Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

Bundesgesetz über die staatlichen elektronischen Identifikationsmittel (eID-Gesetz)

Erläuternder Bericht zum Vorentwurf

Bern, 20. Juni 2014

1 Allgemeiner Teil

1.1 Ausgangslage

Die aktuelle Identitätskarte wird seit dem Jahr 1995 in der heutigen Form herausgegeben. Aus technischen und vergaberechtlichen Gründen steht die Ablösung mit einer neuen, weiter entwickelten Identitätskarte (IDK) an. Damit stellt sich die Frage, ob die neue IDK auch ein staatliches elektronisches Identifikationsmittel (eID) enthalten soll.

Der Bundesrat hat sich in den letzten Jahren verschiedentlich mit der Frage einer staatlichen elektronischen Identitätskarte befasst. Die Frage stellte sich schon im Zusammenhang mit der Regelung der elektronischen Signatur im Jahr 2001 und später in verschiedenen Strategiearbeiten zur Förderung von E-Government und der E-Economy in der Schweiz. Zusammen mit einem umfassenden Gesetzgebungspaket zur Förderung des elektronischen Geschäftsverkehrs hat der Bundesrat am 19. Dezember 2012 dem EJPD den Auftrag erteilt, im Rahmen der Beschaffung der neuen Identitätskarte auch ein Konzept und einen Gesetzgebungsentwurf für ein staatliches elektronisches Identifikationsmittel auszuarbeiten.

Mehrere Gründe sprechen dafür, die neue Identitätskarte mit einer eID zu versehen:

a. In mehreren Studien wurde eine staatliche eID als wichtiger Eckpfeiler für die Entwicklung von Sicherheit und Vertrauen im elektronischen Geschäftsverkehr – in E-Government, E-Business und E-Health – erkannt[1].
b. Die meisten Länder, die in letzter Zeit eine neue Identitätskarte einführten, haben diese auch mit einer eID versehen.
c. Die EU hat eine Verordnung für die gegenseitige Anerkennung und Interoperabilität von eID-Systemen der Mitgliederländer verabschiedet. Dies zeigt, dass auch die EU diesem Werkzeug eine grosse Bedeutung beimisst.
d. Durch die Kombination mit der Identitätskarte, die sowieso eine anspruchsvolle Prüfung der Identität bei einer Behörde verlangt, kann die eID mit sehr geringen Mehrkosten der ganzen Bevölkerung abgegeben werden.

1.2 Entstehung des vorliegenden Gesetzesentwurfs

In einer ersten Phase hat das Bundesamt für Polizei fedpol als federführende Stelle im Projekt «Beschaffung einer neuen IDK» die Ziele und Anforderungen an eine eID-Lösung mit einer breit abgestützten verwaltungsinternen Arbeitsgruppe aufgearbeitet und eine informelle Konsultation zu den Lösungsvarianten durchgeführt. Diese richtete sich an die Staatskanzleien, die schweizerische Informatikkonferenz, die federführenden Organisationen von E-Government Schweiz, die Dachverbände der Wirtschaft und weitere interessierte Kreise. Die Basis für die informelle Konsultation von Mitte August bis Mitte Oktober 2013 bildete die «Konzeptstudie elektronischer Identitätsnachweis»[2]. Sie erläutert die unterschiedlichen Lösungsvarianten, welche sich nicht nur in funktionaler und technischer Hinsicht, sondern insbesondere auch in der Verteilung der Aufgaben zwischen Privatwirtschaft und Staat unterscheiden. In der Studie wurden eine privatwirtschaftliche Variante und drei verschieden ausgestaltete staatliche Varianten präsentiert.

---

[1] Vgl. Literaturhinweise im Anhang der «Konzeptstudie elektronischer Identitätsnachweis», S. 36.

[2] Unterlagen zur Konzeptstudie sind einsehbar unter: http://www.schweizerpass.admin.ch/content/pass/de/home/aktuell/konsultation.html

Die im Rahmen der informellen Konsultation eingegangenen Stellungnahmen ergaben keinen klaren Favoriten. Mit wenigen Ausnahmen waren sich aber alle Stellungnehmenden über folgende wichtige Ziele und Anforderungen für die künftige eID einig:

a. Die eID soll zusammen mit der IDK, im gleichen Antragsprozess und ohne wesentliche Mehrkosten angeboten werden;
b. Die eID muss mittelfristig auch allen in der Schweiz aufenthaltsberechtigten Ausländerinnen und Ausländern zugänglich sein;
c. Die eID soll sich sowohl im E-Government wie auch im E-Business breit einsetzen lassen.
d. Die eID soll konzeptionell und technisch so ausgestaltet sein, dass sie international, insbesondere im europäischen Umfeld, interoperabel sein wird.

In der Folge hat der Bundesrat unter Berücksichtigung der Ergebnisse der informellen Konsultation nachstehende Eckpunkte für die Ausgestaltung der künftigen eID festgelegt:

a. Die eID soll vom Staat herausgegeben werden;
b. Die eID soll auch hochsensitive Anwendungen wie E-Health und Vote électronique unterstützen;
c. Die neue IDK soll in zwei Varianten angeboten werden, eine rein konventionelle und eine mit Chip mit elektronisch gespeicherten biometrischen Daten und eID-Funktionen.

Aus gesetzestechnischer und systematischer Sicht stellte sich die Frage, ob die neuen Gesetzesbestimmungen für die eID in das Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG; SR 143.1) integriert werden sollen oder ob sie einen eigenständigen Erlass bilden sollten. Im Hinblick darauf, dass die eID-Funktion künftig allen Einwohnerinnen und Einwohnern der Schweiz zugänglich sein soll, und darum – wenn auch in separaten Projekten – künftig insbesondere auch in den verschiedenen Ausländerausweisen enthalten sein könnte, entschied man sich für ein separates eID-Gesetz.

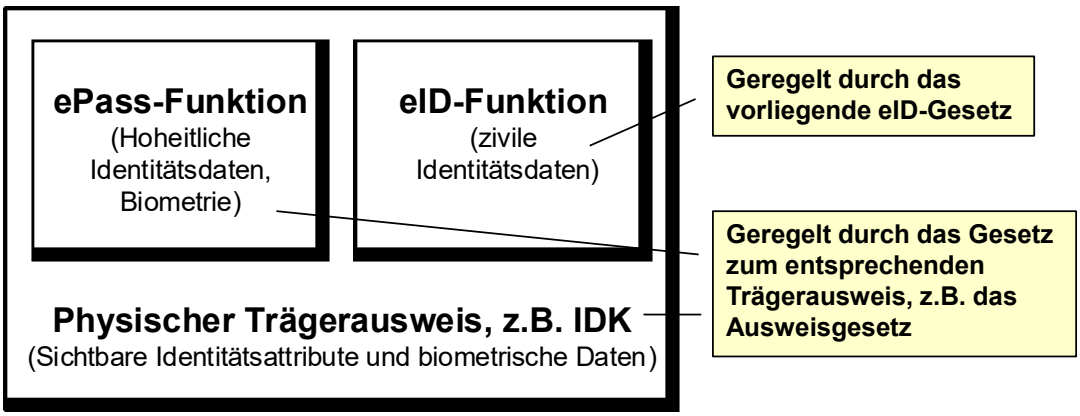
Zurzeit soll die eID im Auslängerausweis noch nicht integriert werden. Im Folgenden werden deshalb die verschiedenen Themen und Fragestellungen aus der Sicht der ersten Einführung der eID – zusammen mit der neuen Identitätskarte – geschildert.

1.3 Konzept und Funktion der eID

Die IDK gilt als Nachweis des Schweizer Bürgerrechts und der Identität (Art. 1 Abs. 2 AwG) und wird regelmässig für vielfältige Identifizierungszwecke eingesetzt. Ziel dieser neuen und erweiterten Konzeption der IDK ist es, die bisherigen ‚konventionellen' Funktionen der IDK um elektronische Funktionen zu ergänzen, so dass die Karte in gleicher Weise als Ausweis in physischen wie elektronischen Kontakten eingesetzt werden kann. Der Bezug einer eID wird jedoch freiwillig bleiben und Bürgerinnen und Bürgern können jederzeit auch eine herkömmliche IDK ohne Chip und eID beantragen.

Aufgedruckt auf der physischen Identitätskarte sind bereits heute eine Reihe von zivilen personenbezogenen Attributen wie Name, Geburtsdatum, Nationalität und Heimatort zusammen mit biometrischen Daten wie Gesichtsbild, Schriftzug der Unterschrift, Geschlecht und Körpergrösse. Dies alles sind Attribute, die für hoheitliche Authentifizierungen zum Beispiel im Reiseverkehr aber auch in Geschäftsprozessen wie zum Beispiel der Eröffnung eines Bankkontos oder dem Abschluss eines Natel-Abos verlangt werden. Auch die neuen elektronischen Funktionen der IDK sollen sowohl die Funktionen der Identitätskarte als digitales Reisedokument unterstützen (ePass-Funktion) als auch die Identifizierung und Authentifizierung

im elektronischen Geschäftsverkehr ermöglichen (eID-Funktion). In der elektronischen Welt hingegen wird die hoheitliche ePass-Funktion klar von der eID-Funktion getrennt. Die neue IDK beinhaltet somit drei Funktionen: Klassischer physischer Identitätsausweis, digitales Reisedokument (ePass) und elektronisches Identifikationsmittel (eID).



Während die gespeicherten Identitätsdaten der ePass-Funktion durch die internationalen Regeln der ICAO eindeutig bestimmt sind, hat jedes Land für die Festlegung der eID-Funktion und die Definition der Nutzungsszenarien innerhalb der auf europäischer Ebene vorgeschlagenen Industrienorm (European Citizen Card – ECC, CEN/TS 15480) einen gewissen Spielraum, der für die Schweiz mit dem vorliegenden Vorentwurf definiert wird. Die personenbezogenen Attribute der schweizerischen eID sind:

- amtlicher Name und Vornamen
- Geburtsdatum und Geburtsort
- Nationalität
- Sozialversicherungsnummer

Daneben sind in der eID weitere Parameter mit Angaben zur Antragstelle, zur Gültigkeit und Prüfzahlen für die Sicherheit gespeichert.

Zusätzlich enthält die eID auch einen Code, der die Erstellung eines Pseudonyms ermöglicht, das für jeden Dienst unterschiedlich definiert wird. Diese Pseudonymitätsfunktion schützt die Person vor unerwünschter digitaler Verfolgung (Profiling) über mehrere unabhängige Dienste hinweg. Die eID-Funktion erfüllt damit ein wichtiges Anliegen des Datenschutzes und des Schutzes der Privatsphäre.

