Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

18.xxx

# Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste

vom …

---

Sehr geehrter Herr Nationalratspräsident
Sehr geehrte Frau Ständeratspräsidentin
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf des Bundesgesetzes über elektronische Identifizierungsdienste.

Gleichzeitig beantragen wir Ihnen, den folgenden parlamentarischen Vorstoss abzuschreiben:

| | | | |
|---|---|---|---|
| 2018 | M | 17.3083 | Digitalisierung. Eine elektronische Identität für den landesweiten Bürokratieabbau (N 8.3.2017, FDP-Liberale Fraktion; N 20.9.2017, S 28.02.2018) |

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrte Frau Ständeratspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

## Übersicht

***Die Digitalisierung der Gesellschaft schreitet voran. Die Möglichkeit, sich im Internet auf sichere und einfache Weise auszuweisen, spielt eine entscheidende Rolle bei der Akzeptanz und weiteren Verbreitung von digitalen Online-Anwendungen. Mit dem in dieser Botschaft vorgestellten Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID) wird die Basis für die Herausgabe von elektronischen Identifizierungsmitteln geschaffen, die es den Einzelnen ermöglichen, sich aufgrund staatlich bestätigter Daten im digitalen Raum zu identifizieren.***

*Das E-ID-Gesetz bezweckt die Förderung des sicheren elektronischen Geschäftsverkehrs unter Privaten und mit Behörden. Zur Erreichung dieses Ziels sollen die Aufgaben gemäss dem vorliegenden Gesetz zwischen Staat und Privatwirtschaft aufgeteilt werden. Der Staat wird weiterhin seine Hauptaufgabe erfüllen: die amtliche Überprüfung und Bestätigung der Identität einer Person. Angesichts der Dynamik des technologischen Wandels wäre er jedoch nicht in der Lage, die technischen Trägermittel für die Identifizierung selbst zu entwickeln und herzustellen. Die Privatwirtschaft ist näher an den Nutzerinnen und Nutzern und an den erforderlichen digitalen Technologien und kann diese Funktion besser erfüllen. Der Betrieb des E-ID-Systems sowie die Ausstellung der E-ID sind folglich Sache von privaten Anbieterinnen (Identity Provider, IdP). Der Staat wird jedoch auch in diesem Bereich eine wichtige Rolle übernehmen, denn er wird die Anbieterinnen und die von ihnen eingerichteten Systeme einem strengen Anerkennungsverfahren und sie und ihre Systeme regelmässigen Kontrollen unterziehen. So werden die Anforderungen an die Sicherheit und den Schutz der Daten überprüft und ständig an die neusten Entwicklungen angepasst werden. Die gemeinsame Nutzung der Fähigkeiten von Staat und Privatwirtschaft bietet die optimalen Voraussetzungen für die Einführung und den Einsatz der E-ID.*

*Das E-ID-Gesetz enthält keine abschliessende Regelung für die Identifizierung im Internet. Es regelt lediglich die Ausstellung und Nutzung von E-ID. Daneben können auf dem Markt künftig auch andere E-ID angeboten und verwendet werden, die allerdings nicht über das qualifizierte Vertrauen verfügen, das die staatliche Anerkennung verleiht.*

*Mit einer E-ID können sich natürliche Personen sicher und bequem bei privaten und öffentlichen Online-Portalen (E-ID-verwendenden Diensten) registrieren und später wieder anmelden. Die E-ID wird den Kontakt mit Behörden erleichtern, die zunehmend ihre Dienste auch über «virtuelle Schalter» anbieten. Die Nutzung von E-Government-Anwendungen könnte zukünftig vollständig elektronisch erfolgen. Im Bereich E-Health wird die E-ID in einem ersten Schritt ergänzend zu den gemäss Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (EPDG) herausgegebenen Identifizierungsmitteln zum Einsatz kommen und diese mittelfristig wohl ablösen.*

*Der Gesetzesentwurf legt nicht fest, auf welchem Träger die E-ID geführt werden soll. Heute gängige elektronische Identifizierungsmittel sind sowohl auf Mobiltelefonen (z.B. Mobile-ID), auf Karten oder Speichermedien mit integrierten Chips (sog. Integrated Circuit Card ICC oder Smartcard, z. B. SuisseID) erhältlich. Manche sind gar nicht materialisiert, sondern über das Internet mit Nutzername, Passwort und allenfalls über das Smartphone zugesandtem einmal nutzbaren Transaktionscode einsetzbar (vgl. Online-Banking-Lösungen).*

*Im Gesetzesentwurf werden drei verschiedene Sicherheitsniveaus festgelegt. Nicht für jeden Geschäftsprozess ist das gleiche Sicherheitsniveau erforderlich, und nicht alle Trägermittel sind für jedes Sicherheitsniveau geeignet. Aus diesem Grund sollen die IdP E-ID-Systeme den praktischen Bedürfnissen entsprechend auf drei unterschiedlichen Sicherheitsniveaus anbieten können, wie diese auch von der EU und dem National Institute of Standards and Technology festgeschrieben werden. Für eine Anerkennung muss der IdP über ein E-ID-System verfügen, das mindestens das Sicherheitsniveau «niedrig» erfüllt. E-ID-Systeme der Sicherheitsniveaus «substanziell» und «hoch» erfüllen die Mindestanforderungen und darüber hinaus weitere Voraussetzungen.*

*Das Gesetz formuliert strenge datenschutzrechtliche Rahmenbedingungen und regelt den Zweck und die Voraussetzungen für die Bearbeitung und Weitergabe der Daten im Rahmen der Ausstellung und Nutzung der E-ID. Der IdP darf die Identifizierungsdaten ausschliesslich zum Zweck der Identifizierung nach diesem Gesetz und nur während einer bestimmten Zeit bearbeiten. Ausserdem darf er den Betreiberinnen von E-ID-verwendenden Diensten nur diejenigen Personenidentifizierungsdaten weitergeben, die für die Identifizierung der betreffenden Person und somit für die Funktion der E-ID notwendig sind und in deren Übermittlung die Inhaberin oder der Inhaber der E-ID eingewilligt hat. Die Übermittlung ist erforderlich, damit das E-ID-System seine Funktion, eine einfache und sichere Identifizierung zu ermöglichen, erfüllen kann. Schliesslich umfasst das vorliegende Gesetz eine Gesetzesgrundlage für die Bearbeitung und Weitergabe der Daten durch die betreffenden Bundesorgane.*

*Der Gesetzesentwurf berücksichtigt internationale Regelungen, insbesondere die 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. Auch wenn völlig offen ist, ob, wann und wie die Schweiz sich mittels eines bilateralen Vertrags in dieses System einbinden wird, ist die schweizerische E-ID-Lösung von Beginn an so konzipiert, dass sie grundsätzlich notifiziert werden könnte.*

## Inhaltsverzeichnis

# Botschaft

## 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. Damit auch anspruchsvollere Geschäftsprozesse online abgewickelt werden können, müssen die Geschäftsanbietenden (in der Folge als Betreiberinnen von E-ID-verwendenden Diensten*[1] bezeichnet) Vertrauen in die Identität des Gegenübers haben. Gesicherte Identitäten sind die Basis für Rechtssicherheit, auch über Staatsgrenzen hinaus. Diesem Bedürfnis 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 Identifizierungszwecke 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. Vertrauenswürdige E-ID sind damit ein Beitrag für die Implementierung von elektronischen Geschäftsprozessen.

