationsmittel und eID-Gesamtsystem

Wenn es darum geht, durch Identifikation der Kommunikationspartner Sicherheit und Vertrauen im elektronischen Geschäftsverkehr herzustellen, ist das elektronische Identifikationsmittel nur eine Komponente in einem umfassenderen eID-System mit verschiedenen Infrastruktur-Teilen und Diensten.

In seiner Gesamtheit muss das eID-System eine Reihe unterschiedlicher Fragen beantworten, die sich zwischen zwei Partnern im Hinblick auf einen sicheren Geschäftsverkehr stellen können:

- Ist X der, für den er sich ausgibt und wie sicher weiss ich das?
- Ist X der bei mir als Kunde geführte A und wie sicher ist das?
- Welche Nationalität hat X, wie alt ist er, ...?
- Wo ist X niedergelassen, ist er gegebenenfalls greifbar für eine Betreibung oder Klage?
- Hat X eine Vertretungsbefugnis für die Firma F, wenn ja, welche und wie sicher?
- Ist X tatsächlich Notar, Geometer, Grundbuchbeamter, ... und wie sicher?

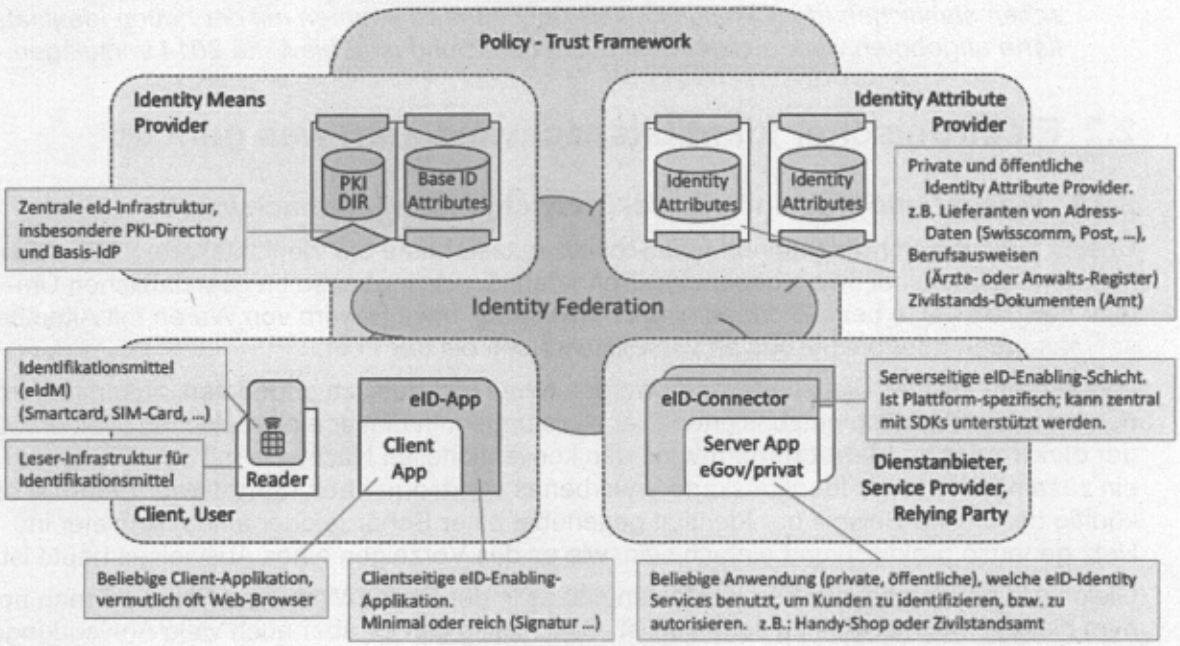


Abbildung 1: eID-Gesamtsystem

Ein fortgeschrittenes, komplettes eID-Gesamtsystem wird solche und weitere Fragestellungen alle online und in Echtzeit beantworten können. Dabei kann eine Person eine oder mehrere von einem Identitätsdienst-Anbieter bereitgestellte elektronische Identitäten (eID) besitzen. Eine solche besteht aus einem elektronischen Identifikationsmittel (eIdM) und weiteren Elementen, wie z.B. einem PKI-Directory, den mit der eID verbundenen Identitätsdaten und Diensten, sowie dem gesetzlichen und vertraglichen Rechtsrahmen. Die eID ermöglicht dem Inhaber über das Internet einen elektronischen Identitätsnachweis gegenüber einem Dienstanbieter. Für den Nachweis weiterer Funktionen oder Berechtigungen kann der Inhaber seine eID mit zusätzlichen Identitätsattribut-Anbietern verknüpfen lassen.

Zu diesem Identitäts- und Vertrauens-Gesamtsystem, heute oft auch 'Identity Ecosystem'[1] genannt, braucht der Staat nur einen Teil beizutragen. Die meisten Infrastrukturen und Dienste werden vom Markt entwickelt und bereitgestellt. Nur an gewissen neuralgischen Stellen braucht es den Staat, sei es in der Rolle als klassischer Gesetzgeber, z.B. im Vertragsrecht, sei es als letzte Instanz oder Anker für die Vertrauenswürdigkeit von privaten Akteuren (Zertifizierungen) oder sei es in der Bereitstellung gewisser Basis-Infrastrukturen, die

[1] Siehe (NIST, 2011) und das entsprechende Hauptkapitel unter dem Ritter 'Identity Ecosystem'.

unter rein marktwirtschaftlichen Gegebenheiten nicht oder nicht in der erwünschten Form bereitgestellt werden (Ausweise, Register).

Dieser letzte Punkt, welchen Anteil der Staat zu diesem eID-Gesamtsystem idealerweise beizutragen habe, wird je nach Land unterschiedlich beantwortet. In Kontinentaleuropa und in verschiedenen asiatischen Ländern herrscht die Haltung vor, dass der Staat auch in der elektronischen Welt die wichtigsten Komponenten bereitstellt, insbesondere natürlich ein starkes elektronisches Identifikationsmittel auf einer elektronischen Identitätskarte (eIDK). Anders die meisten angelsächsischen Staaten, wo traditionell auch schon der konventionellen Identitätskarte gegenüber grosse Skepsis herrscht. Die USA wurde im Jahr 2011 vom Präsidenten eine 'National Strategy for Trusted Identities in Cyberspace' (NSTIC)[2] lanciert, welche ein vom Staat mit-koordiniertes aber freiwilliges und von verschiedenen Akteuren der Privatwirtschaft getragenes eID-Gesamtsystem zum Ziel hat.

2.3 Rahmenbedingungen

2.3.1 Rechtliche Rahmenbedingungen

Für die Identitätskarte bildet das Ausweisgesetz[3] (AwG) den rechtlichen Rahmen, für die an Ausländer abgegebenen Ausweise das Ausländergesetz[4] (AuG) und das BGIAA[5].

Aus dem Ausweisgesetz sind in Kontext einer elektronischen Identitätskarte insbesondere drei Bestimmungen von Bedeutung:

- Artikel 2 Absatz 2bis sieht vor, dass jeder Ausweis, also sowohl der Pass wie auch die Identitätskarte, einen Datenchip mit den Angaben auf dem Ausweis und zusätzlich dem Gesichtsbild und Fingerabdrücken enthalten kann. Der Pass enthält provisorisch seit 2006 und definitiv seit dem 1. März 2010 diese ePass-Funktion. In diesem Dokument wird die ePass-Funktion nur insofern behandelt, als eine Lösungsvariante für den Identitätsnachweis darauf basiert.
- Artikel 2 Absatz 2ter schreibt vor, dass auch eine Identitätskarte ohne Chip bestellt werden kann.
- Artikel 2 Absatz 2^{quater} schliesslich bestimmt, dass ein Ausweis auch "elektronische Identitäten für Authentisierungs-, Signatur- und Verschlüsselungsfunktionen" enthalten kann.

Je nach Lösungsvariante resp. künftiger Ausgestaltung einer elektronischen Identitätskarte sind die erforderlichen Rechtsgrundlagen neu zu schaffen oder bestehende Rechtsgrundlagen anzupassen (vgl. dazu hinten 4.3).

Beim Ausländerausweis ist in diesem Kontext besonders erwähnenswert, dass der Aufenthaltstitel für Drittstaatenangehörige schon seit dem 24.1.2011 als biometrischer Ausländerausweis ('AA10'), also mit der ePass-Funktion ausgestaltet ist. Dies Aufgrund einer entsprechenden europäischen Normierung (Verordnung (EG) Nr. 380/2008), welche die Schweiz im Rahmen der Weiterentwicklung des Schengen-Besitzstandes übernehmen musste.

---

[2] Siehe (The White House, 2011) und die NSTIC-Homepage (NIST, 2011).

[3] Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG) vom 22. Juni 2001 (SR 143.1 <26.06.2013>).

[4] Bundesgesetz über die Ausländerinnen und Ausländer (Ausländergesetz, AuG) vom 16. Dezember 2005 (SR 142.20 <26.06.2013>).

[5] Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) vom 20. Juni 2003 (SR 143.51 <26.06.2013>).

2.3.2 Einordnung der eID in die E-Strategien des Bundes

Die Bereitstellung eines starken elektronischen Identifikationsmittels kommt in mehreren Strategien des Bundes vor, sei es als direktes Ziel oder als Voraussetzung für die Erreichung anderweitiger Ziele. Erwähnt seien hier diesbezüglich:

- Die Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz vom März 2012[6]: Darin ist zum Ziel des Schutzes vor Internetkriminalität als Handlungsschwerpunkt des Bundes aufgeführt: „Er erarbeitet in diesem Rahmen auch Lösungen für den Nachweis von Identitäten, Berechtigungen und Funktionen."
- Die E-Government-Strategie Schweiz[7]: Priorisierten Vorhaben B2.07; *SuisseID*: "Die Bereitstellung der digitalen Identität und Identifikation für die Authentisierung im elektronischen Geschäfts- und Behördenverkehr ist ein Eckstein für die künftige Entwicklung des elektronischen Wirtschaftsraum in der Schweiz".
- Die E-Government-Strategie Schweiz: Priorisierten Vorhaben B2.15; *National und im EU-Raum barrierefrei anerkannte elektronische Identität*: "Schaffung und Einführung einer einheitlichen elektronischen Identität, welche sowohl in der Schweiz wie auch im EU-Raum für den elektronischen Geschäftsverkehr von privaten und juristischen Personen sowie den Behörden ohne Einschränkung anerkannt wird."
- Die E-Government-Strategie Schweiz: Priorisierten Vorhaben B2.06; *Dienste für die Identifikation und Berechtigungsverwaltung*:
- Bundesrätliches Gesetzgebungspaket zur Förderung des elektronischen Geschäftsverkehrs, BRB vom 19. Dezember 2012, Punkt 6.2 (siehe Zitat im Kapitel 2.1, Anlass und Begründung).

2.3.3 Rahmenbedingungen gemäss EU-Verordnungs-Vorschlag

Die EU ist daran, ihre Signatur-Richtlinie zu überarbeiten und den neuen Bedürfnissen anzupassen. Am 4. Juni 2012 hat die Kommission den ‚Vorschlag für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt'[8] zuhanden des Parlaments und des Rats verabschiedet und in Englisch, Französisch und Deutsch publiziert (vgl. zugehörige mehrsprachige Pressemitteilung der EU).

Nebst der Regelung und Zertifizierung der Anbieter der elektronischen Signatur und weiterer Vertrauensdienste in der Art der bisherigen Richtlinie enthält der Vorschlag als besonderes und neues Thema die Notifikation und damit gegenseitige Anerkennung von staatlichen Schemen für die elektronische Identifizierung (eID bzw. Authentifizierung) in den Artikeln 5 ff. Im Kern sind die Mitgliedstaaten verpflichtet, dort wo sie für den Zugang zu Behördendiensten eine eID verlangen, auch die ausländischen eID aller notifizierten eID-Systeme zu akzeptieren. Die Anforderungen an die zu notifizierende nationale eID-Lösung stehen in Artikel 6 des erwähnten EU-Verordnungs-Vorschlags.

In dieser Konzeptstudie wird davon ausgegangen, dass die Schweiz ein Interesse daran hat, am europäischen System für die Interoperabilität von elektronischen Identitäten beteiligt zu sein, sei es, damit Inhaber einer schweizerischen eID mit ausländischen Behörden verkehren können, sei es, dass Ausländer mit ihrer nationalen eID mit Schweizer Behörden sicher verkehren können. Selbstverständlich gibt es für die Schweiz keine rechtliche Verbindlichkeit

---

[6] Siehe dazu die Website des BAKOM zur Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz unter http://www.bakom.admin.ch/themen/infosociety/00695/ <26.06.2013>.

