Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

Bern, 22. Februar 2017

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Erläuternder Bericht zum Vorentwurf

1 Grundzüge der Vorlage

1.1 Ausgangslage

Mit der Verbreitung des Internets und der hohen Verfügbarkeit von leistungsfähigen Mobilgeräten können Geschäftsprozesse immer einfacher in die digitale Welt verlagert werden. Die gut ausgebildeten und technologieaffinen Nutzerinnen und Nutzer des Internets, die sehr gut vernetzt und ständig online sind, begünstigen diesen sozioökonomischen Wandel. Damit auch anspruchsvollere Geschäftsprozesse online abgewickelt werden können, müssen die Geschäftsanbietenden (in der Folge als Betreiberinnen von E-ID-verwendenden Diensten bezeichnet) Vertrauen in die Identität und Authentizität des Gegenübers haben. Gesicherte Identitäten sind die Basis für Rechtssicherheit, auch über Staatsgrenzen hinaus. Diesem Bedarf soll in der Schweiz mit der Schaffung von anerkannten elektronischen Identifizierungseinheiten (oft auch als elektronische Identität, E-ID oder eID bezeichnet) für natürliche Personen nachgekommen werden. Für juristische Personen ist mit der Unternehmens-Identifikationsnummer (UID) bereits ein eindeutiger Identifikator vorhanden, der für Identifikationszwecke in geeignete IT-Werkzeuge eingebaut werden kann. Eine E-ID erlaubt es einer Betreiberin eines E-ID-verwendenden Dienstes, die Inhaberin oder den Inhaber als berechtigte Person online zu identifizieren und zu authentifizieren.

Vertrauenswürdige E-ID sind damit ein Beitrag für die Implementation von elektronischen Geschäftsprozessen.

Mit Bundesratsbeschluss vom 19. Dezember 2012 wurde das EJPD beauftragt, in Zusammenarbeit mit der BK, dem WBF, dem UVEK und dem EFD ein Konzept und einen Rechtsetzungsentwurf für elektronische staatliche Identifikationsmittel zu erstellen, die mit der Identitätskarte (IDK) abgegeben werden können. Im ersten Entwurf des Konzepts, vorgestellt im Aussprachepapier vom 28. Februar 2014, wurde davon ausgegangen, dass der Staat als hoheitlicher Identitätsdienstleister (Identity Provider, IdP) auftritt und allen Schweizerinnen und Schweizern zusätzlich zur IDK auch eine E-ID abgegeben wird. Das Konzept wurde 2014 und 2015 bei den Ämtern und bei Marktteilnehmern in Konsultation gegeben.

Aufgrund der Rückmeldungen und der Erfahrungen in anderen Ländern wurde das Konzept grundlegend überarbeitet. Eigenentwicklungen durch den Staat und staatlich abgegebene E-ID führen in der Regel zu hohen ungedeckten IKT-Kosten für die öffentliche Hand (z. B. für Support, Lesegeräte, Software), da zu wenig flexibel auf die schnell ändernden Bedürfnisse und Technologien reagiert werden kann. Hingegen verbreiten sich heute privatwirtschaftliche elektronische Identifizierungsangebote verschiedener Sicherheitsniveaus (z. B. Apple-ID, Google ID, Mobile ID, OpenID, SuisseID, SwissPass etc.). Welche der derzeit gängigen E-ID auch mittel- und längerfristig bestehen werden, ist heute kaum abzuschätzen. Deshalb geht das neue Konzept von einer Aufgabenteilung zwischen Staat und Privaten aus.

Parallel zu den Ergebnissen der Konsultation wurden die neuesten Entwicklungen in der EU berücksichtigt und die rechtlichen Abhängigkeiten zur Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizie-

rung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG[1] (sogenannte eIDAS-Verordnung) abgeklärt.

Der Bundesrat hat am 13. Januar 2016 Kenntnis vom E-ID-Konzept genommen, das EJPD mit der Ausarbeitung eines Gesetzes beauftragt und die Rahmenbedingungen für die Gesetzgebung festgelegt.

1.2 Die beantragte Neuregelung

1.2.1 Konzept der E-ID

Rechtssicherheit und Vertrauen sind wesentliche Voraussetzungen für die Abwicklung von Geschäften. Dazu gehören adäquate Kenntnisse über die Identität der Beteiligten. Für die physische Welt stellt der Bund dazu bereits heute konventionelle Identifizierungsmittel aus, nämlich Schweizer Pass, Identitätskarte und Ausländerausweis. Ergänzend dazu soll nun die Identität einer natürlichen Person auch elektronisch nachgewiesen werden können. Staatlich anerkannte E-ID werden es den Inhaberinnen und Inhabern ermöglichen, sich bei Online-Diensten sicher zu registrieren und sich später erneut sicher anzumelden. Weitere Vertrauensdienste wie die elektronische Signatur können von IdP angeboten werden, sind jedoch nicht Bestandteil der E-ID.

Das nun umgesetzte Konzept stützt sich auf die Vorarbeiten des EJPD (fedpol) aus den Jahren 2013–2015, im Rahmen derer auch wichtige Marktteilnehmerinnen und -teilnehmer konsultiert wurden. Es berücksichtigt weiter die Erkenntnisse aus bisherigen E-ID-Lösungen anderer Länder resp. die internationalen Entwicklungen für praxisnahe E-ID-Lösungen und die Vorgaben für die EU-Kompatibilität gemäss eIDAS-Verordnung.

1.2.2 Aufgabenteilung zwischen Staat und Markt

Der Vorentwurf geht von einer Aufgabenteilung zwischen Staat und Markt aus. Die notwendige Akzeptanz für die E-ID soll mit vertrauenswürdigen rechtlichen und organisatorischen Rahmenbedingungen verbunden mit der Leistungsfähigkeit und Dynamik des Marktes erreicht werden. Neuerdings sind zwei private Initiativen bekannt geworden, die das gewählte Vorgehen bestätigen. In einem Projekt arbeiten die Grossbanken Credit Suisse und UBS zusammen mit der Swisscom an einem „Passepartout fürs Internet“, in einem anderen wollen SBB und die Post gemeinsam Lösungen für die Anmeldung bei Online-Portalen anbieten.

Geeignete IdP werden vom Bund zur Ausstellung von anerkannten E-ID und zum Betrieb von anerkannten E-ID-Systemen ermächtigt. Alle anerkannten E-ID-Systeme müssen untereinander interoperabel sein, damit ein hoher Kundennutzen entsteht.

1.2.3 Funktion der E-ID

Mit einer E-ID können sich natürliche Personen sicher und bequem bei Online-Portalen (E-ID-verwendenden Diensten) registrieren und später wieder anmelden. Bei der Registrierung müssen die persönlichen Angaben nicht manuell eingegeben werden; vielmehr werden

[1] Der Link zur Fundstelle in der Europäischen Rechtsdatenbank Eur-Lex ist im Fundstellenverzeichnis aufgeführt.

sie nach Freigabe durch die Inhaberin oder den Inhaber mittels der E-ID elektronisch übermittelt. Wird das Portal später erneut besucht, identifiziert und authentifiziert sich der Inhaber oder die Inhaberin mit der E-ID. Die einmal registrierte E-ID wird wiedererkannt und gewährleistet eine verlässliche Anmeldung. Die E-ID ist also eine der Grundlagen für die sichere Nutzung von Online-Diensten.

Es werden drei Sicherheitsniveaus unterschieden, wie sie auch die EU für die E-ID ihrer Mitgliedsländer und die USA für Vertrauensdienste vorsehen. Der Bund seinerseits stellt den IdP via eine elektronische Schnittstelle die staatlich geführten Personenidentifizierungsdaten zur Verfügung (z. B. E-ID-Registrierungsnummer, Name, Vornamen usw.). Die erste Übermittlung der Daten an einen IdP oder eine Betreiberin eines E-ID-verwendenden Dienstes erfordert die ausdrückliche Zustimmung der betroffenen Person (vgl. Art. 6 und 17 Abs. 1 Bst. f des Vorentwurfs, VE). Der tägliche Gebrauch der E-ID erfolgt aber ohne weiteren Rückgriff auf die Infrastruktur des Bundes.

Die Einhaltung der vorgegebenen Prozesse und technischen Standards durch die IdP wird durch eine Anerkennungsstelle für Identitätsdienstleister (Anerkennungsstelle, Verwaltungseinheit des Bundes, Art. 21 VE) regelmässig überprüft (Art. 4 und Art. 11 f. VE). Bei erfolgreicher Prüfung wird die Anerkennung erteilt oder verlängert. Details zu den einzuhaltenden Prozessen und Standards werden auf Verordnungs- und allenfalls Weisungsebene geregelt und sind auf die bestehenden Regelungen im Bereich der elektronischen Signaturen[2] und Zustellplattformen abgestimmt, so dass für anerkannte IdP Synergien bei den verlangten Zertifizierungen entstehen. Das Anerkennungsverfahren für E-ID-Systeme ist ähnlich demjenigen für Plattformen für die sichere Zustellung im Bereich elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren. Es wird eine Liste der anerkannten IdP und ihrer anerkannten E-ID-Systeme veröffentlicht (Art. 22 VE).

1.2.4 Ausstellung der E-ID

Eine E-ID wird in der Regel nach Vorsprache bei einem IdP ausgestellt. Die Registrierung beinhaltet eine Identifizierung, die je nach Sicherheitsniveau mittels elektronischer Medien oder anlässlich einer persönlichen Vorsprache durchgeführt wird. Der Registrierungsvorgang erfolgt in mehreren Schritten (vgl. Art. 6 und Art. 17 Abs. 1 Bst. b VE):

1. Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP. Je nach Sicherheitsniveau ist dafür die persönliche Vorsprache oder eine gleichwertige virtuelle Präsenz (z. B. Videoidentifikation) nötig.
2. Der IdP überprüft den vorgelegten Ausweis (Pass, IDK oder Ausländerausweis) und macht bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) elektronisch eine Anfrage, um die Angaben des Ausweises bestätigen zu lassen.
3. Die Identitätsstelle vergleicht die vom IdP übermittelten Daten des Ausweises mit den in den Personenregistern des Bundes gespeicherten Personenidentifizierungsdaten.
4. Die antragsstellende Person erklärt sich einverstanden, dass ihre Personenidentifizierungsdaten einer E-ID-Registrierungsnummer zugeordnet werden und beides an den IdP übermittelt wird.
5. Die Identitätsstelle übermittelt die E-ID-Registrierungsnummer mit den bestätigten Daten dem IdP.

---

[2] Vgl. Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur, Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03

6. Der IdP ordnet der antragsstellenden Person ein Authentifizierungsmittel (Trägermittel der E-ID) zu, mit dem sie oder er sich online identifizieren kann.
7. Der IdP sorgt für die richtige Zuordnung der E-ID-Registrierungsnummer zur E-ID mit dem Authentifizierungsmittel und aktiviert die E-ID für den Gebrauch durch die Inhaberin oder den Inhaber.

Der ganze Vorgang sollte nicht mehr als ein paar Minuten dauern. Die technischen Vorgänge im Hintergrund werden über Standards und technische Protokolle definiert.

1.2.5 Sicherheitsniveaus

Nicht alle Geschäftsprozesse erfordern dasselbe Sicherheitsniveau. Zu hohe Sicherheitsanforderungen können in der Praxis als störend empfunden werden und Umgehungshandlungen begünstigen sowie höhere Kosten verursachen. Dies ist weder für die Akzeptanz noch die Sicherheit eines E-ID-Systems gut. Deshalb werden geeignete E-ID-Systeme auf einem von drei Sicherheitsniveaus anerkannt. Die Sicherheitsniveaus unterscheiden sich durch den Ausstellungsprozess, den Betrieb und den Einsatz und können sich durch weitere technische oder organisatorische Sicherheitsmassnahmen unterscheiden.

Das Gesetz definiert lediglich die möglichen Kategorien von E-ID, hier Sicherheitsniveaus genannt (vgl. Art. 5 VE). Jedes Sicherheitsniveau vermittelt ein unterschiedliches Mass an Vertrauen. Welches Sicherheitsniveau für welche Art der Anwendung in Frage kommt, wird in den jeweiligen Spezialerlassen festgehalten bzw. durch die privaten Betreiberinnen von E-ID-verwendenden Diensten definiert. So kann für E-Education ein anderes Sicherheitsniveau gewählt werden, als es für Vote électronique vorgeschrieben oder für E-Health-Anwendungen notwendig ist.

Die Bezeichnung und Ausgestaltung der Sicherheitsniveaus wurde aus der eIDAS-Verordnung und den dazugehörenden Durchführungsbestimmungen[3] übernommen. Es wird zwischen den Niveaus „*niedrig*“, „*substanziell*“ und „*hoch*“ unterschieden. Die verschiedenen Sicherheitsniveaus vermitteln ein unterschiedliches Mass an Vertrauen in die zugeordneten Daten. Grundsätzlich können E-ID der Sicherheitsniveaus „*substanziell“* und „*hoch“* auch bei E-ID-verwendenden Diensten eingesetzt werden, die ein tieferes Sicherheitsniveau verlangen.

Die drei Sicherheitsniveaus für schweizerisch anerkannte E-ID-Systeme sind so definiert, dass sie bezüglich Sicherheit die gleichen Anforderungen erfüllen, die für die drei in der eIDAS-Verordnung der EU definierten E-ID-Sicherheitsniveaus gelten (Art. 8 der eIDAS Verordnung und dazugehörige Durchführungsrechtsakte). Die gleichen drei Sicherheitsniveaus werden auch durch das NIST[4] für E-Government Anwendungen in den USA definiert und gelten heute als weltweiter Standard. Jedes Sicherheitsniveau wird sich, zur Erfüllung ihres Zwecks, durch spezifische technische Spezifikationen, Normen und Verfahren einschliesslich technischer Überprüfungen auszeichnen und im Detail noch auszuarbeiten sein.

Mit diesem Modell ist es zum Beispiel möglich, eine für das Sicherheitsniveau „*substanziell“* in technischer Hinsicht geeignete E-ID vorerst auf Niveau „*niedrig“* zu registrieren und diese später bei Bedarf mittels einer persönlichen Vorsprache auf ein höheres Sicherheitsniveau

---

[3] Vgl. Zusammenstellung im Fundstellennachweis

[4] National Institute of Standards and Technology, U.S. Department of Commerce

anzuheben. Dies erleichtert den Einstieg in anerkannte E-ID-Systeme. Mit dem Sicherheitsniveau „*niedrig“* wird der Zugang zu anerkannten E-ID einfach gehalten, was einen essentiellen Erfolgsfaktor für die Anbieter von anerkannten E-ID-Systemen im Markt darstellt. Zudem kann eine Person mehrere E-ID von verschiedenen IdP auf unterschiedlichen Sicherheitsniveaus besitzen, wenn sie das möchte.

Sicherheitsniveau „*niedrig“*
Die E-ID hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung zu vermindern. Die Registrierung kann online gestützt auf einen staatlichen Ausweis erfolgen. Beim Sicherheitsniveau „*niedrig“* werden nur wenige Daten zugeordnet (Name, Vorname, Geburtsdatum und E-ID-Registrierungsnummer; vgl. Art. 7 Abs. 1 VE). Der Einsatz der E-ID verlangt mindestens eine Ein-Faktor-Authentifizierung. Die Handhabung einer solchen E ID ist damit vergleichbar mit einem Zutrittsbadge oder den einer kontaktlosen Bezahllösungen für kleinere Beträge.

Sicherheitsniveau „*substanziell“*
Das Sicherheitsniveau „*substanziell*“ bezieht sich auf eine elektronische Identifizierungseinheit, die ein substanzielles Mass an Vertrauen in die beanspruchte oder behauptete Identität einer Person vermittelt. Die E-ID dieses Sicherheitsniveaus hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung erheblich zu vermindern. Die Registrierung erfolgt mit persönlicher Vorsprache beim IdP oder einer Videoidentifikation gestützt auf einen staatlichen Ausweis. Im Sicherheitsniveau „*substanziell“* werden neben dem Namen und dem Geburtsdatum noch weitere Personenidentifizierungsdaten zugeordnet (z. B. Geschlecht, Geburtsort, Zivilstand, vgl. Art. 7 Abs. 2 VE). Der Einsatz der E-ID verlangt mindestens eine 2-Faktor-Authentifizierung. Die Handhabung einer solchen E-ID ist somit zum Beispiel mit im Bankenbereich üblichen Lösungen vergleichbar (Kontokarten, Kreditkarten mit PIN, E-Banking-Lösungen).

Sicherheitsniveau „*hoch“*
Die E-ID mit dem Sicherheitsniveau „*hoch*“ hat im Rahmen eines E-ID-Systems den Zweck, die Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung zu verhindern. Die Registrierung erfolgt mit persönlicher Vorsprache beim IdP oder mit Videoidentifikation gestützt auf einen staatlichen Ausweis. Zusätzlich wird die Echtheit des Ausweises und mindestens ein biometrisches Merkmal gestützt auf eine behördliche Quelle überprüft (Ausweisgültigkeit und Gesichtsbild oder anderes biometrisches Erkennungsmerkmal). Beim Sicherheitsniveau „*hoch“* werden der E-ID-Registrierungsnummer alle verfügbaren Personenidentifizierungsdaten zugeordnet (vgl. Art. 7 Abs. 2 VE). Das Authentifizierungsmittel der E-ID muss zudem sehr hohe Anforderungen bezüglich technischer Sicherheit erfüllen.