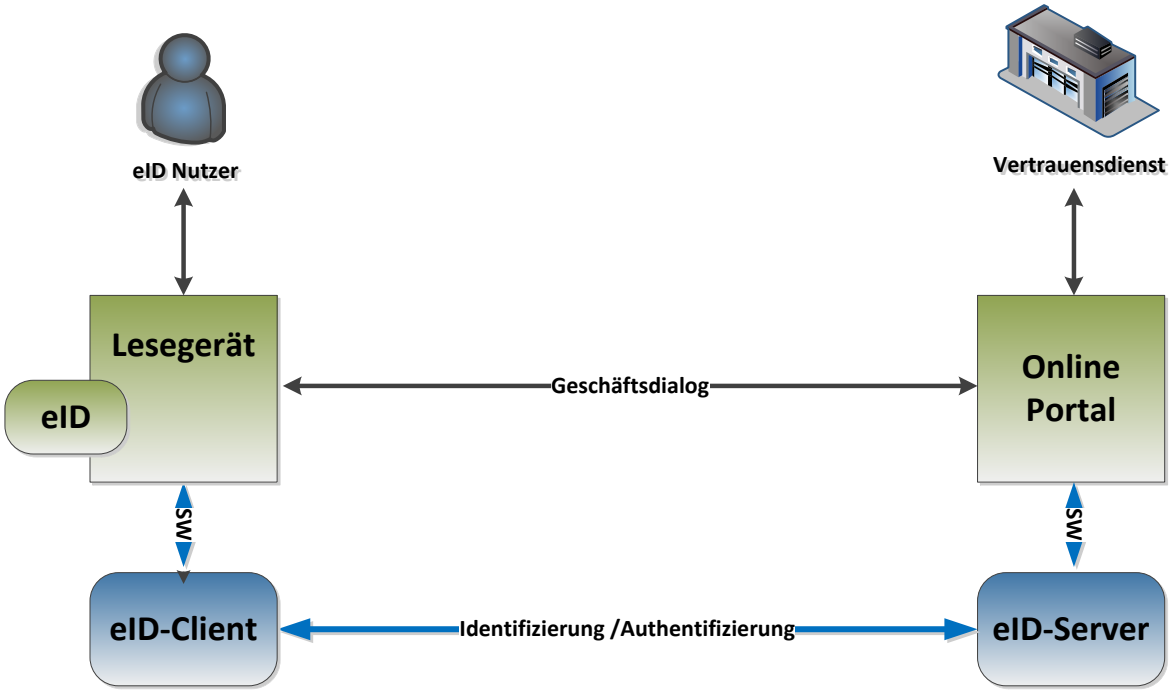
Bei der Konzeption der Nutzungsszenarien wurde die Anwenderfreundlichkeit als wichtigste Anforderung gesetzt, damit der neue Ausweis auch im elektronischen Geschäftsleben rasch eine weite Verbreitung erreichen kann und so der Volkswirtschaft einen möglichst grossen Nutzen bringt. Die eID soll in vielfältigen Umgebungen, sowohl zuhause am Heimcomputer, unterwegs mit mobilen Lesegeräten aber auch an Eintrittsbarrieren bei Veranstaltungen oder im ÖV einfach einsetzbar sein.

Entscheidend für die Entwicklung der digitalen Gesellschaft und für die Akzeptanz von elektronischen Kontakten und Transaktionen sind das Vertrauen der Geschäftspartnerinnen und -partner untereinander und die Transparenz der elektronisch unterstützten Abläufe. Die Identifizierung und die Authentifizierung mittels einer staatlich garantierten eID sowie die Kommunikation über sichere Medien sind wesentliche Voraussetzungen, um das Vertrauen und die Akzeptanz in der Bevölkerung zu generieren. Der geplanten eID wird hier eine entscheidende Rolle zukommen.

Wie bei einem physischen Kontakt von Geschäftspartnerinnen und -partner im normalen Geschäftsleben müssen auch im elektronischen Geschäftskontakt bei einer Identifizierung gewisse zivile Identitätsattribute in vertrauenswürdiger Weise mitgeteilt werden können. Dies geschieht mit Hilfe der eID, die eine Überprüfung der Identitätsattribute oder in gewissen Situationen sogar direkt ein Auslesen der Attribute aus der eID ermöglicht. Selbstverständlich sind solche Identitätsdaten schützenswert und die Inhaberin oder der Inhaber muss immer die volle Kontrolle haben, ob, wann und welche Daten mitgeteilt und durch die eID garantiert werden. Die Überprüfung oder direkte Übermittlung von solchen Daten erfolgt deshalb immer nur, wenn die Karteninhaberin oder der Karteninhaber ihre resp. seine Karte an einem Lesegerät willentlich einsetzt und mit der Eingabe einer Geheimzahl (PIN) bestätigt, dass sie oder er damit einverstanden ist.
In vielen Fällen und insbesondere im mobilen Geschäftsverkehr ist es jedoch oft nicht nötig, eine Person bei jedem Kontakt neu zu identifizieren. Es genügt meistens festzustellen, dass es sich um eine bekannte Person handelt, die sich in einem früheren Erstkontakt bereits identifiziert und beim Dienst unter einem Nutzername registriert hatte. Auch in diesem Fall kann die eID die bei jeder Anmeldung notwendige Authentifizierung mit Hilfe eines Pseudonyms, das nur vom berechtigten Dienst interpretiert werden kann, in vertrauenswürdiger Weise leisten.
In gewissen Fällen genügt sogar die anonyme Feststellung einer Eigenschaft wie zum Beispiel ein (gesetzliches) Mindestalter, ein Aufenthaltsrecht oder sogar die Feststellung, dass die Person einen Ausweis hat. Die eID kann auch in dieser Situation eine verbindliche Bestätigung liefern. In all diesen letztgenannten Fällen genügt es, die Identitätskarte mit der eID kurz an das Lesegerät zu halten, um die Bestätigung zu erbringen. Obschon die eID zum Beispiel im Vergleich mit anderen elektronischen Ausweisen im Gebrach deutlich vereinfacht und im Anwendungsbereich wesentlich verbreitert ist, wird der Schutz und die Sicherheit der Daten genauso gewährleistet.

Sowohl die Identifizierung bei der elektronischen Geschäftsabwicklung, als auch die einfache pseudonyme oder sogar anonyme Authentifizierung im täglichen Leben eröffnen eine Reihe von nutzbringenden und kostensparenden Anwendungen für natürliche Personen, Wirtschaft und Verwaltung. Dies wird nachfolgend durch ein paar konkrete Beispiele illustriert:
Eine elektronische Anwendung, welche mit der eID in Zukunft ermöglicht wird, ist die elektronische Zugangskontrolle zu einer Veranstaltung. Der Inhaber löst im Internet ein Ticket und identifiziert sich mit seiner eID. Die Veranstalterin erhält von der eID ein nur ihr bekanntes Pseudonym. Beim Zutritt zur Veranstaltung authentifiziert sich der Inhaber mit seiner eID am Terminal der Eingangskontrolle und die Veranstalterin weiss dann genau, welches Ticket vom Besucher gelöst wurde und welche Berechtigung damit verbunden ist. Dasselbe Szenario kann auch auf jede Art von Abonnementsdiensten angewendet werden. Durchaus denkbar ist es auch, dass das Lösen von individuellen Tickets im öffentlichen Verkehr genauso abgewickelt wird. Der Fahrgast registriert sich beim zuständigen Internet Portal und kann dann jeweils durch Vorweisen seiner eID an einem Lesegerät auf dem Bahnsteig oder direkt im Zug das Ticket bis zum Zielort lösen, wo er sich auf die gleiche Weise abmeldet. Für Veranstalterinnen und Dienstanbieter werden sich die notwendigen Startinvestitionen rechnen, weil sie selbst keine Trägermedien mehr ausstellen müssen.
Ein anderes Anwendungsbeispiel ist der Finanzbereich. Hier muss beispielsweise eine Neukundin heute noch persönlich am Schalter vorsprechen und einen staatlichen Ausweis vorlegen, um ein Konto zu eröffnen. Mit der staatlichen eID könnte die Kontoeröffnung online realisiert werden. Die Bank überprüft die gemeldeten Identitätsattribute der Inhaberin der eID elektronisch und erfüllt damit die regulatorisch verlangte Kundenidentifizierung. Für die Nutzerin vereinfacht sich das Anmeldeverfahren deutlich.

Die Integration eines Chips mit der eID in die neue IDK ist natürlich nicht ausreichend, um eine sinnvolle Nutzung des elektronischen Identifikationsmittels zu ermöglichen. Es braucht dazu eine umfassendere Infrastruktur, die den Aufbau einer transparenten und sicheren Kommunikation zwischen der eID der Inhaberin oder des Inhabers mit dem Identitäts- und Zugang-Management-Systems einer Dienstanbieterin oder eines -anbieters ermöglicht. Zu dieser Infrastruktur gehört ein Lesegerät, das auf der einen Seite über die Luftschnittstelle mit der eID (NFC-Technologie[3]) Verbindung aufnimmt und auf der anderen Seite über das Internet mit einem eID-Server verbunden ist. Der eID-Server führt im Auftrag des Identitäts- und Access-Management-Systems der Dienstleisterin die notwendigen Sicherheitsprotokolle für eine Authentifizierung oder Identifizierung aus. Der eID Server kann direkt vom vertrauenden Dienst oder von einer zwischengeschalteten Dienstleisterin betrieben werden.



Diese einfache operative Systemarchitektur stützt sich auf ein Hintergrundsystem, das vom Staat erstellt und betrieben wird. Das fedpol ist verantwortlich für die Spezifikation der Eigenschaften des Trägerchips und dessen Integration in den physischen Trägerausweis, das Laden der Identitätsdaten, die abgesicherten Ausgabe an die Inhaberin oder den Inhaber und die Sperrung von verlorenen oder gestohlenen eIDs. Ebenfalls Aufgabe von fedpol ist die Bereitstellung bzw Delegation der digitalen Sicherheitsfunktionen, der kryptographischen Zertifikate und der dazugehörigen Sicherheitskette. All diese Aufgaben sollen so weit als möglich von den bereits heute bestehenden staatlichen Strukturen für die Verwaltung der Pässe und IDKs sowie weiterer staatlicher Ausweise erbracht werden. Die spezifischen, mit der eID neu entstehenden Aufgaben werden von einem Kompetenzzentrum beim fedpol durchgeführt und koordiniert. Das eID-Kompetenzzentrum organisiert die Herstellung und Auslieferung der Ausweise mit eID an die kantonalen und kommunalen Behörden, die weiterhin die direkten Ansprechpartner für die Bürgerinnen und Bürger sind, die eine neue IDK mit eID erhalten wollen. Zusätzlich garantiert das Kompetenzzentrum den permanenten Support für Fragen und Probleme, die bei der Nutzung der eID auftreten können. Weiter organisiert das Kompetenzzentrum die Registrierung der Dienste, die die eID nutzen wollen,

[3] Die sog. Near Field Communication (abgekürzt: NFC) ist ein internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten per Funktechnik über kurze Strecken von wenigen Zentimetern.

und den damit verbundenen Bezug der Berechtigungszertifikate. Ebenfalls Aufgabe des Kompetenzzentrums ist die Organisation der Sicherheitsmassnahmen zum Schutz vor Missbrauch, die natürlich dem Standard eines staatlich garantierten Identifikationsmittels entsprechen müssen.