[7] Siehe dazu die Website von E-Government Schweiz mit dem Katalog der priorisierten Vorhaben unter http://www.egovernment.ch/de/umsetzung/katalog_vorhaben.php <26.06.2013>.

[8] Englischer Titel: ‚Regulation on electronic identification and trusted services for electronic transactions in the internal market', abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF <26.06.2013>. Der aktuelle Stand der Behandlung der Vorlage innerhalb der EU-Institutionen kann auf der entsprechenden 'PreLex'-Seite unter http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201689 <28.06.2013> verfolgt werden.

zur Übernahme der EU-Verordnung. In Anbetracht der Internationalität des elektronischen Geschäftsverkehrs scheint es jedoch mehr als geraten, ein neues schweizerisches eID-System, wenn immer möglich, so zu konzipieren, dass es grundsätzlich notifiziert werden könnte.

Technisch würde die Interoperabilität unterschiedlicher eID-Systeme nach Art der bisherigen STORK-Projekte (siehe Kapitel 2.3.4.2) umgesetzt.

2.3.4 Internationale (technische) Standards

Ein international einsetzbarer Ausweis für physischen und elektronischen Einsatz hat zahlreiche internationale Standards in den verschiedensten Aspekten einzuhalten. Dazu gehören beispielsweise die Vorschriften der internationalen Zivilluftfahrt-Organisation ICAO für maschinenlesbare Reisedokumente[9], aber auch zahlreiche Standards für die elektronischen Aspekte. Im Kontext von Identitätskarte und elektronischem Identitätsnachweis sind die nachstehend beschriebenen zwei Normierungs-Vorhaben auf europäischer Ebene von besonderer Bedeutung.

2.3.4.1 Standardisierung als European Citizen Card (ECC)

Nachdem die ersten europäischen Länder ihre elektronischen Identitätskarten (eIDK) zwar ähnlich aber doch unterschiedlich aufgebaut hatten, wurde der Ruf nach Standardisierung und Interoperabilität laut. Die EU hat zwar keine Kompetenz, die nationale Identitätskarte vorzuschreiben, sie konnte jedoch einen Standard mit empfehlendem Charakter erarbeiten und gab im Jahr 2004 der europäischen Normierungsbehörde CEN einen entsprechenden Auftrag unter dem Titel European Citizen Card (ECC). Der ECC-Standard (CEN/TS 15480) soll eine hochsichere Chipkarte definieren, die im Alltag national und grenzüberschreitend für den Nachweis der Identität zur sicheren Nutzung von Online-Diensten eingesetzt werden kann[10].

In seinen aktuell 5 Teilen beschreibt der ECC-Standard nicht eine einzige eID-Karte, sondern legt die Standards für verschiedene Profile von eID-Karten fest, die sich aus einigen vorgegebenen Elementen und optionalen Zusätzen zusammensetzen lassen. Dabei können neu entwickelte Optionen oder Ausprägungen von Optionen nach einem vorgegebenen Verfahren aufgenommen werden.

2.3.4.2 Europäische Interoperabilität mit STORK

STORK (Secure idenTity acrOss boRders linKed) ist ein EU-Projekt zur grenzüberschreitenden Authentisierung mit eID-Karten. STORK soll es ermöglichen, dass eine Person von ihrem Heimatland aus, bzw. mit der Authentisierung in ihrem Heimatland, auf einen Service in einem verbundenen fremden Land zugreifen kann. Wer eine STORK-konforme eID besitzt, kann sich mit dem Umweg über sein Heim-E-Government-System und die STORK-Funktionalität auch dem ausländischen STORK-integrierten System gegenüber authentisieren.

Als Anwendungsfälle der grenzüberschreitenden Authentisierung werden u.a. Behördenkontakte im Zusammenhang mit der Niederlassung, Steuer-Rückforderungen und Firmengründungen genannt. STORK lancierte mehrere grenzüberschreitende Pilot-Anwendungen zur praktischen Demonstration der eID-Interoperabilität.

Nach dem ersten STORK-Projekt von 2008 bis 2011 läuft aktuell das Nachfolgeprojekt STORK2, an dem auch die Schweiz, vertreten durch die Berner Fachhochschule, beteiligt ist[11].

Für ein europäisches Land dürfte es wichtig sein, dass das nationale eID-System STORK-konform ausgestaltet ist. Dies ist allerdings keine sehr hohe Hürde, weil STORK aufgrund

---

[9] Siehe dazu (Schmeh, 2009), Seite 105 ff.

[10] Eine kurze Beschreibung der ECC findet sich in (Eurosmart, 2008)

[11] Siehe dazu u.a. (Bernold, et al., 2011).

der gewachsenen eID-Situation in Europa technisch so ausgelegt werden musste, dass eine breite Palette von eID-Systemen angeschlossen werden kann. So ist beispielsweise auch die SuisseID in technischer Hinsicht STORK-konform.

Der regulatorische Rahmen für die europäische Interoperabilität wird künftig durch die im Entstehen begriffene EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste (siehe Kapitel 2.3.3) bestimmt.

2.4 IST-Situation

2.4.1 Elektronische Identität im europäischen Umfeld

In den letzten ca. 15 Jahren haben nach und nach zahlreiche Staaten eine mit der Identitätskarte verbundene eID als Kernstück eines nationalen eID-Systems eingeführt. Pionier war Finnland, welches im Jahr 1999 eine elektronische Identitätskarte einführte. Es folgten Estland, Belgien, Spanien und Portugal. Deutschland hat im Jahr 2010 seinen elektronischen Personalausweis (ePA) eingeführt. Inzwischen haben die meisten europäischen Länder eine elektronische Identitätskarte eingeführt, sind daran sie einzuführen (Italien) oder planen mindestens eine solche (Frankreich).

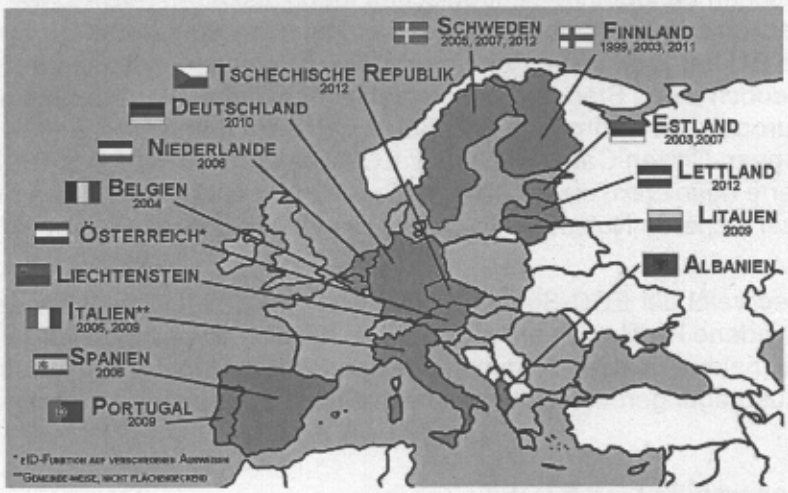


Abbildung 2: EU-Länder mit eID-Karten

Im Unterschied zum elektronischen Reisepass sind elektronische Identitätskarten heute noch sehr unterschiedlich ausgestaltet[12]. In der Anfangszeit bestanden sie aus den klassischen ICAO-Sichtausweisen auf einer Smartcard mit PKI-Schlüsselpaaren bzw. Zertifikaten, je eines für die Authentisierung, die elektronische Signatur, gegebenenfalls die Chip-Authentisierung und gelegentlich für die Verschlüsselung. Aktuelle Entwicklungen respektieren mehrheitlich den ECC-Standard (siehe Kapitel 2.3.4.1) und enthalten die maschinenlesbare Zone (MRZ) sowie die ePass-Funktion gemäss ICAO. Schweden, Monaco, Lettland, Finnland (2. Auflage), die Niederlande, Deutschland sowie weitere Länder haben solche Identitätskarten[13].

[12] Die eID-Länderprofile aus den Jahren 2007 und 2009 von 32 Ländern und zahlreiche Übersichten findet man auf der Webseite des IDABC-Projekts der EU (IDABC, 2009).

[13] Weitere Beschreibungen und Übersichten zu nationalen eID-Systemen finden sich in (Graux & Dumortier, 2009), (Stevens, Elliot , Hoikkanen, Maghiros, & Lusoli, 2010), (Castro, 2011).

Nachstehend sind die wichtigsten Elemente einer aktuellen elektronischen Identitätskarte am Beispiel der neuen schwedischen Identitätskarte aufgezeigt:

Symbol für E-Dokumente, welche die Spezifikation ICAO Doc 9303 erfüllen

Kontakt für eID-Chip (eID könnte auch kontaktlos implementiert sein)

MRZ: Machinenlesbare Zone (Machine Readable Zone)

2.4.1.1 Beispiel 1: Belgische ‚Elektronische Identiteitskaart'

Belgien hat relativ früh, nämlich im Jahr 2004 eine Smartcard-basierte elektronische Identitätskarte nach den damaligen Standards und eigener Konzeption eingeführt. Sie enthält das klassische eID-Set, bestehend aus Zertifikaten bzw. Schlüsselpaaren und Funktionen für die Authentisierung des Inhabers und für qualifizierte elektronische Signatur, technisch vergleichbar mit der SuisseID.

Jeder belgische Bürger über 12 Jahren muss eine solche Identitätskarte besitzen. Für Kinder und die verschiedenen Ausländer-Kategorien gibt es Ausweise mit den gleichen elektronischen Funktionen. Belgien hat die Anwendung der Karte vom Staat aus über Jahre intensiv gefördert. Zur Information der Bürger ist eine 'eID-Website' in Niederländisch, Französisch, Deutsch und Englisch eingerichtet.

Inzwischen besitzen sämtliche ca. 8 Mio. erwachsenen Bürger die neue eID-Karte und zusätzlich 600'000 Kinder sowie 850'000 Ausländer die entsprechenden elektronischen Ausweiskarten. Belgien ist somit eines der wenigen Beispiele, wo man sehen kann, wie eine staatliche eID-Karte eingesetzt wird, wenn sie einmal flächendeckend verbreitet ist.

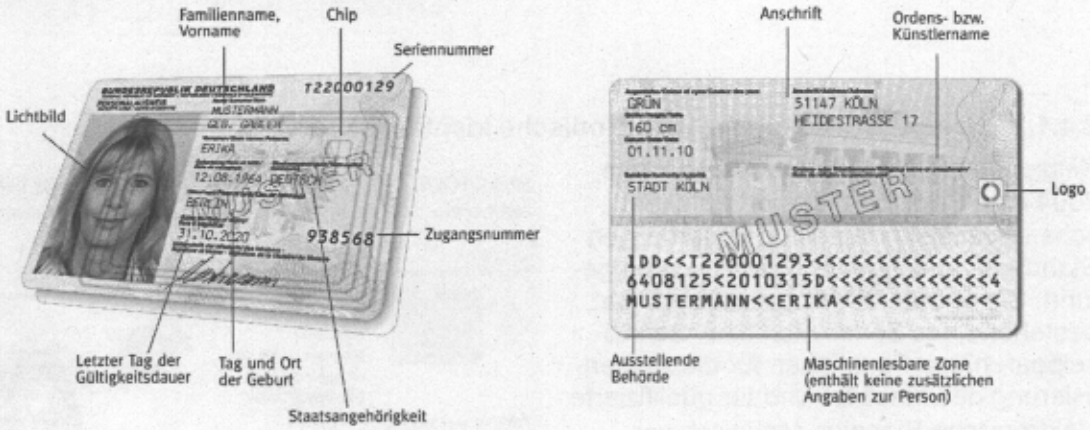
2.4.1.2 Beispiel 2: Deutscher elektronischer Personalausweis

Deutschland hat im Jahr 2010 eine neue elektronische Identitätskarte - das erste Mal im Smartcard-Format - unter dem Namen elektronischer Personalausweis (ePA) eingeführt.

Der ePA ist eine vom Staat ausgegebene Identitätskarte, ausgestaltet als klassisches Reisedokument, mit den ePass-Funktionen nach ICAO, einer eID-Funktion und Platz für eine optionale qualifizierte elektronische Signatur. Darüber hinaus weist sie ein paar zusätzliche Qualitäten, Funktionen und Verbesserungen auf, namentlich:

- Alle Applikationen, Geräte (Leser) und Zertifikate wurden durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) streng spezifiziert und reguliert.
- Die elektronische Ausweis-Funktion (eID-Funktion) ist beim Bezug standardmässig eingeschaltet, kann aber vom Benutzer deaktiviert werden.
- Jeder Dienstanbieter (Service Provider) muss sich gegenüber eIDK authentisieren und die Berechtigung für den Bezug bestimmter Attribute nachweisen, wozu er vorgängig bei einer Behörde ein Bewilligungsverfahren durchlaufen muss.
- Gegenseitige Authentisierung zwischen Karte und Lesegerät mittels eines neu entwickelten Verfahrens namens PACE (Password Authenticated Connection Establishment).
- Restricted Identity: Ein Pseudonymisierungs-Funktion, die dafür sorgt, dass sich der Personalausweis jedem Dienst gegenüber mit einer verschiedenen Karten-Identifikation meldet, damit keine Profile über die Benutzung erstellt werden können, was zugleich eine wichtige Voraussetzung für den Einsatz eines elektronischen Identifikationsmittels im E-Voting darstellt.