Der Einsatz der E-ID verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss («inhärenter Faktor» gemäss eIDAS Durchführungsrechtsakte). Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung. Die biometrische Authentifizierung bewirkt eine noch engere Bindung zwischen der E-ID und deren Inhaberin oder Inhaber. Bei Verlust des Authentifizierungsmittels der E-ID schützt die biometrische Authentifizierung die Inhaberin oder den Inhaber vor der Tätigung missbräuchlicher Transaktionen in deren Namen. Mit Blick auf den Identitätsmissbrauch müssen Inhaberinnen und Inhaber auch vor Cyberangriffen geschützt werden können. Dies betrifft sowohl Cyberangriffe auf das Authentifizierungsmittel der E-ID selbst als auch Cyberangriffe auf weitere technische Hilfsmittel, die gegebenenfalls für den Einsatz des Authentifizierungsmittels der E-ID erforderlich sind, aber nicht in den Regelungsbereich dieses Gesetzes fallen. Missbräuchliche Transaktionen in fremdem

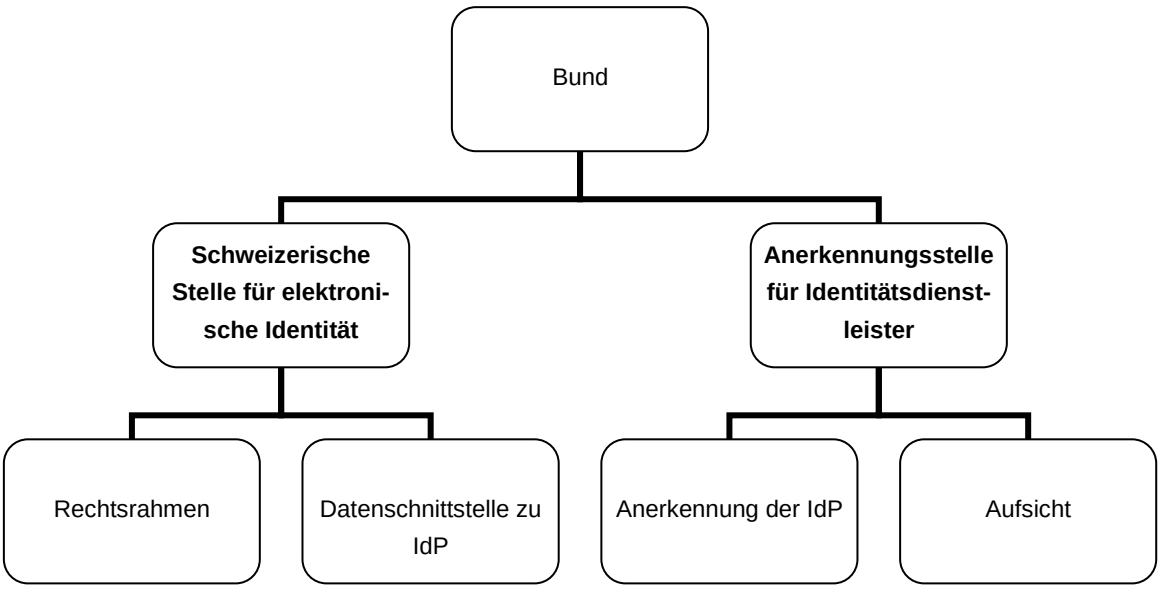
Namen müssen auch dann verhindert werden können, wenn die technischen Hilfsmittel mittels Cyberangriff manipuliert wurden oder Informationen aus diesen herausgelesen wurde. Um dies zu gewährleisten muss das Authentifizierungsmittel der E-ID über besonders vertrauenswürdige Komponenten verfügen, die dem Stand der Technik entsprechen.

1.2.6 Beitrag des Staates zu den E-ID-Systemen

Überblick
Eine staatlich anerkannte E-ID bestätigt die Existenz und Identität einer natürlichen Person aufgrund der Personenidentifizierungsdaten, die in staatlich geführten und gepflegten Registern hinterlegt sind. Der Staat auf allen föderalen Ebenen geniesst dabei besonderes Vertrauen für die Bestätigung der Identität einer Person. Basis ist die regelmässig wiederkehrende Identifizierung bei einer staatlichen Stelle anlässlich einer Ausweiserstellung.

Der Bund legt die Vertrauensbasis für anerkannte E-ID-Systeme und übernimmt dazu mehrere Aufgaben im Bereich der anerkannten E-ID.
1. Er erarbeitet und pflegt die Rechtsgrundlagen und bewirkt damit Transparenz und Sicherheit;
2. er definiert einzuhaltende Standards, Sicherheits- und Interoperabilitätsanforderungen für den Betrieb eines E-ID-Systems;
3. er betreibt eine elektronische Schnittstelle, über welche anerkannte IdP staatlich geführte Personenidentifizierungsdaten beziehen können;
4. er anerkennt IdP und ihre E-ID-Systeme; und
5. er beaufsichtigt anerkannte IdP und E-ID-Systeme.

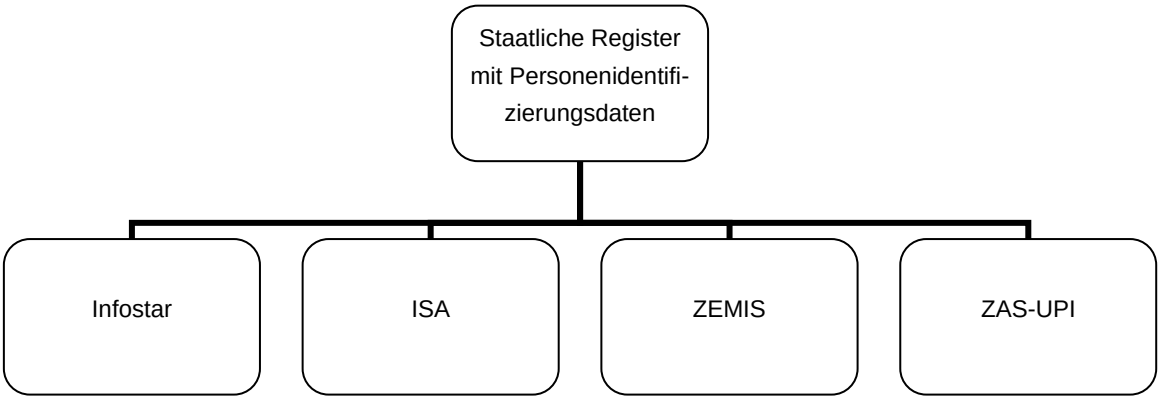
Diese Aufgaben sollen beim Bund von zwei Verwaltungseinheiten wahrgenommen werden: der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) und der Anerkenungsstelle für Identitätsdienstleister (Anerkennungsstelle).



Register mit Personenidentifizierungsdaten
Die Schweizer Behörden der verschiedenen föderalen Ebenen pflegen mehrere Register, die Personenidentifizierungsdaten enthalten. Als Beispiele seien hier die kantonalen und kom-

munalen Einwohnerregister, das elektronische Zivilstandsregister (Infostar) und das Zentralregister der zentralen Ausgleichsstelle der AHV (ZAS-UPI[5]) erwähnt. UPI ist das zentrale Versichertenregister der AHV für die Personenidentifikation bei der Zuordnung und der Verwaltung der AHV-Nummer (AHVN13). Weiter enthält das Informationssystem Ausweisschriften (ISA) Personenidentifizierungsdaten für Schweizerinnen und Schweizer und dient als Basis für die Ausstellung von Ausweisen (Identitätskarte und Schweizer Pass). Ausländerausweise werden hingegen aufgrund der Daten des Zentralen Migrationssystems (ZEMIS) ausgestellt.

Das Registerharmonisierungsgesetz vom 23. Juni 2006 (RHG, SR 431.02) bestimmt die AHV-Nummer (AHVN13) als einzigen und eindeutigen Personenidentifikator in den von der Volkszählung betroffenen Registern. Zu diesen Registern zählen die Personenregister des Bundes sowie die kantonalen und kommunalen Einwohnerregister. Der Bund hat keinen Zugriff auf die kantonalen und kommunalen Einwohnerregister und kann dadurch keine Wohnsitze und -adressen bestätigen.



Verhältnis des Personenidentifikators AHVN13 zur E-ID-Registrierungsnummer
Die AHVN13 ist eine eindeutige Personenidentifikationsnummer, die allerdings gemäss heutiger Praxis nur in Teilbereichen eingesetzt werden kann, sofern dafür die formalgesetzlichen Grundlagen bestehen. Die Möglichkeit, die AHVN13 systematisch zu verwenden, birgt das Risiko der Vernetzung von Personendatensätzen zwischen einzelnen Systemen. Daher ist die systematische Verwendung der AHVN13 nur unter den Voraussetzungen der Artikel 50d und Artikel 50e des Bundesgesetzes vom 20. Dezember 1946[6] über die Alters- und Hinterlassenenversicherung (AHVG) zulässig. In Artikel 50a AHVG wird geregelt, an welche Stellen in Abweichung von Artikel 33 des Bundesgesetzes vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG)[7] Daten, insbesondere die Versichertennummer (AHVN13), bekanntgegeben werden dürfen. Gemäss Artikel 50e AHVG ist eine systematische Verwendung der AHVN13 nur zulässig, wenn ein Bundesgesetz dies vorsieht und wenn der Verwendungszweck sowie die Nutzungsberechtigten bestimmt sind.

Institutionen ohne Behördencharakter, denen gesetzlich die Erfüllung einer öffentlichen Aufgabe übertragen wurde, sollen gemäss Bundesratsbeschluss zur Verwendung der AHVN13 befugt sein, sofern eine spezialgesetzliche Grundlage dies vorsieht. Im Verkehr des Bürgers

---

5 UPI ist das Akronym für «Unique Person Identification»

6 SR **831.10**

7 SR **830.1**

mit Verwaltungsstellen wird die AHVN13 in zahlreichen Fällen benötigt. Könnte sie künftig im elektronischen Verkehr zwischen Bürger und Verwaltung nicht über die IdP bezogen und bestätigt werden, müssten dafür kostspielige Umgehungslösungen bereitgestellt werden. Das würde den Komplexitätsgrad der Systeme markant erhöhen und die Akzeptanz der E-ID schmälern. Den IdP soll deshalb erlaubt werden, die AHVN13 – ausschliesslich – zu diesem eingeschränkten Zweck systematisch zu verwenden. IdP dürfen die AHVN13 nur jenen Betreiberinnen eines E-ID-verwendenden Dienstes bekannt geben, die selbst zur systematischen Verwendung der AHVN13 berechtigt sind (Art. 9 VE).

Die übrigen Privaten sollen hingegen von der systematischen Verwendung der AHVN13 ausgeschlossen sein. Daher braucht es eine zusätzliche Identifikationsnummer, die im Verkehr mit Privaten gebraucht werden kann und unabhängig von der AHVN13 ist. Deshalb wird die E-ID-Registrierungsnummer eingeführt. Sie dient darüber hinaus zur Verbindung der Person mit der ausgegebenen E-ID. Der Bezug einer E-ID ist freiwillig und voraussichtlich mit Kosten verbunden. Da zudem nur Personen mit einem Schweizer Ausweis oder einem Ausländerausweis eine E-ID erhalten können, ist die E-ID-Registrierungsnummer insgesamt nicht als allgemeiner Personenidentifikator geeignet.

Schweizerische Stelle für elektronische Identität (Identitätsstelle)

Rechtsrahmen

Die Identitätsstelle pflegt im Betrieb in Zusammenarbeit mit der Anerkennungsstelle die rechtlichen, organisatorischen und technischen Vorgaben. Insbesondere definiert sie die Standards der Schnittstellen für die Interoperabilität der E-ID-Systeme und passt die technischen und organisatorischen Anforderungen im Bereich der Anerkennung der IdP und E-ID-System dem technischen und sozioökonomischen Fortschritt und den aktuellen Sicherheitsbedürfnissen an.

Die vom Bundesrat vorgegebenen Rahmenbedingungen verlangen die Ausarbeitung des Rechtsrahmens in einer Form, die einer späteren Anerkennung der schweizerischen E-ID bei der EU, bzw. einzelner EU-Mitgliedstaaten, grundsätzlich ermöglicht. Der VE hält die Vorgaben der eIDAS-Verordnung und der Durchführungsbeschlüsse[8] der EU ein.

Schnittstelle

Die Identitätsstelle stellt die beim Bund geführten Personenidentifizierungsdaten über eine elektronische Schnittstelle für die anerkannten IdP bereit (Art. 20 VE). Durch die Etablierung einer E-ID-Registrierungsnummer können die Personenidentifizierungsdaten eindeutig und dauerhaft einer Person und ihrer E-ID widerspruchsfrei zugeordnet werden. Diese Schnittstelle ist ausschliesslich den anerkannten IdP zugänglich.

Die Identitätsstelle ist für den Betrieb der Schnittstelle zur Übermittlung der Personenidentifizierungsdaten verantwortlich. Sie ist Ansprechstelle einerseits für die anerkannten IdP und andererseits für die Betreiber der angeschlossenen staatlichen Register.

Die Identitätsstelle bezieht die verschiedenen Personenidentifizierungsdaten aus unterschiedlichen Registern (Art. 20 VE). Der Name einer Person wird aus Infostar bestätigt, wohingegen beispielsweise die Ausweisnummer oder das Gesichtsbild aus ISA resp. ZEMIS stammen. Die Personenidentifizierungsdaten können mit zusätzlichen Metadaten, wie etwa eine Quellenangabe oder dem Datum der Erhebung, ergänzt werden (Art. 7 Abs. 3 VE).

[8] Vgl. Zusammenstellung im Fundstellennachweis

Die IdP sind gehalten, die zu einer E-ID-Registrierungsnummer bezogenen Personenidentifizierungsdaten periodisch zu aktualisieren. Je nach Sicherheitsniveau müssen die IdP die Aktualisierungen jährlich (Sicherheitsniveau „*niedrig*“), quartalsweise (Sicherheitsniveau „*substanziell*“) oder wöchentlich (Sicherheitsniveau „*hoch*“) vornehmen (Art. 8 Abs. 1 VE).

Anerkennungsstelle für Identitätsdienstleister (Anerkennungsstelle)
Anerkennung
Geeignete IdP (privatwirtschaftliche und solche der öffentlichen Hand) können sich und ihre E-ID-Systeme auf einem der vorgesehenen Sicherheitsniveaus von der Anerkennungsstelle anerkennen lassen. Ein IdP kann mehrere E-ID-Systeme auf unterschiedlichem Sicherheitsniveau betreiben und alle oder nur einzelne anerkennen lassen. Dazu werden vom Bundesrat rechtliche, organisatorische und technische Auflagen für die IdP festgelegt, deren Erfüllung von der Anerkennungsstelle überprüft wird.

Die Anerkennungsstelle publiziert eine Liste mit den anerkannten IdP und E-ID-Systemen, anhand derer die Betreiberinnen von E-ID-verwendenden Diensten und natürliche Personen den Status eines konkreten IdP resp. E-ID-Systems prüfen können (Art. 22 VE).

Aufsicht
Die Anerkennungsstelle übt die Aufsicht über die anerkannten IdP und E-ID-Systeme aus und reagiert im Falle von Abweichungen von den Vorgaben oder Vorfällen im IKT-Sicherheitsbereich. Dazu fordert die Anerkennungsstelle von den anerkannten IdP in den festgelegten zeitlichen Abständen die notwendigen Konformitätsnachweise ein und prüft sie. Die Anerkennungsstelle kann einem IdP oder E-ID-System Massnahmen auferlegen und unter bestimmten Voraussetzungen die Anerkennung entziehen (Art. 12 VE).

1.3 Begründung und Bewertung der vorgeschlagenen Lösung

1.3.1 Marktlösung

Bereits heute sind verschiedene E-ID im Gebrauch. Zum Beispiel wird mit der Anmeldung beim mobilen internetfähigen Gerät in der Regel ein E-ID-Profil erstellt (z. B. AppleID, Google ID). Damit kann die Inhaberin oder der Inhaber sich auch auf einfache Weise bei anderen Internet-Diensten registrieren lassen. Diese anderen Dienste vertrauen dabei auf diese Identifizierung.

Staatliche Internet-Dienste im E-Government-Bereich sind angewiesen auf eine eindeutige und vertrauenswürdige Identifizierung, die durch standardisierte Prozesse sicherstellt, dass der Inhaber oder die Inhaberin einer E-ID verifiziert wurde. Mehrere Staaten haben eigene E-ID herausgegeben, bei denen entweder alles in staatlicher Hand ist oder private Lösungen anerkannt wurden. Diese rein staatlichen Lösungen beinhalten jedoch keine Garantie für die Akzeptanz beim Bürger und sind für die öffentliche Hand mit einem hohen Investitions- und insbesondere Betriebsaufwand verbunden. Rein staatliche Systeme können mit der Entwicklung der Technologien nur sehr schwer und mit kostspieligen Anpassungen oder gestützt auf eine Neuausschreibung mithalten. Staatliche Lösungen erreichen vielfach nicht die gewünschte Verbreitung und werden zum Teil unter Zwang und nur einmal jährlich zum Einreichen der Steuererklärung eingesetzt. Weitere Ausführungen zu den Entwicklungen der staatlich herausgegebenen E-ID finden sich unter Ziffer 1.5.

Die vorgeschlagene Lösung entlastet den Staat grösstenteils von dieser Marktdynamik und den damit verbundenen hohen Kosten.

Mittlerweile gibt es verschiedene vertrauensschaffende elektronische Identitäten auch von inländischen IdP auf dem Markt, deren Akzeptanz stetig wächst (z. B. Mobile ID der Mobiltelefonieanbieterinnen oder die SuisseID der Post). Diese E-ID-Systeme sollen durch die Anerkennung gestärkt werden und im E-Government-Bereich zur Anwendung kommen. Darüber hinaus sollen die klaren Regeln auch weitere mögliche IdP dazu motivieren, sich auf diesen Markt zu begeben (z. B. Banken oder Kreditkartenherausgeberinnen).

Die Anforderungen an schweizerische anerkannte E-ID-Systeme werden so ausgestaltet, dass sie die Voraussetzungen für eine Notifizierung von E-ID-Systemen gemäss der eIDAS-Verordnung möglichst erfüllen werden.

1.3.2 Anerkennungsverfahren

Im Bereich der elektronischen Signatur wird das Anerkennungsverfahren durch eine private Anerkennungsstelle durchgeführt. Diese Anerkennungsstelle ist nach dem Akkreditierungsrecht für die Anerkennung und die Überwachung der Anbieterinnen von Zertifizierungsdiensten akkreditiert. Die Akkreditierung wiederum erfolgt durch eine vom Bundesrat bezeichnete Akkreditierungsstelle.

Demgegenüber ist bei den Plattformen für die sichere Übermittlung eine Verwaltungseinheit des EJPD – das Bundesamt für Justiz BJ – zuständig für die Entgegennahme und Prüfung der Gesuche um Anerkennung. Nur die Einhaltung der technischen Standards wird im Detail nach den Regeln des Akkreditierungsrechts beurteilt. Die Voraussetzungen und das Verfahren für die Anerkennung von Plattformen für die sichere Zustellung regelt die Anerkennungsverordnung Zustellplattformen vom 16. September 2014 (SR 272.11). Technische Vorgaben und die genaue Bezeichnung der aktuellsten Standards, die einzuhalten sind, werden als Anhang zu dieser Verordnung aufgeführt und im Internet auf den Seiten des BJ publiziert. So wird sichergestellt, dass die technische Entwicklung im Bereich der sicheren Übermittlung zeitnah berücksichtigt werden kann.

Dieses Vorgehen ist einfacher und hat sich bewährt. Deshalb wird das Anerkennungsverfahren für IdP demjenigen für Zustellplattformen nachgebildet: Die Anerkennungsstelle ist gemäss vorliegendem Erlass zuständig für die Entgegennahme und Prüfung der Gesuche um Anerkennung von IdP und E-ID-Systemen und übt damit die gleiche Funktion aus wie das BJ im Bereich der Anerkennung von Zustellplattformen. Es ist vorgesehen, dass die technischen Vorgaben und die Bezeichnung der einzuhaltenden Standards wiederum als Verordnung eines Departementes erlassen und aktualisiert werden. Sie werden auf die bestehenden Regelungen im Bereich der elektronischen Signaturen und Zustellplattformen abgestimmt, so dass für anerkannte IdP Synergien bei den verlangten Zertifizierungen entstehen.