An dieser Stelle ist zu erwähnen, dass bei der Konzeption der eID bewusst darauf verzichtet wurde, auch eine Signaturanwendung zu integrieren. Diese Funktion kann durch private Dienstleisterinnen und Dienstleister ergänzend zur eID erbracht werden. Bereits heute ist mit der SuisseID ein solches Identifikationsmittel mit qualifizierter elektronischer Signatur auf dem Markt. In Zukunft wird die SuisseID auch direkt online bestellt werden können, wenn sich die zukünftige Nutzerin oder der Nutzer mit ihrer resp. seiner eID identifiziert. Die eID kann auch Basis für den Betrieb von zusätzlichen Identitätsdiensten werden. Zum Beispiel können elektronisch konsultierbare Berufsregister, Stimmrechtsregister oder Patientendossiers mit Hilfe des staatlich garantierten Identitätsnachweises der eID abgesichert und verwaltet werden.

1.4 Ziele des Gesetzesentwurfs

Hauptziele des Gesetzesentwurfs bzw. der eID sind:

- den **sicheren elektronischen Geschäftsverkehr** unter **Privaten und Behörden** zu fördern; und
- die **Standardisierung und Interoperabilität im Bereich der eID auf nationaler und internationaler Ebene** sicherzustellen.

*Die eID trägt dazu bei, den **sicheren elektronischen Geschäftsverkehr** unter **Privaten und Behörden** zu fördern.*
Es wird immer wichtiger, die eigene Identität oder bestimmte Merkmale (Alter, Nationalität usw.) auch elektronisch verlässlich nachweisen zu können. Beispiele für solche Dienstleistungen sind Bezüge von amtlichen Dokumenten wie Geburtsscheine oder Strafregisterauszüge (E-Government), Warenbestellung mit Altersnachweis (E-Business), Banktransaktionen (E-Banking) und zukünftig Zugriffe auf elektronische Patientendossiers (E-Health) und Abstimmungen (Vote électronique).
Der IDK und der eID ist gemeinsam, dass sie eindeutig und insbesondere vertrauenswürdig einer konkreten Person zugeordnet sein müssen. Bei der Beantragung einer IDK erfolgt eine sorgfältige Überprüfung der Identität der antragstellenden Person durch die Behörden, wodurch dieses Vertrauen geschaffen wird. Es ist naheliegend, diesen Identifikationsprozess auch für ein elektronisches Identifikationsmittel mit zu verwenden, das zusammen mit der IDK bezogen werden kann.

*Die eID trägt dazu bei, die **Standardisierung und Interoperabilität im Bereich der eID auf nationaler und internationaler Ebene** sicherzustellen.*
Die eID ist nur *eine* Komponente in einem umfassenderen eID-Ökosystem. Damit die eID später auch nutzbringend eingesetzt werden kann, müssen eine ganze Reihe weiterer Infrastruktur-Komponenten und insbesondere entsprechende Online-Anwendungen bereitgestellt werden. Teile davon können der Privatwirtschaft überlassen werden; der Staat muss aber ebenfalls weitere Beiträge leisten, namentlich:

1. die Koordination bei der Konzeption und Einführung eines gesamtschweizerischen eID-Ökosystems, das mit den in Entwicklung begriffenen IAM[4]-Konzepten des Bundes und der vorstehend erwähnten EU-Verordnung abgestimmt ist;
2. den Ausbau aller geeigneten staatlichen Dienste zu Online-Diensten (z.B. Handelsregister, staatliche Berufsregister, Einreichung Steuererklärung); sowie
3. die Koordination und Förderung einer breiten Palette von privaten Dienstleistungen mit starker elektronischer Authentifizierung sowie weiterer Vertrauensdienste.

Diese Arbeiten können nicht im Rahmen des vorliegenden Projekts des EJPD abgewickelt werden und müssen vom Bundesrat im Rahmen eines neuen, grösseren Projektes gesondert in Auftrag gegeben werden.

International besteht aktuell noch kein etablierter eID-Standard[5]. Innerhalb der EU existieren unterschiedliche Lösungen nebeneinander. Nichtsdestotrotz enthält im EU-Raum beinahe jede in den letzten Jahren neu herausgegebene IDK auch eine eID-Funktion. Die verabschiedete EU-Verordnung zu eID und Vertrauensdiensten geht davon aus, dass die Mitgliedstaaten ein System für den elektronischen Identitätsnachweis unter staatlicher Kontrolle bereitstellen. 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 wird in diesem Bereich Konformität und Kompatibilität mit dem europäischen Umfeld angestrebt (vgl. nachstehend Ziffer 1.5).

1.5 Staatliche elektronische Identifikationsmittel im internationalen, insbesondere europäischen Umfeld

Die Schweiz befindet sich mit der Einführung eines elektronischen Identifikationsmittels nicht allein. In einer soeben verabschiedeten EU-Verordnung zu eID und Vertrauensdiensten[6] und mit entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das geplante eID-System richtet sich an diesen internationalen Vorgaben aus, so dass die schweizerische eID auch im internationalen Kontext eingesetzt werden kann.

1.5.1 Situation in anderen Ländern

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 Identitätskarte mit eID 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 Identitätskarte mit eID eingeführt, sind daran sie einzuführen (Italien, Luxemburg) oder planen mindestens eine solche (Frankreich).

---

[4] Identity and Access Management

[5] Der internationale Standard ISO/IEC 24727 definiert für den sicheren Gebrauch von kontaktlosen Chipkarten eine Referenzarchitektur, die für die Technologie der schweizerischen eID wegweisend ist.

[6] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, COM(2012)238final. Verabschiedet vom Europäischen Parlament am 3. April 2014 (Dokument P7_TA-PROV(2014)0282).

In den letzten Jahren haben insbesondere Länder im Nahen Osten und in Asien neue staatliche Identitätskarten mit eID-Funktion eingeführt. Hingegen planen weder die USA noch das Vereinigte Königreich eine staatliche eID, was sich mit der generellen Skepsis gegenüber Identitätskarten in diesen Ländern deckt.

Im Unterschied zum international stark standardisierten elektronischen Reisepass sind Identitätskarten mit eID heute noch sehr unterschiedlich ausgestaltet. In der Anfangszeit bestanden sie aus dem klassischen Sichtausweis gemäss den Spezifikationen der Internationalen Zivilluftfahrtorganisation ICAO, ausgestaltet als Chipkarte mit zwei Schlüsselpaaren je für die eID-Funktion und die elektronische Signatur. Aktuelle Entwicklungen respektieren mehrheitlich den ECC-Standard (European Citizen Card) und enthalten die ePass-Funktion gemäss ICAO, sowie eine an die ePass-Funktion angelehnte Funktion für die elektronische Online-Identifikation. Schweden, Monaco, Lettland, Finnland (2. Auflage), die Niederlande, Deutschland sowie weitere Länder haben solche Identitätskarten. Die konkrete Ausgestaltung im Detail variiert aber noch stark, bzw. entwickelt sich weiter, sowohl bezüglich der verfügbaren Funktionen wie auch bezüglich der technischen Details.

1.5.2 Europäische Harmonisierung und Interoperabilität

Ist schon für den klassischen Sichtausweis die internationale Verwendbarkeit wichtig, trifft dies erst recht für die eID zu. Als Online-Ausweis wird diese auf dem von Natur aus grenzenlosen Internet eingesetzt. Für die EU, die sich der Realisierung eines schrankenlosen einheitlichen europäischen Binnenmarktes verpflichtet hat, ist dieses Anliegen besonders wichtig. Da sie keine Kompetenz besitzt, die Ausweise für Staatsangehörige zu reglementieren, hat sie vorerst die Aufenthaltspapiere für Drittstaatenangehörige detailliert standardisiert. Auch die Schweiz hat diesen Standard im Rahmen der Schengen-Weiterentwicklung übernommen. In einem zweiten Schritt ist die EU nun daran, die länderübergreifend besonders wichtige und von der ICAO nicht standardisierte eID-Komponente der Identitätskarten der Mitgliederländer im Hinblick auf Realisierung des Binnenmarktes in rechtlicher, organisatorischer und technischer Hinsicht zu harmonisieren.

Nebst dem technologischen Rahmen für die Anwendungsumgebung von eID Karten, der durch die ISO/IEC Standards 14443[7] und 24727[8] abgesteckt wird, sind aktuell die drei nachstehend beschriebenen Normierungs-Vorhaben im Kontext von Identitätskarte und eID auf europäischer Ebene von besonderer Bedeutung. Wobei das erste und älteste Vorhaben die elektronischen Komponenten der Ausweise technisch spezifiziert, die zweite und jüngste die rechtlichen und organisatorischen Aspekte der Interoperabilität regelt, und die dritte die internationale eID-Interoperabilität primär in konzeptioneller und technischer Hinsicht lösen soll.

1.5.2.1 Standardisierung einer European Citizen Card (ECC)

Nachdem die ersten europäischen Länder ihre elektronischen Identitätskarten zwar ähnlich aber doch unterschiedlich aufgebaut hatten, wurde schon vor etwa 10 Jahren 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) definiert eine hochsichere Chipkarte, die im Alltag national und grenzüber-

[7] Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[8] Identification cards – Integrated circuit card programming interfaces

schreitend für den Nachweis der Identität zur sicheren Nutzung von Online-Diensten eingesetzt werden kann.

In seinen aktuell fünf 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.

Der ECC-Standard konnte sich noch nicht als eigentliche Referenz für eine staatliche eID-Karte durchsetzen. Das mag daran liegen, dass er einerseits verschiedene Variationen von Technologien ermöglicht, andererseits eine aktuelle eID nicht vollständig spezifiziert ist.

1.5.2.2 EU-Verordnung über Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)

Am 3. April 2014 hat das Europäische Parlament den Vorschlag der Kommission für eine Verordnung über Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (COM(2012)0238) in erster Lesung behandelt und verabschiedet (Dokument P7_TA-PROV(2014)0282).

Nebst der Regelung und Zertifizierung der Anbieterinnen und Anbieter der elektronischen Signatur und weiterer Vertrauensdienste in der Art der bisherigen Richtlinie enthält die neue Verordnung in den Artikeln 6 ff. als besonderes und neues Thema die Notifikation und damit gegenseitige Anerkennung von staatlichen Systemen für die elektronische Identifizierung (eID bzw. Authentifizierung). Im Kern werden 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 eIDAS-Verordnung bildet die rechtliche Grundlage für den länderübergreifenden eID-Einsatz, den das schon länger existierende und nachstehend in Ziffer 1.5.2.3 beschriebene Projekt STORK entwickelt. Nach heutiger Planung soll die eIDAS-Verordnung Mitte 2016 in Kraft treten, zusammen mit umfangreicher Umsetzungs-Gesetzgebung auf tieferer Stufe.