Der deutsche ePA entspricht in vielerlei Hinsicht dem ECC-Standard, hat aber diverse Verbesserungen und Zusätze, die über den aktuellen Standard hinausgehen und möglicherweise in die Weiterentwicklung von ECC einfliessen werden.



Deutschland hat mit viel Aufwand und Budget auch die Anwendung des ePA in E-Government und E-Commerce gefördert. Zur Information der Bürger ist ein sogenanntes Personalausweisportal (BMI, 2010) eingerichtet.

Per Frühjahr 2013 sind 20 Mio. neue Personalausweise ausgegeben, wovon ca. 1/3 die eID-Funktion aktiviert haben. Bis zum gleichen Zeitpunkt wurden 143 Service Provider bewilligt, 60% davon aus der Privatwirtschaft.

Mit einer übergreifenden Strategie hat Deutschland dafür gesorgt, dass die Aufenthaltstitel für Ausländer (eAT) mit kompatiblen 'Online-Ausweisfunktionen' ausgestattet sind.

Nachdem elektronische Ausweise schon bisher als eher komplex bzw. nur schwer in der Breite einsetzbar galten, war man in Fachkreisen skeptisch, ob der deutsche Ansatz gelingen würde, da er die Komplexität durch mehrere zusätzliche Funktionen und Verbesserungen[14] noch deutlich erhöhte. Heute kann man sagen, dass die Komplexität in technischer und organisatorischer Hinsicht gemeistert wurde. Wie sich das Gesamtsystem in der breiten Anwendung durchsetzen wird, kann man zurzeit erst langsam abzuschätzen beginnen. Im Moment wird primär bemängelt, dass die Zertifizierung als Dienstanbieter zu aufwendig und zu teuer sei.

[14] Zu den Unterschieden zwischen dem Identitätsnachweis mit herkömmlichen Chipkarten und dem neuen deutschen Personalausweis siehe (Hühnlein, Schmölz, Wich, & Horsch, 2012).

2.4.2 Elektronische Identität in der Schweiz

In der Schweiz gibt es seit vielen Jahren eine Identitätskarte im Kreditkartenformat (ID1-Format) und seit 2011 den Aufenthaltstitel für Drittstaatenangehörige mit der von ICAO genormten und europäisch vorgeschriebenen ePass-Funktion, jedoch bisher keine staatliche eID. Hingegen existiert seit 2010 die SuisseID (siehe Kapitel 2.4.2.3) als staatlich geförderte, aber privatwirtschaftlich bereitgestellte Karte für qualifizierte elektronische Signatur und starken elektronischen Identitätsnachweis.

Im Verlauf der letzten ca. 15 Jahre zielten mehrere parlamentarische Vorstösse in die Richtung[15] eines staatlichen elektronischen Identifikationsmittels und der Bundesrat hat sich bei deren Beantwortung und auch in seinen E-Strategien (siehe Kapitel 2.3.2) verschiedentlich mit dieser Frage befasst.

2.4.2.1 Die Schweizer Identitätskarte

Die Identitätskarte (IDK) dient gemäss Ausweisgesetz zum Nachweis der Schweizer Staatsangehörigkeit und der Identität. Jährlich werden rund 750'000 Identitätskarten ausgestellt, womit ein grosser Teil der Staatsangehörigen eine IDK besitzt. Die Identitätskarte hat für Erwachsene zehn Jahre Gültigkeit und für Kinder und Jugendliche bis zum vollendeten 18. Lebensjahr fünf Jahre. Ausländer erhalten keine Identitätskarte, sondern einen Ausländerausweis (siehe nächstes Kapitel).

Die heutige Identitätskarte (IDK) stammt aus dem Jahr 1995. Die damals eingeführten Merkmale, wie z.B. das Kartenformat, die maschinenlesbare Zone und eine Reihe von Sicherheitsmerkmalen entsprechen einem Standard der ICAO. Sie haben sich bewährt und international durchgesetzt, insbesondere im europäischen Raum, wo die Identitätskarte auch als Reisedokument eine wichtige Rolle spielt.

Gemäss Bundesratsbeschluss vom 16.12.2011 zur Erneuerung der Ausweise sollen die Bürgerinnen und Bürger künftig bei der Identitätskarte optional Varianten mit elektronisch gespeicherten Daten (ePass-Funktion beim heutigen Pass) und einem elektronischen Identitätsnachweis für E-Government- und E-Business-Anwendungen wählen können. Hier in diesem Dokument geht es innerhalb dieser E-Funktionen der neuen Identitätskarte nur um die Frage, welche Art von elektronischem Identitätsnachweis zusammen mit der IDK realisiert werden soll.

Jede absehbare Lösung für den elektronischen Identitätsnachweis wird auf jeden Fall vom sicheren und bei allen Beteiligten gut eingespielten Antrags-Prozess[16] mit der Personen-Identifikation auf der Gemeinde oder dem Kanton profitieren.

2.4.2.2 Der Ausländerausweis

Der Ausländerausweis[17] unterscheidet sich je nach Art der Aufenthaltsbewilligung. Personen aus der Europäischen Union (EU) oder der Europäischen Freihandelsassoziation (EFTA), sowie Personen aus Drittstaaten, die sich nicht auf ein Freizügigkeitsabkommen berufen können, erhalten einen konventionellen Aufenthaltstitel auf Papier. Andere Drittstaatenangehörige erhalten in Umsetzung des Schengen-Rechts seit 2011 den von der EU genormten biometrischen Ausländerausweis[18](AA10) in Kreditkarten-Format und mit elektronisch gespeicherten Ausweisdaten und biometrischen Merkmalen (ePass-Funktion).

---

[15] So z.B. die Motion Noser (04-3228) *E-Switzerland - Schaffung einer digitalen Identität* und die Interpellation Häberli-Koller (06.3685) *Elektronische Bürgerinnen- und Bürgerkarte.*

[16] Zur Identitätskarte an sich und zum Antragsverfahren siehe die Homepage des fedpol zur Identitätskarte unter www.fedpol.admin.ch/content/pass/de/home/ausweise/identitaetskarte.html <28.06.2013>

[17] Zu den gesetzlichen Grundlagen der Ausländerausweise siehe Kapitel 2.3.1

[18] Siehe dazu die Webseite des Bundesamtes für Migration zum biometrischen Ausländerausweis unter www.bfm.admin.ch/content/bfm/de/home/themen/aufenthalt/ref_biometr_auslaenderausweis.html.

2.4.2.3 Die SuisseID

In den Jahren 2009-2010 hat der Bund im Rahmen des dritten Pakets der konjunkturellen Stabilisierungsmassnahmen unter Federführung des SECO und in Zusammenarbeit mit den vier anerkannten Anbietern von Zertifizierungsdiensten nach ZertES die SuisseID[19] lanciert. Eine SuisseID besteht aus einem Set von standardisierten Geräten und Diensten, die spezifisch auf die sichere elektronische Identifikation ausgerichtet sind. SuisseID-konforme Produkte dürfen nur von einer nach ZertES anerkannten Anbieterin von Zertifizierungsdiensten (CSP) herausgegeben werden und erweitern im Wesentlichen die schon länger erhältlichen ZertES-konformen Signaturkarten um einen standardisierten elektronischen Identitätsnachweis. Die Sicherheitsanforderungen und Haftungsbestimmungen sind an die entsprechenden ZertES-Bestimmungen angelehnt.

Für den elektronischen Identitätsnachweis stellt die SuisseID ein Schlüsselpaar, ein X.509-Zertifikat und eine Authentisierungseinheit (Computer-Chip, Betriebssystem, Speicher) für starke Authentisierung zur Verfügung. Im Zertifikat selbst befinden sich nur minimale Informationen, zusätzliche Daten befinden sich in einem IdP-Server, der die Ausweisdaten des SuisseID-Inhabers bereit hält und sie gegen starke Authentisierung dem Inhaber zuhanden eines Dienstanbieters beweisbar abgibt (Beispiele: Altersnachweis oder Übergabe der Ausweisdaten für den Bezug eines Strafregisterauszugs oder einer Kreditkarte).

Die physische Gestalt (‚form factor') ist für eine SuisseID nicht vorgegeben. Sie kann somit grundsätzlich in verschiedenste Geräte einzeln oder zusammen mit anderen Komponenten eingebaut werden, z.B. in einen USB-Stick oder eine Smartcard. Im Falle der Smartcard könnte sie also auch mit einer Kreditkarte oder mit der Identitätskarte kombiniert werden.

Die SuisseID wurde im Mai 2010 eingeführt, konnte sich jedoch nur in professionellen Nischen etablieren. Dort hat sie ihre Praxistauglichkeit allerdings bewiesen (Quade & Wölfle, 2010). Um die 200 Anwendungen verschiedenster Art, vor allem im Bereich Business-to-Business und Business-to-Government verwenden die SuisseID alleine oder in Kombination mit dem IdP-Dienst.

Als Schwächen bzw. Gründe für die mangelnde Verbreitung werden insbesondere die aufwendige Beschaffung, die wenig komfortable Installation sowie der Mangel an Anwendungen und internationaler Interoperabilität genannt.

[19] Siehe SuisseID-Homepage unter (Verein Trägerschaft SuisseID, 2010).

3 Ziele und Anforderungen

3.1 Zielsetzung des Vorhabens

Aus der Entstehungsgeschichte dieses Vorhabens lassen sich zwei übergeordnete Ziele ableiten, die zeigen, in welchem strategischen Kontext die staatliche anerkannte eID (in diesem Dokument künftig **'qualifizierte eID'**, **'QeID'** genannt) zu sehen ist.

1. Die qualifizierte eID trägt dazu bei, den **Übergang der Schweiz zu einer entwickelten Informationsgesellschaft** zeitgerecht und gut zu schaffen.
2. Die qualifizierte eID trägt dazu bei, ein System von **Sicherheit und Vertrauen im elektronischen Geschäftsverkehr** (E-Business und E-Government) aufzubauen.

Damit konkrete Ziele für die qualifizierte elektronische Identität definiert werden können, müssen – wie schon im Kapitel 2.2.2 ausgeführt – gewisse Annahmen über das zukünftige eID-Gesamtsystem getroffen werden. Gewisse Ziele muss die qualifizierte eID (QeID) als solche erfüllen, andere Ziele können nur vom eID-Gesamtsystem erfüllt werden - es braucht hier also zusätzliche Komponenten und Leistungen von anderen Akteuren, bis das angestrebte Ziel erreicht werden kann. Auch schon bei der qualifizierten eID stellt sich die Frage, welche QeID-Komponenten (Identifikationsmittel, Infrastrukturen, rechtliche Regelungen, Prozesse usw.) vom Staat und welche von der Privatwirtschaft bereitgestellt werden sollen. Die durch dieses Projekt umzusetzende Lösung wird nur *die vom Staat zusammen mit der neuen Identitätskarte zur Verfügung gestellten eID-Komponenten* umfassen.