1.4 Abstimmung von Aufgaben und Finanzen

1.4.1 Neue Aufgaben

Das E-ID-Gesetz bringt neue Aufgaben für die Bundesverwaltung. Einerseits wird die Identitätsstelle mit der Bereitstellung einer Schnittstelle zur Übermittlung von Personenidentifizierungsdaten beauftragt, andererseits braucht es die Anerkennungsstelle, die Anerkennungen

vornimmt und die anerkannten IdP beaufsichtigt (vgl. Ziffer 1.2.6). Diese beiden Stellen müssen nicht der gleichen Verwaltungseinheit des Bundes zugeordnet werden.

Die Identitätsstelle ist für die folgenden Aufgaben zuständig:
a) Anwendungsverantwortung und Pflege der bei der Identitätsstelle notwendigen IKT-Infrastruktur (Schnittstelle zu den IdP und Anbindung der bundesinternen Datenquellen wie ISA, Infostar usw.),
b) Fachsupport für die beteiligten bundesinternen Datenbanken,
c) Fachsupport für die anerkannten IdP,
d) Erarbeitung und Pflege der organisatorischen und technischen Vorgaben für die Anerkennung von IdP und E-ID-Systemen,
e) Beschaffung der beim Bund notwendigen IdP-Dienstleistungen, sowie
f) Informationsbeschaffung über aktuelle technologische Entwicklungen im Bereich E-ID und zugehörige Fragen der IKT-Sicherheit.

Artikel 19 VE erwähnt die Identitätsstelle als Verwaltungseinheit des EJPD (fedpol). Das EJPD (fedpol) ist zuständig für die Rechtsetzung im Bereich Ausweisschriften und hat die E-ID-Konzepte ausgearbeitet. Die meisten Datenbanken, die als Quellen für die Bestätigung der Personenidentifizierungsdaten dienen, werden beim EJPD geführt. Für die allenfalls notwendige Bereinigung von Personenidentifizierungsdaten könnte auf die bestehende Clearingstelle der ZAS-UPI zurückgegriffen werden.

Die Anerkennungsstelle hat folgende Aufgaben:
a) die Anerkennung von IdP,
b) die Beaufsichtigung und Überwachung der anerkannten IdP und deren E-ID-Systeme, und
c) die Pflege und Publikation der Liste der anerkannten IdP.

Die Anerkennungsstelle nimmt neben den Anerkennungs- auch Aufsichtsfunktionen wahr, die denjenigen der Aufsichtsstelle gemäss eIDAS gleichkommen. Weitere entsprechende Aufsichtsfunktionen werden beim Bund durch das EFD (ISB) wahrgenommen. Der VE erwähnt deshalb in Artikel 21 die Ansiedlung der Anerkennungsstelle beim EFD (ISB).

1.4.2 Finanzierung

Vorleistungen des Bundes
Für die Einführung anerkannter E-ID sind beim Bund finanzielle Mittel von insgesamt 6,5 Millionen Franken erforderlich. Da es sich bei der Einführung von anerkannten E-ID um ein strategisches Vorhaben handelt, welches den öffentlichen Verwaltungen bei Bund, Kantonen und Gemeinden sowie der Privatwirtschaft und der Bevölkerung gleichermassen zu Gute kommt, wird eine Co-Finanzierung beantragt, welche vom EJPD, von E-Government Schweiz und aus zentralen IKT-Mitteln des Bundes getragen wird.

Aus heutiger Sicht wird mit IKT-Betriebskosten von jährlich rund 1,5 Millionen Franken gerechnet. Hinzu kommen die Personalkosten von rund 0,7 Millionen Franken. Diese Ausgaben werden aber mittelfristig durch die Einnahme von kostendeckenden Gebühren ausgeglichen. Das Finanzierungskonzept für die Betriebskosten wird nach der Vernehmlassung zusammen mit der Botschaft vorgelegt werden.

Gebührenfinanzierung
Für die Leistungen des Staates gegenüber dem IdP wurden verschiedene Finanzierungsmodelle geprüft. Verworfen wurde ein „prepaid“-Modell, bei dem die IdP dem Staat eine möglichst kostendeckende Gebühr überweist, ohne sicher sein zu können, durch die schnelle Verbreitung der E-ID entsprechende Einnahmen zu generieren. Verworfen wurde auch die kostenlose Überprüfung der bestätigen Daten über die Erstbestätigung hinaus, da dadurch erhebliche Defizite generiert werden, was aufgrund der politischen Sparvorgaben nicht angebracht ist. Vorgeschlagen wird nun ein gebührenfinanziertes „pay-per-use“-Modell.

Für dieses Modell wird eine Gebührenverordnung erlassen werden. Zur Beschleunigung der Verbreitung der E-ID, kann die Erstübermittlung von Personenidentifizierungsdaten im Herausgabeprozess unentgeltlich gestaltet werden, sofern der Bezug für die antragsstellende Person auch unentgeltlich ist, für jede weitere Übermittlung von Personenidentifizierungsdaten wird hingegen eine moderate Gebühr erhoben. Diese wird sich aufgrund einer noch zu erlassenden bundesrätlichen Verordnung im Rahmen eines zweistelligen Rappenbetrages bewegen. Je nach Verbreitung von anerkannten E-ID, insbesondere der Sicherheitsniveaus „*substanziell“* und „*hoch“*, werden damit neue Einnahmen für einen ausreichenden Kostendeckungsgrad erreicht.

Abgeltung durch die Betreiberinnen von E-ID-verwendenden Diensten
Von der Anwendung der E-ID profitieren in erster Linie die Betreiberinnen von E-ID-verwendenden Diensten, unabhängig davon, ob es sich um private Unternehmen oder Behörden handelt: Sie können durch den Gebrauch von E-ID ihre Prozesse vereinfachen und damit die eigenen Kosten senken (z. B. weniger Schalter, Papier und Medienbrüche, rascherer Durchlauf, innovative Geschäftsmodelle). Betreiberinnen von E-ID-verwendenden Diensten dürften deshalb bereit sein, die Anwendung der E-ID-Systeme zu entgelten. Wie die Abrechnung der Dienstleistung erfolgt, soll dem Markt überlassen werden.

1.5 Staatliche elektronische Identifizierungsmittel im internationalen, insbesondere europäischen Umfeld

1.5.1 Vorbemerkung

Die Schweiz befindet sich mit der Einführung eines elektronischen Identifizierungsmittels nicht allein. Das Thema ist seit gut 15 Jahren auf der Agenda vieler Staaten. In Anbetracht der globalen Natur von Online-Diensten im Internet, ist es wichtig, ein vom Staat anerkanntes elektronisches Identifizierungsmittel in konzeptioneller, technischer und rechtlicher Hinsicht so zu gestalten, dass es später international eingesetzt werden kann, insbesondere im europäischen Raum. In der eIDAS-Verordnung und den entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das Konzept für schweizerisch anerkannte E-ID-Systeme richtet sich an diesen internationalen Vorgaben aus, sodass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten.

Unter anderem wird mit dem vorliegenden Gesetz ein Rechts- und Standardisierungsrahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der IdP geschaffen. Dieser ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der E-ID-Systeme zwischen

der Schweiz und der EU, oder einzelner Mitgliedstaaten, möglich bleibt. Dazu wären bilaterale Verträge nötig.

1.5.2 Entwicklungen in den letzten fünfzehn Jahren

In der ersten Phase der Beschäftigung der Staaten mit dem Thema der E-ID ging es primär um die Frage, ab wann, mit welcher Technologie und mit welchen Funktionen ein Staat seine Identitätskarte um die E-ID erweitern würde.

Die wesentlichen Fragen waren, welche Chip-Technologie verwendet würde, welches Chip-Betriebssystem und ob der Chip kontaktbasiert oder per Funk (NFC) mit der Umwelt kommunizierte. Ein wichtiges juristisches und politisches Thema war, ob sich die E-ID auf einen bestehenden Personenidentifikator bezog und welcher Art dieser war. In funktioneller Hinsicht war zu entscheiden, ob der Chip gleichzeitig einen Schlüssel für die elektronische Signatur enthielt, und später, ob auch die inzwischen von der Internationale Zivilluftfahrtorganisation (ICAO von englisch International Civil Aviation Organization) standardisierte elektronische Pass-Funktion mit Funktechnologie enthalten sei.

Mit solchen Überlegungen haben in den letzten fünfzehn Jahren nach und nach die meisten europäischen Staaten eine mit der Identitätskarte verbundene E-ID als Kernstück eines nationalen E-ID-Systems eingeführt. Pionier war Finnland, welches im Jahr 1999 eine Identitätskarte mit E-ID herausgab. Es folgten Estland, Belgien, Spanien und Portugal. Deutschland hat im Jahr 2010 einen elektronischen Personalausweis (ePA) eingeführt. In den letzten Jahren haben insbesondere Länder im Nahen Osten und in Asien neue staatliche Identitätskarten mit E-ID-Funktion herausgegeben. Nicht selten vielleicht auch darum, weil man auf keinen Fall in Rückstand geraten wollte. Hingegen haben weder die USA noch das Vereinigte Königreich eine staatliche E-ID eingeführt, was sich mit der generellen Skepsis gegenüber Identitätskarten in diesen Ländern deckt, dafür aber haben mehrere US-Bundesstaaten E-Führerausweise eingeführt.

Eine erste typische Konstellation waren SmartCards mit kontaktbasierten Chips, aufbauend im Wesentlichen auf der Technologie der Signaturkarten. Beispiele dieser Art waren die finnische, die estnische und die belgische E-ID-Karte, sowie übrigens im Kern auch die SuisseID.

Eine weitere verbreitete Konstellation ergab sich aus den Bemühungen der europäischen Chip-Industrie, ein Set von Standards mit Optionen für eine European Citizen Card (ECC) zu definieren. Diese Karten enthalten die E-Pass-Funktion gemäss ICAO sowie eine daran angelehnte Funktion für die elektronische Online-Identifikation. Schweden, Monaco, Lettland, Finnland (2. Auflage) und die Niederlande haben solche Identitätskarten. Der ECC-Standard hat sich nie ganz stabilisieren können. Eine Ausprägung davon hat sich aber insbesondere in den EU-Mitgliedstaaten bei den Ausländerausweisen (Aufenthaltspapiere für Drittstaatenangehörige) durchgesetzt. Grund dafür ist, dass die EU in diesem Bereich – im Unterschied zu den Identitätskarten – legiferieren darf. Auch der schweizerische biometrische Ausländerausweis folgt diesem Standard.

Eine Art Kulminationspunkt dieser Phase der E-ID-Entwicklung ist der 2010 von Deutschland eingeführte elektronische Personalausweis (ePA). Er enthält im Wesentlichen die vorstehend erwähnten Komponenten, wurde aber an einigen Punkten verbessert und insbesondere um mehrere technisch anspruchsvolle Verfahren zur Verstärkung des Persönlichkeitsschutzes erweitert. So müssen sich Dienstanbieter (Service Provider, Betreiberinnen von E-ID-

verwendenden Diensten) für den Bezug bestimmter Attribute vom Staat registrieren lassen und sich bei der Anwendung ebenfalls authentisieren.

Mit einer übergreifenden Strategie hat Deutschland dafür gesorgt, dass die Aufenthaltstitel für Ausländerinnen und Ausländer mit kompatiblen «Online-Ausweisfunktionen» ausgestattet sind. In den letzten Jahren ist der deutsche ePA ein Stück weit die Messlatte für neue staatliche E-ID weltweit geworden. In Deutschland ist inzwischen etwa die Hälfte der Bevölkerung mit dem ePA ausgerüstet und noch ist nicht klar, ob die E-ID-Funktion tatsächlich einmal breit eingesetzt werden wird. Es zeigt sich, dass der ePA insbesondere in der Privatwirtschaft und bei den Bürgerinnen und Bürgern wenig Akzeptanz findet, weil er zwar bezüglich Sicherheit hervorragend, aber in der täglichen Handhabung zu kompliziert und zu teuer ist. Weiter müssen von den Bürgerinnen und Bürgern Infrastrukturkomponenten wie Lesegeräte und Software angeschafft und eingesetzt werden. Zudem muss der Staat konstant Änderungen und Updates bei diesen Komponenten entwickelt und verteilt werden, was den Betrieb stark verteuert.

Auch andere E-ID-Lösungen, die zusätzliche Infrastrukturkomponenten bei den Bürgerinnen und Bürgern verlangen, haben Akzeptanzprobleme. Zu einem richtigen Durchbruch hat es die klassische auf einer Karte basierende E-ID nirgends richtig geschafft. Jedoch hat sich gezeigt, dass verschiedene flexible Lösungen auf Smartphones eine höhere Akzeptanz erreichen. Auch im bezüglich E-ID Einsatz führenden Estland werden E-ID heute hauptsächlich über ein Smartphone als Trägergerät eingesetzt.

1.5.3 Alternative Lösungswege

In den letzten Jahren hat sich der Fokus der Überlegungen zur staatlichen Förderung der E-ID in eine neue Richtung entwickelt. Der wichtigste Grund dürfte sein, dass der Produktezyklus einer staatlichen Identitätskarte im Vergleich zur Geschwindigkeit der Entwicklung in der elektronischen Welt viel zu lang ist.

Angeführt vom US-amerikanischen Projekt der gemeinsamen Entwicklung eines Identity Ecosystems[9] begann man sich in vielen Ländern grundsätzlicher zu überlegen, wie eine gute Architektur für das gesamte nationale und internationale Oekosystem rund um die E-ID, unter Einbezug aller Akteure auszusehen hätte und welchen Beitrag der Staat dazu leisten kann. Die einzelnen Länder kamen dabei zu unterschiedlichen Schlüssen. In den USA beschränkt sich die Rolle des Staates auf die eines Organisators und Förderers des E-ID-Oekosystems; er stellt selbst keine Dienste zur Verfügung, hat jedoch einen grossen Einfluss auf den Markt als Bezüger von E-ID für seine Mitarbeitenden und als Betreiberin von E-ID-verwendenden Diensten im Rahmen der E-Government-Angebote. In den USA sind auch wichtige konzeptionelle Grundlagen für ein vertrauenswürdiges interoperables Identitätsmanagement erarbeitet worden.

In Schweden, Norwegen und Dänemark wurden die Banken zu den wichtigsten Anbietern von E-ID für alle Branchen erkoren, bieten sie doch für ihre eigenen Dienstleistungen schon länger solche Produkte an. Staatliche Minimalanforderungen sorgen für eine definierte Qualität und Interoperabilität. Diese E-ID werden bei staatlichen Stellen akzeptiert und können bei E-Government-Anwendungen eingesetzt werden.

---

9 National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem. Vgl. Link im Fundstellennachweis

Die EU hat in der vorstehend schon erwähnten eIDAS-Verordnung diese Entwicklung schliesslich nachvollzogen und akzeptiert für die gegenseitige Anerkennung neben den vom Staat herausgegebenen E-ID auch staatlich anerkannte, von der Privatwirtschaft betriebene E-ID-Systeme.

1.5.4 Folgerungen für die Schweiz

Wenn staatliche Systeme auf eine feste Verbindung der E-ID mit einem konventionellen Ausweis setzen, beispielsweise mittels Chip auf der IDK, können sie mit der Entwicklung der Technologien nur sehr schwer und mit kostspieligen Anpassungen mithalten. Ausgehend von den Erfahrungen in den Nachbarländern drängt sich deshalb für die Schweiz eine andere Lösung auf. Diese entlastet den Staat von dieser technologischen Dynamik und den damit verbundenen hohen Kosten. Gleichzeitig bietet sie der Privatwirtschaft den nötigen Raum für flexible und ihren Bedürfnissen angepassten Lösungen. Die Rolle des Staates wird dabei auf das notwendige Minimum der Bereitstellung einer Vertrauensbasis beschränkt.

Ein Vergleich des im Gesetzesentwurf umgesetzten Konzepts für die Anerkennung elektronischer Identifizierungseinheiten mit den Entwicklungen, Erfahrungen und aktuellen Überlegungen im internationalen Umfeld ergibt folgendes Bild:

- Die Schweiz hat die Lehren aus den Erfahrungen der letzten fünfzehn Jahre gezogen und geht mit ihrem Konzept einer anerkannten E-ID einen neuen Weg, der von verschiedenen Stellen als wegweisend beurteilt wird.
- Das schweizerische Konzept ist grundsätzlich EU-, bzw. eIDAS-konform.
- Das schweizerische Konzept berücksichtigt die aktuellsten theoretischen und technischen Grundlagen für ein Identitätsmanagement in digitalen Ökosystemen, z. B. diejenige von NIST.
- Das schweizerische Konzept ist sehr flexibel und kann durch die ausreichende Flexibilität auch einschneidende technologische und ökonomische Entwicklungen nachvollziehen.

1.5.5 eIDAS und Anforderungen für eIDAS-Kompatibilität

Ist schon für den klassischen Ausweis mit sichtbaren Daten die internationale Verwendbarkeit als Reisedokument und zur Identifizierung im Ausland wichtig, so trifft dies erst recht für die E-ID zu. Selbst wenn eine E-ID vorläufig nicht als Reisedokument dient, wird sie als Online-Ausweis im 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.

Am 23. Juli 2014 hat die EU die eIDAS-Verordnung erlassen. Nebst der Regelung und Zertifizierung der Anbieter der elektronischen Signatur und weiterer Vertrauensdienste enthält die Verordnung als neues Thema die Notifikation und damit verbunden die gegenseitige Anerkennung von nationalen Systemen für die elektronische Identifizierung. Alle Mitgliedstaaten werden verpflichtet, überall dort, wo sie für den Zugang zu Behördendiensten eine E-ID verlangen, auch jede ausländische E-ID aus jedem notifizierten System zuzulassen (Art.6 eIDAS-Verordnung). Diese Verpflichtung gilt selbst für einen Mitgliedstaat, der selbst kein notifiziertes E-ID-System besitzt.

Welche Anforderungen sind an ein schweizerisches E-ID-System zu stellen, wenn dieses konform zur eIDAS-Verordnung sein soll, damit es später gegebenenfalls notifiziert werden könnte? Selbstverständlich gibt es für die Schweiz keine rechtliche Verbindlichkeit zur Über-

nahme 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. Auch wenn vorläufig völlig offen ist, ob, wann und wie die Schweiz sich mittels eines bilateralen Vertrags in dieses System einbinden wird, soll das schweizerische E-ID-System von Beginn an so konzipiert werden, dass es grundsätzlich notifiziert werden könnte.