Selbstverständlich gibt es für die Schweiz keine rechtliche Verbindlichkeit zur Übernahme der EU-Verordnung. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern wird aber davon ausgegangen, dass die Schweiz ein Interesse daran hat, früher oder später in das europäische System für die Interoperabilität von elektronischen Identitäten eingebunden zu sein. Dies würde es ermöglichen, dass einerseits Inhaberinnen und Inhaber einer schweizerischen eID mit ausländischen Behörden verkehren können, und andererseits Ausländerinnen und Ausländer mit ihrer nationalen eID sicher mit Schweizer Behörden verkehren können. Auch wenn vorläufig offen ist, ob, wann und wie die Schweiz sich staatsvertraglich in dieses System einbinden wird, soll das schweizerische eID-System von Beginn an so konzipiert werden, dass es grundsätzlich notifiziert werden könnte.

1.5.2.3 EU-Projekt STORK für 'Sichere Elektronische Identität in Europa'

STORK (**S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed) ist ein EU-Projekt zur grenzüberschreitenden Authentifizierung mit staatlichen elektronischen Identifikationsmitteln. STORK soll es ermöglichen, dass eine Person von ihrem Heimatland aus, bzw. mit der Authentifizierung 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-Go-

vernment-System und die STORK-Funktionalität auch dem ausländischen STORK-integrierten System gegenüber authentifizieren. Der regulatorische Rahmen für den späteren Betrieb dieser europäischen eID-Interoperabilität wird durch die vorstehend beschriebene eIDAS-Verordnung bereitgestellt.

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

Nach dem ersten STORK-Projekt von 2008 bis 2011 läuft aktuell das Nachfolgeprojekt STORK2. Es ist auf den internationalen Nachweis von Funktionen (z.B. Beamtin, Notar, Ärztin, Firmen-Vertreter) ausgerichtet. An diesem zweiten Projekt ist auch die Schweiz beteiligt. Sie wird vertreten durch die Berner Fachhochschule.

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

1.5.3 Der neue elektronische Personalausweis in Deutschland

Deutschland hat im Jahr 2010 eine neue elektronische Identitätskarte unter dem Namen elektronischer Personalausweis (ePA) eingeführt, dem sogenannten «neuen Personalausweis» mit «Online-Funktion».

Der neue deutsche Personalausweis ist eine vom Staat ausgegebene Identitätskarte, ausgestaltet als klassisches Dokument für den Nachweis von Identität und Staatsangehörigkeit, mit den ePass-Funktionen nach ICAO, einer eID-Funktion und Platz für eine optionale qualifizierte elektronische Signatur. Darüber hinaus weist er ein paar zusätzliche Qualitäten, Funktionen und Verbesserungen auf, namentlich:

- Alle Applikationen, Geräte (Leser) und Zertifikate wurden durch das deutsche Bundesamt für Sicherheit in der Informationstechnik streng spezifiziert und reguliert.
- Die elektronische Ausweis-Funktion (eID-Funktion) ist beim Bezug standardmässig eingeschaltet, kann aber von der Benutzerin oder vom Benutzer deaktiviert werden.
- Alle Dienstanbieterinnen und -anbieter (Service Provider) müssen sich gegenüber der eID-Komponente authentifizieren und die Berechtigung für den Bezug bestimmter Attribute nachweisen, wozu sie vorgängig bei einer Behörde ein kostenpflichtiges Bewilligungsverfahren durchlaufen müssen.
- Gegenseitige Authentifizierung zwischen Chip und Lesegerät mittels eines neu entwickelten Verfahrens namens PACE (Password Authenticated Connection Establishment).
- Restricted Identity: Ein Pseudonymitätsfunktion, 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. Diese Funktion stellt zugleich eine wichtige Voraussetzung für den Einsatz einer eID im Vote électronique dar.

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

tegie hat Deutschland dafür gesorgt, dass die Aufenthaltstitel für Ausländerinnen und Ausländer mit kompatiblen «Online-Ausweisfunktionen» ausgestattet sind.

Per Frühjahr 2014 sind etwa 25 Mio. neue Personalausweise ausgegeben, wovon ca. 1/3 die eID-Funktion aktiviert haben. Deutschland hat mit viel Aufwand und Budget auch die Anwendung der eID-Funktion in E-Government und E-Commerce gefördert. Obwohl es insgesamt schon über 200 private und öffentliche Dienstanbieterinnen und -anbieter gibt, wird der noch bestehende Mangel an Anwendungsmöglichkeiten als kritisch für den Erfolg angesehen.

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 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 Dienstanbieterin oder -anbieter zu aufwendig und zu teuer sei.

2 Erläuterungen zu den einzelnen Bestimmungen

2.1 Struktur

Der Gesetzesentwurf weist folgende **Struktur** auf:

- Der 1. Abschnitt des Gesetzesentwurfs enthält die **allgemeinen Bestimmungen** wie Regelungsgegenstand sowie Begriffe und regelt den **Inhalt der eID.**
- Im 2. Abschnitt werden die **Rechte und Pflichten der Inhaberinnen und Inhaber der eID** geregelt. Es wird unter anderem vorgeschrieben, wie sich die Inhaberinnen und -Inhaber der eID bei Verlust oder Diebstahls eines Ausweises mit eID zu verhalten haben und welche Sorgfaltspflichten im Allgemeinen zu beachten sind. Weiter wird die Einsicht in die eID geregelt.
- Der 3. Abschnitt enthält Bestimmungen zur **Herausgabe und Gültigkeit der eID**. In diesem Zusammenhang wird die für die Herausgabe der eID zuständige Stelle und das eID-Kompetenzzentrum genannt sowie die entsprechenden Prozesse festgelegt.
- Der 4. Abschnitt bestimmt die **Verwendung der eID**. Es wird insbesondere aufgelistet, welche Funktionen die eID zur Verfügung stellt. Weiter sind in diesem Abschnitt Vorschriften zum Auslesen der Daten zu finden.
- Der 5. Abschnitt bestimmt den Umgang mit **Berechtigungszertifikaten.** Neben Rechten und Pflichten der vertrauenden Dienste wird die für die Herausgabe von Berechtigungszertifikate zuständige Stelle genannt und deren Aufgaben erläutert.
- Der 6. Abschnitt enthält schliesslich die **Schlussbestimmungen.**
- Die **Änderung anderer Erlasse** ist in einem Anhang geregelt.

2.2 eID-Gesetz

1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Zweck und Gegenstand

Absatz 1 Buchstabe a, b und c

Die drei Buchstaben nennen je einen Kreis von Norm-Adressaten, den Herausgeber, die Inhaberinnen und Inhaber der eID, sowie die der eID vertrauenden Dienste.
Buchstabe a zeigt zudem auf, dass sich eine eID auf verschiedenen vom Bund herausgegebenen Ausweisen befinden kann. In erster Linie ist das die Identitätskarte, später sollen die Ausländerausweise dazu kommen, und von der Konzeption her könnten auch weitere Ausweise, wie beispielsweise der Pass oder der Führerausweis, damit ausgerüstet werden.

Absatz 2 Buchstabe a

Die eID trägt dazu bei, ein System von Sicherheit und Vertrauen im elektronischen Geschäftsverkehr (E-Business und E-Government) aufzubauen. Schweizerinnen und Schweizer sollen sich zukünftig auch in der elektronischen Welt vertrauenswürdig ausweisen können. Genau wie mit einem Identitätsausweis in der physischen Welt, können damit gewisse, nicht biometrische Identitätsattribute einer Person, wie zum Beispiel Nationalität, Name, Vorname oder Alter (vgl. Art. 3 und 11), in der Online-Welt nachgewiesen werden. Der Hauptnutzen einer eID besteht darin, dass sie vertrauenswürdige Online-Geschäfte wie E-Government oder E-Business ermöglicht, ohne dass sich die Partnerinnen und Partner physisch treffen müssen. Damit der elektronische Geschäftsverkehr unter Privaten und Behörden sicher abgewickelt werden kann, muss die eID im Hinblick auf den Datenschutz Anforderungen der höchsten Qualitäts- und Sicherheitsstufe erfüllen.

Absatz 2 Buchstabe b

Die eID trägt dazu bei, den Übergang der Schweiz zu einer entwickelten Informationsgesellschaft zeitgerecht und gut zu schaffen. Dies gelingt durch die Übernahme der geltenden Standards auf internationaler Ebene, die eine Interoperabilität bei der Anwendung der eID sicherstellen.

Artikel 2 Begriffe

Bei der Wahl der Terminologie musste einerseits auf die aktuelle Regelung der Ausweisschriften, insbesondere das Ausweisgesetz Rücksicht genommen werden. Neue Begriffe wurden so gut wie möglich mit den Regelungen der EU und der umliegenden Länder abgeglichen.
Einige terminologische Klärungen waren notwendig, weil sich eine eID nach diesem Gesetz grundsätzlich auf irgendeinem mit einem Chip versehenen Ausweis befinden kann. Dieser im Prinzip beliebige herkömmliche Ausweis, auf dessen Chip die eID geschrieben wird, heisst 'Trägerausweis', die dafür verantwortliche Behörde 'Antragstelle' (Art. 2 Bst. h). Die für die eID verantwortliche Behörde wird 'Herausgeber der eID' genannt (Art. 7).

Artikel 3 Inhalt der eID

Die eID enthält die folgenden Identitätsattribute (Abs. 1), die auch schon auf der existierenden IDK enthalten sind:
- Name und Vornamen;
- Geburtsdatum;
- Nationalität;

- Antragstelle;
- Datum der Ausstellung (identisch mit dem Datum der Ausstellung der physischen Karte, dem Trägerausweis);
- Datum des Ablaufs (identisch mit dem Datum des Ablaufs der physischen Karte);
- Nummer und Art des Trägerausweises.

Hingegen soll auf der eID der Geburtsort anstelle des Heimatorts als Identitätsattribut verzeichnet werden. Das entspricht der internationalen Praxis.
Zusätzlich soll auf der eID auch die Sozialversicherungsnummer als unverwechselbarer Identifikator für alle Personen, die eine eID erwerben können, enthalten sein.

Auf Verlangen kann die eID zusätzlich Allianz-, Ordens-, Künstler- oder Partnerschaftsnamen enthalten (Abs. 2).

Zusätzlich enthält die eID eine Reihe von Sicherheitsdaten, die für die Überprüfung der Echtheit und Gültigkeit der eID nötig sind (vgl. Details dazu und zu den Funktionen der eID im Kommentar zu Art. 11).

2. Abschnitt: Rechte und Pflichten der Inhaberinnen und Inhaber einer eID

Artikel 4 Einsicht

Das Recht auf Einsicht in die zentral gespeicherten Daten richtet sich nach den Artikeln 8, 9 und 25 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1). Das entsprechende Einsichtsgesuch ist an den Herausgeber der eID (vgl. Art. 7) zu richten.
Damit die Inhaberin oder der Inhaber einer eID jederzeit die korrekte Funktion der eID prüfen und die auf dem Chip gespeicherten Daten einsehen kann, werden die Antragstellen (vgl. Art. 2 Bst. h) durch den Bund mit einem sicheren und zertifizierten Lesegerät mit integrierter Anzeige und Tastatur ausgerüstet. Allenfalls könnten zusätzlich die im ePass-Bereich bereits vorhandenen Public Reader Stationen mit dieser Funktionalität erweitert werden.