3.1.1 Ziele für die qualifizierte elektronische Identität

Folgende Ziele sind mit dem Vorhaben zur Einführung einer qualifizierten eID verbunden:

Nr.	Ziel	Priorität	Bemerkungen
Z01	Wer sich eine IDK beschafft, kann – im gleichen Antragsprozess und ohne wesentlichen Mehraufwand – eine qualifizierte eID für starke elektronische Authentisierung bestellen.	1	-> Rahmenbedingung: auch IDK ohne Chip muss möglich sein.
Z02	Auch alle in der Schweiz aufenthaltsberechtigten Ausländer müssen ohne grossen Mehraufwand eine gleichwertige qualifizierte eID bestellen können.	1 (2)	Inhaltlich prioritär, auf der Zeitachse evtl. verschoben.
Z03	Wird die qualifizierte eID auf der IDK ausgeliefert, dürfen sich die Kosten der IDK für den Bürger nicht mehr als um ein Viertel des heutigen Preises für eine IDK ohne Chip erhöhen.	2	nicht für jede Lösungsvariante anwendbar

3.1.2 Ziele für das eID-Gesamtsystem

Folgende Ziele soll das schweizerische eID-Gesamtsystem nach Einführung des neuen, elektronischen Identifikationsmittels erfüllen:

Nr.	Ziel	Priorität	Bemerkungen
Z51	Die qualifizierten elektronischen Identitäten der Schweiz können auf einfachste Weise und sicher für den elektronischen Geschäftsverkehr (E-Government, E-Business) verwendet werden.	1	
Z52	Die qualifizierten eID-Systeme der Schweiz sind europäisch notifizierbar, womit die Inhaberinnen und Inhaber über die Landesgrenzen hinaus sicheren Geschäftsverkehr durchführen können.	1	Als potentielle Fähigkeit ('Notifizierbarkeit')
Z53	Das eID-Gesamtsystem stellt Vertrauensdienste, z.B die qualifizierte elektronische Signatur sowie weitere Dienste wie Attributprovider (z.B. zum Nachweis von Berufen), bereit.	2	'Signature as a Service' 'Funktionsnachweis als Service'
Z54	Das eID-Gesamtsystem unterstützt Vote électronique. Wenn möglich können die qualifizierten elektronischen Identitäten der Schweiz für Teilprozesse von Vote électronique verwendet werden (z.B. für die Registrierung).	2	
Z55	Das eID-Gesamtsystem bietet für in der Schweiz bestehende eID-Lösungen (z.B. die SuisseID) einen Aufwärtspfad bzw. für deren Anbieter eine Entwicklungsmöglichkeit.	2	Darf aber nicht zu Kompromissen für neue Lösung führen

3.1.3 Verworfene Ziele

Als mögliche Ziele diskutiert, aber schliesslich explizit nicht als Ziel gesetzt wurden folgende potentiellen Ziele:

Nr.	Potentielles Ziel	Priorität	Bemerkungen
-Z91	Das QeIDM kann direkt für die Stimmabgabe bei Vote électronique verwendet werden.	x	Effektive Unterstützung ist zu hohe Anforderung
-Z92	Das QeIdM ermöglicht eine qualifizierte elektronische Signatur auf der lokalen Client-Infrastruktur.	x	Siehe aber Z53
-Z93	Das QeIdM unterstützt eine starke Verschlüsselung.	x	Ist keine gute Lösung[20]

3.1.4 Abgrenzung des Vorhabens zu eID-Anwendungen

Es wird gelegentlich die Meinung vertreten, es sei sinnlos, ein elektronisches Identifikationsmittel einzuführen, ohne gleichzeitig für die entsprechenden Anwendungen zu sorgen. Trotzdem wird im Rahmen dieses Vorhabens nur das Identifikationsmittel eingeführt, und dies mit folgender Begründung:

---

[20] Eine zertifikatsbasierte Verschlüsselung auf Benutzer-Ebene benötigt ein System für die Schlüsselhinterlegung und erzeugt gemäss Erfahrung sehr grossen Support-Aufwand.

1. Wie vorstehend aufgezeigt, ist ein eID-Gesamtsystem ein komplexes Gebilde aus zahlreichen Elementen, die zusammenspielen müssen. Es ist schlicht nicht möglich, alle diese Elemente im Rahmen des gleichen Vorhabens zu entwickeln. Auslöser *dieses* Vorhabens ist die Bereitstellung einer neuen Identitätskarte.
2. Die weiteren für ein funktionierendes eID-Gesamtsystem notwendigen Komponenten, seien es weitere Identity-Dienste oder eID-Anwendungen, sollen von weiteren Akteuren bereitgestellt werden. Soweit es Aufgaben der öffentlichen Hand sind, beispielsweise der Zugriff auf gewisse Register oder E-Government-Anwendungen, sollen die entsprechenden Vorhaben separat durchgeführt und im Rahmen der vorstehend erwähnten E-Strategien koordiniert werden.
3. Wie die Geschichte zeigt, ist es nicht immer nötig, vom selben Akteur gleichzeitig die Infrastruktur und die Anwendungen dieser Infrastruktur zur Verfügung zu stellen. Zahlreiche Beispiele zeigen, dass die Bereitstellung der richtigen Infrastruktur-Elemente zum richtigen Zeitpunkt ganze Zweige von Anwendungen gleichsam explosionsartig entwickeln lassen kann. Strassen, Schienen und Stromnetze sind solche Beispiele, aber - aus neuerer Zeit - insbesondere das Internet bzw. TCP/IP und HTTP.

3.2 Anforderungen

Auch bei den Anforderungen ist zu berücksichtigen, dass sie sich entweder auf die qualifizierte eID und die dazu notwendigen Komponenten oder dann auf das eID-Gesamtsystem beziehen können. In diesem Fall werden nicht separate Kataloge geführt, sondern der Fokus wird bei jeder einzelnen Anforderung genannt.

3.2.1 Technisch-funktionale Anforderungen

Nr.	Funktionale Bedürfnisse und Anforderungen in technischer Hinsicht	Priorität	Bemerkungen
A11	Die qualifizierte eID bzw. das dabei zur Verfügung gestellte elektronische Identifikationsmittel ermöglicht eine starke Authentisierung.	1	
A12	Auch Inhaber des Ausländerausweises haben gleichermassen Zugang zu gleichwertigen eID-Funktionen.	1	In separatem Projekt mit eigenem Zeitplan.
A13	Jede qualifizierte eID enthält einen eindeutigen, persistenten Identifikator, der unabhängig von der Existenz des Identifikationsmittels (bzw. Ausweises) weiter existiert.	1	
A14	Optional kann der Herausgeber der QeID auch eine qualifizierte elektronische Signatur anbieten. (Evtl. als Vertrauensdienst, 'Server-Signing')	2	
A15	Jede qualifizierte eID kann für internationale starke Authentisierung gemäss STORK eingesetzt werden.	1	
A16	Die QeIDM muss auf folgenden Plattformen eingesetzt werden können: aktuelles Windows, aktuelles Mac-OS, verbreitete Linux-Distributionen, verbreitete Smartphone-Systeme (noch festzulegen).	1/ 2	

3.2.2 Funktionale Anforderungen organisatorischer und rechtlicher Art

Nr.	Funktionale Bedürfnisse und Anforderungen in organisatorischer und rechtlicher Hinsicht	Priorität	Bemerkungen
A21	Die Personen-Identifikation für die Beschaffung der IDK oder des Ausländerausweises genügt auch für die Beschaffung der QeID.	1	
A22	Ist die QeID auf der IDK, gilt das elektronische Identifikationsmittel so lange wie die physische ID-Karte, allenfalls notwendige Verlängerungen müssen online geschehen können.	1	
A23	Jedes QeID-System ist - vorbehältlich staatsvertraglicher Barrieren - gemäss künftiger EU-Verordnung notifizierbar	1	
A24	Das qualifizierte eID ist architektonisch mit den IAM-Grundprinzipien des Bundes bzw. von eCH abgeglichen.	2	
A25	Für jede qualifizierte elektronische Identität muss eine klar definierte Supportorganisation bereitgestellt werden. Diese muss für jede Benutzergruppe (Endkunden, Dienstleistungsanbieter) einheitliche Anlaufstellen (SPOC) zur Verfügung stellen.	2	
A26	Dienstleistungsanbieter, welche die Verwendung von qualifizierten elektronischen Identitäten akzeptieren, müssen eine klar definierte Supportorganisation bereitstellen. Diese muss eine einheitliche Anlaufstelle (SPOC) zur Verfügung stellen.	2	(geht in Richtung D, resp. Zertifizierung der Anbieter, ist aber sicher von grossem Kundeninteresse).

3.2.3 Nicht-funktionale Anforderungen

Über die rein funktionalen Anforderungen hinaus muss qualifizierte eID oder das eID-System die nachstehenden Bedürfnisse und Anforderungen im Sinne von Optimierungen erfüllen:

Nr.	Nicht-funktionale Bedürfnisse und Anforderungen	Priorität	Bemerkungen
A31	Einfaches Produkt, das mit geringem Schulungsaufwand verwendet werden kann.		
A32	Möglichst tiefe Entwicklungskosten.		
A33	Möglichst geringe Betriebskosten (inkl. Support).		
A34	Möglichst wenig Risiken (Funktionsfähigkeit, Zeit, Kosten) bei der Beschaffung.		
A35	Insgesamt gibt es für die Identitätskarte möglichst wenige Produktvarianten.		
A36	Für einen Service-Provider darf die Teilnahme am System nicht zu aufwendig und/oder zu teuer werden.		
A37	Die Lösung soll insgesamt möglichst international konform sein.		

A38	Die QeID muss sich mit weiteren eID-Systemen und –Funktionen kombinieren bzw. erweitern lassen.		
A39	Es können sich zahlreiche Einsatzmöglichkeiten – E-Government und E-Business – entwickeln.		
A40	Das eID-Gesamtsystem muss entwicklungsfähig sein.		

3.2.4 Anforderungen an Sicherheit und Datenschutz

Nr.	Bedürfnisse und Anforderungen aus Sicht Datensicherheit und Datenschutz	Prio-rität	Bemerkungen
A41	Sicherheit: Sowohl das elektronische Identifikations-mittel wie auch die schweizerische eID-Gesamtlösung sollen möglichst gegen Missbrauch abgesichert sein.	1	
A42	Sowohl das QeID wie auch die schweizerische eID-Gesamtlösung sollen möglichst datenschutzfreundlich ausgestaltet sein.	1	Datensparsamkeit, 'user centric', ...
A43	Beschaffung und Support geschehen über etablierte, sichere Wege.	2	
A44	Der anonyme und/oder pseudonyme Einsatz der QeID muss – mindestens als Service – möglich sein.	2	Anforderung fraglich

4 Lösungen

Wenn nachstehend von Varianten die Rede ist, betrifft das nur die eID-Funktionalität der neuen Identitätskarte. Unabhängig von der später gewählten eID-Variante wird eine neue Identitätskarte mit einigen neuen Sicherheitsmerkmalen eingeführt und als Option die ePass-Funktion als weiterer Schutz vor Missbrauch.

4.1 Massgebliche Kriterien und mögliche Ausprägungen

Auch wenn die prioritären funktionalen Anforderungen als Ausschlusskriterien für die zu wählende Lösung gelten, bleiben mehrere deutlich unterschiedliche Varianten für eine Lösung.

Für den Entscheid über die grundsätzlichen Design-Parameter des zu schaffenden eID-Systems werden nachstehend die wichtigsten Kriterien (oder Unterscheidungsmerkmale) mit ihren jeweiligen Ausprägungen aufgeführt. Diese bilden beim Lösungsüberblick im nächsten Kapitel (Abbildung 3) je eine Zeile.

Die einzelnen Kriterien und ihre Ausprägungen sind folgende:

K1 Staatliches Engagement für eID: Wie weit engagiert sich der Staat für die QeID? So wenig wie möglich. Oder bietet er zwar eine eID auf der IDK an, engagiert sich aber darüber hinaus möglichst nicht mehr? Oder engagiert er sich gar in der vollen Breite, inklusive Betrieb und Support.

K2 Anzahl QeID pro Person: Kann eine Person mehrere qualifizierte eID gleichzeitig haben oder gibt es wie bei der Identitätskarte immer nur eine gültige?

K3 ECC-Konformität: Soll das elektronische Identifikationsmittel den ECC-Standard (European Citizen Card) einhalten?

K4 Vertrauenswürdigkeit der Dienstanbieter: Soll sich ein (staatlicher oder v.a. privater) Service-Provider der Client-eID gegenüber authentisieren müssen, bevor er mit ihr arbeiten kann (wie ePass und deutscher ePA) oder nicht (wie SuisseID). Oder soll als minimaler Schutz des eID-Inhabers vom Staat eine Liste mit - in einem gewissen Umfang - geprüften Dienstanbietern, also eine Art ‚Konformitäts-Label' publiziert werden.

K5 Kontakt-Art: eID-Chip arbeitet über konventionelle Smartcard-Kontakte (goldener Punkt auf Smartcards) oder über Funk (RFID nach NFC-Standard). Kontaktbehaftete eID und ePass zusammen ergäben dann die sogenannte 'Dual-Interface'-Variante.

K6 Vote électronique-Unterstützung: Wie weitgehend soll die qualifizierte eID das Vote électronique unterstützen. Eine gewisse Unterstützung bei der Kommunikation bedarf nur einer sicheren elektronischen Signatur, eine umfassende Unterstützung auch bei der Stimmabgabe hingegen verlangt ausgefeilte Kryptografie-Funktionen (z.B. ‚Zero-Knowledge-Proof, Restricted Identity). Eine herkömmliche eID bietet diese Funktionen nicht, der neue deutsche ePA jedoch weitgehend schon.