Mit Bundesratsbeschluss vom 19. Dezember 2012 wurde das Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt, in Zusammenarbeit mit der Schweizerischen Bundeskanzlei (BK), dem Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF), dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) und dem Eidgenössischen Finanzdepartement (EFD) ein Konzept und einen Rechtsetzungsentwurf für elektronische staatliche Identifizierungsmittel 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 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 in der Folge grundlegend überarbeitet. Eigenentwicklungen durch den Staat und staatlich abgegebene E-ID führen in der Regel zu hohen ungedeckten IKT-Kosten für die öffentliche Hand, weil zu wenig flexibel auf die schnell ändernden Bedürfnisse und Technologien reagiert werden kann. Deshalb geht das Konzept von einer Aufgabenteilung zwischen Bund und Privaten aus. Bereits heute bestehen privatwirtschaftliche elektronische Identifizierungsangebote verschiedener Sicherheitsniveaus (z.B. Apple-ID, Google-ID, Mobile-ID, OpenID, SuisseID*, SwissID*,

1 Die mit einem Sternchen versehenen Begriffe werden im Glossar erklärt.

SwissPass etc.). Welche dieser derzeit gängigen E-ID neben der E-ID nach diesem Gesetz auch mittel- und längerfristig bestehen werden, ist heute kaum abzuschätzen.

Die neuesten Entwicklungen in der EU sind im Konzept berücksichtigt und die Kompatibilität mit der Verordnung (EU) Nr. 910/2014[2] (sog. eIDAS-Verordnung*) wurden abgeklärt.

Der Bundesrat hat am 13. Januar 2016 Kenntnis vom überarbeiteten E-ID-Konzept genommen, das EJPD mit der Ausarbeitung eines Gesetzesvorentwurfes beauftragt und die Rahmenbedingungen für die Gesetzgebung festgelegt. Das Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) dauerte vom 22. Februar 2017 bis zum 29. Mai 2017. Der Bundesrat hat an seiner Sitzung vom 15. November 2017 das EJPD nach Kenntnisnahme der Resultate der Vernehmlassung beauftragt, einen Gesetzesentwurf auszuarbeiten.

## 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 konventionelle Identifizierungsmittel aus, nämlich Schweizerpass, Identitätskarte und Ausländerausweis. Pass und Identitätskarte sind zudem Reisedokumente und ermöglichen aufgrund von internationalen Vereinbarungen die Einreise in andere Staaten. Ergänzend dazu soll nun die Identität einer natürlichen Person auch in der elektronischen Welt mittels einer E-ID nachgewiesen werden können. E-ID nach diesem Gesetz werden es den Inhaberinnen und Inhabern ermöglichen, sich bei Online-Diensten sicher zu registrieren und sich später erneut sicher anzumelden.

Über die reine Identifizierung hinausgehende Vertrauensdienste wie die elektronische Signatur gemäss Bundesgesetz vom 18. März 2016[3] über die elektronische Signatur (ZertES) können von den Anbieterinnen von Identitätsdienstleistungen (Identity Provider, IdP*) angeboten werden, sie sind jedoch nicht Bestandteil der E-ID und des vorliegenden Gesetzesentwurfs. Ebenso wenig regelt der vorliegende Gesetzesentwurf die Ausgestaltung von Zugangsberechtigungen zu Online-Diensten (Access-Management). Dabei geht es nicht nur um die Identifizierung von Personen, sondern auch darum, nur denjenigen Personen Zugang zu einem Dienst zu gewähren, die auch wirklich das Recht dazu haben. Es steht den IdP frei, neben den Identi-

2 Verordnung (EU) Nr. 910/2014 des europäischen 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.
Eine Liste der EU-Rechtsgrundlagen (inkl. Links) ist veröffentlicht unter Startseite BJ > Staat & Bürger > Laufende Rechtsetzungsprojekte > E-ID-Gesetz.

3 SR **943.03**

fizierungslösungen eben gerade auch sicheres Access-Management anzubieten und damit den E-ID-verwendenden Diensten eine Gesamtlösung im sogenannten «IAM - Identity and Access Management*» zu offerieren.

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 Zusammenspiel von Staat und Privaten

Der Entwurf geht von einem Zusammenwirken von Staat und Privaten aus. Die vertrauensbildende Kraft staatlicher Anerkennung und Aufsicht soll mit dem technologischen Knowhow und der Dynamik privatwirtschaftlicher Initiative kombiniert werden. Auf diese Weise soll die nötige Akzeptanz für die E-ID gewährleistet werden. Geeignete IdP werden vom Bund zur Ausstellung von E-ID und zum Betrieb von E-ID-Systemen* ermächtigt. Alle E-ID-Systeme müssen untereinander interoperabel sein, damit ein hoher Kundennutzen entsteht.

Es wird weiterhin Aufgabe des Staates sein, die Identität einer Person mittels Angaben aus den Informationssystemen des Bundes amtlich zu überprüfen und zu bestätigen. Eine eigens dafür geschaffene Identitätsstelle* bei fedpol, die die amtlichen Register mit den entsprechenden Daten führt, wird diese Aufgabe übernehmen. Sie wird überprüfen, ob die Nutzerinnen und Nutzer die persönlichen Voraussetzungen erfüllen, und wird für die Feststellung der Identität der Personen anlässlich der Erstidentifizierung zuständig sein. Ausserdem wird die Identitätsstelle den Personenidentifizierungsdaten* der Nutzerinnen und Nutzer die E-ID-Registrierungsnummern* zuweisen. Die IdP ihrerseits werden die E-ID den betreffenden Personen zuordnen und diesen die Zugangsmittel übergeben.

Angesichts des technologischen Wandels und der Vielfalt möglicher technischer Lösungen wäre der Bund jedoch nicht in der Lage, die Träger der vom Staat bestätigten Identitätsangaben selbst zu entwickeln und herzustellen. Dabei kann es sich beispielsweise um Mobiltelefone, Bankkarten oder Abonnemente für den öffentlichen Verkehr handeln. Die Privatwirtschaft ist näher an den Nutzerinnen und Nutzern und an den erforderlichen digitalen Technologien und kann diese Funktion besser erfüllen und innovative Lösungen anbieten. Dem Staat wird jedoch auch hier eine wichtige Funktion zukommen: Er wird die Anbieterinnen und die von ihnen eingerichteten Systeme einem strengen Anerkennungsverfahren* und sie und die von ihnen eingerichteten Systemen regelmässigen Kontrollen unterziehen. Die Anerkennungsstelle* wird dem Informatiksteuerungsorgan des Bundes (ISB) angegliedert sein.