Mit dem vorliegenden Gesetz wird u. a. ein Rechts- und Standardisierungsrahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der IdP geschaffen. Dieser ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der anerkannten E-ID-Systeme zwischen der Schweiz und der EU, oder einzelner Mitgliedstaaten, möglich bleibt.

1.6 Umsetzung

Die Einführung der anerkannten E-ID trägt zur Umsetzung der Strategie „Digitale Schweiz“ und des operativen Ziels Nr. 5 des Schwerpunktplans der E-Government Strategie Schweiz bei (vgl. Ziffer 3).

Im Rahmen des Auftrags zur Erneuerung des Schweizer Passes wurden im EJPD Konzepte erarbeitet und erste Vorarbeiten geleistet, die auch für die Umsetzung der E-ID herangezogen werden können. Ein System von Bundesrats- und Departementsverordnungen sowie Weisungen wird organisatorische und technische Details der Umsetzung regeln. Die Erarbeitung dieser weiteren Erlasse beginnt, sobald die Gesetzesvorlage in den Räten behandelt wurde.

Darüber hinaus braucht es die Bestimmung der Verwaltungseinheiten, bei denen die Identitätsstelle und die Anerkennungsstelle angesiedelt sind.

1.7 Struktur

Der erste Abschnitt des Gesetzesentwurfs enthält die allgemeinen Bestimmungen sowie Begriffe. Im zweiten Abschnitt wird die Ausstellung der E-ID geregelt: die persönlichen Voraussetzungen für Bezügerinnen und Bezüger, die Anerkennung von IdP, der Ausstellungsprozess und die Sicherheitsniveaus. Der dritte Abschnitt bestimmt die Pflichten der Inhaberinnen und Inhaber von E-ID. In weiteren Abschnitten werden die Pflichten der Betreiberinnen von E-ID-verwendenden Diensten und der IdP statuiert. In den Abschnitten sechs und sieben werden die Organisation und die Aufgaben der Identitätsstelle und der Anerkennungsstelle festgelegt. Die Kompetenz zur Regelung der Gebühren wird im achten Abschnitt geregelt und der neunte Abschnitt weist auf die Haftungsregeln hin. Das Gesetz endet, wie jeder Erlass, mit Schlussbestimmungen im zehnten Abschnitt. In einem Anhang wird die Änderung anderer Erlasse geregelt.

1.8 Erläuterung E-ID-Gesetz

1.8.1 Ingress

Die Kompetenz zur Regelung von anerkannten elektronischen Identifizierungseinheiten (E-ID) ergibt sich indirekt aus der Bundesverfassung vom 18. April 1999 (BV, SR 101). Erwähnt werden insbesondere Artikel 95 Absatz 1 BV, die den Bund ermächtigt, wirtschaftspolizeiliche Vorschriften über die Ausübung privatwirtschaftlicher Erwerbstätigkeit zu machen. Die Ausstellung von E-ID wird anerkannten Identitätsdienstleistern überlassen. Für die Anerkennung müssen diese verschiedene Auflagen erfüllen, was die privatwirtschaftliche Erwerbstätigkeit einschränkt.

Insoweit die Vertragsverhältnisse zwischen den Identitätsdienstleistern, Inhaberinnen und Inhabern sowie Betreiberinnen von E-ID-verwendenden Diensten betroffen sind, werden im vorliegenden Bundesgesetz zivilrechtliche Aspekte geregelt. Es stützt sich deshalb auch auf Artikel 122 Absatz 1 BV, der dem Bund die Kompetenz zur Regelung des Zivilrechts gibt.

1.8.2 1. Abschnitt: Allgemeine Bestimmungen

Artikel 1 Gegenstand und Zweck

Absatz 1

Das Gesetz regelt neben der Anerkennung der Anbieterinnen und Anbieter von Identitätsdienstleistungen auch die Rechte und Pflichten der Inhaberinnen und Inhaber einer E-ID und der Betreiberinnen von E-ID-verwendenden Diensten, sowie Inhalt, Ausstellung, Widerruf und Verwendung von anerkannten elektronischen Identifizierungseinheiten (E-ID).

Absatz 2 Buchstabe a und b

Die E-ID trägt dazu bei, Sicherheit und Vertrauen im elektronischen Geschäftsverkehr (E-Business und E-Government) aufzubauen. Schweizerinnen und Schweizer und Ausländerinnen und Ausländer mit entsprechenden Identitätspapieren sollen sich zukünftig auch in der elektronischen Welt vertrauenswürdig ausweisen können. Genau wie mit einem Identitätsausweis in der physischen Welt, können damit Personenidentifizierungsdaten, wie zum Beispiel Name, Vornamen oder Alter, in der Online-Welt nachgewiesen werden. Der Hauptnutzen einer E-ID besteht darin, dass sie vertrauenswürdige Online-Geschäfte wie E-Government oder E-Business ermöglicht, ohne dass sich die Geschäftspartnerinnen und -partner physisch treffen müssen. Die E-ID trägt dazu bei, den Übergang der Schweiz zu einer entwickelten Informationsgesellschaft zeitgerecht und gut zu schaffen.

Artikel 2 Begriffe

Bei der Wahl der Begriffe wurde einerseits die Terminologie des ZertES und andererseits diejenige der eIDAS-Verordnung soweit als möglich berücksichtigt. Insbesondere werden die international gebräuchlichen Abkürzungen der englischen Begriffe eingeführt und im Gesetz verwendet.

Buchstaben a und b

Im Kontext dieses Gesetzes, ist mit E-ID immer die anerkannte elektronische Identifizierungseinheit gemeint. Die anerkannte E-ID ist jedoch nicht die einzige elektronische Identifizierungseinheit. Wie bereits im ersten Teil der Erläuterungen erwähnt, gibt es bereits heute mehrere elektronische Identifizierungsangebote verschiedener Sicherheitsniveaus.

Der Begriff der "E-ID" entstand aus der ursprünglichen Konzeption der elektronischen Identifizierungsmittel (Abgabe mit der staatlichen Identitätskarte, vgl. Ausgangslage Ziff. 1.1). Obwohl nun darauf verzichtet wird, das elektronische Identifizierungsmittel auf dem Personalausweis, bzw. der schweizerischen Identitätskarte (ID oder IDK) oder dem Ausländerausweis anzubringen, hat sich der Begriff "E-ID" oder international auch „eID“ weit verbreitet. Zudem folgt die Bezeichnung "E-ID" einer einfachen Logik: die E-ID kann im elektronischen Geschäftsverkehr das Gleiche wie ein konventioneller Identitätsausweis mit Gesichtsbild in Kombination mit einer persönlichen Begegnung, nämlich die Identität der Inhaberin oder des Inhabers nachweisen.

Mit E-ID ist im Folgenden ausschliesslich die elektronische Identifizierungseinheit gemeint, die von einem IdP nach den Vorgaben des vorliegenden Gesetzes ausgestellt wird.

Buchstabe c
Der Begriff „Identity Provider – IdP“ ist national und international geläufig. Deshalb wird für den Anbieter von Identitätsdienstleistungen nach diesem Gesetz die Abkürzung „IdP“ verwendet.

Buchstaben d und e
Eine Identifizierung findet bei der Registrierung beim IdP (Bezug einer E-ID) und bei der Registrierung bei einem E-ID-verwendenden Dienst (Informatikanwendung) statt. Identifizierung bedeutet, dass die Identität einer Person in Form ihrer Personenidentifizierungsdaten und Authentifizierungsfaktoren in einem kontrollierten Prozess registriert wird.

Eine Authentifizierung findet bei jeder weiteren Anmeldung beim E-ID-verwendenden Dienst statt. Authentifizierung bedeutet, dass die registrierte und von der Person angegebene Identität mittels den Authentifizierungsfaktoren der E-ID in einem kontrollierten Prozess überprüft wird.

Buchstabe f
Die Personenidentifizierungsdaten sind die staatlich erfassten Identitätsattribute einer Person wie Name oder Geburtsdatum usw. Dieser staatlich geführte Datensatz enthält auch eine E-ID-Registrierungsnummer, die als Anker für die Personenidentifizierungsdaten dient.

Buchstabe g
Das E-ID-Gesetz führt eine vom Staat eindeutig zugeordnete Identifikationsnummer für natürliche Personen ein (E-ID-Registrierungsnummer). Analog zur Unternehmens-Identifikationsnummer UID[10] soll jeder Person, die eine E-ID bezieht, eine E-ID-Registrierungsnummer zugeordnet werden. Da es grundsätzlich möglich und jedenfalls nicht verboten ist, mehrere E-ID zu führen (z. B. auf verschiedenen Trägern), wird über die E-ID-Registrierungsnummer die jeweilige widerspruchsfreie Zuordnung der Personenidentifizierungsdaten zu ein und derselben Person erreicht. Zudem kann mit der E-ID-Registrierungsnummer sichergestellt werden, dass die von den verschiedenen Personenregistern bezogenen Daten dauerhaft einer bestimmten Person zugeordnet werden. Dies sichert die Datenintegrität der mit einer E-ID verwendeten Personenidentifizierungsdaten.

---

[10] Vgl. Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG, SR 431.03)

Buchstabe h
Der IdP betreibt mindestens ein E-ID-System. Die Trennung von IdP und E-ID-System ist für die Anerkennung wichtig. Bei der Anerkennung eines IdP werden insbesondere die Erfüllung der Voraussetzungen gemäss Artikel 4 VE und die Prozesse in Bezug auf die Ausstellung und den Betrieb geprüft. Wohingegen bei der Anerkennung eines E-ID-Systems die Einhaltung der technischen Sicherheitsvorgaben im Vordergrund stehen. Es ist möglich, dass ein anerkannter IdP mehrere E-ID-Systeme auf verschiedenen Sicherheitsniveaus betreiben wird, die allenfalls nicht alle anerkannt sind. Weitere Bestimmungen zur Anerkennung finden sich in Artikel 4 ff. VE.

Buchstabe i und j
Auch bei der Betreiberin von E-ID-verwendenden Diensten wird zwischen der natürlichen oder juristischen Person als Betreiberin und der technischen Anwendung unterschieden. Die Kommunikation findet entweder zwischen Menschen, nämlich dem IdP und der Betreiberin von E-ID-verwendenden Diensten (relying party), oder Informatikanwendungen, nämlich dem E-ID-System und dem E-ID-verwendenden Dienst (relying party application), statt.

Zu den juristischen Personen, die einen E-ID-verwendenden Dienst betreiben können, gehören auch Bund, Kantone und Gemeinden bzw. Verwaltungseinheiten oder Behörden, die zu ihnen gehören und für sie handeln.

1.8.3 2. Abschnitt: Ausstellung von E-ID

Artikel 3 Persönliche Voraussetzungen
Vorbemerkung
Kein IdP soll verpflichtet sein ein Vertragsverhältnis eingehen zu müssen, nur weil jemand die Voraussetzungen erfüllt. Durch die Kann-Formulierung in Absatz 1 wird sichergestellt, dass ein IdP nicht zur Ausstellung einer E-ID gezwungen werden kann.

Durch den Bezug einer E-ID werden die antragsstellenden Personen zu Inhaberinnen und Inhaber einer E-ID.

Absatz 1
Ausweis als Identitätsnachweis
Um eine staatlich anerkannte E-ID zu erhalten, muss die Identität der antragstellenden Person feststehen. Für die Ausstellung genügt ein gültiger Schweizer Ausweis (Bst. a) oder ein gültiger Schweizer Ausländerausweis (Bst. b).

Minderjährige
Für Minderjährige und für Personen, deren Handlungsfähigkeit teilweise oder vollständig entzogen worden ist, können E-ID ausgestellt werden. Für die vertretene Person muss ein entsprechender Ausweis ausgestellt sein. Die vertretungsberechtigte Person beantragt im Namen der vertretenen Person eine E-ID; die vertretene Person wird Inhaberin oder Inhaber der E-ID. Die Anwendung hat dann aber unter Aufsicht der vertretungsberechtigten Person zu erfolgen.

Ausländer
Die E-ID und damit die mögliche Nutzung von E-Government-Anwendungen soll auch Ausländerinnen und Ausländern offen stehen, die über einen gültigen Ausländerausweis gemäss

Artikel 41 des Bundesgesetzes vom 16. Dezember 2005 über die Ausländerinnen und Ausländer (Ausländergesetz, AuG, SR 142.20) verfügen.

Absatz 2
Der Ausländerausweis hält die Art der erteilten Bewilligung (z. B. in Bezug auf Niederlassung, Aufenthaltsberechtigung und Erwerbstätigkeit) fest. Er muss mit einem Gesichtsbild der Ausländerin oder des Ausländers sowie der Unterschrift versehen sein und alle den ausländerrechtlichen Status betreffenden Angaben enthalten. Das EJPD (SEM) legt die Form (biometrisch oder nicht) und den Inhalt des Ausweises fest.

Folgende Ausländerausweise werden aufgrund Artikel 71 Absatz 1 der Verordnung vom 24. Oktober 2007 über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE, SR 142.201) an Ausländerinnen und Ausländer in der Schweiz abgegeben und berechtigen ohne weiteres zum Bezug einer E-ID:

1. Ausweis „C“ für Niedergelassene Ausländerinnen und Ausländer;
2. Ausweis „B“ für Aufenthalterinnen und Aufenthalter;
3. Ausweis „L“ für die Ausübung einer kurzfristigen Erwerbstätigkeit und für andere vorübergehende Aufenthalte.

Diese Ausländerausweise können je nach Herkunftsland als biometrische oder als nicht biometrische Ausweise (heute Papier, ab 2019 Polycarbonat-Ausländerausweiskarte) ausgestellt werden. Dabei werden für Drittstaatsangehörige die Anforderungen gemäss dem Schengen-Assoziierungsabkommen berücksichtigt. Die Inhaberinnen und Inhaber dieser Ausweise erhalten eine Aufenthaltsbewilligung im Sinne von Artikel 41 Absatz 1 AuG.

Aufgrund von Artikel 71a Abs. 1 VZAE werden weiter die folgenden Ausländerausweise ohne oder mit beschränktem Aufenthaltsrecht ausgestellt:

1. Ausweis „G“ für Grenzgängerinnen und Grenzgänger;
2. Ausweis „N“ für Asylsuchende;
3. Ausweis „F“ für vorläufig aufgenommene Ausländerinnen und Ausländer (Art. 83 und 85 AuG) sowie für vorläufig aufgenommene Flüchtlinge (Art. 59 AsylG);
4. Ausweis „S“ für Schutzbedürftige;
5. Ausweis „Ci“ für erwerbstätige Ehepartner und Kinder von Angehörigen ausländischer Vertretungen oder intergouvernementaler Organisationen (IO).
6. Weiter erhalten Personen mit Vorrechten, Immunitäten und Erleichterungen aufgrund von Art. 71a Abs. 2 VZAE eine Legitimationskarte des EDA. Diese Karte ist nicht biometrisch.

Diese Kategorien von Ausländerausweisen berechtigen nicht ausnahmslos zum Bezug einer E-ID. Der Bundesrat legt fest, welche Kategorien von Ausländerausweisen, bzw. welche Ausländerinnen und Ausländer sich eine E-ID ausstellen lassen können (Abs. 2).

Damit so viele Ausländerinnen und Ausländer wie möglich mit einer E-ID Zugang zu E-Government-Anwendungen erhalten können, ist derzeit vorgesehen, dass alle Ausländerinnen und Ausländer, die über einen Ausländerausweis verfügen, der eine Aufenthaltsbewilligung erhält (Art. 41 Abs. 1 AuG i.V.m. Art. 71 Abs. 1 VZAE; Ausweis L, B, C) sowie die Grenzgänger (Art. 71a VZAE, Ausweis G) sich eine E-ID ausstellen lassen können. Im Bereich des Ausländerrechts ist der Einsatz von E-Government denkbar, wobei dort in den meisten Fällen die Kantone für die Kontakte zuständig sind. Der Bundesrat kann alternative Verfahren zur elektronischen Identifizierung vorsehen.

Für die übrigen Ausländerinnen und Ausländer, insbesondere die mit N-, F- und S-Ausweisen wird derzeit darauf verzichtet, ihnen den Zugang zu E-ID-Funktionen zu gewähren. Viele Asylsuchende können im Asylverfahren keine Identitätsdokumente einreichen, was eine sichere Identifizierung verunmöglicht. Selbst bei vorläufig aufgenommenen Personen werden im EJPD (SEM) zahlreiche Gesuchen um Änderung oder Berichtigung von Personendaten eingereicht, wobei diese Gesuche nicht selten mit nicht tauglichen Dokumenten untermauert werden. Derzeit sind im Asylbereich keine elektronischen Dienste vorgesehen, zu denen Personen mit N-, F- und S-Ausweisen einen direkten Zugang benötigen. Deshalb ist die Ausstellung einer E-ID für diesen Personenkreis nicht vordringlich.

Absatz 3
Die technische Entwicklung im Bereich der E-ID geschieht schnell. Die Identifizierungsprozesse können allenfalls den zulässigen Identifizierungsmethoden im Bankenbereich nachgebildet werden. Im Bankenbereich schreibt die Eidgenössischen Finanzmarktaufsicht FINMA genau vor, welche Methoden für die Identifizierung von Neukunden zulässig sind. Um flexibel auf neueste Technologien reagieren zu können, werden die Details zu den Voraussetzungen zum Bezug, der Prozess und die Sperrung oder Widerruf auf Verordnungsebene geregelt.

Eine Übersicht über die Delegation von Rechtsetzungsbefugnissen findet sich unter Ziffer 4.4.

Artikel 4 Anerkennung von IdP
Vorbemerkung
Mit der Anerkennung der Identitätsdienstleister werden auch deren E-ID-Systeme geprüft und anerkannt. Die technischen Anforderungen an die E-ID-verwendenden Systeme (relying party application) werden hingegen nur mittelbar durch die Anforderungen und Auflagen an die E-ID-Systeme geregelt. Diese Auflagen werden im Bereich Sicherheit und Vertrauen den NIST-Cybersecurity Framework-Anforderungen genügen[11].

Absatz 1 und 2
Will ein IdP anerkannte E-ID ausstellen, muss er verschiedene organisatorische und technische Vorgaben einhalten. Die Einhaltung der Vorgaben wird durch die Anerkennungsstelle für Identitätsdienstleister (Anerkennungsstelle) regelmässig überprüft. Die Einhaltung der Anforderungen stellt sicher, dass ausreichende Kontrolle über die IdP und über die bei ihnen allenfalls gespeicherten Daten ausgeübt werden kann.

Buchstaben a und b
IdP müssen einen Sitz in der Schweiz haben. Sowohl private als auch öffentliche Stellen können E-ID-Systeme betreiben. Voraussetzung für die Anerkennung ist die Führung einer UID-Nummer. Es wird hier indirekt festgelegt, dass natürliche oder juristische Personen ohne Eintrag im Handelsregister keine Anerkennung erlangen und keine anerkannten E-ID-Systeme betreiben können.