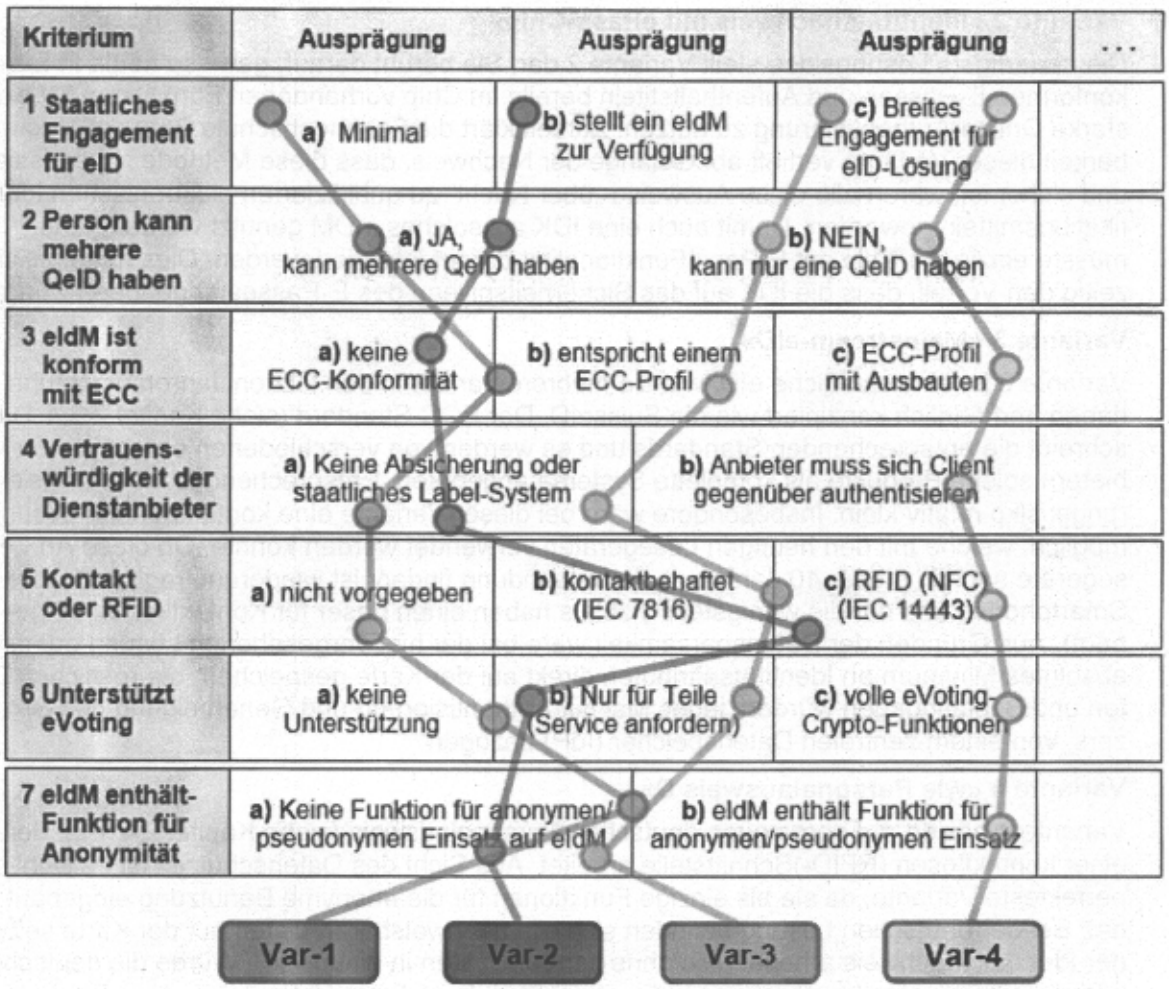
K7 Anonyme/Pseudonyme Identität: Es stellt sich die Frage, ob die qualifizierte elektronische Identität *selbst* einen anonymen und/oder pseudonymen Einsatz ermöglichen muss (unabhängig davon, dass ein solcher Einsatz gemäss Anforderung 44 allenfalls über einen Online-Service realisiert werden könnte).

4.2 Lösungsvarianten

Basierend auf den vorstehenden Überlegungen zu verschiedenen Kriterien und möglichen Ausprägungen werden nachstehend nach der Methodik des ‚Morphologischen Kastens' **vier Lösungsvarianten** für eine zusammen mit der Identitätskarte ausgegebene eID aufgezeigt,

die nach Ansicht des Projektteams allesamt gute, machbare[21] Lösungen darstellen. Mögliche Lösungsvarianten ergeben sich, indem von jeder Zeile des Morphologischen Kasten (Abbildung 3) eine Ausprägung gewählt wird, wobei gewisse Kombinationen auch unmöglich sein können.

Abbildung 3 - Lösungsvarianten im Überblick



Eine Präferenz für die eine oder andere Variante ergibt sich daraus, wie man die Rolle des Staates in diesem Bereich sieht, welche Kosten und Risiken man zu tragen bereit ist und natürlich auch danach, wie man die künftige Entwicklung des eID-Gesamtsystems einschätzt.

Variante 1 «Private Anbieter, staatliche Identifikation und Regulierung»

Es wird keine ausschliesslich hoheitliche staatliche eID geben, sondern es existieren mehrere – in der Regel von privatwirtschaftlichen Unternehmungen angebotene – eID parallel. Die Beziehung zur Identitätskarte besteht darin, dass der starke Identifikationsprozess mitbenutzt werden kann. Bei der Bestellung der IDK wird nach der Identifikation auch die Bestellung für eine private eID aufgenommen und mit den notwendigen Unterlagen weitergeleitet. Wie bei den übrigen Varianten sollen eID von Anbietern, welche die zu schaffenden rechtlichen Auflagen für eine qualifizierte eID einhalten, der EU notifiziert werden können, so dass sie im EU-Raum anerkannt werden. Diese Variante bietet wohl den grössten Spielraum für künftige technologische Weiterentwicklungen (z.B. auf Basis von Smartphones) und kann ei-

[21] Für die nachstehend beschriebene Lösungsvariante 2 ist die Machbarkeit noch in Abklärung. Im Auftrag des Bundes erarbeitet die Fachhochschule Bern bis Ende 2013 eine Machbarkeitsstudie und eine Prototyp-Anwendung zur praktischen Prüfung des konzeptionellen Ansatzes.

nen Aufwärtspfad für bestehende eID-Lösungen (wie z.B. die SuisseID) darstellen. Die Variante 1 stellt zudem insofern eine Besonderheit dar, als dass sie grundsätzlich auch zusätzlich zu jeder der anderen drei Varianten umgesetzt werden könnte. Damit ist gemeint, dass eine staatliche und mehrere nichtstaatliche qualifizierte eID-Lösungen parallel koexistieren könnten. Alle übrigen Varianten gehen von einer rein staatlichen Lösung aus.

Variante 2 «Identitätsnachweis mit ePass-Chip»

Die neuartigste Lösungsidee stellt Variante 2 dar. Sie beruht darauf, gewisse heute in EU-konformen E-Pässen und Aufenthaltstiteln bereits im Chip vorhandenen Funktionen für eine starke Online-Authentisierung zu nutzen. Zurzeit klärt die Fachhochschule Bern die Machbarkeit dieser Variante vertieft ab. Gelänge der Nachweis, dass diese Methode zuverlässig und sicher ist, wären alle diese Ausweise „über Nacht" zu qualifizierten elektronischen Identifikationsmitteln geworden. Damit auch eine IDK als solches eIDM genutzt werden kann, müsste einzig ein Chip mit E-Pass-Funktionalität darauf integriert werden. Dies hätte gleichzeitig den Vorteil, dass die IDK auf das Sicherheitsniveau des E-Passes angehoben würde.

Variante 3 «Mainstream-eID»

Variante 3 ist eine staatliche eID, wie sie mehrere Länder in den letzten Jahren eingeführt haben und ähnlich konzipiert wie die SuisseID. Der ECC-Standard (siehe Kapitel 2.3.4.1) beschreibt die entsprechenden Standards und es werden von verschiedenen europäischen Anbietern solche Produkte als komplette Systeme angeboten. Entsprechend ist das Realisierungsrisiko relativ klein. Insbesondere wäre bei dieser Variante eine kontaktbehafte Lösung möglich, welche mit den heutigen Lesegeräten verwendet werden könnte. Ob diese Art Lesegeräte auch in 5 oder 10 Jahren noch Verwendung finden, ist wiederum fraglich (weder Smartphones und nur die wenigstens Tablets haben einen Leser für Kontaktkarten eingebaut). Aus Gründen der Datensparsamkeit wäre bei der hier vorgesehenen Lösung nur ein absolutes Minimum an Identitätsattributen direkt auf der Karte gespeichert, die restlichen Daten und Bestätigungen würden, jedes Mal mit Authentisierung und Genehmigung des Benutzers, von einem zentralen Datenspeicher (IdP) bezogen.

Variante 4 «wie Personalausweis D»

Variante 4 basiert auf dem neuen deutschen Personalausweis (siehe Kapitel 2.4.1.2), der mit einer kontaktlosen (RFID-)Schnittstelle arbeitet. Aus Sicht des Datenschutzes ist es wohl die perfekteste Variante, da sie als einzige Funktionen für die anonyme Benutzung eingebaut hat. Bei der deutschen Lösung befinden sich alle nachweisbaren Daten auf der Karte selbst, der Identitätsnachweis arbeitet also ohne zentrale Daten in einem IdP. Würde die deutsche Lösung eins-zu-eins übernommen, wäre dies die aufwändigste Variante, da eine Behördenorganisation geschaffen werden muss, welche jeden Portalanbieter für die Nutzung der eID zertifiziert. Diese Anbieterzertifizierung könnte jedoch zur Senkung des Aufwands für den Staat und die Dienstleistungs-Anbieter auch ausgeschaltet werden.

«Null-Lösung»

Die Null-Lösung, bei welcher der Staat bezüglich eID nichts einführen würde, kann als eine Art fünfte Lösung betrachtet werden. Obwohl nicht im ursprünglichen Auftrag des Bundesrates enthalten, empfiehlt sich eine kritische Prüfung der voraussichtlichen Akzeptanz und Nutzung einer staatlichen eID-Lösung in der breiten Bevölkerung. Die Erfahrung in vielen Ländern zeigt, dass die eID nur spärlich angewendet wird und selbst in Ländern mit intensiver Benutzung, wie Belgien und Estland, ist fraglich, ob diese Benutzung ohne die obligatorischen Anwendungen auch zustande gekommen wäre. Kritische Stimmen verneinen den Bedarf für eine eID und vertreten die Meinung, dass eine breite Nutzung nur mit monetären Anreizen (Bspw. Online Transaktion gratis - Gebühr für konventionelle Transaktion) oder Zwang (Bspw. Bankbezüge ab einem bestimmten Betrag nur mit eID, wie in Estland ab 200€) erreicht werden kann. Solche Marketing- und Fördermassnahmen wären aber, wie bereits ausgeführt, nicht die Aufgabe des vorliegenden Projekts, sondern müsste im Rahmen anderer Projekte beigetragen werden.

4.2.1 Variante 1: Private eID mit staatlicher Identifikation und Regulierung

Kurzbeschreibung	Bei der Bestellung der Identitätskarte kann man zusätzlich eine oder mehrere eID von zertifizierten Anbietern bestellen. Das Identifikationsmittel wird dann nicht auf der Identitätskarte, sondern vom zertifizierten Anbieter auf einem anderen Träger geliefert und unterstützt. Der Staat trägt somit in erster Linie den IDK-Identifikationsprozess und die Regulierung bei.

Technische und organisatorische Implementierung

Die technische Implementierung ist weitgehend offen, bzw. den privaten Anbietern überlassen. Je nach technologischer Entwicklung und Kundenbedürfnissen kann der Träger eine Smartcard, eine SIM-Card, ein USB-Stick oder sonst ein sicherer Träger sein. Wie heute bei der Signaturkarte müssen einfach die einschlägigen technischen Vorschriften eingehalten werden. Die eID-Funktion kann auch mit anderen Produkten kombiniert angeboten werden, beispielsweise auf einer Kreditkarte oder einem Mobiltelefon-Chip.

Governance und rechtliche Implementierung

Der Staat ist nur für die Regulierung und die internationale Anerkennung der eID zuständig, ähnlich wie heute bei der elektronischen Signatur. Zusätzlich stellt er den zertifizierten Anbietern seinen IDK-Identifikations- und Bestellprozess zur Verfügung. Die eID selbst wird von mehreren zertifizierten privaten Anbietern in Konkurrenz angeboten.