Das funktionale Zusammenwirken zwischen Staat und Privaten bietet optimale Voraussetzungen für den einfachen und benutzerfreundlichen Einsatz der E-ID durch Verwaltung, Private und Unternehmen. Gleichzeitig ist gewährleistet, dass

flexibel auf die technologischen Entwicklungen, namentlich im Bereich der Sicherheit, reagiert werden kann.

### 1.2.3 Einsatz 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 jeweiligen Registrierung bei einem E-ID-verwendenden Dienst müssen die persönlichen Angaben nicht manuell eingegeben werden. Setzt die sich registrierende Person eine nach diesem Gesetz ausgestellte E-ID ein, so werden diese Daten automatisch an den Dienst übermittelt, sofern der Inhaber oder die Inhaberin der E-ID dazu ihre Zustimmung gegeben hat. 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 und einfache Nutzung von Online-Diensten und bringt dem Einzelnen mehr Sicherheit und Komfort im Internet.

Die E-ID wird den Kontakt mit Behörden erleichtern, die zunehmend ihre Dienste auch über «virtuelle Schalter» anbieten. Heute wird die Identifizierung* vielfach über Zugangsdaten erreicht, die der Einwohnerin oder dem Einwohner auf Papier an eine Postadresse zugestellt werden, z.B. Nutzernamen und einmal verwendbare Passwörter oder Listen mit Zahlenfolgen zum Abstreichen. Zum Abschluss des Vorgangs ist oft wiederum die Rücksendung eines Formulars auf Papier notwendig. Diese Schritte können entfallen, wenn die Identifizierung über eine E-ID sichergestellt wird. Die Nutzung von E-Government-Anwendungen könnte zukünftig vollständig elektronisch erfolgen.

Im Bereich E-Health wird die E-ID in einem ersten Schritt ergänzend zu den gemäss Bundesgesetz vom 19. Juni 2015[4] über das elektronische Patientendossier (EPDG) herausgegebenen Identifizierungsmitteln zum Einsatz kommen und könnte diese mittelfristig ablösen. Der Zugang zum eigenen Patientendossier wird durch den Einsatz einer E-ID mit dem entsprechenden Sicherheitsniveau allenfalls erst ermöglicht, auf jeden Fall aber vereinfacht.

Den E-ID-verwendenden Diensten im E-Commerce bringt die E-ID Sicherheit über die Identität der Kundinnen und Kunden. Da Verwechslungen ausgeschlossen sind, wird darüber hinaus die Bonitätsprüfung erleichtert. Da mit der E-ID auch eine verlässliche Altersabfrage möglich ist, können Kinder und Jugendliche vor ungeeigneten Medieninhalten, beeinträchtigenden Mitteilungen im Rahmen der Online-Kommunikation und intransparenter Bearbeitung persönlicher Daten besser geschützt werden. Regulatorische Eingriffe mit dem Ziel des Kinder- und Jugendmedienschutzes könnten mit der Einführung einer E-ID und der damit verbundenen technischen Entwicklung einfach und sicher umgesetzt werden. Anbieter könnten z. B. gesetzlich verpflichtet werden, ihre potenziell gefährdenden Inhalte nur an

4 SR **816.1**

Nutzerinnen und Nutzer zu übermitteln, deren Alter durch eine E-ID sicher nachgewiesen ist.[5]

Der Entwurf legt nicht fest, auf welchem Träger die E-ID geführt werden soll. Heute gängige elektronische Identifizierungsmittel sind sowohl auf Mobiltelefonen (z.B. Mobile-ID) vorhanden oder auf Karten oder Speichermedien mit integrierten Chips (sog. Integrated Circuit Card ICC oder Smartcard, z. B. SuisseID); manche sind gar nicht materialisiert und über das Internet mit Nutzername, Passwort und allenfalls über das Smartphone zugesandtem einmal nutzbaren Transaktionscode einsetzbar (vgl. z.B. Online-Banking-Lösungen). Es wird erwartet, dass unterschiedliche Träger angeboten werden, die den Präferenzen der einzelnen Nutzerin und des einzelnen Nutzers entgegen kommen.

### 1.2.4 Ausstellung der E-ID

Bevor eine E-ID nach diesem Gesetz ausgestellt werden kann, ordnet das fedpol die E-ID-Registrierungsnummer den Personenidentifizierungsdaten der antragstellenden Person zu. Jede Person erhält nur eine eindeutige E-ID-Registrierungsnummer. Die Ausstellung beinhaltet eine Identifizierung, die je nach Sicherheitsniveau mittels elektronischen Medien oder anlässlich einer persönlichen Vorsprache bei einem IdP durchgeführt wird. Der Ausstellungsvorgang erfolgt in mehreren Schritten (vgl. Art. 6 BGEID):

1. Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP. Dieser leitet die antragstellende Person für die initiale Überprüfung der beanspruchten Identität an fedpol weiter. Fedpol überprüft die Identität der antragstellenden Person aufgrund eines gültigen Ausweises (Pass, IDK oder Ausländerausweis).
2. Fedpol verlangt von der antragstellenden Person zusätzliche identifizierende persönliche Daten (z. B. Informationen über die Eltern, andere Ausweisdokumente usw.) und vergleicht diese mit den in den Personenregistern des Bundes gespeicherten Daten. Die von der antragstellenden Person gemachten Angaben müssen mit den staatlich erfassten Daten übereinstimmen, damit das fedpol der Ausstellung einer E-ID zustimmt.
3. Die antragstellende Person erklärt sich dem fedpol gegenüber einverstanden, dass fedpol die Personenidentifizierungsdaten inklusive der E-ID-Registrierungsnummer an den IdP übermittelt.[6]
4. Fedpol übermittelt die E-ID-Registrierungsnummer mit den Personenidentifizierungsdaten, die dem beantragten E-ID-Sicherheitsniveau entsprechen, an den IdP.

5 Vgl. Jugend und Medien, Zukünftige Ausgestaltung des Kinder- und Jugendmedienschutzes der Schweiz, Bericht des Bundesrates vom 13. Mai 2015 in Erfüllung der Motion Bischofberger 10.3466 «Effektivität und Effizienz im Bereich Jugendmedienschutz und Bekämpfung von Internetkriminalität».

6 Siehe zu den Personenidentifizierungsdaten Artikel 5.

5. Der IdP ordnet der antragstellenden Person ein Authentifizierungsmittel mit einem persönlichen Nutzernamen zu, mit dem sich die antragstellende Person online identifizieren kann. Je nach Sicherheitsniveau ist vorgängig noch die persönliche Vorsprache oder gleichwertige virtuelle Präsenz (z. B. Videoidentifikation) der Antragstellerin oder des Antragstellers notwendig.
6. Der IdP sorgt mit dem Authentifizierungsmittel für die richtige Zuordnung der E-ID-Registrierungsnummer zur E-ID 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.

Das BGEID regelt auch, wie mit elektronischen Identifizierungseinheiten zu verfahren ist, die der IdP vor Inkrafttreten des Gesetzes ausgestellt hat. Während einer Übergangszeit von zwei Jahren anerkennt das ISB auf Antrag eines IdP elektronische Identifizierungseinheiten*, die dieser vor dem Inkrafttreten des vorliegenden Gesetzes ausgestellt hat, als E-ID des Sicherheitsniveaus niedrig. Das ISB anerkennt solche Identifizierungseinheiten auch als E-ID des Sicherheitsniveaus substanziell, wenn zusätzlich eine Identifizierung in einem gesetzlich geregelten und beaufsichtigten Verfahren durchgeführt wurde, das eine vergleichbare Sicherheit bietet wie die nach diesem Gesetz vorgesehenen Verfahren.