Buchstaben c und d
Eine organisatorische Vorgabe betrifft die Personen, die im Ausstellungsprozess die Prüfung der vorgelegten Identitätspapiere vornehmen und im Betrieb Einfluss auf die Datenweitergabe nehmen können. Diese Personen sollen ausreichend geschult sein, über Fachkenntnisse,

[11] Vgl. Link im Fundstellennachweis

Erfahrungen und Qualifikationen verfügen und insbesondere kein Risiko für die Sicherheit darstellen.

Als Sicherheitsrisiko würde beispielsweise die Beschäftigung einer Person gelten, die aufgrund von bestimmten Straftaten rechtskräftig verurteilt wurde (vgl. Erläuterungen zu Art. 12 Abs. 2 Bst. d) oder einer Person, die verschuldet ist und deshalb allenfalls für Bestechung offen sein könnte. Die Nachweise dafür lassen sich durch Auszüge aus dem Strafregister und den Betreibungsregistern erbringen.

Buchstabe e
Der Nachweis über die Verlässlichkeit und Vertrauenswürdigkeit ist durch die Einhaltung der jeweils aktuell gültigen Sicherheitsstandards und durch Zertifizierung der Prozesse zu erbringen.

Buchstabe f
Der IdP hat sicherzustellen, dass die Datenbearbeitung und Datenhaltung ausschliesslich in der Schweiz erfolgt. Jeglicher unerlaubte Zugriff vom Ausland von Dritten auf die Daten ist zu verhindern. Unter Datenbearbeitung ist jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Archivieren oder Vernichten von Daten gemeint. Diese Bestimmung betrifft alle Daten, welche der IdP im Rahmen der Dienstleistungen nach diesem Gesetz bearbeitet, insbesondere auch vorübergehende Daten, Daten aus Zwischenspeicherung oder Randdaten.

Buchstabe g
Der IdP muss sich gegen die Haftungsrisiken versichern. Die Haftung richtet sich nach dem Obligationenrecht (vgl. 9. Abschnitt Art. 24).

Absatz 3
Die technischen Entwicklungen im Bereich elektronische Identifizierung und Authentifizierung sind kaum einzuschätzen. Deshalb muss die Anerkennung in regelmässigen Abständen erneuert werden. Ein IdP erstellt jährlich einen Sicherheitsbericht, der alle durch ihn betriebenen anerkannten E-ID-Systeme umfasst, und übermittelt diesen der Anerkennungsstelle. Form und Inhalt des Sicherheitsberichts werden durch den Bundesrat festgelegt.

Absatz 4
Wie an anderer Stelle wird auch hier die Regelung des Verfahrens und technischer Details an den Verordnungsgeber delegiert.

Auf Verordnungs- und Weisungsebene werden insbesondere die anwendbaren Standards und technischen Protokolle für die E-ID-Systeme geregelt. Die Anwendung der Standards und Protokolle wird durch die Anerkennungsstelle regelmässig geprüft. Dadurch wird auch eine Anerkennung der E-ID-Systeme erreicht.

Artikel 5 Sicherheitsniveaus
Absatz 1
Nicht alle Geschäftsprozesse erfordern dasselbe Sicherheitsniveau. Oft führt eine höhere Sicherheit zu mehr Aufwand beim Bezug, einer reduzierten Benutzerfreundlichkeit und höheren Kosten. Aus diesem Grund sollen IdP E-ID-Systeme marktgerecht auf drei unterschiedlichen Sicherheitsniveaus anbieten können, wie diese auch von der EU und der NIST festgeschrieben werden. Betreiberinnen von E-ID-verwendenden Diensten können selbst bestimmen, welches Sicherheitsniveau sie akzeptieren wollen (vgl. Art. 15 VE).

Für eine Anerkennung muss ein E-ID-System mindestens das Sicherheitsniveau „*niedrig“* erfüllen. E-ID-Systeme der Sicherheitsniveaus „*substanziell“* und „*hoch“* erfüllen die Mindestanforderungen und darüber hinaus weitere Voraussetzungen. Das heisst, dass mit einer E-ID des Niveaus „*hoch“* auch die Anforderungen an E-ID der Sicherheitsniveaus „*substanziell* und „*niedrig“* erfüllt werden, aber nicht umgekehrt.

Je nach Sicherheitsniveau des Systems, wird durch die E-ID ein unterschiedliches Mass an Vertrauen vermittelt. Die Sicherheitsniveaus „*niedrig“* und „*substanziell“* bezwecken eine Minderung der Gefahr des Identitätsmissbrauchs, beim Niveau „*hoch“* wird eine Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung bezweckt.

Absatz 2
Die Details zu den unterschiedlichen Sicherheitsniveaus werden auf Verordnungsstufe festgehalten. Die Sicherheitsniveaus unterscheiden sich durch den Ausstellungsprozess, den Betrieb und die Anwendung und können sich durch weitere technische oder organisatorische Sicherheitsmassnahmen unterscheiden. Die Anforderungen sind auf Gesetzesstufe möglichst technologieneutral umschrieben und werden auf Verordnungs- oder Weisungsstufe im Detail und für verschiedene E-ID-Trägerformen genauer bestimmt.

Absatz 3
Eine E ID eines höheren Sicherheitsniveaus soll auch bei einem E-ID-verwendenden Dienst eingesetzt werden können, wenn dieser ein niedrigeres Sicherheitsniveau verlangt. Inhaberinnen und Inhaber können deshalb ihre E ID bei allen E-ID-verwendenden Diensten einsetzen, vorausgesetzt die E ID erfüllt oder übertrifft das von der Betreiberin von E-ID-verwendenden Diensten geforderte Sicherheitsniveau.

Artikel 6 Ausstellungsprozess
Vorbemerkung
Der Ausstellungsprozess findet zwischen der antragsstellenden Person, dem IdP und der Identitätsstelle statt. Je nach Sicherheitsniveau ist eine persönliche Vorsprache oder eine gleichwertige Identifizierung Voraussetzung für die Ausstellung. Der Bundesrat regelt den Ausstellungsprozess je Sicherheitsniveau; die entsprechenden Delegationen finden sich in verschiedenen Bestimmungen des Vorentwurfs (vgl. insbesondere Art. 3 Abs. 3, Art. 5 Abs. 4).

Absatz 1
Der IdP darf nicht von sich aus eine E-ID ausstellen, selbst wenn ihm die Person bereits durch bestehende Kundenbeziehungen bekannt ist. Der Antrag muss von der späteren Inhaberin oder dem späteren Inhaber der E-ID ausgehen (antragstellende Person). Gleichzeitig besteht auch keine Pflicht, eine E-ID zu beziehen.

Absatz 2 und 3
Der IdP überprüft, ob die antragsstellende Person die persönlichen Voraussetzungen nach Artikel 3 erfüllt und beantragt anschliessend bei der Identitätsstelle die Übermittlung der Personenidentifizierungsdaten in elektronischer Form. Falls er die E-ID nur einem eingeschränkten Personenkreis (Kunden) abgeben will, gehört auch die Kundenbeziehung zu den persönlichen Voraussetzungen. Die antragstellende Person muss der Übermittlung der Personenidentifizierungsdaten ausdrücklich zustimmen. Die Identitätsstelle stellt durch technische und organisatorische Massnahmen sicher, dass Personenidentifizierungsdaten nicht miss-

bräuchlich abgerufen werden können. So soll es dem IdP z. B. nicht möglich sein, Personenidentifizierungsdaten allein gestützt auf die Angabe einer Ausweisnummer und ohne ausdrückliches Einverständnis der Inhaberin oder des Inhabers abzurufen. Für diese Einverständniserklärung muss allenfalls ein direkter Kontakt zwischen Identitätsstelle und antragsstellender Person stattfinden.

Absatz 4
Der IdP ordnet die Personenidentifizierungsdaten der E-ID zu und stellt sicher, dass die E-ID der entsprechenden natürlichen Person zugeordnet wird (Bindung). Dies geschieht z. B. bei einer Mobile ID durch die Zuordnung der E-ID an eine SIM-Karte, die wiederum für das Abonnement der antragsstellenden Person verwendet und in deren Gerät eingesetzt wird. Je nach Sicherheitsniveau werden unterschiedliche Anforderungen an diese Zuordnung gestellt, wobei für die Nutzung einer E-ID mindestens ein Authentifizierungsfaktor geprüft werden muss, z. B. Besitz eines personalisierten Geräts, Kenntnis eines Geheimnisses oder ein biometrisches Merkmal.

Absatz 5
Der Antrag auf Übermittlung der Personenidentifizierungsdaten wird elektronisch beim Informationssystem der Identitätsstelle gestellt. Das Informationssystem der Identitätsstelle protokolliert die Anfrage.

Artikel 7 Personenidentifizierungsdaten
Absatz 1 und 2
Voraussetzung für die Freigabe von Personenidentifizierungsdaten nach Absatz 2 sind höhere technische und organisatorische Anforderungen an den Registrierungsprozess, das E-ID System und die Authentifizierung beim Einsatz.

Einige der genannten Personenidentifizierungsdaten sind biometrische Daten (Gesichtsbild, Unterschriftsbild). Da nur Daten bestätigt werden können, die in den Informationssystemen des Bundes (vgl. Art. 20 VE) geführt werden, ist die Aufzählung abschliessend. Die Inhaberin oder der Inhaber kann die Personenidentifizierungsdaten einschränken, welche bei einer konkreten Anwendung der E-ID vom IdP an eine Betreiberin von E-ID-verwendenden Diensten übermittelt werden (vgl. Art. 17 Abs. 1 Bst. f VE). Die Bezeichnung der Personenidentifizierungsdaten folgt soweit möglich der Terminologie des Registerharmonisierungsgesetzes.

Absatz 3
Die Personenidentifizierungsdaten können durch die Identitätsstelle mit weiteren Informationen versehen werden, die dem IdP bei der Verwaltung der E-ID helfen. So kann beispielsweise übermittelt werden, aus welchen Informationssystemen sie stammen und wann die Daten dort letztmals aktualisiert wurden.

Absatz 4
Über die Personenidentifizierungsdaten hinaus kann der IdP einer E-ID (bzw. der E-ID-Registrierungsnummer) weitere Daten zuordnen, zum Beispiel eine Adresse, Telefon- oder Kundennummer. Denkbar wäre auch, dass eine Bank als IdP agiert und einer Kreditkarte oder einer Kontokarte eine anerkannte E-ID hinzufügt.

Artikel 8 Aktualisierung der Personenidentifizierungsdaten

Absatz 1

Einige der Identitätsattribute sind veränderbar. Der Vollzug des geänderten Namensrechts des Zivilgesetzbuches (ZGB, SR 210, insbes. Art. 29 ff. und Art. 160) hat gezeigt, dass immer mehr Namen angepasst werden, also nicht mehr von Geburt bis Tod der gleiche amtliche Name getragen wird. Anpassungen des Zivilstandes und auch Änderungen des Geschlechts sind häufiger zu verzeichnen als im letzten Jahrhundert. Dieser Tatsache wird durch die Pflicht zur regelmässigen Aktualisierung Rechnung getragen.

Das Vertrauen in die E-ID wird durch regelmässige Aktualisierung der Personenidentifizierungsdaten mit den staatlichen Informationssystemen erhöht. Es wird vorgeschrieben, in welchen maximalen Abständen für jedes Sicherheitsniveau dieser Abgleich zu erfolgen hat. Die Zuständigkeit für die Aktualisierungsabfrage liegt beim IdP. Für die regelmässigen Aktualisierungen werden Gebühren erhoben.

Absatz 2

Die Identitätsstelle ermöglicht die systematische Überprüfung der Gültigkeit der E-ID-Registrierungsnummer in einem gebräuchlichen Verfahren (vgl. Art. 20 Abs. 4 VE). Derzeit ist dies die Führung einer elektronischen Liste. Die IdP müssen diese Informationen periodisch abfragen. Sie sind verpflichtet E-ID, welche zu einer als ungültig gelisteten E-ID-Registrierungsnummer ausgestellt worden sind umgehend zu sperren, respektive zu widerrufen. Diese Abfrage des IdP bei der Identitätsstelle erhöht das Vertrauen in anerkannte E-ID und ist deshalb kostenlos. IdP sind verpflichtet, ebenfalls eine kostenlose Abfragemöglichkeit einzurichten, die sich auf die von ihnen herausgegebenen E-ID beschränkt (Art. 17 Abs. 1 Bst. c VE).

Je nach Ergebnis der Abfrage, ist die E-ID zu sperren oder zu widerrufen. Es ist nötig, zwischen Sperrung und Widerruf einer E-ID und der Sperrung und dem Widerruf der E-ID-Registrierungsnummer zu unterscheiden. Wird beispielsweise gemeldet, dass das Trägermittel und damit die E-ID verloren gegangen sind und Dritten zugänglich sein könnten, wird die spezifische E-ID vorübergehend ungültig; der Status der E-ID-Registrierungsnummer wird dadurch aber nicht betroffen, da diese an die staatliche Identität der Person gebunden ist, die unabhängig von einer E-ID gültig ist. Die E-ID kann nach dem Wegfall des Grundes der Sperrung wieder aktiviert und weiter verwendet werden. Der Widerruf aller einer E-ID-Registrierungsnummer zugeordneter E-ID erfolgt jedoch, wenn eine E-ID-Registrierungsnummer dauerhaft nicht mehr verwendet werden darf, beispielsweise beim Tod der Inhaberin oder des Inhabers. Eine widerrufene E-ID-Registrierungsnummer kann nicht wieder aktiviert werden, eine vorübergehend gesperrte jedoch schon.

Die Aktualisierung der Personenidentifizierungsdaten erfolgt gegen eine Gebühr. Der Bundesrat wird eine Gebührenverordnung erlassen. Die Gebühr muss kostendeckend sein und dürfte sich im zweistelligen Rappenbereich pro Aktualisierung der Daten für eine E-ID bewegen.

Artikel 9 Systematische Verwendung der Versichertennummer zum Datenaustausch

Vorbemerkung

Die Versichertennummer (AHVN13) gemäss AHVG soll nicht breitflächig und unkontrolliert bekanntgegeben werden können, da dies – im Ergebnis – auch jenen Kreisen eine systematische Nutzung ermöglichen würde, die dazu nicht befugt sind. Artikel 9 VE enthält die ge-

setzliche Grundlage und Bearbeitungsgrundsätze im Zusammenhang mit der systematischen Nutzung der AHVN13 für die E-ID. Die Regelung sieht im Einzelnen wie folgt aus:

Absatz 1
Die AHVN13 wird im Ausstellungsprozess und bei der Datenaktualisierung (Art. 8 VE) von der Identitätsstelle zur Identifizierung der Personen verwendet und dient als eindeutiger Identifikator bei der Abfrage von anderen Datenbanken, die die Versichertennummer ebenfalls systematisch verwenden. Die Versichertennummer ist unerlässlich, um Daten zwischen verschiedenen Datenbanken automatisiert abzugleichen oder weiterzuleiten. Nur die Versichertennummer kann sicherstellen, dass sich eine Person auch nach einer Namensänderung in den verschiedenen Registern noch eindeutig identifizieren lässt. Die in den letzten Jahren eingeführten Änderungen des Namensrechts erleichtern es Personen, ihre ursprüngliche Identität zu verwischen und auf legale Weise eine neue aufzubauen. Mit der Namensänderung werden nämlich auch die amtlichen Ausweisschriften neu ausgestellt, die keine Rückschlüsse auf die alte Identität zulassen. Die Versichertennummer ermöglicht jedoch eine eindeutige Zuordnung.

Absatz 2
IdP haben die Berechtigung, die AHVN13 in ihren Systemen zu speichern. Den Betreiberinnen von E-ID-verwendenden Diensten wird die AHVN13 nur übermittelt, falls sie selbst nutzungsberechtigt sind. Die AHVN13 soll im Rahmen der Verwendung der E-ID nur jenen Stellen weitergegeben werden können, die gemäss den genannten Bestimmungen des AHVG zur systematischen Verwendung der AHVN13 befugt sind. Die Übermittlung dieses Attributs an die nicht zur systematischen Verwendung der AHVN13 zugelassenen Dritten muss demnach technisch unterbunden werden. Auf dem Rapport über die Datenübermittlungen wird die AHVN13 ausgeblendet. Die E-ID-Registrierungsnummer ist die eindeutige Identifizierungsnummer für den IdP.

Artikel 10 Datenbearbeitung und Datenweitergabe
Vorbemerkung
Datenbearbeitung und Datenweitergabe ist die eigentliche Tätigkeit der IdP. Identifizierung und Authentifizierung wird als Dienstleistung sowohl für die Betreiberin von E-ID-verwendenden Diensten als auch für die Inhaberin oder dem Inhaber der E-ID erbracht. IdP stehen als Vermittler dazwischen. Umso wichtiger ist die Regelung des Datenschutzes.

Absatz 1 und 2
Die in Absatz 1 und 2 formulierten Datenschutzbestimmungen gehen nicht über die Regelungen der Datenschutzgesetzgebung hinaus. Bei der Anwendung der E-ID kann die Inhaberin oder der Inhaber auswählen, welche Personenidentifizierungsdaten dem E-ID-verwendenden Dienst übermittelt werden sollen. Es können aber nur diejenigen Personenidentifizierungsdaten übermittelt werden, die dem vom E-ID-verwendenden Dienst geforderten Sicherheitsniveau entsprechen.

Absatz 3
Es wird sowohl dem IdP als auch der Betreiberin von E-ID-verwendenden Diensten untersagt, die staatlich bestätigten Personenidentifizierungsdaten der Sicherheitsniveaus „*substanziell“* und „*hoch“* weiterzugeben, insbesondere damit zu handeln. Das Geschäftsmodell der IdP und der Betreiberinnen von E-ID-verwendenden Diensten soll nicht darauf basieren, Daten oder Nutzungsprofile zu verkaufen, die durch den Staat bestätigt wurden und dadurch besonders aussagekräftig sind. Diese Daten sollen aber auch nicht unentgeltlich weiterge-

geben werden dürfen, z.B. zur kommerziellen Nutzung durch eine andere Unternehmung innerhalb eines Konzerns. Das Verbot des Handels bezieht sich ausdrücklich nicht auf die zusätzlichen Daten, die gemäss Artikel 7 Absatz 4 VE der E-ID zugeordnet sind.

Absatz 4
Mit dem Verweis auf die Datenschutzgesetzgebung sind sowohl das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1) als auch untergeordnete Erlasse gemeint. Insbesondere unterstehen IdP und Betreiberinnen von E-ID-verwendenden Diensten Art. 16 bis Art. 25bis DSG und der Aufsicht gemäss Art. 27 DSG.