Als gesetzliche Grundlage sollte das nach aktueller Vorlage revidierte ZertES genügen. Auf dem Verordnungsweg wird nebst der qualifizierten elektronischen Signatur neu auch die eID geregelt (vgl. dazu Kapitel 4.3.1). Später muss die Schweiz für die internationale Anerkennung bzw. EU-Notifizierung sorgen (vgl. dazu Kapitel 4.3.3).

Anwendungsprofil, Funktionen

Je nach konkreter Ausgestaltung der einzelnen Produkte ist ein sehr breiter Einsatz im E-Commerce möglich. Im Bereich des E-Government würde ein solches elektronisches Identifikationsmittel als starke Authentisierung akzeptiert, gleich wie das heute schon bei der SuisseID der Fall ist, die selbst für den als besonders heikel einzustufenden Bezug eines Strafregister-Auszugs verwendet werden kann.

Weniger klar ist die Verwendbarkeit solcher elektronischer Identifikationsmittel für das E-Voting. Möglicherweise müssten für einen solchen Einsatz zusätzliche Anforderungen implementiert und zertifiziert sein.

Entwicklungsstand, Erfahrungen

Es gibt schon diverse Produkte (SuisseID, MobileID) und es obliegt dem Markt, weitere Produkte zu entwickeln und Erfahrungen im Einsatz zu gewinnen.

Vorteile	- Schützt die Investitionen aller bisherigen Anbieter. - Flexible Lösung, welche die technische Weiterentwicklung nutzen kann. - Identifikation als teuerster Teil kann mehrfach genutzt werden.
Nachteile	- Keine Gewähr, dass ein zufriedenstellendes Angebot entsteht. - Uneinheitliche Lösungen, evtl. unübersichtliches Angebot für Kunden. - Einsatz für E-Voting nur sehr beschränkt möglich.
Kosten	- Aus Sicht des Staates kaum Kosten, nur Gesetzgebung, Beratung bei und Weiterleitung der Bestellung
Risiken	- Für den Staat keine grösseren Realisierungsrisiken. - Haftungsrisiko des Staates für mehrere EU-notifizierte Anbieter. - Keine Garantie, dass sich QeID-Anbieter zertifizieren lassen werden.

Optionen, Variationen

- Variationen in der Bewerbung und Unterstützung durch Staat möglich.

4.2.2 Variante 2: Identitätsnachweis mit der ICAO-ePass-Funktion

Kurzbeschreibung	Es wird eine starke elektronische Authentisierung mit den standardmässig beim ePass-Chip vorhandenen Sicherheitskomponenten realisiert. Auf diese Art wären sowohl die neue Identitätskarte mit Chip wie auch der E-Pass und der Ausländerausweis (AA10) 'tel quel' als eIdM einsetzbar.

Technische und organisatorische Implementierung

Es werden die in der ePass-Funktion enthaltenen Authentisierungsmöglichkeiten genutzt. Dabei sorgt die lokale Lese-Anwendung dafür, dass diese Funktion sich gegenüber jeder Anwendung wie ein normales elektronisches Identifikationsmittel verhält.

Für PIN-Prüfung und eventuell zusätzliche Identity-Attribute ist ein zentraler Identity-Provider-Dienst (IdP) notwendig.

Governance und rechtliche Implementierung

Diese eID steht voll unter staatlicher Verantwortung, was eine entsprechende gesetzliche Grundlage erfordert. (vgl. dazu Kapitel 4.3.1)

EU-Interoperabilität: Primäres Ziel wäre, diese Lösung notifizieren zu lassen, wobei evtl. zusätzlich auch private eID-Lösungen notifiziert würden, was von der EU vorgesehen ist (siehe Variationen und Kapitel 4.3.3).

Anwendungsprofil, Funktionen

Es stellt sich die Frage, wie breit ein solches Authentifizierungsmittel eingesetzt werden soll. Denkbar wäre ein stark eingeschränkter Einsatz für bestimmte E-Government-Dienste, primär um den Support-Aufwand in Grenzen zu halten.

Je nach erreichbarem Benutzerkomfort ist aber auch ein breiter Einsatz bis hin zu den üblichen E-Commerce-Diensten denkbar.

E-Voting wird wahrscheinlich beschränkt unterstützt werden können.

Entwicklungsstand, Erfahrungen

Zurzeit (bis Ende 2013) klärt die Fachhochschule Bern im Auftrag des Bundes die Machbarkeit dieses Ansatzes konzeptionell und mit einer Prototyp-Anwendung ab.

Vorteile	- Keine zusätzlichen Funktionen und Daten auf der IDK. - Jeder ePass-konforme Ausweis ist auch als eID geeignet.
Nachteile	- Kein Standard bzw. nicht Mainstream. - Einsatz für E-Voting wahrscheinlich nur sehr beschränkt möglich. - Ungewisser Entwicklungspfad (langfristig)
Kosten	- Keine Kosten für die Ausrüstung der Karte. - Kosten für die Entwicklung der Client-Anwendung (eID-App). - Kosten für Realisierung und Betrieb des IdP. - Betriebskosten beim Staat, insbesondere für Support.
Risiken	- Gewiss Realisierungs-Risiken, da Eigenentwicklung. - Wird nicht eingesetzt, weil nicht komfortabel genug (Integration) - Ungewissheit über Funktionsfähigkeit bei technischer Weiterentwicklung.

Optionen, Variationen

- Unterschiedlich breites Anwendungs-Spektrum denkbar.
- Zur eID gehöriger Attribut-Server (IdP) und Anzahl der abrufbaren Attribute.
- Zusätzlich Regulierung und Notifikation für private eID-Angebote denkbar, wie in Variante 1.

4.2.3 Variante 3: Klassische staatliche Mainstream-ECC-eID

Kurzbeschreibung	Zur IDK kann eine klassische eID-Option gewählt werden, bestehend aus 2-3 Schlüssel-Paaren, gemässe den Spezifikationen der European Citizen Card (ECC, Kap. 2.3.4.1). Es gibt ECC-Standards und Produkte zu kontaktbehafteten ('dual-interface') wie auch zu kontaktlosen Implementierungen der eID-Funktion (die ePass-Funktion ist immer kontaktlos)

Technische und organisatorische Implementierung

Es wird eine klassische eID 'ab der Stange' mit der zugehörigen eID-Infrastruktur (IdP) evaluiert und beschafft. Die IDK-Prozesse werden entsprechend angepasst bzw. erweitert.
Zusätzlich wird eine bestimmte Menge an Einführungs- und Support-Aufwand definiert und bereitgestellt.

Governance und rechtliche Implementierung

Der Staat ist umfassend für das elektronische Identifikationsmittel zuständig. Dafür braucht es eine umfassende gesetzliche Regelung (Ausbau Ausweisgesetz oder eigenes Gesetz; vgl. dazu Kapitel 4.3.1 und 4.3.2).
EU-Interoperabilität: Primär würde diese eID-Lösung notifiziert, wobei evtl. zusätzlich auch private eID-Lösungen notifiziert würden, was von der EU vorgesehen ist (vgl. dazu Kapitel 4.3.3).

Anwendungsprofil, Funktionen

Der Einsatzbereich ist grundsätzlich sowohl für einfache wie auch anspruchsvolle Anwendungen im E-Commerce wie im E-Government möglich.
Der Einsatz für E-Banking und E-Voting ist je nach Ausgestaltung evtl. nur beschränkt möglich.

Entwicklungsstand, Erfahrungen

Solche eID-Lösungen sind komplett realisiert und - je nach Ausprägung - seit Jahren im Einsatz. Von diesen Entwicklungen und Erfahrungen kann profitiert werden.

Vorteile	- Kauf einer im Einsatz geprüften Lösung 'ab der Stange'.
Nachteile	- Starre Lösung (für lange Einsatzzeit von mind. 20 Jahren). - Einsatz für E-Voting nur sehr beschränkt möglich.
Kosten	- Geringe Zusatzkosten für Karte und Chip (wenige Franken). - Kosten für Client- und Server-Anbindung gering bzw. im Voraus bekannt - Kosten für Lesegerät je nach Lösung 0.- bis ca. 40.- - Betriebskosten, insbesondere für den Support
Risiken	- Wird nicht oder nicht genug eingesetzt; obsolet bevor Nutzung steigt. - Wird technisch obsolet, weil innerhalb des IDK-Lebenszyklus eine Weiterentwicklung nicht möglich ist

Optionen, Variationen

- Kontaktbehaftete oder kontaktlose eID-Schnittstelle.
- Breite des Einsatzgebiets kann variiert werden.
- Evtl. eID-Funktionen nur mal ausrollen, vorläufig ohne aktive Unterstützung (wie Schweden).
- Im Prinzip auch staatliche eIdM auf einem separaten, zweiten Träger möglich.

4.2.4 Variante 4: eID à la Deutschland

Kurzbeschreibung	Es wird grundsätzlich die deutsche Lösung (siehe Kapitel 2.4.1.2) übernommen, evtl. mit gewissen Abweichungen in Details, wie z.B. einem einfacheren Verfahren für die Erteilung von Berechtigungen an Service Provider. .

Technische und organisatorische Implementierung

Die Lösung ist grundsätzlich technisch realisiert, die Übernahme geschieht wohl am Besten im Rahmen einer institutionalisierten Zusammenarbeit mit Deutschland.

Die organisatorische Abstimmung mit den bisherigen Prozessen für die Bestellung und Ausgabe der Identitätskarte scheint nicht besonders komplex.

Es muss ein eigener Support aufgebaut werden.

Allenfalls müsste für die Umgehung bzw. Vereinfachung der Authentisierung der Service Provider für den Zugriff auf die eID ein gewisser Aufwand in technischer und organisatorischer Hinsicht getrieben werden.

Governance und rechtliche Implementierung

Der Staat ist umfassend für das elektr. Identifikationsmittel zuständig. Dafür braucht es eine umfassende gesetzliche Regelung (Ausbau Ausweisgesetz oder eigenes Gesetz; vgl. dazu Kapitel 4.3.1 und 4.3.2).

Anwendungsprofil, Funktionen

Der deutsche elektronische Personalausweis ist für einen sehr breiten Einsatz konzipiert. Einfache und anspruchsvolle Anwendungen im E-Commerce wie im E-Government sind möglich, bis hin zu einem Einsatz für E-Banking auf der einen und E-Voting auf der anderen Seite.

Entwicklungsstand, Erfahrungen

Grundsätzlich ist diese Lösung komplett realisiert. Es kann laufend von den Erfahrungen in Deutschland profitiert werden. Nur schon bis zum Start der Auslieferungen im Jahr 2017 dürfte einiges mehr über die Erfahrungen in Deutschland bekannt sein.

Die Anpassungen und erwähnten Vereinfachungen halten sich in einem überschaubaren Rahmen.

Vorteile	- Lösung kann (fast) komplett übernommen werden, inkl. technische Richtlinien und Software-Module für Benutzer- und Dienstanbieter-SW. - Sehr hoher Datenschutzstandard.
Nachteile	- Komplexe Lösung - Abhängigkeit von Deutschland
Kosten	- Karte mit Chip voraussichtlich günstig, da grosse Stückzahlen (D+CH) - Betriebskosten, insbesondere für den Support und Zulassung von Dienstleistungsanbietern.
Risiken	- Insgesamt keine grossen Realisierungs-Risiken weil fertig entwickelt; - Evtl. Gefahr für Lock-In, technische Sackgasse.

Optionen, Variationen

- Verschiedene Modalitäten in der Intensität der Zusammenarbeit mit Deutschland denkbar.
- Evtl. eID-Funktionen nur ausrollen, vorläufig ohne aktive Unterstützung (wie Schweden).

4.3 Rechtsgrundlagen

4.3.1 Beurteilung des Rechtsetzungsbedarf der vier eID-Varianten

Alle vier eID-Varianten ziehen eine Anpassung bestehender oder die Schaffung neuer Rechtsgrundlagen nach sich. Nachfolgend eine erste Beurteilung des Rechtsetzungsbedarfs der vier eID-Varianten. Diese kann im jetzigen Zeitpunkt sinnvollerweise nur summarisch bleiben und kann sich noch ändern, je nach Berücksichtigung der beschriebenen Variationsmöglichkeiten für jede eID-Variante.