Wer ein gültiges qualifiziertes Zertifikat nach Artikel 2 Buchstabe h ZertES besitzt, kann sich damit von einem IdP auf Antrag ohne weitere Identifizierung ebenfalls eine E-ID des Sicherheitsniveaus substanziell ausstellen lassen.

In allen drei Fällen müssen die persönlichen Voraussetzungen nach Artikel 3 erfüllt sein, die Inhaberinnen und Inhaber der Ausstellung der E-ID zugestimmt haben und die Personenidentifizierungsdaten (wie die Nummer der Identitätskarte, Name, Vorname und Geburtsdatum) den im Informationssystem nach Artikel 24 gespeicherten Daten entsprechen.

Der Bundesrat erlässt auf Verordnungsstufe nähere Vorschriften zum Ausstellungsprozess.

### 1.2.5 Sicherheitsniveaus

Nicht alle Geschäftsprozesse erfordern dasselbe Sicherheitsniveau. Zu hohe Sicherheitsanforderungen können in der Praxis als störend empfunden werden, Umgehungshandlungen begünstigen sowie höhere Kosten verursachen. Dies ist weder für die Akzeptanz noch die Sicherheit eines E-ID-Systems vorteilhaft. Deshalb sieht das Anerkennungsverfahren drei unterschiedliche Sicherheitsniveaus mit unterschiedlichen Voraussetzungen vor. Diese drei Sicherheitsniveaus unterscheiden sich durch die enthaltenen Personenidentifizierungsdaten, 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. 4 BGEID). Jedes Sicherheitsniveau vermittelt ein unterschiedliches Mass an Vertrauen. Welches Sicherheitsniveau für welche Art der Anwendung in Frage kommt, muss in den jeweiligen Spezialerlassen festgehalten bzw. durch die privaten Betreiberinnen von E-ID-verwendenden Diensten definiert werden. So kann beispielsweise für E-Education ein anderes Sicherheitsniveau gewählt werden, als es etwa für Vote électronique vorzuschreiben oder für E-Health-Anwendungen notwendig wäre.

Die Bezeichnung und Ausgestaltung der Sicherheitsniveaus wurde aus der eIDAS-Verordnung und den dazugehörenden Durchführungsbestimmungen übernommen. Es wird zwischen den Niveaus *«niedrig»*, *«substanziell»* und *«hoch»* unterschieden. Grundsätzlich können E-ID der Sicherheitsniveaus *«substanziell»* und *«hoch»* auch bei E-ID-verwendenden Diensten eingesetzt werden, die ein tieferes Sicherheitsniveau verlangen (Abwärtskompatibilität).

Der Bund stellt den IdP via eine elektronische Schnittstelle staatlich geführte Personenidentifizierungsdaten zur Verfügung (E-ID-Registrierungsnummer, amtlicher Name, Vornamen sowie Geburtsdatum für das Sicherheitsniveau *«niedrig»* resp. zusätzlich Geschlecht, Geburtsort und Staatsangehörigkeit für die Sicherheitsniveaus *«substanziell»* und zusätzlich das Gesichtsbild für die Sicherheitsniveaus *«hoch»*). 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 Abs. 2 Bst. c BGEID).

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 anzuheben. Dies erleichtert den Einstieg in E-ID-Systeme nach diesem Gesetz. Mit dem Sicherheitsniveau «*niedrig»* wird der Zugang zu E-ID nach diesem Gesetz einfach gehalten, was einen essenziellen Erfolgsfaktor für die Anbieterinnen und 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. Ihre E-ID-Registrierungsnummer bleibt aber immer dieselbe.

Die drei Sicherheitsniveaus für E-ID-Systeme nach diesem Gesetz sind so definiert, dass sie bezüglich Sicherheit die gleichen Anforderungen erfüllen, wie sie für die drei in der eIDAS-Verordnung der EU definierten E-ID-Sicherheitsniveaus gelten (Art. 8 der eIDAS Verordnung und dazugehörige Durchführungsbestimmungen). Die gleichen drei Sicherheitsniveaus werden auch durch das NIST*[7] für E-Government Anwendungen in den USA definiert und gelten heute als weltweiter Standard. Jedes Sicherheitsniveau wird sich zur Erfüllung seines Zwecks durch technische Spezifikationen, Normen und Verfahren einschliesslich technischer Überprüfungen auszeichnen und im Detail in Verordnungen, Weisungen und technischen Standards geregelt. Damit stellt der Gesetzesentwurf die grundsätzliche Kompatibilität zur EU oder der USA sicher.

7 National Institute of Standards and Technology, U.S. Department of Commerce

**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. 5 Abs. 1 BGEID). Der Einsatz der E-ID des Sicherheitsniveaus *«niedrig»* verlangt mindestens eine Ein-Faktor-Authentifizierung*. Die Handhabung einer solchen E-ID ist damit vergleichbar mit einem Zutrittsbadge oder einer kontaktlosen Bezahllösung 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, mit Videoidentifikation gestützt auf einen staatlichen Ausweis oder einen Abgleich des Gesichtbildes, welches dem Ausweis zugeordnet ist. Im Sicherheitsniveau *«substanziell»* werden neben dem Namen und dem Geburtsdatum der E-ID noch weitere Personenidentifizierungsdaten zugeordnet (Geschlecht, Geburtsort und Staatsangehörigkeit, vgl. Art. 5 Abs. 2 BGEID). Der Einsatz der E-ID des Sicherheitsniveaus *«substanziell»* verlangt mindestens eine 2-Faktor-Authentifizierung. Die Handhabung einer solchen E-ID ist somit zum Beispiel mit im Bankenbereich üblichen Lösungen vergleichbar (Kontokarten oder 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). Die beim Einsatz der E-ID zur Identifizierung eingesetzten Mittel (Authentifizierungsmittel) müssen zudem sehr hohe Anforderungen bezüglich technischer Sicherheit erfüllen. Das Authentifizierungsmittel ist der antragstellenden Person persönlich zu übergeben.

Der Einsatz der E-ID mit dem Sicherheitsniveau *«hoch»* verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss. Zusätzlich muss das Authentifizierungsmittel einen direkten Nachweis der Authentifizierung der Inhaberin oder des Inhabers liefern können, der vom E-ID verwendenden Dienst überprüft werden kann. Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung, integriert in einem abgesicherten Bereich mit persönlichen Zertifikat. 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 des Sicherheitsniveaus «*hoch*» deshalb über Komponenten verfügen, die besonders vertrauenswürdig sind und dem Stand der Technik entsprechen.