Artikel 11 Erlöschen der Anerkennung
Absatz 1
Voraussetzung für den Betrieb eines E-ID-Systems ist ein leistungsfähiger IdP. Bei Eröffnung des Konkurses entfällt diese Leistungsfähigkeit und die Anerkennung erlischt von Gesetzes wegen. Die E-ID-Systeme sind nicht pfändbar und fallen nicht in die Konkursmasse. Die Daten, die über die E-ID-Systeme bestätigt werden, sind nicht handelbar und haben dadurch keinen wirtschaftlichen Wert.

Absatz 2 und 3
E-ID-Systeme sind über die Interoperabilität (Art. 18 VE) verbunden und sind Knoten in den Netzen, die E-ID-verwendenden Dienste verbinden. Die Bestimmung in Absatz 3 soll den Erhalt einmal aufgebauter E-ID-Netze sichern. Dadurch, dass der Erlös aus der Übernahme gegebenenfalls in die Konkursmasse fällt, erhalten E-ID-Systemen als Ganzes einen wirtschaftlicher Wert, selbst wenn die einzelnen Daten nicht handelbar sind.

Artikel 12 Aufsichtsmassnahmen und Entzug der Anerkennung
Absatz 1 und 2
Die Anerkennungsstelle wird aktiv, wenn sie bei den regelmässigen Kontrollen oder aufgrund einer Meldung feststellt, dass ein IdP Vorgaben missachtet oder die Voraussetzungen für die Anerkennung (Art. 4 VE) nicht mehr erfüllt sind. Als nötige Massnahmen kommen insbesondere technische Vorgaben, z. B. Einhaltung der neuesten Standards, oder organisatorische Massnahmen, z. B. Auflagen zur Schulung von Mitarbeitenden, in Frage. Die Anerkennungsstelle setzt eine Frist zur Behebung der festgestellten Mängel. Werden die Mängel innert der angemessenen Frist nicht behoben, kann die Anerkennung entzogen werden.

Absatz 3
Buchstabe a bis c
Der Entzug der Anerkennung ist eine verwaltungsrechtliche Sanktion. Die Anerkennung kann entzogen werden, wenn gegen die Bestimmungen des Gesetzes verstossen wird, die Anerkennungsvoraussetzungen nicht mehr oder Auflagen aus dem Anerkennungsverfahren nicht fristgerecht erfüllt werden. Durch die Kann-Formulierung wird sichergestellt, dass diese Sanktion mit schwerwiegenden Konsequenzen nur ausgesprochen wird, wenn die Verhältnismässigkeit gewahrt bleibt.

Buchstabe d
In Frage kommen mit Internetkriminalität in Bezug stehende Straftaten, insbesondere Straftatbestände, die zu einem Identitätsmissbrauch führen können. Als Identitätsmissbrauch wird die missbräuchliche Nutzung von persönlichen Daten (der Identität) einer fremden Person bezeichnet. Identitätsmissbrauch wird häufig mit dem Ziel betrieben, jemanden in seinem Ruf

zu schädigen oder sich einen unrechtmässigen Vermögensvorteil zu verschaffen. Bezweckt die Täterin oder der Täter, sich oder einer anderen Person dadurch einen unrechtmässigen Vorteil zu verschaffen, kann sie oder er sich des Betrugs (Art. 146 des Strafgesetzbuches, StGB, SR 311.0) oder eines Versuchs hierzu schuldig machen und mit Freiheitsstrafe bis zu fünf Jahren bestraft werden. Auch im Rahmen des strafbaren Phishings wird zum Teil auf eine fremde Identität zurückgegriffen, um einen Vermögensvorteil zu erlangen. Dringt die Täterin oder der Täter im Zusammenhang mit den persönlichen Daten in ein Computersystem ein, macht sie oder er sich des Hackings (Art. 143bis StGB) schuldig. Gelangt sie oder er unrechtmässig an fremde, nicht für sie oder ihn bestimmte Daten, liegt ein Fall von unbefugter Datenbeschaffung (Art. 143 StGB) vor. Abhängig von der Intention der Täterin oder des Täters und vom konkreten Fall können auch Tatbestände wie Datenbeschädigung, arglistige Vermögensschädigung, Drohung oder Nötigung (Art. 144bis, 151, 180 oder 181 StGB) zur Anwendung gelangen. Begeht die Täterin oder der Täter schliesslich mittels Missbrauchs einer fremden Identität eine Ehrverletzung oder eine Handlung gegen den Geheim- oder Privatbereich, finden die Strafbestimmungen der Artikel 173ff. StGB Anwendung. Für den seltenen Fall des Missbrauchs einer Identität ohne einen der beschriebenen Zwecke sehen verschiedene Kantone Bestimmungen im Übertretungsstrafrecht vor, nach welchen der grobe Unfug oder die Belästigung einer Person mit Busse bedroht wird.

Artikel 13 Subsidiäres E-ID-System des Bundes

Wie erwähnt, geht das vorliegende Gesetz von einem funktionierenden Markt aus. Falls hingegen keine privaten IdP ein Interesse daran haben, E-ID-Systeme der Sicherheitsniveaus „*substanziell*“ oder „*hoch*“ anerkennen zu lassen, behält sich der Bund vor, ein eigenes E-ID-System betreiben zu dürfen, insbesondere für die Identifizierung und Authentifizierung bei elektronischen Dienstleistungen und Kontakten im Verwaltungsbereich (E-Government-Anwendungen). Es werden in Absatz 2 gleichzeitig die Rechtsgrundlagen geschaffen, ein staatliches E-ID-System, allenfalls in Zusammenarbeit mit einem Privaten, zu errichten und zu betreiben.

1.8.4 3. Abschnitt: Inhaberinnen und Inhaber von E-ID

Artikel 14 Pflichten

Absatz 1 und 2

In der heutigen Zeit ist sich beinahe jedermann gewöhnt, mit digitalen Mitteln umzugehen. Die hier auferlegten Pflichten für Inhaberinnen und Inhaber von E-ID gehen nicht über die Sorgfaltspflichten hinaus, die üblicherweise für eine Kredit- oder Bankkontokarte angewendet werden müssen. Beispielsweise ist es notwendig und zumutbar, die allenfalls notwendige PIN nicht offenzulegen und mit dem E-ID-Träger zusammen aufzubewahren. Ebenso zumutbar sind beispielsweise die Aktivierung des Zugangsschutzes (z. B. PIN oder Fingerabdruckerkennung) und die Installation eines Virenschutzes auf dem als E-ID-Träger genutzten mobilen Gerät.

Absatz 3

Im Rahmen der deliktischen Haftung stellt Artikel 14 des Vorentwurfs eine Schutznorm im haftungsrechtlichen Sinn dar. Auf Verordnungsebene kann der Bundesrat insbesondere regeln, welche zusätzlichen Sorgfaltspflichten einzuhalten sind. Die klare Bestimmung der Sorgfaltspflichten bringt die Entlastungsmöglichkeit im Fall der ausservertraglichen (deliktischen) Haftung. Auf Verordnungseben vorgeschrieben wird z. B. dass Fehler in den Personenidentifizierungsdaten unverzüglich dem IdP anzuzeigen sind, ebenso jeder Verlust oder

der Verdacht auf Missbrauch einer E-ID.

1.8.5 4. Abschnitt: Betreiberinnen von E-ID-verwendenden Diensten

Artikel 15 Vereinbarung mit IdP

Jede Betreiberin von e-ID-verwendenden Diensten hat ein Vertragsverhältnis mit mindestens einem IdP. In diesem Vertrag werden zumindest das anwendbare Sicherheitsniveau und die anwendbaren technischen und organisatorischen Prozesse geregelt.

Artikel 16 Behörden als Betreiberinnen von E-ID-verwendenden Diensten

Behörden als Betreiberin von E-ID-verwendenden Diensten dürfen für die Benutzung ihrer Dienste nur dann eine elektronische Identifizierung verlangen, wenn diese im konkreten Fall notwendig ist. Wird aber eine elektronische Identifizierung vorgeschrieben, müssen auch Behörden von Kantonen und Gemeinden alle anerkannten E-ID auf dem entsprechenden Sicherheitsniveau akzeptieren, soweit sie Bundesrecht vollziehen. Dies schliesst nicht aus, dass heute eingesetzte elektronische Identifizierungsmittel weiterhin verwendet werden können.

Diese Bestimmung unterstreicht die Bedeutung und bundesinterne Akzeptanz einer staatlich anerkannten E-ID, wie sie sowohl in der Strategie „Digitale Schweiz“ als auch der E-Government Strategie des Bundesrates definiert ist (vgl. Ziffer 3). Nicht zuletzt sollen so die vom Bund für die E-ID zu tätigenden Investitionen geschützt und eine breite Basis für die Anwendung der E-ID bei E-Government-Prozessen geschaffen werden. Davon profitieren nicht nur Bund, Kantone und Gemeinden, welche mit einer staatlich anerkannten E-ID Kosten einsparen können, sondern auch alle Einwohnerinnen und Einwohner der Schweiz.

1.8.6 5. Abschnitt: Anbieterinnen von Identitätsdienstleistungen (IdP)

Artikel 17 Pflichten

Absatz 1

Buchstabe a

Der IdP betreibt mindestens ein E-ID-System. Ein IdP kann mehrere E-ID-Systeme verschiedener Sicherheitsniveaus anbieten und diese anerkennen lassen, muss aber nicht. Die Sicherheit der Betriebsumgebung ist Teil der organisatorischen und technischen Anerkennungsvoraussetzungen, die auf Verordnungs- oder Weisungsebene geregelt werden.

Buchstabe b

Der IdP ist im Ausstellungsprozess für die richtige Zuordnung der E-ID zu den Personenidentifizierungsdaten und die korrekte Bindung und Auslieferung der E-ID an die natürliche Person zuständig. Dies geschieht in drei Schritten und kann je nach Sicherheitsniveau unterschiedlich ausgestaltet sein:

1. Der IdP ordnet die von der Identitätsstelle übermittelten Personenidentifizierungsdaten (Art. 7 VE) mit der E-ID-Registrierungsnummer eindeutig der E-ID mit dem zugehörigen Authentifikationsmittel zu, das die Inhaberin oder den Inhaber authentifiziert. Zumindest auf höheren Sicherheitsniveaus ist das Authentifikationsmittel meist direkt in eine Trägereinheit integriert (z. B. Chip auf Karte oder SIM-App in Mobiltelefon).
2. Er stellt sicher, dass die E-ID der identifizierten natürlichen Person zugeordnet ist (z. B. die übrigen Daten auf dem Chip zur identifizierten Person gehören, bzw. das Mobiltelefon-Abonnement auf diesen Namen läuft).

3. Er sorgt dafür, dass die E-ID dieser Person zukommt (z. B. durch briefliche Zustellung mit Empfangsbestätigung oder bei der persönlichen Vorsprache vor Ort oder auch im Rahmen einer sicheren Online Verbindung wobei das Authentifikationsmittel an die richtige Person gebunden werden muss).

Buchstabe c
Die technische Entwicklung im Bereich der sicheren Übermittlung schreitet schnell voran. Deshalb wird im Gesetz die Überprüfung der Gültigkeit aller E-ID mit einem gebräuchlichen Verfahren vorgeschrieben, was der Formulierung im revidierten ZertES entspricht. Als gebräuchliches Verfahren gelten derzeit elektronische Listen. So kann die Identitätsstelle beispielsweise eine Liste mit vorübergehend oder dauerhaft für den Bezug oder den Einsatz einer E-ID ungültigen E-ID-Registrierungsnummern führen und publizieren. Dies kann insbesondere bei Verschollenerklärung oder Tod einer Person, allenfalls auch bei Beendigung der Aufenthaltsbewilligung für Ausländerinnen und Ausländer der Fall sein. Der IdP hat die Pflicht, diese Liste der gesperrten oder widerrufenen E-ID-Registrierungsnummern regelmässig zu konsultieren und mit seinem gebräuchlichen Verfahren abzugleichen.

Buchstabe d
Der IdP ist verpflichtet, aktiv die neuesten Sicherheitsanforderungen abzufragen und zu überprüfen, ob die von ihm betriebenen Systeme sie einhalten.

Buchstabe e
Die Aktualisierung der Personenidentifizierungsdaten führt zu mehr Sicherheit. Die Periodizität ist je nach Sicherheitsniveau unterschiedlich und wird in Artikel 8 Absatz 1 festgelegt.

Buchstabe f
Sollen beim Einsatz einer E-ID Personenidentifizierungsdaten übermittelt werden (typischerweise bei der Registrierung bei einem E-ID-verwendenden Dienst), muss der IdP das Einverständnis der Inhaberin oder des Inhabers einholen.

Ein Beispiel: Eine Inhaberin will in einem Online-Casino spielen. Dafür muss sie nachweisen, dass sie das achtzehnte Altersjahr zurückgelegt hat. Dieses Casino hat eine Vereinbarung mit einem IdP. Die Inhaberin verfügt über eine E-ID, die auf dem Smartphone implementiert ist und gibt dies dem Casino bekannt. Das Casino kontaktiert online den IdP. Die Inhaberin erhält vom IdP eine Meldung auf ihr Smartphone mit der Frage, ob sie den Namen, Vornamen und das Geburtsdatum diesem Casino übermitteln will. Sie bestätigt ihr Einverständnis und die freigegebenen Daten werden vom IdP an das Casino übermittelt. Damit verfügt das Casino über einen staatlich bestätigten Altersnachweis und darf die Inhaberin zum Online-Spiel zulassen, sofern keine anderen Ausschlussgründe vorliegen. Bei jedem weiteren Besuch genügt die einfache Anmeldung mit der E-ID.

Buchstabe g
Protokolldaten beim IdP über den Einsatz der E-ID sind nach einer Frist von sechs Monaten zu löschen. Durch diese Vorschrift nicht betroffen sind Protokoll-, Registrierungs- und Transaktionsdaten beim E-ID-verwendenden Dienst.

Absätze 2, 3 und 4
Der IdP stellt sicher, dass eine Störung im Gebrauch der E-ID oder der Verlust des Trägers gemeldet werden kann. Ob für diese Meldung eine telefonische Hotline eingerichtet oder per E-Mail oder über andere Kanäle kommuniziert wird, soll dem Markt überlassen werden.

Unter Umständen merken Betreiberinnen von E-ID-verwendenden Diensten oder IdP vor der Inhaberin oder dem Inhaber, dass Gefahr des Missbrauchs der E-ID besteht (z. B. Anwendung an ungewöhnlichem Ort). Es könnte ebenfalls möglich sein, dass ein Dritter missbräuchlich versucht, eine E-ID zu sperren. Der IdP muss sich deshalb vor der Sperrung vergewissern, dass die Person, welche die Sperrung beantragt, dazu befugt ist.

Artikel 18 Interoperabilität

Interoperabilität zwischen den E-ID-Systemen ist eine wichtige Voraussetzung für die Verbreitung von E-ID. Deshalb wird hier festgehalten, dass IdP ihre E-ID-Systeme gegenseitig anerkennen. Dies wird ermöglicht durch technische Standards und definierte Schnittstellen, die auf dem Verordnungs- oder Weisungsweg erlassen werden.

Inhaberinnen und Inhaber sollten ihre E-ID bei allen E-ID-verwendenden Diensten einsetzen können, vorausgesetzt die E-ID erfüllt zumindest das geforderte Sicherheitsniveau. Dies soll unabhängig davon möglich sein, ob die Betreiberin von E-ID-verwendenden Diensten mit demjenigen IdP eine Vereinbarung hat, der die E-ID ausgestellt hat. Um dies zu erreichen, müssen die IdP ihre Identitätsdienstleistungen gegenseitig föderieren, ähnlich einem Kreditkartennetzwerk oder dem Roaming im Mobiltelefonie-Bereich. Dies kann entweder durch die Einhaltung von Interoperabilität Standards und Regeln, die durch alle IdP einzuhalten sind, oder durch eine Plattform realisiert werden, an den alle IdP angeschlossen sein müssten. Im zweiten Fall braucht es eine Organisation, die allenfalls durch Bund und Kantone im Rahmen des Identitätsverbunds Schweiz IDV aufgestellt werden könnte. Zu gegebener Zeit wird die geeignetste und wirtschaftlich günstigste Lösung gefunden werden, wobei den Interessierten aus Wirtschaft und Verwaltung ein Mitspracherecht einzuräumen ist.

1.8.7 6. Abschnitt: Schweizerische Stelle für elektronische Identität

Artikel 19 Organisation

Die Schweizerische Stelle für elektronische Identität (Identitätsstelle) wird im EJPD geführt. Der Bundesrat regelt die Organisation. Vgl. dazu die Ausführungen unter Ziffer 1.4.1.

Artikel 20 Aufgaben und Pflichten

Absatz 1

Die Identitätsstelle ordnet die Personenidentifizierungsdaten einer E-ID-Registrierungsnummer zu und übermittelt sie an den IdP. Der Umfang der übermittelten Personenidentifizierungsdaten variiert je nach Sicherheitsniveau (vgl. Art. 7 VE).

Absatz 2 und 3

Die Identitätsstelle führt ein Informationssystem, das Zugriff hat auf die Personenregister, die auf Bundesebene geführt werden und einen Abgleich mit diesen Registern durchführt. Es sind dies zum Zeitpunkt der Erarbeitung dieses Gesetzes:

a. das Informationssystem Ausweisschriften (ISA) gemäss Artikel 11 des Bundesgesetzes vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG, SR 143.1) und Artikel 10 der Verordnung vom 20. September 2002 über die Ausweise für Schweizer Staatsangehörige (Ausweisverordnung, VAwG, SR 143.11);

b. das Zentrale Migrationsinformationssystem (ZEMIS) gemäss Artikel 101 ff. des Bundesgesetzes vom 16. Dezember 2005 über die Ausländerinnen und Ausländer (Ausländergesetz, AuG, SR 142.20) und der Verordnung vom 12. April 2006 über das Zentrale Migrationsinformationssystem (ZEMIS-Verordnung, SR 142.513);
c. das elektronische Personenstandsregister Infostar gemäss Artikel 39 des Schweizerisches Zivilgesetzbuches (ZGB, SR 210) und Artikel 6a der Zivilstandsverordnung vom 28. April 2004 (ZStV, SR 211.112.2);
d. das Zentralregister der zentralen Ausgleichsstelle der AHV (ZAS-UPI) gemäss Artikel 71 AHVG (SR 831.10)

Absatz 4
Vgl. Erläuterungen zu Artikel 8 Absatz 2.