Artikel 5 Meldepflicht

Absatz 1

Verlust oder Diebstahl einer IDK mit eID richtet sich beispielsweise nach Artikel 8 Ausweisgesetz. Für andere Ausweise sind die entsprechenden Bestimmungen anwendbar.

Absatz 2 und 3

Besteht die Gefahr oder hat die Inhaberin oder der Inhaber den begründeten Verdacht, dass Dritte Zugang zur eID (insbesondere Kenntnis der Geheimzahl) haben könnten, ist unverzüglich der Herausgeber gemäss Artikel 7 zu kontaktieren, damit die eID gesperrt werden kann. Sobald eine eID als gesperrt vermerkt ist, kann sich jeder vertrauender Dienst (vgl. Art. 2 Bst. c) auf einer Sperrliste (vgl. Art. 9 Abs. 2) darüber informieren, dass auf die entsprechende eID nicht mehr zugegriffen werden sollte.

Artikel 6 Sorgfaltspflichten

Die Inhaberin oder der Inhaber haftet bei Verletzung ihrer resp. seiner Sorgfaltspflichten im Umgang mit der eID. Diese Folge ergibt sich aus Artikel 41 OR. Danach haftet eine Person, wenn sie einer anderen widerrechtlich Schaden zufügt. Das Tatbestandsmerkmal «widerrechtlich» ist dann erfüllt, wenn die Sorgfaltspflicht nach Artikel 6 nicht beachtet wird. Im Üb-

rigen ist auf die Bestimmungen des ausservertraglichen Haftpflichtrechts (Art. 41 ff. OR) zu verweisen.

Absatz 1
Die Inhaberin oder der Inhaber hat dafür zu sorgen, dass der Trägerausweis mit eID und der dazugehörigen Geheimnummer Dritten nicht so ausgehändigt wird, dass sie die eID unbeaufsichtigt nutzen können. Zu achten ist darauf, dass keine andere Person Kenntnis von der Geheimnummer erlangt. Die Geheimnummer darf insbesondere nicht auf dem Ausweis vermerkt oder in anderer Weise zusammen mit diesem aufbewahrt werden.

Absatz 2
Die Inhaberin oder der Inhaber haben zumutbare Massnahmen technischer oder organisatorischer Art zu treffen, um eine missbräuchliche Verwendung der eID zu verhindern. Im Schadensfall muss glaubhaft dargelegt werden können, dass die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen sowie nur solche technischen Systeme und Bestandteile eingesetzt wurden, die als für diesen Einsatzzweck sicher bewertet werden. Beispielsweise wäre ein völlig ungesicherter Computer ohne jegliche Anti-Viren-Software jedenfalls als unsicher einzustufen.
Mit verschiedenen Informationsmassnahmen sind die Inhaberinnen und Inhaber der eID im Detail darüber zu informieren, was die Umsetzung der Sorgfaltspflicht in der Praxis bedeutet. Entsprechende Beispiele sind bezüglich Identifikationsmittel für das E-Banking bekannt. Die notwendigen und zumutbaren Sicherheitsvorkehrungen können sich je nach konkret verwendeter Umgebung und Bedrohungslage verändern.

Absatz 3
Wenn die Inhaberin oder der Inhaber einer eID einen Fehler in den Identitätsattributen nach Artikel 3 entdeckt, so hat sie bzw. er diese unverzüglich bei der Antragstelle zu melden. Diese Pflicht gilt ausschliesslich für das Feststellen von Fehlern. Änderungen in den Identitätsattributen nach Artikel 3 (zum Beispiel Namenswechsel aufgrund einer Heirat oder Geschlechtsumwandlung) hat die Inhaberin oder der Inhaber einer eID nicht zu melden. Diese Änderungen erfolgen von Amtes wegen.

3. Abschnitt: Herausgabe und Gültigkeit der eID

Artikel 7 Herausgeber
Das fedpol ist verantwortlich für die Organisation des Lebenszyklus der eID. Zur Erfüllung der anfallenden Aufgaben betreibt das fedpol ein Kompetenzzentrum (vgl. Art. 10). Dieses definiert die Spezifikation und die Vergabe der Herstellung des physischen Trägerausweises mit Chip, organisiert die sichere Aufbringung der elektronischen Daten auf den Chip im Trägerausweis, bestimmt die Verwaltung und Absicherung der kryptographischen Mechanismen und Sicherheitsmassnahmen, die für die Nutzung der eID nötig sind, registriert die berechtigten Dienstleister und liefert diesen Zertifikate, die die Nutzung der eID-Funktion ermöglichen und ist zuständig für die Pflege der zentralen Infrastruktur, die für einen sicheren und nutzerfreundlichen Betrieb gebraucht wird.
Dienstleistungsanbieter, welche die eID-Funktionalitäten bei ihren Portalen und Applikationen integriert haben, müssen jederzeit die Gültigkeit einer eID prüfen können. Dazu wird ein im Internet öffentlich zugänglicher Dienst bereitgestellt. Die Verwendung einer ungültigen oder gesperrten eID kann somit jederzeit festgestellt und durch die Dienstleistungsanbieter zuverlässig verhindert werden. Als dafür gebräuchliches Verfahren (Abs. 2) kann das fedpol

beispielsweise eine sog. Sperrliste führen und öffentlich via Internet und Webservice zugänglich machen.

Artikel 8 Prozess

Für die eID werden ausser der Sozialversicherungsnummer keine zusätzlichen – als die auf dem Ausweis ersichtlichen – Daten erfasst. Deshalb muss der heutige Ausstellungsprozess für Ausweise nicht wesentlich verändert werden. Die Sozialversicherungsnummer soll aus Infostar übernommen oder wie die übrigen Personalien zumindest mit Infostar abgeglichen werden. Die Antragstellerin oder der Antragsteller werden sich neu aber entscheiden müssen, ob sie eine IDK mit oder ohne Chip erhalten möchten. Nur die IDK mit Chip enthält auch die eID-Funktionalität. Da die eID zusammen mit der herkömmlichen IDK beantragt wird, ist jeweils auch die gleiche – vom Wohnsitzkanton zu bezeichnende – Behörde für die Entgegennahme von Anträgen zuständig.
Für die Antragstelle wird sich allenfalls ein kleiner Mehraufwand für die Beratung der Antragstellerin oder des Antragstellers ergeben. Es ist vorgesehen, alle Informationen zur eID auch im Internet und als Flyer bereit zu stellen, so dass die Beratung vor Ort minimiert wird.
Nach der Erfassung und Prüfung der für die Ausstellung notwendigen Daten in den entsprechenden Fachanwendungen (ISA für die IDK) durch die Antragstelle, wird der entsprechende Trägerausweis mit Chip und eID-Funktionalität hergestellt. Danach wird der Trägerausweis der rechtmässigen Inhaberin oder dem rechtmässigen Inhaber abgegeben oder zugestellt. Die Zustellung der für die Nutzung der eID notwendigen Angaben (z.B. initiale Geheimnummer) erfolgt separat.

Absatz 1

Diese Bestimmung verlangt, dass die antragstellende Person und gegebenenfalls ihre gesetzliche Vertretung persönlich bei der Antragstelle erscheinen. Weitere Informationen im Zusammenhang mit der persönlichen Vorsprache sind in Artikel 12 der Verordnung über die Ausweise für Schweizer Staatsangehörige (Ausweisverordnung, VAwG; SR 143.11) zu finden. Die Bestimmungen der Ausweisverordnung sind nötigenfalls anzupassen.
Im Rahmen der persönlichen Vorsprache sind alle Attribute, welche in die eID aufgenommen werden sollen, von der Antragstelle zu prüfen und zu bestätigen. Nur staatlich bestätigbare Attribute können in die eID aufgenommen werden. Angaben zu Allianz-, Ordens-, Künstler- oder Partnerschaftsnamen sind freiwillig (vgl. Art. 3 Abs. 2). Die antragstellende Person ist jedoch verpflichtet, die erforderlichen Nachweise zu erbringen.

Absatz 2

Die eID wird immer zusammen mit einer physischen Karte, dem Trägerausweis, ausgestellt. Damit kann der Ausstellprozess so einfach wie möglich ausgestaltet werden und führt nicht zu einer grossen zusätzlichen Belastung der Antragstelle. Insbesondere können Synergien bei der arbeitsintensiven Erfassung der Antragsdaten genutzt werden.
Wenn beispielsweise ein Kanton bestimmt hat, dass die IDK auch bei der Wohnsitzgemeinde beantragt werden kann, gilt dies selbstverständlich auch für die eID.

Absatz 3

Diese Bestimmung sieht die Möglichkeit vor, für die Ausstellung einer eID eine kostendeckende Gebühr zu erheben. Diese soll zur Deckung des Verwaltungsaufwandes und der Betriebskosten der eID Infrastruktur dienen. Für die Identitätskarte werden die Einzelheiten dazu im 4. Kapitel der Ausweisverordnung zu regeln sein. Dabei ist davon auszugehen, dass auch für eine IDK mit eID kostendeckende und familienfreundlich ausgestaltete Gebühren (vgl. insbesondere Art. 9 Abs. 2 AwG) erhoben werden.

Artikel 9 Gültigkeit, Sperrung und Ungültigkeitserklärung

Absatz 1

Die Gültigkeitsdauer des Trägerausweises richtet sich nach den Vorschriften des Ausweisgesetzes. Gemäss Artikel 3 AwG sind Ausweise befristet gültig. Der Bundesrat regelt die Einzelheiten zur Gültigkeitsdauer in Artikel 5 VAwG. Grundsätzlich werden Ausweise (ordentlicher Pass und die IDK) für Personen, die im Zeitpunkt des Antrages das 18. Lebensjahr zurückgelegt haben, für 10 Jahre ausgestellt. Hat die Person zum Zeitpunkt des Antrags das 18. Lebensjahr nicht zurückgelegt, werden Ausweise (ordentlicher Pass und IDK) lediglich für 5 Jahre ausgestellt.

Absatz 2 bis 4

Die eID teilt das Schicksal des Trägerausweises. Wird dieser z.B. für ungültig erklärt, verliert automatisch auch die eID ihre Gültigkeit (Abs. 2). Umgekehrt ist dies nicht der Fall: Wird nur die eID gesperrt, bleibt der Trägerausweis weiterhin gültig (Abs. 4).
Ungültige eIDs werden in eine öffentlich zugängliche Sperrliste eingetragen. Dieser Eintrag kann auch auf Antrag erfolgen (Abs. 3), wenn beispielsweise die eID nicht mehr benutzt werden können soll. Ein Eintrag in der Sperrliste kann rückgängig gemacht werden und die eID wieder für gültig erklärt werden, solange der Trägerausweis weiterhin gültig ist.