### 1.2.6 Funktion des Staates im Zusammenhang mit E-ID-Systemen

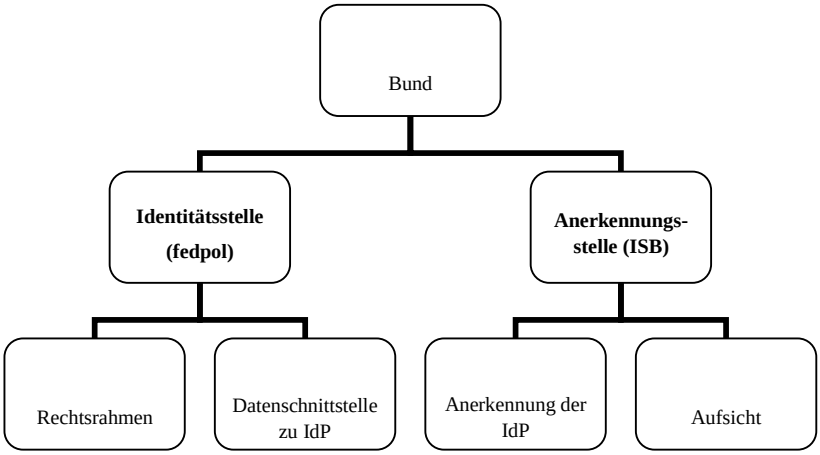
#### 1.2.6.1 Überblick

Eine nach diesem Gesetz ausgestellte E-ID bestätigt die Existenz und Identität einer natürlichen Person aufgrund der Personenidentifizierungsdaten, die in staatlich geführten und gepflegten Registern hinterlegt sind. Weil der Staat für die Erstellung von Ausweisen Personen regelmässig identifizieren muss und bei ihm die Meldungen von Änderungen in staatlichen Registern eingehen, geniesst er im Zusammenhang mit der Bestätigung der Identität einer Person besonderes Vertrauen.

Der Bund legt die Vertrauensbasis für E-ID-Systeme nach diesem Gesetz und übernimmt dazu mehrere Aufgaben im Bereich der E-ID:

1. Er erarbeitet und pflegt die Rechtsgrundlagen und bewirkt damit Transparenz und Sicherheit.
2. Er definiert Standards, Sicherheits- und Interoperabilitätsanforderungen für den Betrieb eines E-ID-Systems.
3. Er betreibt eine Anmeldeplattform für die anfängliche Feststellung der Identität der Antragstellerin oder des Antragstellers.
4. Er überprüft die Identität einer Person und ordnet ihr die E-ID-Registrierungsnummer zu.
5. Er betreibt eine elektronische Schnittstelle, über welche anerkannte IdP staatlich geführte Personenidentifizierungsdaten beziehen können.
6. Er anerkennt IdP und ihre E-ID-Systeme.
7. Er beaufsichtigt anerkannte IdP und ihre E-ID-Systeme.
8. Er kann unter gewissen Voraussetzungen einem IdP die Anerkennung entziehen.

Diese Aufgaben sollen beim Bund von zwei Verwaltungseinheiten wahrgenommen werden: vom fedpol (Identitätsstelle) und vom ISB (Anerkennungsstelle).

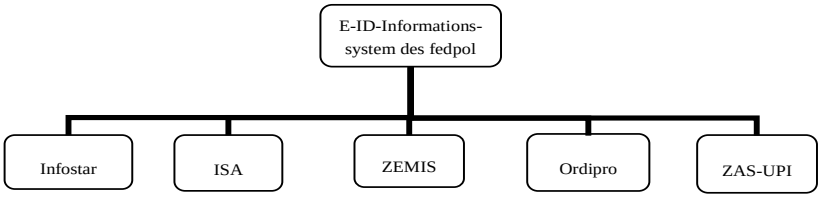



### 1.2.6.2 Register mit Personenidentifizierungsdaten

Die Schweizer Behörden der verschiedenen staatlichen Ebenen pflegen mehrere Register, die Personenidentifizierungsdaten enthalten. Als Beispiele seien hier die kantonalen und kommunalen Einwohnerregister, das elektronische Personenstandsregister (Infostar)* und das Zentralregister der zentralen Ausgleichsstelle der AHV (ZAS-UPI*[8]) erwähnt. UPI ist das zentrale Versichertenregister der AHV für die Personenidentifizierung 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 Identitätskarte und Schweizerpass. Ausländerausweise werden hingegen aufgrund der Daten des Zentralen Migrationsinformationssystems (ZEMIS)* ausgestellt, Legitimationskarte nach der Gaststaatgesetzgebung aufgrund der Daten von Ordipro*.

Die Daten aus den erwähnten Registern des Bundes werden im Informationssystem des fedpol nach Artikel 24 zusammengeführt:

8 UPI ist das Akronym für «Unique Person Identification»




### 1.2.6.3 Verhältnis der Versichertennummer AHVN13 zur E-ID-Registrierungsnummer

Die AHVN13 ist eine eindeutige Personenidentifikationsnummer, die allerdings gemäss heutiger Praxis nur in den Bereichen eingesetzt werden kann, für die 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 50*d* und 50*e* des Bundesgesetzes vom 20. Dezember 1946[9] über die Alters- und Hinterlassenenversicherung (AHVG) zulässig. In Artikel 50*a* AHVG wird geregelt, an welche Stellen in Abweichung von Artikel 33 des Bundesgesetzes vom 6. Oktober 2000[10] über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) Daten, insbesondere die AHVN13, bekannt gegeben werden dürfen. Gemäss Artikel 50*e* Absatz 1 AHVG ist eine systematische Verwendung der AHVN13 ausserhalb der Sozialversicherung des Bundes nur zulässig, wenn ein Bundesgesetz dies vorsieht und wenn der Verwendungszweck sowie die Nutzungsberechtigten bestimmt sind.

Im Verkehr der Bürgerinnen und Bürger mit Verwaltungsstellen wird die AHVN13 in zahlreichen Fällen benötigt. Könnte sie künftig im elektronischen Verkehr zwischen Bürgerinnen und Bürgern und Verwaltung nicht über fedpol (Identitätsstelle) bezogen und bestätigt werden, so müssten dafür kostspielige Umgehungslösungen bereitgestellt werden. Das würde den Komplexitätsgrad der Systeme markant erhöhen und die Akzeptanz der E-ID schmälern. Fedpol soll deshalb erlaubt werden, die AHVN13 – ausschliesslich – zur Identifizierung von Personen systematisch zu verwenden. Fedpol darf zur Identifizierung von Personen die AHVN13 durch ein Abrufverfahren nur den Betreiberinnen eines E-ID-verwendenden Dienstes zugänglich machen, die selbst zur systematischen Verwendung der AHVN13 berechtigt sind (Art. 8 Abs. 2 BGEID).

Die IdP und die übrigen Privaten sollen hingegen von der systematischen Verwendung der AHVN13 ausgeschlossen sein. Daher braucht es eine zusätzliche Identifizierungsnummer, die im Verkehr mit Privaten gebraucht werden kann und unabhängig von der AHVN13 ist: Die neu eingeführte E-ID-Registrierungsnummer. Sie dient insbesondere der Verbindung der Person mit der ausgegebenen E-ID. Da der

9 SR **831.10**
10 SR **830.1**

Bezug einer E-ID freiwillig ist und keine Pflicht besteht, dass alle Berechtigten eine E-ID beziehen müssen, wird keine umfassende Abdeckung mit der E-ID-Registrierungsnummer erreicht, d.h. sie ist nicht als allgemeiner Personenidentifikator geeignet.