Absatz 5
Die verschiedenen Informationssysteme werden durch unterschiedliche Quellen mit Daten versorgt. Infostar ist das zentrale Zivilstandsregister und wird durch die regionalen Zivilstandsämter der ganzen Schweiz mit Daten gespeist. Das ISA übernimmt Daten aus Infostar oder den Einwohnerkontrollregistern, sofern diese gestützt auf Heimatscheine oder das Familienregister geführt werden. ZEMIS wird beim SEM geführt und enthält Personendaten des Ausländer- und Asylbereichs über Ausländerinnen und Ausländer, die in der Schweiz aufgrund internationaler Verträge aufenthaltsberechtigt sind.

Wenn nun z. B. eine in ZEMIS registrierte Person ein Zivilstandsereignis (z. B. Heirat, Scheidung, Geburt) registrieren lässt, kann es zu unterschiedlichen Erfassungen kommen (z. B. Schreibweise eines Vornamens). Der Bundesrat regelt das Vorgehen in diesen Fällen. Abklärungen zu vermeintlich oder tatsächlich widersprüchlichen Personenidentifizierungsdaten werden bereits heute im Bereich der AHVN13 von der „Clearingstelle“ der ZAS-UPI vorgenommen. Die Abklärungen im Bereich der E-ID könnten ebenfalls dieser Stelle übertragen werden.

1.8.8 7. Abschnitt: Anerkennungsstelle für IdP

Artikel 21 Zuständigkeit
Die Anerkennungsstelle für Identitätsdienstleister (Anerkennungsstelle) wird beim EFD geführt. Das Verfahren zur Anerkennung von IdP ist dem Verfahren zur Anerkennung von Zustellplattformen nachgebildet (vgl. Ziffer 1.3.2). Eine Verwaltungseinheit ist verantwortlich für die Durchführung der Anerkennungsverfahren. Diese Funktion ist in der eIDAS-Verordnung der nationalen Aufsichtsstelle zugeordnet. Da weitere Funktionen der nationalen Aufsichtsstelle gemäss eIDAS-Verordnung durch das EFD (ISB) wahrgenommen werden, wird hier vorgeschlagen, die Anerkennungsstelle auch dort anzusiedeln. Vgl. auch dazu die Ausführungen unter Ziffer 1.4.1.

Artikel 22 Liste der anerkannten IdP
Die Anerkennungsstelle veröffentlicht eine Liste mit allen anerkannten IdP und mit allen anerkannten E-ID-Systemen mit ihren Sicherheitsniveaus. Sie hält diese Liste aktuell. Diese Regelung ist der Veröffentlichung von anerkannten Zustellplattformen nachgebildet.

1.8.9 8. Abschnitt Gebühren

Artikel 23

Für die Bemessung der Gebühren, die die Identitätsstelle und die Anerkennungsstelle von den IdP erheben, sind verschiedene Möglichkeiten denkbar. Welche Möglichkeit gewählt wird, soll der Bundesrat in Würdigung der konkreten Umstände des Gesetzesvollzugs entscheiden. Er soll insbesondere entscheiden, ob beispielsweise für die ersten Jahre auf eine volle Kostendeckung des Verwaltungsaufwands, insbesondere der Identitätsstelle, verzichtet werden soll. Ermässigte Gebühren für den Fall, dass ein IdP die E-ID den Bezügern unentgeltlich ausstellt, könnten im Sinn eines Anschubs dazu beitragen, dass sich die E-ID rasch verbreitet und dass sich deshalb mittel- bis langfristig Effizienzvorteile des elektronischen Verkehrs, sei es unter Privaten oder mit Behörden, realisieren lassen.

Es wird weiter davon ausgegangen, dass die anerkannte Identifizierungseinheit auf einem Träger angebracht wird, der selbst eine Funktion hat, sei es z. B. auf einer Bankkarte, auf dem abgesicherten Bereich eines Smartphones oder auf dem Träger eines Signaturmittels (z. B. SuisseID). Denkbar ist auch die Anbindung an einen Sichtausweis für Mitarbeitende eines Unternehmens (z. B. Krankenhaus). Das Unternehmen könnte dadurch die Identifizierung ihrer Mitarbeitenden an einen anerkannten IdP auslagern und dessen E-ID-System für die Authentisierung an ihrer IKT-Infrastruktur nutzen. Es wird dem Markt überlassen, ob und wie bei der Anwendung der E-ID anfallende Kosten verrechnet werden. Das Konzept geht von einem Pay-per-Use Modell aus ohne dabei andere Modelle auszuschliessen.

1.8.10 9. Abschnitt: Haftung

Artikel 24

Vorbemerkung

Die Haftung für Schäden, die bei der Verwendung der E-ID entstehen könnten, unterliegt den bekannten und bewährten Haftungsregeln nach dem Obligationenrecht (OR, SR 220) oder dem Verantwortlichkeitsgesetz (SR 170.32).

Die Bestimmungen haben hier deklaratorischen Charakter und dienen der Klarstellung, dass sämtliche Haftungsregeln, z. B. in Bezug auf den Schadensbegriff, die Entlastungsmöglichkeiten oder die Haftung für Hilfspersonen gelten. Es wird heute darauf verzichtet, weitergehende Haftungsnormen zu formulieren.

Insbesondere besteht kein Anlass, die Haftungsregelung, die gemäss Artikel 59a OR für Signaturschlüsselinhaber gegenüber Dritten gilt, auf die Inhaberin und den Inhaber einer E-ID auszudehnen. Mit der E-ID allein können keine Rechtsgeschäfte abgeschlossen werden; das vorliegende Gesetz beschäftigt sich ausschliesslich mit der sicheren Identifikation von Teilnehmern im elektronischen Geschäftsverkehr.

Derzeit wird ebenfalls darauf verzichtet, eine Kausalhaftung des IdP analog Artikel 17 revidiertes ZertES einzuführen. Demzufolge richten sich auch die Verjährungsregeln nach dem OR. Zum Zeitpunkt der Aushandlung eines bilateralen Vertrags zur Notifizierung der schweizerischen anerkannten E-ID bei der EU sind die nötigen Anpassungen an diesem Gesetz vorzunehmen, mit besonderem Augenmerk auf zwischenstaatliche Haftungsregelungen.

Absatz 1

Die Haftpflicht der Inhaberin oder des Inhabers, der E-ID-verwendenden Diensten und der IdP – oder kurz gesagt: die Haftung der privaten Akteure - richtet sich nach dem Obligationenrecht. Ob es sich dabei um eine vertragliche Haftung oder ausservertragliche (delikti-

sche) Haftung (Art. 41 ff. OR) handelt, ist im Einzelfall zu beurteilen.

Absatz 2
Die Identitätsstelle und die Anerkennungsstelle sind Verwaltungseinheiten des Bundes zugeordnet und unterstehen dem Verantwortlichkeitsgesetz vom 14. März 1958.

1.8.11 10. Abschnitt: Schlussbestimmungen

Artikel 25 Änderung anderer Erlasse

Im Anhang zum Gesetz wird die Änderung anderer Erlasse vorgeschlagen. Insbesondere wird die Identitätsstelle ermächtigt, auf die erwähnten Informationssysteme ISA, ZEMIS und Infostar zuzugreifen. Das Informationssystem ZAS-UPI muss nicht im Abrufverfahren erreichbar sein.

Artikel 26 Referendum und Inkrafttreten

Wie jedes Bundesgesetz untersteht auch das neue E-ID-Gesetz dem fakultativen Referendum und der Bundesrat wird das Datum des Inkrafttretens bestimmen können.

1.8.12 Anhang: Änderung anderer Erlasse

Vorbemerkungen

Identifizierung und Authentifizierung zu E-ID-verwendenden Diensten des Bundes
Die bisherigen Abklärungen haben ergeben, dass die Anforderungen an die Identifizierung und Authentifizierung für E-Government- Anwendungen wenn überhaupt, dann auf Verordnungs- oder Weisungsebene geregelt sind.

Zum Beispiel sind im Landwirtschaftsbereich die materiellen Zugriffsrechte für das Informationssystem für den öffentlichen Veterinärdienst in der Verordnung vom 6. Juni 2014 über die Informationssysteme für den öffentlichen Veterinärdienst (ISVet-V, SR 916.408) geregelt. Für das Informationssystem AGATE finden sich Informationen zu den Zugriffsdaten im Anhang zur Verordnung vom 23. Oktober 2013 über Informationssysteme im Bereich der Landwirtschaft (ISLV, SR 919.117.71). Auf dem Portal selbst wird die Anmeldung mit einer SuisseID oder einem AdminPKI-Zertifikat beschrieben und für gewisse Anwendungen verlangt.

StartBiz, ein Online-Dienst des SECO für KMU, kann nach der Anmeldung mit einer SuisseID genutzt werden. Die Online-Bestellung eines Strafregisterauszugs beim BJ ist ebenfalls mit einer SuisseID möglich.

E-ID als Dokument
Eine E-ID nach diesem Gesetz soll als beweiskräftiges Identifikationsdokument dienen. Insbesondere Finanzinstitute und Spielcasinos, die dem Geldwäschereigesetz unterstehen, sollen eine sichere elektronische Identifikation mit der E-ID vornehmen können. Die E-ID ist ein beweiskräftiges Dokument im Sinne von Artikel 3 des Geldwäschereigesetzes vom 10. Oktober 1997 (SR 955.0). Das Geldwäschereigesetz selbst regelt nicht abschliessend, was ein beweiskräftiges Dokument ist, sondern überlässt der Geldwäschereiverordnung der FINMA dieses näher zu definieren. Gegebenenfalls ist diese Verordnung so anzupassen, dass eine

E-ID im elektronischen Geschäftsverkehr mit Finanzinstituten und Casinos eingesetzt werden kann.

1. Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG; SR 143.1)

Artikel 1 Absatz 3 zweiter Satz
Grundsätzlich werden Schweizer Diplomaten- und Dienstpässe nur an Personen mit Schweizer Bürgerrecht abgegeben. Für gewisse Empfangsstaaten oder zur Übernahme von bestimmten Aufgaben im Interesse und im Auftrag der Schweiz ist es aus Sicherheitsgründen notwendig, auch an Personen ohne Schweizer Bürgerrecht einen Schweizer Diplomaten- oder Dienstpass auszustellen. Es soll verhindert werden, dass ausländischen Begleitpersonen von Schweizer Diplomaten oder anderen Angestellten einer Auslandsvertretung ernsthafte Nachteile drohen. Teilweise können auch die Anmeldung im Empfangsstaat und allenfalls die Ausstellung eines Visums nur erfolgen, wenn ein Schweizer Diplomaten- oder Dienstpass vorliegt. Die gesellschaftlichen Veränderungen im Bereich von Partnerschaften und hier insbesondere auch der Umstand, dass immer mehr Diplomatinnen und Diplomaten über fremdländische Ehe- oder Lebenspartner verfügen, hat die erwähnte Problematik zusätzlich verschärft. Weiter geht es auch darum, in Einzelfällen die Funktionsausübung ausländischer Mitarbeitender zu erleichtern. Für gewisse Einsätze in Krisen- oder Kriegsregionen, die erhöhte Risiken für Leib und Leben mit sich bringen, ist das EDA darauf angewiesen, Spezialisten zu rekrutieren, die gegebenenfalls nicht über das Schweizer Bürgerrecht verfügen, da keine Schweizer Bürgerinnen oder Bürger sich für diese Stelle interessieren. Zu einer Schweizer Bürgerin oder zu einem Schweizer Bürger wird die Person trotzdem nicht. Im Pass wird auf der Personalienseite in der Rubrik Nationalität entsprechend auch der Heimatstaat der Person aufgeführt und der Heimatort mit „ ******* “ersetzt.

Artikel 11 Absatz 1 Buchstabe k
Der in ISA zu einer Person geführte Personendatensatz soll um die AHVN13 sowie allenfalls die E-ID-Registrierungsnummer ergänzt werden. Dies ist notwendig, um die für eine E-ID aus verschiedenen Registern des Bundes notwendigen Daten eindeutig einer Person zuordnen zu können. Sofern die AHVN13 (Bst. k) innerhalb der Bundesverwaltung als EPID verwendet werden kann, ist die Aufnahme einer zusätzlichen E-ID-Registrierungsnummer nicht notwendig.

Artikel 12 Absatz 2 Buchstabe g und h
Die Identitätsstelle soll die eine E-ID notwendigen Daten aus ISA abfragen können. Insbesondere geht es um die Angaben, welche in Infostar nicht verzeichnet sind, wie Ausweisnummern, Gesichtsbild und Unterschriftenbild. Für die Ausstellung einer E-ID sind die Daten mit Hilfe der ebenfalls geführten AHVN13 resp. Der E-ID-Registrierungsnummer fehlerfrei einer Person zuweisbar.

Artikel 14
Da Daten aus ISA mit der Einführung der anerkannten E-ID auch in den Informationssystemen der anerkannten IdP und der Identitätsstelle geführt werden, müssen diese Stellen vom Verbot der Paralleldatensammlung ausgenommen werden.

2. Schweizerisches Zivilgesetzbuch (ZGB, SR 210)

Artikel 43a Absatz 4 Ziffer 5
Artikel 43a des ZGB regelt den Zugang im Abrufverfahren zu den elektronischen Registern zur Führung des Personenstandes. Die Auflistung von Stellen, die Zugriff auf Infostar haben, wird um die Identitätsstelle erweitert.

3. Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG, SR 831.10)

Artikel 50a Absatz 1 Buchstabe b^{quater}
In Artikel 50a AHVG wird geregelt, an welche Stellen in Abweichung von Artikel 33 des Bundesgesetzes vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1) Daten, insbesondere die Versichertennummer (AHVN13), bekanntgegeben werden dürfen. Die Identitätsstelle wird neu als eine dieser Stellen erwähnt. Die formalgesetzliche Voraussetzung für die systematische Nutzung der AHVN13 durch SID und IdP wird in Artikel 9 VE geschaffen.

4. Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES, SR 943.03)

Art. 9 Abs. 1bis
Im Ausgabeprozess für eine elektronische Signatureinheit ist die persönliche Vorsprache vorgeschrieben. Diese entfällt, wenn der Identitätsnachweis durch eine E-ID erbracht werden kann.

2 Auswirkungen

2.1 Auswirkungen auf den Bund

2.1.1 Sichere Online-Identifizierung

Verschiedene Bundesstellen werden voraussichtlich von der E-ID guten Gebrauch machen können. Die E-ID wird dort angewendet werden, wo natürliche Personen im direkten Kontakt mit der Bundesverwaltung stehen und sich bei staatlichen Stellen sicher identifizieren sollen. Mit der E-ID steht verschiedensten Informationssystemen eine adäquate Lösung für die sichere Identifizierung und Authentifizierung der Personen zur Verfügung. Beispiele hierfür sind die Online-Bestellung von Auszügen aus dem Straf- oder Betreibungsregister oder die Online-Eingabe von Daten in land- und veterinärwirtschaftliche Informationssysteme.

Die E-ID kann darüber hinaus für vielfältige Identifizierungs- und Authentifizierungszwecke auch für Angestellte der Bundesverwaltung eingesetzt werden. Damit bildet die E-ID eine wichtige Komponente für die in Entwicklung begriffenen IAM-Konzepte des Bundes.

Der Ressourcenbedarf und die Finanzierung wurden unter Ziffer 1.4.2 aufgezeigt. Weiterer Aufwand wird sich auf Anpassungen bei Informatiklösungen und die Beschaffung der Dienst-

leistungen der IdP beschränken, wobei durch Vereinfachung der Prozesse auch Einsparungen realisierbar sind.

Mit Blick auf die verschiedenen im Ausland realisierten Lösungen und deren aktuelle Verwendung besteht auch ein gewisses Risiko, dass die vorgeschlagene Lösung, trotz aller Abklärungen und positiven Rückmeldungen sich am Markt nicht durchsetzt. Dafür kann es unterschiedliche Gründe geben. Beim vorliegenden Konzept wurde den Erfahrungen im Ausland Rechnung getragen und versucht, aus den dortigen Fehlern die richtigen Schlüsse zu ziehen, letztendlich werden aber die Nutzer und der Markt darüber entscheiden, ob sich dieses Vorhaben durchsetzt.

2.1.2 Bemerkung zum öffentlichen Beschaffungswesen

Behörden als Betreiberinnen von E-ID-verwendenden Diensten
Behörden, die einen E-ID-verwendenden Dienst anbieten sind Betreiberinnen eines E-ID-verwendenden Dienstes nach diesem Gesetz und müssen mit mindestens einem IdP eine Vereinbarung über die Verwendung eines E-ID-Systems abschliessen.

Die Identifizierungsleistungen werden für eine E-Government Anwendung benötigt, die in Ausführung einer Aufgabe im öffentlichen Interesse betrieben wird. Die Behörde ist eine Stelle, die dem öffentlichen Beschaffungsrecht untersteht. Identitätsdienstleistungen sind Informatikleistungen, die dem öffentlichen Beschaffungsrecht unterstehen. Mit diesem Gesetz wird ein Markt für die Leistung geschaffen und sie wird gegen Geld (Steuergelder) erbracht.

Für die Leistungen, des IdP ist also ein Beschaffungsverfahren gemäss den anwendbaren Regeln des öffentlichen Beschaffungswesens (Bundesgesetz vom 16. Dezember 1994 über das öffentliche Beschaffungswesen, BöB, SR 172.056.1 oder kantonales Recht) durchzuführen, es sei denn, der Bundesrat bezeichne eine Verwaltungseinheit, die ein E-ID-System für die Bedürfnisse der Behörden betreibt (Art. 13 VE).

Anbieter von Identitätsdienstleistungen
Die Anerkennung von IdP hingegen ist kein Beschaffungsvorgang, sondern ein wirtschaftspolizeilicher Akt der Kundenschutz bringt. Diese wirtschaftspolizeiliche Regelung stützt sich auf Artikel 95 Absatz 1 der Bundesverfassung (vgl. Ziff. 4.1).

Die Anerkennung bewirkt keine wirtschaftspolitische Steuerung: die Anzahl erteilter Anerkennungen ist nicht limitiert und anerkannte IdP geniessen keine Exklusivitätsrechte. Nicht anerkannte IdP können elektronische Identifizierungseinheiten herausgeben, diese sind aber keine E-ID im Sinne des vorliegenden Gesetzes. Eine Anerkennung wird erteilt und erneuert, solange die Anerkennungsvoraussetzungen (Art. 4 VE) erfüllt werden und die technischen und organisatorischen Vorgaben eingehalten sind.

2.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Auf Kantons- und Gemeindeebene ist eine grosse Anzahl E-Government-Lösungen im Einsatz. Die Prozesse bei der Identifizierung und Authentifizierung, um Zugang zu diesen Systemen zu erhalten, werden durch die Anwendung der E-ID erheblich vereinfacht. Heute ist beispielsweise im Kanton Bern die elektronische Erfassung der Steuererklärung zwar mög-

lich, aber nur nach Eingabe eines Passwortes, das auf dem Postweg zugestellt wird und mit Einsendung eines handschriftlich unterschriebenen Formulars. Diese Zustellungen könnten entfallen, wenn die oder der Steuerpflichtige über eine E-ID verfügte.