Artikel 10 eID-Kompetenzzentrum

Für die spezifischen, mit der eID neu entstehenden Aufgaben betreibt das fedpol ein Kompetenzzentrum. Das eID-Kompetenzzentrum organisiert die Herstellung und Beschriftung der Trägerausweise mit sichtbaren und elektronischen Daten. Es betreibt auch die notwendigen Schnittstellen zu den kantonalen und kommunalen Behörden, die weiterhin die direkten Ansprechpartner für die Bürgerinnen und Bürger sind, die eine neue IDK mit eID erhalten wollen. Zusätzlich garantiert das Kompetenzzentrum den permanenten Support für Fragen und Problemen, die bei der Nutzung der eID auftreten können.
Dieser Support kann an Dritte delegiert werden (Abs. 2), die beim Erfüllen dieser Tätigkeit insbesondere auch wie Bedienstete des Bundes gemäss Verantwortlichkeitsgesetz haften.

4. Abschnitt: Verwendung der eID

Artikel 11 Funktionen und Anwendungen der eID

Die eID enthält einen Code, der die Erstellung eines Pseudonyms ermöglicht, das für jede Dienstleisterin und jeden Dienstleister unterschiedlich definiert wird (Abs. 1). Die Pseudonymitätsfunktion schützt die Person vor unerwünschter digitaler Verfolgung (Profiling) über mehrere unabhängige Dienste hinweg. Diese Funktion der eID erfüllt damit ein wichtiges Anliegen des Datenschutzes und des Schutzes der Privatsphäre.
Die Mitteilung der Attribute an die überprüfende Stelle kann auf verschiedenen Wegen erfolgen. Ein möglicher Weg ist das direkte Auslesen der Daten aus der eID. Dieser Weg mit Auslesen der eID-Daten wird als Transfermodus (Auslesen von Identitätsattributen; Abs. 2 Bst. e) bezeichnet. Die ausgelesenen Attribute sind bereits durch die Tatsache bestätigt, dass sie direkt von einer als echt festgestellten eID stammen.
In vielen Fällen hat die überprüfende Stelle aber bereits Kenntnis von Identitätsattributen einer Person und möchte diese lediglich bestätigt erhalten. In diesem Fall kann die eID zur Bestätigung der behaupteten Attribute eingesetzt werden. Diese Nutzung der eID wird als Verifikationsmodus (Bestätigung von Identitätsattributen; Abs. 2 Bst. d) bezeichnet.

In gewissen Fällen genügt es der überprüfenden Stelle sogar, wenn festgestellt wird, dass es sich um die gleiche Person handelt, die sich schon früher beim Dienst angemeldet hat. Dies wird als pseudonyme Authentifizierung bezeichnet (Abs. 2 Bst. b).
In wieder anderen Fällen kann es sogar ausreichend sein, festzustellen, dass eine Person eine gültige eID hat. Dies wird dann als anonyme Authentifizierung bezeichnet (Abs. 2 Bst. a).
Oft verlangen Regulierungen oder Geschäftskonditionen die Erfüllung von bestimmten Alterslimiten wie zum Beispiel ein Mindestalter zum Bezug von Alkohol oder für ein vergünstigtes Abonnement. Auch solche Nachweise von abgeleiteten Behauptungen können mit der eID erbracht werden (Abs. 2 Bst. c). Dabei wird von der eID nicht das Geburtsdatum bekanntgegeben, sondern nur die Frage nach einem bestimmten Mindestalter mit ja oder nein beantwortet.

Nach dem Erhalt des Ausweises mit eID und der initialen Geheimnummer kann die Inhaberin oder der Inhaber die eID-Funktionalität in Betrieb nehmen. Als erstes muss mit der initialen Geheimnummer ein vom fedpol betriebenes Portal aufgerufen, dort die Akzeptanz der Nutzungsbedingungen bestätigt und auf dem elektronischen Identifikationsmittel eine neue eigene Geheimnummer festgelegt werden. Diese kann später von der Ausweisinhaberin oder dem Ausweisinhaber jederzeit auf dem gleichen Portal geändert werden. Zusätzlich muss noch die vom Bund auf dem Internet bereitgestellte eID-Applikation heruntergeladen und für den Gebrauch mit älteren Datenendgeräten - eventuell ein zusätzliches auf dem freien Markt erhältliches kontaktloses Standardlesegerät - gekauft werden. Im Normalfall wird der Zugriff mittelfristig auf die eID mit einem NFC-fähigen Endgerät, zum Beispiel ein Smartphone, erfolgen können.

Artikel 12 Auslesen der Daten
Auch wenn der Trägerausweis mit eID über einen kontaktlos auslesbaren Chip verfügt, können und dürfen die darauf enthaltenen Identitätsdaten nicht ohne Wissen der Inhaberin oder des Inhabers ausgelesen werden. Einerseits ist dafür immer ein gültiges Berechtigungszertifikat des berechtigten Dienstes erforderlich (vgl. dazu die nachfolgenden Ausführungen im 5. Abschnitt). Andererseits ist dazu das willentliche Vorweisen der eID an einem Lesegerät und die Eingabe der Geheimnummer auf der Tastatur des Geräts erforderlich, nachdem der vertrauende Dienst die Inhaberin oder den Inhaber der eID dazu aufgefordert hat. Zudem erfolgt die Übertragung der Daten zwischen Karte, Lesegerät und eID-Server verschlüsselt.
Für eine blosse Authentifizierung (Feststellung, dass es sich um eine Person handelt, die sich bereits früher bei einem berechtigten Dienst mit ihrer eID angemeldet und registriert hat) genügt das Vorweisen des Ausweises mit der eID am Lesegerät. Dabei werden aber nur technische Daten über die Gültigkeit der eID und eine einmalige Identifikationsnummer übertragen, die es dem berechtigten Dienst erlaubt, festzustellen, wer diesen Dienst nutzen will und sich dazu vorgängig registriert hat. Diese einfache Authentifizierung erlaubt es, die eID in neuen Nutzungsbereichen wie zum Beispiel als Ticket für den Zugang zu Anlässen oder für den Bezug von Mobilitätsleistungen einzusetzen, ohne dass von der Inhaberin oder vom Inhaber eine umständliche zusätzlich Handlung oder Eingabe verlangt wird. Ohne die vorgängige Registrierung kann ein Dienst aus der Identifikationsnummer keine Rückschlüsse irgendwelcher Art ableiten, aussert, dass eine gültige eID vorhanden ist.
Ebenfalls ohne Eingabe der Geheimnummer kann der Inhaber einer eID gegenüber einem Lesegerät im öffentlichen Raum (zum Beispiel ein Automat für Zigaretten) bestätigen, dass er oder sie eine gewisse Alterslimite erfüllt. Eine solche Altersbestätigung kann pro Vorzeigeakt nur einmal gemacht werden, so dass die Anonymität der Inhaberin oder des Inhabers geschützt bleibt.

Vertraut jemand diesen eingebauten Sicherheitsfunktionen nicht, ist es ein Leichtes, kontaktlos auslesbare Chip eigenhändig gegen jeden Zugriff zu schützen. Dazu genügt es, die Trägerkarte in Alufolie einzupacken oder in ein entsprechendes Etui zu verstauen, wie diese beispielsweise für Bahn-Punktekarten in Wintersportgebieten abgegeben werden.

Absatz 1 und 2
Identitätsattribute nach Artikel 3 dürfen nur mit expliziter Zustimmung abgefragt werden. So weiss die Inhaberin resp. der Inhaber immer genau, wem sie bzw. er die persönlichen Daten und in welchem Umfang anvertraut.
Der vertrauende Dienst legt fest, welche Identitätsattribute angefordert werden sollen. Deren Freigabe ist beispielsweise durch Aktivieren eines entsprechenden Einverständnisfeldes zu bestätigen. Danach muss die eID an einem Lesegerät vorgewiesen werden. Erst wenn aber die korrekte Geheimnummer eingegeben wird, werden die angeforderten Identitätsattribute übermittelt. Die Daten werden verschlüsselt übertragen, sodass ein Mitlesen durch Dritte ausgeschlossen ist.

Absatz 3
Bei jedem Vorweisen der eID an einem Lesegerät wird die Gültigkeit der eID überprüft, wozu die dafür notwendigen Angaben übermittelt werden.
Mit entsprechender Zugriffsberechtigung (gemäss Abs. 1) können auch die in Artikel 3 genannten Identitätsattribute übermittelt werden.

Artikel 13 Verwendung der eID für staatliche Dienste
Nicht jede Nutzung staatlicher Online-Dienste erfordert eine Personenidentifikation und somit den Einsatz der eID (Abs. 1). So wäre es z.B. nicht notwendig und daher nicht verhältnismässig, wenn beim Online-Bestellen einer unpersönlichen Parkkarte ein elektronischer Identitätsnachweis mit der eID verlangt wird.
Gegenüber der staatlichen eID skeptische Kreise hegen die Befürchtung, dass der Staat zuerst ein Mittel für die Identifikation im Internet einführe, später für jede Benutzung des Internets den elektronischen Identitätsnachweis verlange und damit schliesslich ein vollständiges Nutzerprofil jeder Person erhielte, die das Internet benutzt. Diese Bestimmung zeigt auf, dass der Staat keine solchen Absichten hegt.
Zudem soll die Inhaberin oder der Inhaber auch bei einem notwendigen Identitätsnachweis nicht gezwungen werden, unnötige persönliche Informationen preiszugegeben. Dies kann erreicht werden, indem staatliche Online-Dienste immer nur diejenige eID-Anwendung gemäss Artikel 11 Absatz 2 einsetzen, die im konkreten Fall den geringsten Eingriff in die Privatsphäre nach sich zieht (Abs. 2).

5. Abschnitt: Berechtigungszertifikate

Artikel 14 Zuständige Stelle
Damit ein vertrauender Dienst überhaupt die Funktionalität der eID nutzen kann, braucht er gemäss Artikel 16 Absatz 1 ein Berechtigungszertifikat. Nur damit kann er sich gegenüber der eID authentifizieren und die Berechtigung für die Verifikation bestimmter Attribute oder daraus abgeleiteter Behauptungen nachweisen. Der Bundesrat beauftragt das Kompetenzzentrum des fedpol oder gemäss Absatz 1 eine andere Stelle mit Herausgabe und Verwaltung der Berechtigungszertifikate. Dies könnte das Bundesamt für Informatik und Telekommunikation BIT mit der von ihm aufgebauten Swiss Government PKI sein.

Die Aufgaben der oben genannten Stelle sind in Absatz 2 aufgezählt.

Artikel 15 Verfahren

Dienstleistungsanbieter, welche die eID-Funktionalität mit ihren Portalen und Applikationen nützen wollen, müssen sich im Berechtigungsregister eintragen. Das hierzu notwendige Portal wird vom Bund bereitgestellt. Nachdem eine Registrierung dahingehend geprüft wurde, dass es sich um eine gültige UID-Einheit handelt, werden automatisiert zeitlich beschränkt gültige Berechtigungszertifikate an die UID-Einheit versandt.