#### 1.2.6.4 Bundesamt für Polizei (Identitätsstelle)

*Rechtsrahmen*

Fedpol pflegt in Zusammenarbeit mit dem ISB die rechtlichen, organisatorischen und technischen Vorgaben. Insbesondere definiert es 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-Systeme dem technischen Fortschritte, den sich wandelnden Nutzungsanforderungen und den aktuellen Sicherheitsbedürfnissen an.

*Anmeldeseite*

Fedpol stellt im Internet ein Anmeldeportal zur Verfügung, auf der die von den IdP weitergeleiteten Antragstellerinnen und Antragsteller ihre Identität nachweisen müssen und gleichzeitig ihr Einverständnis für die Übertragung der Personenidentifizierungsdaten an den IdP abgeben.

*Schnittstelle*

Fedpol stellt die beim Bund geführten Personenidentifizierungsdaten über eine elektronische Schnittstelle für die anerkannten IdP bereit (Art. 23 Abs. 1 BGEID). Durch die Etablierung einer E-ID-Registrierungsnummer können die Personenidentifizierungsdaten eindeutig, dauerhaft und widerspruchsfrei einer Person und ihrer E-ID zugeordnet werden. Diese Schnittstelle ist ausschliesslich den anerkannten IdP für die Erstidentifizierung und für die regelmässige Aktualisierung der Personenidentifizierungsdaten zugänglich.

Fedpol ist für den Betrieb der Schnittstelle zur Übermittlung der Personenidentifizierungsdaten verantwortlich. Es ist Ansprechstelle einerseits für die anerkannten IdP und andererseits für die Betreiberinnen der angeschlossenen staatlichen Register.

Fedpol bezieht die verschiedenen Personenidentifizierungsdaten aus unterschiedlichen Registern (Art. 24 Abs. 3 BGEID). Der Name einer Person wird über Infostar bestätigt, wohingegen beispielsweise die Ausweisnummer oder das Gesichtsbild aus ISA resp. ZEMIS stammen. Soweit dies für die Erfüllung seiner Aufgaben nach dem BGEID erforderlich ist, kann fedpol die Personenidentifizierungsdaten mit zusätzlichen Metadaten über ihre letzte Aktualisierung im Informationssystem nach Artikel 24 ergänzen (Art. 5 Abs. 4 BGEID).

Die IdP sind gehalten, die zu einer E-ID-Registrierungsnummer bezogenen Personenidentifizierungsdaten periodisch zu aktualisieren. Je nach Sicherheitsniveau müssen die IdP die Aktualisierungen mindestens jährlich (Sicherheitsniveau *«niedrig»*),

quartalsweise (Sicherheitsniveau «*substanziell*») oder wöchentlich (Sicherheitsniveau «*hoch*») vornehmen (Art. 7 BGEID).

#### 1.2.6.5 Informatiksteuerungsorgan des Bundes (Anerkennungsstelle)

*Anerkennung*

IdP, welche die gesetzlichen Voraussetzungen erfüllen, können sich für den Betrieb von E-ID-Systemen auf einem der vorgesehenen Sicherheitsniveaus vom ISB anerkennen lassen. Ein IdP kann auch mehrere E-ID-Systeme auf unterschiedlichem Sicherheitsniveau betreiben und sich für alle oder nur für einzelne anerkennen lassen. Dazu werden vom Bundesrat rechtliche, organisatorische und technische Auflagen für die IdP festgelegt, deren Erfüllung vom ISB überprüft wird. Durch die Erneuerung der Anerkennung in regelmässigen Abständen leistet der Bund einen massgebenden Beitrag an dauerhaft sichere E-ID-Lösungen.

Das ISB publiziert eine Liste mit den anerkannten IdP und deren 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. 25 Abs. 2 BGEID). Es führt ein Informationssystem für die Anerkennung von IdP sowie für die Aufsicht über sie (Art. 26 BGEID).

*Aufsicht*

Das ISB übt die Aufsicht über die anerkannten IdP und deren E-ID-Systeme aus und reagiert im Falle von Abweichungen von den Vorgaben oder Vorfällen im IKT-Sicherheitsbereich. Dazu fordert das ISB von den anerkannten IdP in den festgelegten zeitlichen Abständen die notwendigen Konformitätsnachweise ein und prüft sie. Das ISB kann einem IdP Aufsichtsmassnahmen auferlegen und unter bestimmten Voraussetzungen die Anerkennung entziehen (Art. 19 BGEID).

#### 1.2.6.6 Identitätsverbund Schweiz

Der Identitätsverbund Schweiz (IDV Schweiz) bietet eine technische Lösung, um Login-Prozesse im E-Government und in der elektronischen Zusammenarbeit unter Behörden zu vereinfachen. Der IDV Schweiz ist ein strategisches Projekt im Schwerpunktplan von E-Government Schweiz; projektverantwortliche Organisation ist das Staatssekretariat für Wirtschaft (SECO).

Die Einbeziehung des IDV in die E-ID-Systeme wurde in Betracht gezogen. Die Interoperabilität kann allerdings auch ohne IDV sichergestellt werden. Zwei unabhängige Studien der ETH Zürich[11] resp. von IBM Research Zürich[12] haben diese An-

11 Basin, D., Sasse, R., Interoperable, State-approved Electronic Identities, 26. Januar 2018, kann abgerufen werden auf der Website des BJ: www.bj.admin.ch > Staat & Bürger > Laufende Rechtssetzungsprojekte > E-ID-Gesetz.

nahme bestätigt. Der Bundesrat will das E-ID-System so einfach wie möglich gestalten und keine Rollen definieren, die nicht zwingend erforderlich sind. Die Funktion des IDV ist somit nicht Gegenstand des vorliegenden Gesetzes.

## 1.3 Begründung und Bewertung der vorgeschlagenen Lösung

### 1.3.1 Staatliche-private Lösung

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. Apple-ID, Google-ID). Damit kann die Inhaberin oder der Inhaber sich auch auf einfache Weise bei anderen Internet-Diensten registrieren lassen. Diese E-ID sind allerdings nicht staatlich anerkannt, erhalten vom Staat keine Personenidentifizierungsdaten und verfügen somit nicht über das besondere Vertrauen, das dieses Gesetz den auf seiner Basis ausgestellten E-ID zukommen lassen wird.