Variante 1 «Private Anbieter, staatliche Identifikation und Regulierung»

Hier dürfte das revidierte Bundesgesetz über die elektronische Signatur (ZertES, SR 943.03) als gesetzliche Grundlage genügen. Im Rahmen der laufenden Revision wird u.a. der Einsatz von geregelten Zertifikaten für die Authentisierung ermöglicht und dem Bundesrat die Kompetenz übertragen, die technischen Details auf Verordnungsstufe zu regeln. Dazu wird bis Ende 2013 die Botschaft ausgearbeitet, welche mit einem Hinweis zu ergänzen wäre, dass geregelte Zertifikate u.a. auch für die Authentisierung bei einer eID eingesetzt werden. Notwendig sind insbesondere Ausführungsbestimmungen auf Verordnungsstufe. Die Verordnung über die elektronische Signatur (VZertES, SR 943.032) müsste neu auch das Produkt eID regeln und festlegen, welche Bedingungen für das Anbieten einer anerkannten «privaten eID» zu erfüllen sind und welche Rolle der Bund übernimmt bezüglich Haftung / Kontrolle / Aufsicht für und über die Dienstleistungsanbieter.

Variante 2 «Identitätsnachweis mit ePass-Chip»

Für diese eID übernimmt der Staat die Verantwortung. Wie bei der Variante 1 sind auch hier Ausführungsbestimmungen notwendig. Als Rechtsgrundlage genügt Artikel 2 Absatz 2ter des geltenden Ausweisgesetzes (AwG, SR 143.1). Danach legt der Bundesrat auf Verordnungsstufe fest, welche Ausweisarten mit einem Chip zu versehen sind und welche Daten darauf gespeichert werden dürfen.

Sollte man mit einem zusätzlichen Identity Provider Server (IdP) über die im ePass enthaltenen Attribute hinaus noch weitere Attribute zur Verfügung stellen, müsste für diese Datenhaltung zusätzlich eine gesetzliche Grundlage wie in Variante 3 geschaffen werden

Variante 3 «Mainstream-eID»

Der Staat ist umfassend für das elektronische Identitätsmittel zuständig. Dafür sind umfassende, gesetzliche Regelungen erforderlich. Es gibt eine - wenn auch ziemlich «dünne» - gesetzliche Grundlage im AwG. Nach Artikel 2 Absatz 2^{quater} AwG kann der Ausweis zusätzlich zu dem in Artikel 2 Absatz 2ter AwG geregelten Chip elektronische Identitäten für Authentisierungs-, Signatur- und Verschlüsselungs-Funktionen enthalten. Dieser Absatz genügt vielleicht für eine sehr einfache, restriktive eID. Sobald aber erweiterte Funktionen angestrebt oder Personendaten für die eID zentral gehalten werden, wie z.B. bei der ECC-eID, braucht es eine neue, formell-gesetzliche Grundlage. Diese könnte mit einem neuen «eID-Gesetz» geschaffen werden. Eine weitere Möglichkeit wäre eine Ergänzung des bestehenden AwG.

Variante 4 «wie Personalausweis D»

Wenn wir eine eID à la Deutschland einführen, liegt die Verantwortung für das elektronische Identitätsmittel vollumfänglich beim Staat (vgl. Variante «Mainstream»). Das würde bedeuten, dass auch hier ein «neues» Gesetz zu erarbeiten oder das AwG zu ergänzen wäre.

Allerdings kommt der aktuelle deutsche Personalausweis ohne zentral gespeicherte Daten aus. Wenn auch in diesem Punkt die gleiche Lösung gewählt würde, also kein IdP, dann bräuchte es in diesem Teilbereich keine gesetzliche Grundlage.

4.3.2 Möglicher Regelungsinhalt «eID-Gesetz»

In einem neuen «eID-Gesetz» (oder einer Ergänzung des AwG) müssten je nach gewählter Lösung die folgenden Punkte geregelt werden:

- Allgemeine Bestimmungen (Gegenstand, Geltungsbereich, Begriffsdefinitionen);
- Herausgeber der QeID; evtl. mit Anforderungen und Zulassungssystem;
- Haftung, Kontrolle und Aufsicht für und über die Dienstleistungsanbieter;
- Aktivierung, Sperrung und Ungültigkeitserklärung einer QeID;
- Speicherung der eID-Daten (insbesondere Identity Provider);
- Zugriffsberechtigungen (auf eID-Daten);
- Umgang mit Berechtigungszertifikaten;
- Schlussbestimmungen.

4.3.3 Verhältnis zum EU Recht

Die EU ist daran, als Nachfolge zur bestehenden Signatur-Richtlinie eine «Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt» zu beraten. Dieser Verordnungsvorschlag vom 4. Juni 2012 geht thematisch viel weiter als die bisherige Signatur-Richtlinie. In Artikel 5 der Verordnung wird unter anderem die gegenseitige Anerkennung und Akzeptierung von Vertrauensdiensten geregelt. Danach kann jeder Inhaber einer notifizierten staatlichen eID eines Landes auf Online-E-Government-Dienstleistungen aller anderen Mitgliedstaaten zugreifen – und zwar unabhängig von der konkreten technischen Umsetzung seiner eID (vgl. dazu auch vorne Kapitel 2.3.3).

Die Schweiz ist zwar nicht EU-Mitglied, aber in Anbetracht unserer engen Verflechtung mit vielen EU-Staaten und der globalen Natur von Online-Diensten im Internet, empfiehlt es sich, die schweizerische eID so zu gestalten, dass sie vom Konzept her nach den EU-Vorgaben notifizierbar wäre. Für die Notifizierung wäre ein bilateraler Vertrag mit der EU notwendig, welcher u.a. insbesondere auch die Frage einer allfälligen Staatshaftung der Schweiz regeln müsste.

Das Vorhaben hat in der EU recht hohe Priorität. Nach heutiger Planung sollten die Eckpunkte der neuen EU-Verordnung bis September 2013 feststehen, da bis dann alle vorberatenden Komitees dazu getagt haben. Die Behandlung im Rat und im Parlament wäre dann ab Ende 2013 vorgesehen, sodass die Vorlage im Frühjahr 2014 verabschiedet und erste Teile Anfang 2015 in Kraft treten könnten. Eine Überführung der Verordnung ins nationale Recht der EU-Mitgliedstaaten ist nicht erforderlich.

4.4 Vergleich / Bewertung

Die weiter zu evaluierenden Lösungen müssen selbstverständlich alle beschriebenen funktionalen MUSS-Anforderungen erfüllen.

Für die Auswahl der zu realisierenden Lösung können die vier Lösungs-Varianten mit dem nachstehenden Raster bewertet und verglichen werden.

Kriterium	Var. 1 Private	Var. 2 ePass	Var. 3 Mainstr.	Var. 4 wie PA D	Bemerkungen
Einfaches Produkt					
Entwicklungskosten					
Betriebskosten					
Risiken bis Bereitstellung					
Kompatibel zu ID-Prozessen					
Kosten für Benutzer					
Sicherheit					
Datenschutz					
Internat. Konformität					
Kombinierbarkeit					
Entwicklungsfähigkeit					
...					
Bietet Entwicklungspfad für SuisseID-Akteure					
Verständliche, kommunizierbare Lösung					
...					
Durchschnitts-Note					

4.5 Vorgeschlagene Lösung: <Variante>

Zum Zeitpunkt der informellen Konsultation liegen die vier vorstehend beschriebenen Lösungsvarianten gleichberechtigt vor. Es gibt somit noch keinen Lösungsvorschlag. Entsprechend können dieses und die nachfolgenden Kapitel noch gar nicht oder nur ganz rudimentär mit Inhalten gefüllt werden. Sie werden aber trotzdem in einer obersten Gliederung aufgeführt, um jetzt schon aufzuzeigen, wie das Gedanken-Gerüst für den künftigen Antrag aussehen wird.

Ziel der Konsultation ist es, dass sich ein Favorit für eine Lösung aufzeigt, der dann im nächsten Schritt in diesem Kapitel näher beschrieben würde. Ebenso würde die Realisierung inklusive Bereitstellung der notwendigen rechtlichen Grundlagen geplant und in den nachstehenden Kapiteln beschrieben. Sollte sich nach der Konsultation kein klarer Favorit ergeben, kann vielleicht mindestens die eine oder andere Lösungsvariante ausgeschlossen werden und je nachdem würden maximal zwei Lösungsvarianten näher ausgearbeitet und dem Bundesrat zum Entscheid vorgelegt.

4.5.1 Grundlegende Architektur des eID-Systems

Wird im Rahmen des Konzepts für eine Lösung ausgearbeitet werden.

4.5.2 Die wichtigsten eID-Prozesse

Wird im Rahmen des Konzepts für eine Lösung ausgearbeitet werden.

4.5.3 Datenschutz-Betrachtungen[22]

Wird im Rahmen des Konzepts für eine Lösung ausgearbeitet werden.

4.5.4 Rechtliche Regelung

Wird im Rahmen des Konzepts für eine Lösung ausgearbeitet werden.

[22] Ein länderübergreifender Vergleich zum Thema findet sich im 'ENISA Position Paper - Privacy Features of European eID Card Specifications (Naumann & Hogben, 2009).

5 Mittelbedarf

Aus Sicht des Bundes-Projekts für eine neue Identitätskarte hängt der Mittelbedarf für die eID-Lösung stark von der gewählten Lösungsvariante ab. Das nachstehende Raster zeigt schon mal auf, wie sich die Kosten grob zusammensetzen.

Eine ähnliche Kostenberechnung bräuchte es auch für die Implementierung der gleichen eID-Lösung bei den Ausländerausweisen.

A Investitionskosten Bund:

Pos.	Was	Invest.	-> p.a.
A-1	eID-Projekt führen, managen (Mehrkosten für eID-Option)		
A-2	Gesetzgebung planen, realisieren		
A-3	Ausweis-Anwendung anpassen (Mehrkosten)		
A-4	Ausweis evaluieren, prüfen (Mehrkosten)		
A-5	eID-Client-Beschaffung/Entwicklung		
A-6	Einführungs-Aufwand (Mehrkosten)		
A-7	Kommunikation / Marketing / Ausbildung		

B Betriebskosten Bund:

Pos.	Was	p.a.
B-1	Kosten für externe PKI-Dienstleistungen	
B-2	Lizenzkosten, etc.	
B-3	Kosten für Support-Personal	
B-4	Kommunikation / Marketing / Ausbildung	

C Direkte Kosten pro Ausweis:

Pos.	Was	p. Ausweis	p.a.
C-1	Mehrkosten für Chip		
C-2	Zusätzliche Kosten für eID-Prozess-Schritte		
C-3			

D Weitere Kostenblöcke:

Pos.	Was	Invest.	p.a.
D-1			
D-2			

	Total Investitionskosten für staatliche eID		
	→ Amortisation Investition auf 4 Jahre		
	→ Mehrkosten pro Ausweis bei 600'000 Ausweisen p.a.		

6 Planung und Organisation

Das Umsetzungsprojekt für die neue Identitätskarte mit eID gliedert sich in zwei Teilprojekte: Beschaffung und Rechtsetzung. Einerseits muss die neue Identitätskarte spezifiziert und öffentlich ausgeschrieben werden, andererseits muss das notwendige Gesetzgebungspaket für die eID erarbeitet und in Kraft gesetzt werden. Beide Teilprojekte stützen sich auf die Erkenntnisse der vorliegenden Konzeptstudie und den Resultaten aus der geplanten Konsultation, welche also eine wichtige Grundlage für alle weiteren Arbeiten ist. Gemäss Bundesratsbeschluss soll die Vernehmlassung zum Rechtsetzungspaket Mitte 2014 eröffnet werden können, so dass die konzeptionellen Arbeiten bereits Anfangs 2014 mit der Eröffnung der Ämterkonsultation abgeschlossen sein müssen. Damit die neue Identitätskarte in den Jahren 2016/2017 eingeführt werden kann, muss die öffentliche Ausschreibung ebenfalls im Verlaufe des Jahres 2014 erfolgen.

7 Wirtschaftlichkeitsbetrachtungen

Eine echte betriebswirtschaftliche Kosten-/Nutzenrechnung kann für ein Produkt wie ein Ausweis oder eben ein elektronischer Identitätsnachweis nicht aufgestellt werden. Wie oft bei staatlichen Basisleistungen ergibt sich nicht ein betriebswirtschaftlicher, sondern ein volkswirtschaftlicher oder oft auch ein ideeller Nutzen. Sicherheit in polizeilicher Hinsicht wie auch Sicherheit und Vertrauen im Geschäftsverkehr weisen keinen leicht quantifizierbaren Nutzen auf.

Diese Situation ist bei vielen staatlichen Aufgaben gegeben. Die Lösung besteht darin, trotzdem die Kosten möglichst genau vorauszuberechnen und daneben den Nutzen nicht quantitativ zu beschreiben. Anschliessend ist es an den Entscheidungsträgern bis hin zum Souverän, den nicht quantifizierbaren Nutzen mit den quantifizierten Kosten zu vergleichen und über die Realisierung zu entscheiden.