Berechtigungszertifikate werden nur an sogenannte UID-Einheiten abgegeben. Mit der Verwendung des Begriffs «UID-Einheiten» gemäss Bundesgesetz über die Unternehmens-Identifikationsnummer vom 18. Juni 2010 (UIDG, SR 431.03) werden das Gros der juristischen Personen und auch Behörden erfasst. Damit sind nicht nur die im Handelsregister eingetragenen Rechtsträger (Art. 3 Abs. 1 Bst. c Ziff. 1 UIDG) erfasst, sondern auch andere juristische Personen. Unter den Begriff der «UID-Einheit» fallen insbesondere auch Behörden und Gerichte (Art. 3 Abs. 1 Bst. c Ziff. 7 UIDG). Nicht erfasst von dieser Formulierung wären somit einzig die juristischen Personen, die nicht im UID-Register eingetragen sind, wie beispielsweise nicht eingetragene Vereine und Stiftungen.

Diese hätten hier entweder separat genannt werden müssen, oder sie werden nach der vorliegenden Lösung bewusst ausgeschlossen. Einer juristischen Person, deren öffentliches Profil so schwach ist, dass keiner der Gründe gemäss Artikel 3 Absatz 1 Buchstabe c UIDG für eine Eintragung in das UID-Register gegeben ist, die also z.B. zu keiner Behörde eine Beziehung hat, soll auch keine Berechtigungszertifikate erhalten, um als vertrauender Dienst am elektronischen Geschäftsverkehr teilnehmen zu können.

Mit der Verwendung des Begriffs «UID-Einheiten» ist auch sichergestellt, dass diese bereits mit mindestens einer Behörde im Verkehr steht und identifiziert ist. Damit kann auf ein aufwändiges Zertifizierungsverfahren verzichtet werden.

Artikel 16 Rechte und Pflichten der vertrauenden Dienste

Die Gültigkeit der Berechtigungszertifikate und die darin statuierten Rechte (Datenvalidierung oder Datentransfer) werden durch die eID geprüft und unzulässige Verarbeitungen verhindert: Ohne gültiges Berechtigungszertifikat wird kein berechtigter vertrauender Dienst erkannt und keine Nutzung der eID-Funktionen zugelassen (Abs. 1).

Um die Anwendung der eID und den Aufbau einer einheitlichen IT-Architektur zu erleichtern, stellt der Bund den vertrauenden Diensten Software-Bausteine zur Verfügung. Dieses Software-Development-Kit soll es ermöglichen, die eID-Funktionalitäten rasch und unkompliziert auf Dienstleistungsportalen zu integrieren und in Betrieb zu nehmen.

Die Berechtigungszertifikate dürfen nur für die Authentifizierung gegenüber der eID eingesetzt werden und beispielsweise nicht für andere Signaturzwecke verwendet werden. Zudem hat der vertrauende Dienst durch Sicherheitsmassnahmen, die dem Stand der Technik entsprechen müssen, dafür zu sorgen, dass seine Berechtigungszertifikate nicht von unberechtigten Dritten benutzt werden können (Abs. 2).

6. Abschnitt: Schlussbestimmungen

Artikel 17 Vollzug

Vgl. dazu die Ausführungen in Ziffer 4.3.

Artikel 18 Änderung anderer Erlasse
Vgl. die nachfolgenden Ausführungen in Ziffer 2.3.

Artikel 19 Referendum und Inkrafttreten
Wie jedes Bundesgesetz untersteht auch das neue eID-Gesetz dem fakultativen Referendum und der Bundesrat wird das Datum des Inkrafttretens bestimmen können.

2.3 Änderung anderer Erlasse

2.3.1 Ausweisgesetz

2.3.1.1 Artikel 1 Absatz 3

Nach heutiger Interpretation der rechtlichen Grundlagen besteht keine Möglichkeit, Diplomaten- und Dienstpässe an Personen ohne Schweizer Bürgerrecht abzugeben, obwohl dies für gewisse Empfangsstaaten bzw. unter bestimmten Konditionen nicht nur angezeigt ist, sondern geradezu einer Notwendigkeit entspricht. Die gesellschaftlichen Veränderungen im Bereich von Partnerschaften und hier insbesondere der Umstand, dass immer mehr Diplomatinnen und Diplomaten über fremdländische Ehe- bzw. Lebenspartner verfügen, hat die bereits bestehende Problematik im letzten Jahrzehnt noch zusätzlich verstärkt.
Das Ausweisgesetz ermächtigt in Artikel 1 Absatz 3 den Bundesrat, die Besonderheiten von Ausweisen, deren Inhaberinnen und Inhaber nach dem Wiener Übereinkommen vom 18. April 1961 über die diplomatische Beziehungen (WUD) oder nach dem Wiener Übereinkommen vom 24. April 1963 über konsularische Beziehungen (WUK) Vorrechte und Immunitäten geniessen, zu regeln. Artikel 37 Absatz 1 WUD räumt auch den zum Haushalt einer diplomatischen Vertretung gehörenden Familienangehörigen gewisse Vorrechte und Immunitäten ein, sofern sie nicht Angehörige des Empfangsstaates sind. Auch das WUK gewährt den Familienangehörigen in Artikel 53 Absatz 2 solche Rechte.
Den Begriff „Familienangehörige“ im Sinne der beiden Konventionen legen die Vertragsstaaten jeweils autonom aus, womit die Schweiz selbst bestimmt, welche Personen darunter fallen. Solange Familienangehörige einer konsularischen oder diplomatischen Vertretung nicht die Nationalität des Empfangsstaates haben, sind sie grundsätzlich vom Gehalt von Artikel 1 Absatz 3 AwG erfasst. Die gleiche Nationalität wie die oder der entsandte diplomatische oder konsularische Vertreterin oder Vertreter wird für Familienangehörige im Rahmen des WUD resp. WUK nicht gefordert.
Mit der vorgeschlagenen Ergänzung von Artikel 1 Absatz 3 AwG wird präzisiert, dass Diplomaten- und Dienstpässe auch an Personen ohne Schweizer Bürgerrecht abgegeben werden können. Bezüglich Umsetzung bedarf es noch einer entsprechenden Anpassung der Ausweisverordnung sowie der Verordnung des EDA vom 13. November 2002 zur Ausweisverordnung (VVAwG, SR 143.116).

2.3.1.2 Artikel 4*a* Absatz 1

Künftig soll die eID insbesondere auch von den Wohnsitzgemeinden herausgegeben werden können. Damit diese Möglichkeit bestehen wird, bedarf es einer Änderung des bestehenden Artikels 4*a* Absatz 1 AwG. Nach der geltenden Fassung können die Kantone die Wohnsitzgemeinden nur ermächtigen, Anträge auf die Ausstellung von IDK's ohne Chip entgegenzunehmen.

Aus diesem Grund soll die Wohnsitzgemeinde von den Kantonen neu ermächtigt werden können, auch Anträge auf die Ausstellung von IDK's mit Chip entgegenzunehmen. Es wird deshalb vorgeschlagen, "ohne Chip" in Artikel 4*a* Absatz 1 Satz zu streichen.

Für das Ausstellen einer IDK mit eID braucht es keine zusätzlichen technischen Einrichtungen, wie dies für die Erfassung von biometrischen Daten (zum Beispiel Fingerabdrücke) der Fall war.

2.3.2 Erfordernis des persönlichen Erscheinens für den Nachweis der Identität

Nicht überall, wo eine Identität verbindlich nachgewiesen werden muss, ist in Zukunft in jedem Fall ein persönliches Erscheinen zwingend erforderlich. Wenn der Identitätsnachweis z.B. in einer Online-Anmeldung mit der eID erledigt werden kann, ist dies im Gegensatz zu heute nicht mehr zwingend notwendig.
Allerdings wurde darauf verzichtet, im eID-Gesetz eine allgemeine Bestimmung aufzunehmen, die in jedem Fall den Einsatz der eID vom persönlichen Erscheinen dispensieren würde. Dies gilt beispielsweise nicht für Zeugenaussagen oder die Teilnahme an Schlichtungsverhandlungen, wo es nicht nur um den Identitätsnachweis geht, sondern die höchstpersönliche Anwesenheit erforderlich ist.
Nachfolgend sind die Änderungen bestehender Gesetze beschrieben, wo Dank dem Einsatz der eID der Identitätsnachweis auch ohne persönliches Erscheinen möglich sein soll.
Daneben gilt es noch, in verschiedenen Ausführungserlassen die entsprechenden Änderungen vorzunehmen. Insbesondere in folgenden Bestimmungen wird heute noch für die Überprüfung der Identität persönliches Erscheinen verlangt:

- Artikel 11 Absatz 3 der Verordnung vom 27. Oktober 1976 über die Zulassung von Personen und Fahrzeugen zum Strassenverkehr (Verkehrszulassungsverordnung, VZV; SR 741.51)
- Artikel 19*a* der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11)
- Artikel 19 Absatz 1 der Verordnung vom 31. August 1983 über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsverordnung, AVIV; SR 837.02)

2.3.2.1 Bundesgesetz über die Alters- und Hinterlassenenversicherung

Artikel 51 Absatz 3 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG, SR 831.10) bestimmt, dass die Arbeitgeberinnen und -geber die von den Arbeitnehmerinnen und -nehmern in der Anmeldung zum Bezug eines Versicherungsausweises gemachten Angaben auf Grund amtlicher Ausweispapiere zu überprüfen haben. Diese Überprüfungspflicht kann entfallen, wenn bei der entsprechenden Anmeldung mit der eID der Arbeitnehmerin oder des Arbeitnehmers die entsprechende Identität validiert wird.

2.3.2.2 Arbeitslosenversicherungsgesetz

Gemäss Artikel 17 Absatz 2 des Bundesgesetzes vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsgesetz, AVIG; SR 837.0) muss die Anmeldung persönlich bei der Wohngemeinde oder der vom Kanton bestimmten zuständigen Amtsstelle zur Arbeitsvermittlung erfolgen. Auch hier soll das Anmeldeprozedere mit dem Einsatz der eID vereinfacht werden.

2.3.2.3 Bundesgesetz über die elektronische Signatur

Das Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03) gibt dem Bundesrat mit Artikel 8 Absatz 2 bereits heute die Möglichkeit zu bestimmen, dass eine Person, für die ein qualifiziertes Zertifikat ausgestellt werden soll, nicht immer persönlich erscheinen müssen, um den Nachweis ihrer Identität zu erbringen. In Zukunft kann der Identitätsnachweis auch mit der eID erledigt werden und ein persönliches Erscheinen der antragstellenden Person ist nicht mehr zwingend notwendig.

2.3.2.4 Geldwäschereigesetz

In Artikel 3 des Bundesgesetzes vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Finanzsektor (Geldwäschereigesetz, GwG; SR 955.0) wird die Identifizierung der Vertragspartei detailliert geregelt. Auch diese soll mit dem Einsatz der eID vereinfacht werden.

3 Auswirkungen des Gesetzesentwurfs

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen

Für die Einführung der eID müssen verschiedene Systeme entwickelt respektive adaptiert werden. Dabei ist mit Investitionskosten von rund CHF 6.2 Mio. zu Lasten Projekt (Bund) zu rechnen. Die jährlichen Betriebskosten dieser Systeme (inkl. Wartung und Support) dürften rund CHF 1.2 Mio. betragen.