Viele Dienste im Internet sind auf eine eindeutige und vertrauenswürdige Identifizierung angewiesen, die durch standardisierte Prozesse sicherstellt, dass der Inhaber oder die Inhaberin einer E-ID verifiziert wurde. Dies gilt insbesondere für staatliche Internet-Dienste im E-Government-Bereich. Mehrere Staaten haben aus diesem Grund eigene E-ID herausgegeben, bei denen entweder alles in staatlicher Hand ist oder private Lösungen anerkannt werden. Die rein staatlichen Lösungen bieten nach den bisherigen Erfahrungen jedoch keine Garantie für die (technische) Akzeptanz bei den Bürgerinnen und Bürgern und sind für die öffentliche Hand mit einem hohen Investitions- und Betriebsaufwand verbunden. Rein staatliche Systeme können mit der Entwicklung der Technologien oft nur sehr schwer und mit kostspieligen Anpassungen mithalten und sind wegen der beschaffungsrechtlichen Vorgaben und allfälliger Anpassungen von rechtlichen Grundlagen regelmässig auf langwierige Verfahren angewiesen. Staatliche Lösungen erreichen deshalb 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.

Bei der hier vorgeschlagenen Lösung schafft der Bund verlässliche und Sicherheit gewährende Rahmenbedingungen, die er im Rahmen von Anerkennungs- und Aufsichtsverfahren durchsetzt. Er muss aber nicht konkrete technische Ausgestaltungen von E-ID entwickeln und in deren Realisierung investieren. Die technische Umsetzung und die Vermarktung der konkret ausgestalteten E-ID ist Sache privater Akteure.

Mittlerweile gibt es verschiedene vertrauenschaffende elektronische Identitäten auch von inländischen IdP auf dem Markt, deren Akzeptanz stetig wächst. Diese E-ID-

[12] Camenisch, J., Dubovitskaya, M., Evaluation Report, Proof of Concept Interoperabilität E-ID, IBM Research, Zürich, 31. Januar 2018, kann abgerufen werden auf der Website des BJ: www.bj.admin.ch > Staat & Bürger > Laufende Rechtssetzungsprojekte > E-ID-Gesetz.

Systeme können – sofern sie die Voraussetzungen erfüllen – durch die Anerkennung des betreffenden IdP gestärkt werden und auch im E-Government-Bereich zur Anwendung kommen. Darüber hinaus eröffnet das Gesetz auch weiteren Akteuren den Zugang zu diesem Markt, wenn sie das Anerkennungsverfahren erfolgreich durchlaufen.

Die Anforderungen an E-ID-Systeme nach diesem Gesetz 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

Es bestehen heute verschiedene Modelle dafür, wie der Bund Anerkennungsverfahren regelt. 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[13]. 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 hat sich bewährt. Deshalb wird das *Anerkennungsverfahren für IdP* demjenigen für Zustellplattformen nachgebildet: Das ISB (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 in einer Departementsverordnung die technischen Vorgaben erlassen und die einzuhaltenden Standards bezeichnet und aktualisiert werden. Sie werden auf die bestehenden Regelungen im Bereich der elektronischen Signaturen, eHealth und Zustellplattformen abgestimmt, sodass für anerkannte IdP Synergien bei den verlangten Zertifizierungen entstehen.

Mit der Anerkennung und der Erneuerung der Anerkennung in regelmässigen Abständen nimmt der Bund einen Teil seiner Aufsichtsfunktion wahr. Die Anpassung an die technische Entwicklung im Sicherheitsbereich kann so zeitnah erfolgen.

13 SR **272.11**

Datenschutzrechtliche Auflagen werden verfügt und deren Einhaltung wird regelmässig überprüft.

Das vorliegende Gesetz umfasst Massnahmen, damit der Fortbestand eines E-ID-Systems möglichst sichergestellt ist. Falls einem IdP die Anerkennung für die Ausstellung von E-ID des Sicherheitsniveaus substanziell oder hoch nicht erneuert wird oder er keine Erneuerung beantragt, kann das E-ID-System gemäss dem Gesetz von einem anderen IdP oder – wenn sich kein anderer IdP interessiert – vom Bund (ohne finanzielle Gegenleistung) übernommen werden. Die Inhaberinnen und Inhaber einer E-ID, die IdP sowie die E-ID-verwendenden Dienste müssen Vertrauen in die bestehenden E-ID-Systeme haben können. Durch die Übernahme eines E-ID-Systems durch einen anderen IdP oder den Bund können Dienstleistungen ohne Unterbruch gewährleistet werden.

### 1.3.3 Vernehmlassungsverfahren und Überarbeitung des Vorentwurfs

Zur Teilnahme eingeladen wurden die Kantone, die in der Bundesversammlung vertretenen politischen Parteien, die gesamtschweizerischen Dachverbände der Gemeinden, Städte und Berggebiete und der Wirtschaft sowie weitere interessierte Organisationen.

Von den 65 zur Stellungnahme eingeladenen Adressatinnen und Adressaten haben 48 geantwortet. Stellung genommen haben 26 Kantone, 8 politische Parteien und 54 Organisationen und weitere Teilnehmende. Insgesamt gingen damit 88 Stellungnahmen ein. Es sind 40 unaufgeforderte Stellungnahmen eingegangen. Sie stammen zum einen von Verbänden aus der Wirtschaft, insbesondere den Branchen ICT und Finanzdienstleistungen, und dem Bereich E-Government und E-Health, zum anderen von Privatpersonen.

Aufgrund der Rückmeldungen aus der Vernehmlassung wurde der Katalog der Personenidentifizierungsdaten erheblich gekürzt. Insbesondere die AHVN13 wird nicht mehr als Attribut der E-ID geführt. Die E-ID-Registrierungsnummer ist als zufällig generierte und somit nicht auf die AHVN13 rückführbare Nummer konzipiert. Der Abgleich zwischen der E-ID-Registrierungsnummer und der AHVN13 findet im Informationssystem des fedpol gemäss Artikel 24 statt.

Ein wiederkehrendes Thema in den Vernehmlassungsantworten ist die E-ID für juristische Personen. Offenbar besteht das Bedürfnis, juristische Personen im Internet sicher zu identifizieren. Da juristische Personen aber nicht selbst handlungsfähig sind, sondern durch ihre Organe agieren, z. B. durch die natürlichen Personen, die im Handelsregister als zeichnungsberechtigt eingetragen sind, braucht es keine E-ID für juristische Personen. Soll hingegen eine Website, ein Internet-Auftritt einer juristischen Person sicher zugeordnet werden, bestehen bereits heute andere Möglichkeiten der sicheren Authentifizierung, z. B. über Zertifikate gemäss ZertES. Schliesslich erhält heute jedes Unternehmen in der Schweiz eine eindeutige Unternehmens-Identifikationsnummer (UID). Deren Zweck besteht namentlich darin, den Verwaltungsaufwand bei der Identifizierung von Unternehmen zu reduzieren und

die Effizienz der Verwaltung diesbezüglich zu erhöhen. Mit der E-ID hingegen soll nicht nur die Identifizierung der berechtigten Personen erleichtert werden. Dank einer E-ID können deren Inhaberinnen und Inhaber im virtuellen Raum interagieren und eine breite Palette von Dienstleistungen in Anspruch nehmen.