Die Nutzung von E-Government Dienstleistungen, die durch Städte oder Gemeinden angeboten werden, wird durch die einfache und sichere Identifizierung gefördert. Behördengänge können eingespart werden, sofern die Prozesse angepasst werden. Privatpersonen könnten den Verkehr mit den Behörden auf Kantons- und Gemeindeebene ortsunabhängig von internetfähigen Geräten aus pflegen.

2.3 Auswirkungen auf die Volkswirtschaft

Sichere und geregelte Verhältnisse auch im Cyberraum tragen wesentlich zur Attraktivität des Wirtschaftsstandorts Schweiz und zu seiner Wettbewerbsfähigkeit bei. Der Bundesrat verfolgt 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 ZertES oder die Schaffung von einheitlichen Personen- und Unternehmens-Identifikationsnummern und der entsprechenden Register.

Breit verfügbare anerkannte elektronische Identifizierungsmittel bilden einen wichtigen Eckstein in einem umfassenderen E-ID-Ökosystem, das Sicherheit und Vertrauen im elektronischen Geschäftsverkehr herstellen kann. Dadurch können anspruchsvolle Geschäfte mit dem Staat wie auch unter Privaten elektronisch und damit effizienter abgewickelt werden. Zudem eröffnen sich bedeutende neue Geschäftsfelder.

2.4 Auswirkungen auf die Gesellschaft

Die sichere Identifikation der Partnerinnen und Partner bei der elektronischen Kommunikation erschwert oder verhindert Missbrauch und schafft auch im Cyberraum Vertrauen.

Missbrauch im Internet basiert oft 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 von E-Mails als jemand aus, der sie nicht sind, beispielsweise als die Bank der Empfängerin oder des Empfängers, und können damit grossen Schaden anrichten. Anerkannte Identifizierungsmittel helfen die Identität der Inhaberinnen und Inhaber in der heutigen globalisierten und hoch vernetzten Gesellschaft zu schützen. Der für ein Individuum potenziell sehr gefährliche Identitätsdiebstahl wird dadurch deutlich erschwert. Durch die Einführung einer E-ID-Registrierungsnummer entfällt in vielen Fällen die Notwendigkeit den Namen, Vornamen und das Geburtsdatum offenzulegen. Die E-ID-Registrierungsnummer ist damit ein eindeutiges Pseudonym, dass für Aussenstehende keine Rückschlüsse auf weitere persönliche Daten erlaubt. Die Privatsphäre wird dadurch besser geschützt, als wenn Namen offengelegt werden müssen, die von beliebigen Aussenstehenden einfach Personen zugeordnet werden können.

2.5 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. So können zum Beispiel persönliche Vorsprachen und die damit verbundenen Belastungen der Verkehrsinfrastruktur und Emissionen vermieden werden.

2.6 Andere Auswirkungen

Da keine negativen oder lediglich vernachlässigbare Auswirkungen auf die Volkswirtschaft oder auf Unternehmen zu erwarten sind, wird auf eine weitergehende formelle Regulierungsfolgeabschätzung verzichtet.

3 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates

Die Vorlage eines Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E ID-Gesetz) ist in der Botschaft vom 27. Januar 2016[12] zur Legislaturplanung 2015–2019 und im Bundesbeschluss vom 14. Juni 2016[13] über die Legislaturplanung 2015–2019 angekündigt.

Das vorliegende Projekt dient insbesondere der Zielerreichung bei verschiedenen bundesrätlichen Strategien, die ebenfalls Richtliniengeschäfte der Legislaturplanung 2015–2019 sind. So hat der Bundesrat im April 2016 die Strategie „Digitale Schweiz“[14] aktualisiert und dadurch die Handlungsfelder definiert, in denen das Innovationspotenzial von IKT besonders grosse Wirkung erzielen kann. Sichere elektronische Identifizierungsmittel sind in mehreren Aktionsfeldern der bundesrätlichen Strategie „Digitale Schweiz“ Voraussetzung für die Umsetzung und Teil des Kernziels Transparenz und Sicherheit. Durch anerkannte elektronische Identifikationsmittel können sich die Einwohnerinnen und Einwohner der Schweiz in der virtuellen Welt genauso sicher bewegen wie in der realen und sind in der Lage, ihre informationelle Selbstbestimmung auszuüben.

Die E-Government-Strategie Schweiz[15] setzt im Schwerpunktplan die Etablierung einer national und international gültigen elektronischen Identität als operatives Ziel (Nummer 5). Zur Innovations- und Standortförderung soll die Schweiz über ein verlässliches Umsetzungskonzept für eine nachhaltige Identität im „virtuellen Raum“ verfügen und damit langfristige Perspektiven für den Wirtschaftsraum und die digitale Gesellschaft schaffen.

---

12 BBl 2016 1105, hier 1171 und 1222

13 BBl 2016 5183, hier 5185

14 Strategie Digitale Schweiz: Vgl. Link im Fundstellennachweis

15 E-Government-Strategie Schweiz: Vgl. Link im Fundstellennachweis

4 Rechtliche Aspekte

4.1 Verfassungsmässigkeit

Die Kompetenz zur Regelung von E-ID ergibt sich indirekt aus der Bundesverfassung (BV, SR 101). Die Ausstellung von E-ID wird privaten Identitätsdienstleistern überlassen. Für die Anerkennung müssen diese verschiedene Auflagen erfüllen, was die privatwirtschaftliche Erwerbstätigkeit einschränkt. Artikel 95 Absatz 1 BV ermächtigt den Bund, wirtschaftspolizeiliche Vorschriften über die Ausübung privatwirtschaftlicher Erwerbstätigkeit zu machen.

Soweit die Auflagen die Vertragsverhältnisse zwischen den Identitätsdienstleistern und den Nutzer betreffen, werden im Erlass zivilrechtliche Aspekte geregelt. Deshalb stützt sich die Vorlage auch auf Artikel 122 Absatz 1 BV, der dem Bund die Kompetenz zur Regelung des Zivilrechts gibt.

4.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Vorlage ist mit den bestehenden internationalen Verpflichtungen vereinbar. Bei der Erarbeitung der Vorlage wurde darauf geachtet, dass die Notifizierung gemäss eIDAS-Verordnung grundsätzlich möglich bleibt. Falls zu einem späteren Zeitpunkt gewünscht, kann die schweizerische anerkannte E-ID europaweite Anerkennung erlangen. Dazu wird ein bilaterales Abkommen mit der EU oder mit einzelnen Mitgliedstaaten nötig sein.

4.3 Erlassform

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

4.4 Delegation von Rechtssetzungsbefugnissen

Bezug einer E-ID durch Ausländer
Der Bundesrat kann durch Erlass einer Verordnung Ausländer, die nicht aufgrund ausländischer Ausweispapiere sicher identifiziert werden können und die keine Aufenthaltsbewilligung erhalten, vom Bezug einer E-ID ausschliessen. Falls dennoch ein Zugang zu E-ID-verwendenden Diensten, insbesondere im Asylbereich, benötigt wird, können andere Verfahren für die Identifizierung und Authentisierung vorgesehen werden, z. B. durch Zugangscodes auf Papier. Die entsprechende Kompetenz findet sich in Artikel 3 Absatz 2 des Vorentwurfs.

Technische und organisatorische Vorgaben
Um möglichst zeitnah auf technische Entwicklungen reagieren zu können, werden die Voraussetzungen für die Prozesse und technische Vorgaben und Standards auf Verordnungs- und Weisungsebene geregelt.

In Artikel 3 Absatz 3 des Vorentwurfs wird dem Bundesrat die Kompetenz zur Regelung des Bezugs, des Ausstellungsprozesses, sowie der Sperrung und dem Widerruf einer E-ID erteilt.

Voraussetzungen für die Anerkennung kann der Bundesrat aufgrund Artikel 4 Absatz 4 insbesondere in Bezug auf die fachlichen und sicherheitsbezogenen Anforderungen an IdP, die notwendige Versicherungsdeckung und die anwendbaren Standards und technischen Protokollen für E-ID-Systeme erlassen. Internationale und nationale Standards, die zur Anwendung gelangen sollen, werden in kurzen Intervallen neu erarbeitet und herausgegeben. Der Verordnungsgeber kann darauf schneller reagieren, als das Parlament.

Die Mindestanforderungen an die Identifizierungs- und Authentifizierungsprozesse der verschiedenen Sicherheitsniveaus können aufgrund von Artikel 5 Absatz 4 des Vorentwurfs auf Verordnungsebene erlassen werden. Auch hier braucht es eine gewisse Flexibilität, um auf dem jeweils aktuellsten technischen Stand zu bleiben.

Auch die technischen Standards für die Sicherstellung der Interoperabilität der verschiedenen E-ID-Systeme sollen schnell den technischen Möglichkeiten angepasst werden können und sind deshalb auf Verordnungsebene zu regeln (Art. 18 Abs. 2 VE).

Adressat einer Verordnung über die neuesten anwendbaren Standards und technischen Protokolle für die Übermittlung der Personenidentifizierungsdaten ist die Identitätsstelle. Für den Fall, dass verschiedene Personenregister abweichende Daten liefern, regelt der Bundesrat das Vorgehen zur Bereinigung (Art. 20 Abs. 5 VE).

Subsidiäres E-ID-System des Bundes
Falls sich kein IdP findet, der eine E-ID für die Identifizierung und Authentisierung ausstellt, die für E-ID-verwendende Dienste von Behörden geeignet ist, kann der Bundesrat eine Verwaltungseinheit bezeichnen, die ein solches E-ID-System betreibt. Gegebenenfalls kann diese Verwaltungseinheit für die Einrichtung und den Betrieb mit Privaten zusammenarbeiten (Art. 13 VE).

Haftpflichtrechtliche Schutznormen für Inhaberinnen und Inhaber
Der Bundesrat kann aufgrund Artikel 14 Absatz 3 des Vorentwurfs die einzuhaltenden Sorgfaltspflichten für Inhaberinnen und Inhaber einer E-ID auf Verordnungsebene festlegen. Diese Sorgfaltspflichten können sich dem Stand der Technik entsprechend relativ schnell ändern. Eine Regelung auf Verordnungsebene ist deshalb sinnvoll.

Erhebung von Gebühren
Vergleiche die Ausführungen zu Artikel 23.

4.5 Datenschutz

4.5.1 Datenschutzrecht ausreichend

Die Regeln des Datenschutzrechts (Bundesgesetz vom 19. Juni 1992 über den Datenschutz, DSG, SR 235.1 und die zugehörigen Verordnungen) sind ausreichend, um den Datenschutz im Bereich der E-ID sicherzustellen. Trotzdem wird in Bezug auf das Einwilligungserfordernis eine ausdrückliche Regelung im Gesetz eingefügt. Die Bearbeitung der staatlich bestätigten

Personenidentifizierungsdaten wird eingeschränkt. IdP dürfen sie nur bearbeiten, um Identifizierungs- und Authentifizierungsleistungen zu erbringen (Art. 10 Abs. 1 VE).

Im Übrigen wird die Weitergabe gewisser Personenidentifizierungsdaten und der darauf basierenden Nutzungsprofile eingeschränkt (Art. 10 Abs. 3 VE).

4.5.2 Einwilligung in die Übermittlung

Überall, wo Personenidentifizierungsdaten im Spiel sind, ist es wichtig, dass die Voraussetzungen des Datenschutzes eingehalten bzw. erforderlichen Sicherheitsvorkehrungen getroffen werden. Die Inhaberinnen und Inhaber der E-ID geben ihr ausdrückliches Einverständnis zur Übermittlung gewisser Personenidentifizierungsdaten. Bei Ausstellung der E-ID wird der IdP ermächtigt, die Daten bei der Identitätsstelle abzurufen (Art. 6 Abs. 3 VE) und bei der Anwendung bei einem E-ID-verwendenden Dienst wird wiederum das Einverständnis der Inhaberin oder des Inhabers zur Übermittlung der Daten durch den IdP an die Betreiberin von E-ID-verwendenden Diensten eingeholt (Art. 17 Abs. 1 Bst. f VE).

4.5.3 Einschränkung der Handelbarkeit von Daten

Besonderes Augenmerk wird auf die Handelbarkeit der Daten gelegt. Artikel 10 Absatz 3 VE verbietet die Weitergabe von staatlich bestätigten Daten und darauf aufbauenden Nutzungsprofilen an Dritte. Allerdings wird dabei zwischen den Basisdaten, wie sie beim Sicherheitsniveau niedrig übermittelt werden, und den ergänzenden Daten der höheren Sicherheitsniveaus unterschieden. Die Basisdaten E-ID-Registrierungsnummer, Name und Geburtsdatum, sowie die durch den IdP selbst zugeordneten Daten (z. B. Adresse oder Kundennummer) sind nicht vom Handelsverbot betroffen. Hingegen soll nicht mit Nutzungsprofilen, die auf den zusätzlichen bestätigten Daten (z. B. auf dem Geschlecht oder dem Zivilstand) beruhen, gehandelt werden können.

Aus dieser Einschränkung der Handelbarkeit ergibt sich ein verminderter wirtschaftlicher Wert der staatlich bestätigten Personenidentifizierungsdaten. Diese Daten werden ausdrücklich als nicht pfändbar und von der Konkursmasse ausgenommen erklärt (Art. 11 Abs. 1 VE). Um den Fortbestand eines anerkannten E-ID-Systems und den dazugehörigen E-ID im Fall der finanziellen Krise eines IdP zu sichern, können jedoch anerkannte E-ID-Systeme als Ganzes an andere anerkannte IdP verkauft werden. Der Kaufbetrag fällt dann allenfalls in die Konkursmasse (Art. 11 Abs. 3 VE).

5 Weiterführende Dokumentation

- Staatlich anerkannte elektronische Identifizierungsmittel (E-ID), Konzept 2016
- Fundstellennachweis
- Begriffskonkordanz-Tabelle

5.1 Fundstellennachweis zu den Erläuterungen zum VE E-ID-Gesetz

Seite	Dokument	Links (alle aufgerufen am 14. November 2016)
3	eIDAS-Verordnung	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ABl. L 257 vom 28.8.2014, S. 73, berichtigt in ABl. L 155 vom 14.6.2016, S. 44 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02014R0910-20140917
5 9	Durchführungsverordnungen und -beschlüsse zur eIDAS	Durchführungsbeschluss (EU) 2015/296 der Kommission vom 24. Februar 2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 53 vom 25.2.2015, S. 14 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015D0296
		Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 235 vom 9.9.2015, S. 26 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015D1505

		Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden ABl. L 235 vom 9.9.2015, S. 37 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2015.235.01.0037.01.DEU
		Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung gemäß Artikel 9 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 289 vom 5.11.2015, S. 18 http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1476166146152&uri=CELEX:32015D1984
		Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 109 vom 26.4.2016, S. 40 http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32016D0650
		Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 235 vom 9.9.2015, S. 1–6 berichtigt in ABl. L 28 vom 4.2.2016, S. 18–18

		http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1476167531332&uri=CELEX:32015R1501R(01)
		Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ABl. L 235 vom 9.9.2015, S. 7 http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32015R1502
		Durchführungsverordnung (EU) 2015/806 der Kommission vom 22. Mai 2015 zur Festlegung von Spezifikationen für die Form des EU-Vertrauenssiegels für qualifizierte Vertrauensdienste ABl. L 128 vom 23.5.2015, S. 13 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:JOL_2015_128_R_0006
		Verordnung (EU) 2015/1017 des Europäischen Parlaments und des Rates vom 25. Juni 2015 über den Europäischen Fonds für strategische Investitionen, die europäische Plattform für Investitionsberatung und das europäische Investitionsvorhabenportal sowie zur Änderung der Verordnungen (EU) Nr. 1291/2013 und (EU) Nr. 1316/2013 — der Europäische Fonds für strategische Investitionen ABl. L 348 vom 20.12.2013, S. 129, geändert durch Verordnung (EU) 2015/1017, ABl. L 169 vom 1.7.2015, S. 16 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015R1017
14	NSTIC Strategie USA	National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem https://www.nist.gov/itl/nstic
21	NIST Sicherheitsanforde-	Cybersecurity Framework

	rungen	https://www.nist.gov/cyberframework
38	Bundesrätliche Strategien	Strategie "Digitale Schweiz" https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/strategie.html
		E-Government Strategie Schweiz https://www.egovernment.ch/de/umsetzung/e-government-strategie/

5.2 Begriffskonkordanztabelle

eID-Konzept	E-ID-Gesetz	eIDAS Deutsch	English
Anerkennungsstelle für Identitätsdienstleister (AID)	Anerkennungsstelle für IdP (Anerkennungsstelle)	-	Accreditation Authority
Antragsteller	antragstellende Person	Antragsteller	Applicant
Authentifizierung	Authentifizierung	Authentifizierung	Authentication
Eindeutiger Personenidentifikator (EPID)	E-ID-Registrierungsnummer	eindeutige Kennung	Unique Personal Identification Number
staatlich anerkanntes Identifizierungsmittel (E-ID)	anerkannte elektronische Identifizierungseinheit (E-ID)	Elektronisches Identifizierungsmittel	Credential
elektronisches Identifizierungssystem (E-ID-System)	E-ID-System	Elektronisches Identifizierungssystem	Identity System
Elektronische Identifizierung	Elektronische Identifizierung	Elektronische Identifizierung	Identification
staatlich anerkannter Identitätsdienstleister (Identity Provider, IdP), Herausgeber, Aussteller	anerkannte Identity Provider (IdP) oder Anbieterinnen von Identitätsdienstleistungen	Aussteller	Identity Provider (IdP), Credential Service Provider (CSP)
elektronischer Identitätsnachweis	elektronischer Identitätsnachweis	elektronischer Identitätsnachweis	Identity Proofing
Inhaber	Inhaber und Inhaberin	natürliche Person	Claimant/Subscriber
Interoperabilität	Interoperabilität	-	Interoperability
Online-Dienste	Online-Dienste	-	Online Services
Personenidentifizierungsdaten (PID)	Personenidentifizierungsdaten	Personenidentifizierungsdaten	Identity Attribute
Registrierung	Registrierung	Registrierung	Registration
Schweizerische Stelle für elektronische Identität (SID)	Schweizerische Stelle für elektronische Identität (Identitätsstelle)	verlässliche Quelle	Steering Group and Attribute Authority, Root Attribute Authority
Vertrauende Beteiligte (vBt)	Betreiberin von E-ID-verwendenden Diensten	Vertrauender Beteiligter	Relying Party (RP)
vertrauender Dienst	E-ID-verwendender Dienst	-	Relying Service
Sicherheitsniveau	Sicherheitsniveau	Sicherheitsniveau	Level of Assurance / Assurance Level