3.1.2 Personelle Auswirkungen

Für das eID-Kompetenzzentrum fallen beim Bund Personalkosten an. Für die geschätzte Anzahl von 26 Stellen ergibt sich im Endausbau ein jährlicher Personalaufwand von rund CHF 2.7 Mio. Zusammen mit den Arbeitsplatzkosten von rund CHF 0.3 Mio. ergibt sich ein jährlicher Gesamtaufwand von rund CHF 3.0 Mio.

Investitions- und Betriebskosten sowie der gesamte Personalaufwand sollen als Deckungsbeiträge auf die Ausweise für Erwachsene und Kinder umgelegt werden gemäss den Vorgaben der für die Ausweise verantwortlichen Fachstellen. Mit dem heutigen Verteilschlüssel würde eine IDK mit eID für Erwachsene CHF 75 (nur IDK CHF 65) und eine IDK mit eID für Kinder CHF 35 (nur IDK CHF 30) kosten.

3.1.3 Andere Auswirkungen

Verschiedene Bundesstellen werden von der eID guten Gebrauch machen können. Einerseits kann die eID für vielfältige Identifizierungs- und Authentifizierungszwecke für Angestellte der Bundesverwaltung eingesetzt werden. Damit bildet die eID eine wichtige Basis-Komponente für die in Entwicklung begriffenen IAM-Konzepte des Bundes.
Andererseits steht mit der eID auch verschiedenen Registerstellen eine adäquate Lösung für die sichere Authentifizierung von Gesuchstellerinnen und –stellern zur Verfügung. Beispiele

hierfür sind die Online-Bestellung von Geburtsscheinen oder Auszüge aus dem Straf- oder Betreibungsregister.

3.2 Auswirkungen auf die Kantone und Gemeinden

Im Zusammenhang mit der eID kann sich in den Kantonen ein leicht höherer Beratungsaufwand ergeben. Da nur zwei IDK-Modelle angeboten werden sollen, wurde die Entscheidungsfindung für die Bürgerinnen und Bürger vereinfacht und der daraus resultierende Mehraufwand kann mit zwei Minuten eingesetzt werden.
Im Rahmen der Einführung des biometrischen Passes wurde mit den Kantonen die Kosten für eine Arbeitsstunde inklusive aller Nebenkosten auf CHF 125 festgelegt. Somit hat jede Minute Mehraufwand eine Gebührenerhöhung um rund CHF 2.10 zur Folge. Diese soll den Kantone und Gemeinden zu Gute kommen und ist in den in Ziffer 3.1.2 beschriebenen Kosten der neuen IDK mit eID berücksichtigt.

Für die Kantone sind nur sehr geringe Investitionskosten für die notwendigen eID-Lesegeräte absehbar. Sollten neben der vom Bund bezahlten Erstausrüstung weitere Lesegeräte benötigt werden, kosten diese geschätzt CHF 250 pro Stück.

Weitere Mehrkosten im Zusammenhang mit der eID fallen in den Kantonen und Gemeinden nicht an.

3.3 Auswirkungen auf die Volkwirtschaft

Der Bundesrat verfolgt mittlerweile seit bald zwei Jahrzehnten das Ziel, staatlicherseits die Beiträge zu leisten, die es für einen erfolgreichen Übergang der Schweiz in die Informationsgesellschaft braucht. Er hat dazu zahlreiche Massnahmen beschlossen die meist entweder die Anpassung des gesetzlichen Rahmens oder die Bereitstellung von Infrastruktur-Elementen betrafen. Dazu gehören beispielsweise das Bundesgesetz über die elektronische Signatur (ZertES) oder die Schaffung von einheitlichen Personen- und Unternehmens-Identifikatoren und der entsprechenden Register.

Ein breit verfügbares elektronisches Identifikationsmittel bildet einen wichtigen Eckstein in einem umfassenderen eID-Ökosystems, das Sicherheit und Vertrauen im elektronischen Geschäftsverkehr herstellen kann. Dadurch können auch heikle Geschäfte unter Privaten wie auch mit dem Staat elektronisch und damit effizienter abgewickelt werden. Zudem eröffnen sich bedeutende neue Geschäftsfelder. Sichere und geregelte Verhältnisse auch im Cyberraum tragen wesentlich zur Attraktivität des Wirtschaftsstandorts Schweiz und zu seiner Wettbewerbsfähigkeit bei.

3.4 Auswirkungen auf die Gesellschaft

Fast jeder Missbrauch im Internet basiert darauf, dass Kommunikationspartnerinnen und -partner nicht sicher identifiziert werden können. Spam ist möglich, weil sich vertrauenswürdige Absenderinnen und Absender nicht von anderen unterscheiden lassen und weil diese nicht in die Pflicht genommen werden können. Beim Phishing geben sich Absenderinnen und Absender als jemanden aus, der sie nicht sind, beispielsweise die Bank der Empfängerin oder des Empfängers, und können damit grossen Schaden anrichten. Eine staatlich herausgegeben eID hilft die Identität der Inhaberinnen und Inhaber in der heutigen globalisierten

und hoch vernetzten Gesellschaft zu schützen. Der für ein Individuum potenziel sehr gefährliche Identitätsdiebstahl wird dadurch deutlich erschwert.
Die sichere Identifikation der Partnerinnen und Partner bei der elektronischen Kommunikation verhindert Missbrauch und schafft auch im Cyberraum Recht und Vertrauen.

3.5 Auswirkungen auf die Umwelt

Die Vorlage hat keine direkten Auswirkungen auf die Umwelt. Grundsätzlich sollte ein vermehrter Wechsel von physischer zu elektronischer Abwicklung von Geschäften per Saldo Ressourcen einsparen und sich entsprechend vorteilhaft für die Umwelt auswirken.

3.6 Andere Auswirkungen

Über das vorstehend Beschriebene hinaus sind keine nennenswerten Auswirkungen zu erwarten.

4 Rechtliche Aspekte

4.1 Verfassungsmässigkeit

Beim eID-Gesetz handelt es sich um einen neuen Erlass. Analog zur Kompetenzdelegation im Ausweisgesetz und im Ausländergesetz kann sich der Erlass auf Artikel 38 Absatz 1 resp. Artikel 121 Absatz 1 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101) stützen. Artikel 38 BV gibt dem Bund die umfassende Kompetenz zur Regelung des Erwerbs und Verlusts des Bürgerrechts und somit auch die Kompetenz zur Ausgabe eines Ausweises, der die schweizerische Staatsangehörigkeit nachweist (BBl 2000 4751). Der Bund hat gestützt auf Artikel 121 Absatz 1 BV auch eine umfassende Kompetenz zur Gesetzgebung im Ausländerbereich (BBl 2002 3709).

4.2 Erlassform

Ausgehend von Gegenstand, Inhalt und Tragweite des zu erarbeitenden Gesetzgebungsprojektes ist es aufgrund Artikel 164 Absatz 1 BV notwendig, die Bestimmungen zur elektronischen Identifikation in der Form eines Bundesgesetzes zu erlassen.

Diese Form drängt sich insbesondere deshalb auf, weil die Verabschiedung des vorliegenden Gesetzesentwurfs eine Änderung des bestehenden Rechts voraussetzt (vgl. Ziffer 2.3).

4.3 Delegation von Rechtsetzungsbefugnissen

Der Gesetzesentwurf enthält diverse Delegationsnormen, um technische und organisatorische Details auf dem Verordnungsweg (Stufe Bundesrat oder Departement) zu regeln.

4.4 Datenschutz

Überall, wo Personendaten im Spiel sind, ist es wichtig, dass die Voraussetzungen des Datenschutzes eingehalten bzw. erforderlichen Sicherheitsvorkehrungen getroffen werden. Im Gegensatz zur ePass-Funktion mit biometrischen Daten steht die eID nicht im direkten Zusammenhang mit heiklen oder besonders schützenswerten Personendaten. Sie erfordert unter dem Gesichtspunkt des Datenschutzes übliche Sorgfalt und Aufmerksamkeit. Dem Anliegen wird in erster Linie Rechnung getragen, indem eine formelle gesetzliche Grundlage erarbeitet wird. Sowohl die eID als auch die schweizerische eID-Gesamtlösung sind datenschutzrechtlich auszugestalten und müssen gegen Missbrauch abgesichert sein. Es dürfen nur Identitätsdaten bearbeitet werden, die zu Erfüllung der Aufgaben erforderlich sind.

Mehrere Elemente der in dieser Vorlage vorgesehenen eID sind speziell im Hinblick auf die bestmögliche Gewährung des Datenschutzes konzipiert:

- Zweckmässigkeit und Verhältnismässigkeit: Artikel 14 setzt diese beiden Prinzipien für den konkreten Fall explizit um. Der Identitätsnachweis darf von Behörden nur dort verlangt werden, wo er für die entsprechende Aufgabe notwendig ist. Wenn er eingesetzt wird, soll die schonendste Variante gewählt werden. Damit wird ein überbordender Einsatz der eID verhindert.
- Prinzip der Benutzer-Zentrierung ('user centric', Artikel 13): Bevor Daten aus dem Ausweis bezogen werden können, wird die Benutzerin oder der Benutzer darüber informiert und muss den Datenbezug explizit freigeben.
- Pseudonym-Funktion ('restricted identification'): In Fällen, wo es nur darum geht, eine Person zu authentifizieren, bzw. wiederzuerkennen, kann die Pseudonym-Funktion eingesetzt werden. Dabei erhalten Dienstanbieterinnen und -anbieter nur einen pseudonymen Identifikator und darüber hinaus keinerlei Daten. Der pseudonyme Identifikator ist bei jeder Dienstanbieterin und jedem Dienstanbieter ein anderer. Er wird jeweils separat aus dem Berechtigungszertifikat und einem geheimen Schlüssel der eID errechnet.
- Abgeleitete Werte: In vielen Fällen müssen nicht die Personendaten selbst, wie beispielsweise das Alter oder die Nationalität übermittelt werden, sondern es genügt ein weniger aussagekräftiger, abgeleiteter Wert. Muss eine Anwendung nur wissen, ob eine Person älter als 18 Jahre ist, wird nicht das genaue Alter oder das komplette Geburtsdatum übermittelt, sondern nur die Frage 'Über18' angefragt und gegebenenfalls bestätigt.
- Kontrolle der vertrauenden Dienste: Dienstanbieterinnen und -anbieter, welche die eID benutzen wollen, brauchen dazu ein Berechtigungszertifikat (Art. 16). Zwar findet keine umfassende Prüfung der Dienstanbieterinnen und -anbieter statt, diese sind aber immerhin bekannt und klar identifizierbar. Bei Gefahr oder eingetretenem Missbrauch kann das Berechtigungszertifikat gesperrt werden, wodurch die Dienstanbieterin oder der -anbieter innert kurzer Frist auf keine eID mehr zugreifen kann.
- Sichere Verbindungen: Die Verbindungen zwischen der eID und dem vertrauenden Dienst sind mit etablierten Verfahren verschlüsselt und gegen Manipulationen geschützt.