Wie vorstehend im Kapitel 5 erwähnt, sollen die Kosten erst detailliert ermittelt werden, wenn die favorisierte Lösung feststeht.

Zum volkswirtschaftlichen und ggf. ideellen Nutzen kann jetzt schon Nachstehendes aufgeführt werden:

- Ein starkes und weit verbreitetes elektronisches Identifikationsmittel bewirkt auf einfache und kostengünstige Weise Sicherheit und Vertrauen im elektronischen Geschäftsverkehr, was eine Bedingung für dessen Verbreitung auch auf heiklere Geschäfte darstellt.
- Die Umstellung auf elektronische Abwicklung im Wirtschaftsleben wie auch beim Verkehr mit dem Staat kann für alle Beteiligten grosse Einsparungen an Zeit, Aufwand und Geld bewirken.
- Dabei werden sowohl bisherige Geschäfte auf elektronische Abwicklung umgestellt, wie auch völlig neue Geschäftsmodelle entwickelt, die nur mit elektronischer Abwicklung möglich sind.
- Ein weit verbreitetes starkes elektronisches Identifikationsmittel ermöglicht eine Umstellung von unsicheren auf sichere Verfahren und hilft somit, Identitäts-Diebstahl und andere Formen von Cyber-Kriminalität zu verhindern.

8 Konsequenzen

Eine staatliche Identitätskarte wird nur alle ca. 15 bis 20 Jahre neu konzipiert. Hat man sich einmal für eine Lösung entschieden, folgen etwa 5 Jahre für Vorbereitung und Beschaffung, dann wird die Karte etwa 15 Jahre so abgegeben und schliesslich ist die letzte solche Karte noch 10 Jahre gültig. Ab Entscheid dauert es somit etwa 15 Jahre, bis alle Personen die neue IDK haben und etwa 30 Jahre, bis niemand mehr diese Version der IDK hat.

Dies bedeutet auf der einen Seite, dass man im Moment der Festlegung einer neuen IDK die seltene Gelegenheit hat, im Hinblick auf künftige Anwendungen eine bestimmte Komponente auf der IDK zu verteilen. Wenn es so sein sollte, dass eID-Anwendungen sich tatsächlich primär darum nicht verbreiten, weil sie unter dem Huhn/Ei-Problem leiden, dass also niemand eine eID will, weil es keine Anwendungen gibt, und niemand Anwendungen bereitstellt, weil nicht genügend Leute eine eID haben, dann befindet man sich bei der Neugestaltung der IDK in der einmaligen Lage, diese Blockade mindestens langfristig durchbrechen zu können.

Auf der anderen Seite bedeuten aber die geschilderten zeitlichen Verhältnisse auch, dass alles was sich auf der Karte befindet, sehr lange Bestand haben muss. In Anbetracht der Geschwindigkeit des technischen Wandels gerade im Bereich der elektronischen Kommunikation ist das eine gravierende Anforderung.

9 Fragen im Rahmen der informellen Konsultation

Im Rahmen der informellen Konsultation zur vorliegenden Konzeptstudie und zu den vier Lösungsvarianten interessieren uns insbesondere die nachstehenden Fragen.

1. Grundsätzliche Bemerkungen.
2. Sind sie mit den Zielen des Vorhabens einverstanden, wenn nein, wo und warum nicht?
3. Welche Eigenschaften weist Ihrer Meinung nach eine ideale eID-Lösung für die Schweiz auf, welche Eigenschaften darf sie auf keinen Fall haben?
4. Welche der vorgeschlagenen 4 Lösungsvarianten bevorzugen Sie? Und wieso?
5. Welche Optionen oder Sub-Varianten sehen Sie für diese von Ihnen bevorzugte Grund-Variante?
6. Welche anderen Lösungsvarianten scheinen Ihnen auch noch geeignet?
7. Welche Lösungsvariante möchten Sie auf keinen Fall realisiert sehen und warum nicht?
8. In welcher Rolle sind Sie an einer eID-Lösung interessiert;
   a) als Benutzer,
   b) als Anbieter von Identity-Dienstleistungen (welchen),
   c) als potentieller Dienstleistungsanbieter mit elektronischer Identifikation oder
   d) als Vertreter einer Organisation (welcher)?
9. Weitere Bemerkungen und Hinweise (z.B. zu den Kostentreibern und Risiken).

Wenn Sie sich bei Ihrer Stellungnahme an das vorstehende Frageraster halten, erleichtern Sie die Auswertung.

10 Anhänge

10.1 Definitionen, Akronyme und Abkürzungen

Begriff / Abkürzung	Bedeutung
AA10	Der am 24.01.2011 eingeführte biometrische Ausländerausweis.
Authentifizierung Authentisierung	Bei der Authentifizierung stellt ein Dienst die Identität eines Bezügers des Dienstes fest. Bei der Authentisierung belegt ein Bezüger seine Identität gegenüber einem Dienst. Die beiden Begriffe sind reziprok, im Englischen gibt es nur die ‚Authentication'.
Attribute (Service) Provider	Dienst im Netz, der auf Anfrage zu einer bestimmten Identität bestimmte Attribute liefert wie z.B. Alter, Wohnort, berufliche Befähigung etc. In der Ausprägung ‚user centric' werden die Attribute nur mit Einverständnis des Benutzers und einer starken Authentisierung ausgegeben.
BAKOM	Bundesamt für Kommunikation (www.bakom.admin.ch)
BRB	Bundesratsbeschluss
BSI	(Deutsches) Bundesamt für Sicherheit in der Informationstechnik
CSP	Certification Service Provider, Zertifizierungsdienste-Anbieter
Dienstanbieter	In diesem Kontext ein E-Commerce- oder E-Government-Dienst, der einen elektronischen Identitätsnachweis verlangt (='Service Provider')
eCH	Verein zur Förderung, Entwicklung und Verabschiedung von E-Government-Standards für die Schweiz (www.ech.ch).
eID	Elektronische Identität; breiter, eher unscharfer Begriff für alle Komponenten, die es zum Identitätsnachweis in der Online-Welt braucht. Präziser sind die Begriffe Elektronischer Identitätsnachweis und eIdM.
eIdM	siehe Elektronisches Identifikationsmittel
eIDK	Elektronische Identitätskarte; Identitätskarte mit elektronischer Komponente, typischerweise eIdM und/oder ePass
Elektronisches Identifikationsmittel (eIdM)	Physische Komponente („Token") im Besitz der Person, die sich damit authentisieren will, z.B. Smartcard, USB-Stick, Smartphone mit PIN-Card.
Elektronischer Identitätsnachweis	Nachweis der Identität gegenüber einem Online-Dienst (Authentisierung), funktional gesehen.
ePass (-Funktion)	Wird als Begriff sowohl für den elektronischen Pass an sich wie auch für die elektronischen Komponenten verwendet, welche die sichtbaren Daten des Passes und u.U. die Fingerabdrücke speichern und über NFC abrufbar machen. Dient der Missbrauchs-Bekämpfung und nicht dem Online-Einsatz.
IAM	Identity and Access Management
Identifikator	Ein eindeutiges, künstliches Merkmal, das zur Identifizierung eines Objektes dient. Identifikatoren bestehen in der Regel aus Codes und Nummern.
Identity (Service) Provider	Identitätsdienst-Anbieter; Instanz, welche Identifikations-Dienste wie z.B. Single Sign On, Identitäts-Attribute, Bestätigungen etc. anbietet.
IDK	Identitätskarte, konventionell oder mit elektronischen Komponenten als eIDK
IdP	Identity Provider (Service); der auf Anfrage Identitäts-Bestätigungen zu einer eID zuhanden eines Service Providers abgibt.
ISB	Informatiksteuerungsorgan des Bundes
NFC	Near-Field-Communication; Spezialisierung der RFID-Technik für sichere Datenübertragung auf kurze Strecken (max. 10 cm)

Begriff / Abkürzung	Bedeutung
PACE	Password Authenticated Connection Establishment; Authentisierungsmechanismus zwischen Terminal und Chip
PKI	Public Key Infrastructure
QeID	siehe Qualifizierte eID
Qualifizierte elektronische Identität	Auch Qualifizierte eID, QeID: Bezeichnung in diesem Dokument für *die* elektronische Identität (inkl. das eIdM) die gemäss dem Ziel dieses Vorhabens künftig zusammen mit der Identitätskarte beantragt werden kann, vom Staat anerkannt ist und für die Notifizierung bei der EU vorgesehen ist.
RFC	Request for Comments; Standardisierungs-Vorschlag, oft auch Standard
RFID	‚radio-frequency identification'; Verbindung – hier der ID-Karte mit dem Leser – über Radiowellen
SECO	Staatssekretariat für Wirtschaft (www.seco.admin.ch)
Service Provider	Dienstanbieter, 'Relying Party'; in diesem Kontext ein E-Commerce- oder E-Government-Dienst, der einen elektronischen Identitätsnachweis verlangt.
SR	Systematische Rechtssammlung (www.admin.ch/ch/d/sr/sr.html)
STORK	‚Secure Identity Across Borders Linked' (https://www.eid-stork.eu/); EU-Projekt zur grenzüberschreitenden Authentisierung mit eID-Karten.
SuisseID	Schweizer Standard für eine elektronische Identität, umfassend Authentisierung, qualifizierte Signatur und Identitätsdaten-Nachweis (www.SuisseID.ch)
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur; SR 943.03 (www.admin.ch/ch/d/sr/c943_03.html)

10.2 Literaturverzeichnis

Bernold, R., Hassenstein, G., Laube-Rosenpflanzer, A., Riedl, R., Spichiger, A., & Thomas, V. (2011). *Bericht SuisseID - STORK - Integration.* Bern: Berner Fachhochschule. Abgerufen am 30. 7. 2013 von http://www.ict-21.ch/l4d/mod/file/download.php?file_guid=469461

BMI. (2010). *Personalausweisportal.de.* (Bundesministerium des Innern) Abgerufen am 30. 7. 2013 von Der neue Personalausweis: http://www.personalausweisportal.de/DE/Home/home_node.html

Castro, D. (2011). *Explaining International IT Application Leadership: Electronic Identification.* ITIF - The Information Technology & Innovation Foundation. Abgerufen am 02. 07. 2013 von http://www.itif.org/publications/explaining-international-it-application-leadership-electronic-identification-systems

Eurosmart. (2008). *European Citizen Card: One Pillar of Interoperable eID Success.* Bruxelles: Eurosmart - Association representing the Smart Security Industry. Abgerufen am 28. 07. 2013 von http://www.eurosmart.com/images/doc/WorkingGroups/e-ID/Papers/ecc-position-paper-final.pdf

Graux, H., & Dumortier, J. (2009). *Report on the state of pan-European eIDM initatives.* European Network and Information Security Agency. ENISA. Abgerufen am 02. 07. 2013 von http://www.enisa.europa.eu/publications/archive/eidm-report

Hühnlein, D., Schmölz, J., Wich, T., & Horsch, M. (2012). Sicherheitsaspekte beim Chipkarten-basierten Identitätsnachweis. *Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce*, S. 153-168. Abgerufen am 10. 07. 2013 von http://www.ecsec.de/pub/2011_AI3.pdf

IDABC. (2009). *eID Interoperability for PEGS.* (IDABC - European eGovernment Services) Abgerufen am 28. 7. 2013 von http://ec.europa.eu/idabc/en/document/6484.html

Naumann, I., & Hogben, G. (2009). *Privacy Features of European eID Card Specifications - ENISA Position Paper.* European Network and Informationi Security Agency. ENISA. Abgerufen am 02. 07. 2013 von http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-cards-en

NIST. (2011). *Homepage NSTIC.* (National Institute of Standards and Technology, NIST) Abgerufen am 28. 7. 2013 von National Strategy for Trusted Identities in Cyberspace: http://www.nist.gov/nstic/

Quade, M., & Wölfle, R. (2010). *SuisseID in der Praxis - Grundlagen und Fallbeispiele zum elektronischen Identitätsnachweis der Schweiz.* Basel: edition gesowip.

Schmeh, K. (2009). *Elektronische Ausweis-Dokumente - Grundlagen und Praxisbeispiele.* München: Hanser.

Stevens, T., Elliot , J., Hoikkanen, A., Maghiros, I., & Lusoli, W. (2010). *The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies.* Luxembourg: European Communities. Abgerufen am 02. 07. 2013 von http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=3739

The White House. (2011). *Nationl Strategy for Trusted Identities in Cyberspace.* Washington. Abgerufen am 29. 7. 2013 von http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Verein Trägerschaft SuisseID. (2010). *Homepage SuisseID.* Abgerufen am 28. Juni 2013 von SuisseID - Der erste standardisierte elektronische Identitätsnachweis der Schweiz: http://www.SuisseID.ch