Auf Anregung der Vernehmlassungsteilnehmer wurde ausserdem die Möglichkeit geprüft, Identitätsvermittler, sogenannte Identity-Broker, zu errichten. Zwei Studien der ETH Zürich und von IBM Research haben jedoch gezeigt, dass die Interoperabilität der E-ID-Systeme über Protokolle sichergestellt werden kann und dass dafür kein Broker erforderlich ist. Im vorliegenden Gesetz wird die Tätigkeit der Identitätsvermittler deshalb nicht geregelt. Die IdP können im Rahmen ihrer E-ID-Systeme jedoch auf die Dienstleistungen solcher Vermittler zurückgreifen. Allerdings müssen diese ebenfalls von der Anerkennungsstelle anerkannt werden.

## 1.4 Abstimmung von Aufgaben und Finanzen

### 1.4.1 Sichere Online-Identifizierung

Verschiedene Bundesstellen werden voraussichtlich von der E-ID 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 werden unter den Ziffern 1.4.3 und 3.1 aufgezeigt. Weiterer Aufwand wird sich auf Anpassungen bei Informatiklösungen und die Beschaffung der Dienstleistungen der IdP beschränken, wobei durch Vereinfachung der Prozesse Einsparungen realisierbar sind.

### 1.4.2 Neue Aufgaben

Das E-ID-Gesetz bringt neue Aufgaben für die Bundesverwaltung. Einerseits wird fedpol mit der Bereitstellung eines Informationssystems mit Schnittstelle zur Übermittlung von Personenidentifizierungsdaten beauftragt, andererseits braucht es das ISB, das die Anerkennungen vornimmt und die anerkannten IdP beaufsichtigt (vgl. Ziff. 1.2.6).

*Fedpol ist für die folgenden Aufgaben zuständig:*

a. Überprüfung der Identität der antragstellenden Personen,

b. Anwendungsverantwortung und Pflege der bei fedpol notwendigen IKT-Infrastruktur (Anmeldeseite für Antragstellerinnen und Antragsteller, Schnittstelle zu den IdP und Anbindung der bundesinternen Datenquellen wie ISA, Infostar usw.),

c. Fachsupport für die beteiligten bundesinternen Datenbanken, sowie

d. Fachsupport für die anerkannten IdP.

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.

*Das ISB hat folgende Aufgaben:*

a. die Anerkennung von IdP,

b. die Beaufsichtigung und Überwachung der anerkannten IdP,

c. die Pflege und Publikation der Liste der anerkannten IdP,

d. Erarbeitung und Pflege der organisatorischen und technischen Vorgaben für die Anerkennung von IdP, und

e. Informationsbeschaffung über aktuelle technologische Entwicklungen im Bereich E-ID und zugehörige Fragen der IKT-Sicherheit.

Das ISB nimmt neben den Anerkennungs- auch Aufsichtsfunktionen wahr, die denjenigen der Aufsichtsstelle gemäss eIDAS gleichkommen. Weitere entsprechende Aufsichtsfunktionen werden beim Bund bereits durch das ISB wahrgenommen.

Vorbehalten bleiben die Zuständigkeiten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemäss Bundesgesetz vom 19. Juni 1992[14] über den Datenschutz (DSG).

### 1.4.3 Finanzierung

#### 1.4.3.1 Vorleistungen des Bundes

Die Finanzierung des Projektaufwands bis 6 920 000 Franken ist durch beim EJPD vorhandene Mittel bereits sichergestellt (einschliesslich Anteile zentrale IKT-Mittel und Beteiligung eGovernment Schweiz).

Aufgrund der Ergebnisse zur Vernehmlassung des E-ID-Gesetzes muss ein zusätzlicher Dienst zur Abfrage der AHVN13 aufgebaut und implementiert werden. Die dazu notwendigen Mittel von 750 000 Franken fallen zusätzlich an und müssen ergänzend beantragt werden. Ebenfalls muss der E-ID-Demonstrator weiterentwickelt und gepflegt werden. Dies wird zusätzliche Kosten von 230 000 Franken auslösen und führt 2018–2020 zu einem Zusatzaufwand von insgesamt 980 000

14 SR **235.1**

Franken, welcher ebenfalls ergänzend beantragt werden muss. Da 100 000 Franken aus Mitteln von eGovernment Schweiz stammen, müssen insgesamt 880 000 Franken aus den zentralen IKT-Mitteln beantragt werden.

Die Ausgaben gegenüber Dritten werden über den Verpflichtungskredit V0224.00 «Erneuerung Schweizerpass und Identitätskarte» von 19,6 Millionen bei fedpol abgerechnet.

#### 1.4.3.2 Gebührenfinanzierung

Für die Leistungen des Bundes gegenüber dem IdP wurden verschiedene Finanzierungsmodelle geprüft. Verworfen wurde ein «prepaid»-Modell, bei dem die IdP dem Bund eine möglichst kostendeckende Gebühr überweisen, ohne sicher zu sein, dass sie durch die schnelle Verbreitung der E-ID entsprechende Einnahmen generieren. Verworfen wurde auch die kostenlose Überprüfung der bestätigten Daten über die Erstbestätigung hinaus, da dadurch auf Bundesseite erhebliche Defizite entstünden. 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 und die Nutzung der E-ID für die antragstellende Person auch unentgeltlich sind. Für jede weitere Übermittlung von Personenidentifizierungsdaten wird hingegen eine moderate Gebühr erhoben. Diese wird auf Verordnungsebene festgesetzt und wird sich im Rahmen eines zweistelligen Rappenbetrages bewegen. Je nach Verbreitung von E-ID nach diesem Gesetz, insbesondere der Sicherheitsniveaus *«substanziell»* und *«hoch»*, werden damit neue Einnahmen für einen ausreichenden Kostendeckungsgrad erreicht.

#### 1.4.3.3 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, Medienbrüche, rascherer Durchlauf, innovative Geschäftsmodelle, keine eigene E-ID-Lösung). 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.

### 1.4.4 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 erbracht.

Für die Leistungen des IdP ist also ein Beschaffungsverfahren gemäss den anwendbaren Regeln des öffentlichen Beschaffungswesens (Bundesgesetz vom 16. Dezember 1994[15] über das öffentliche Beschaffungswesen (BöB) oder kantonales Recht) durchzuführen, es sei denn, der Bundesrat bezeichnet eine Verwaltungseinheit, die ein E-ID-System für die Bedürfnisse der Behörden betreibt (Art. 10 BGEID).

*Anerkennung der Anbieter von Identitätsdienstleistungen*

Die Anerkennung von IdP hingegen ist kein Beschaffungsvorgang, sondern ein wirtschaftspolizeilicher Akt. Diese wirtschaftspolizeiliche Regelung stützt sich auf Artikel 95 Absatz 1 der Bundesverfassung[16] (vgl. Ziff. 5.1).

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. 13 Abs. 2 BGEID) erfüllt werden und die technischen und organisatorischen Vorgaben eingehalten sind.

## 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 län-

15 SR **172.056.1**
16 SR **101**

derspezifischen Systemen gewahrt wird. Das Konzept für die E-ID-Systeme nach diesem Gesetz richtet sich nach diesen internationalen Regelungen, sodass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten.

Der hier vorgeschlagene Rahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der IdP ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der E-ID-Systeme zwischen der Schweiz und der EU (nach der eIDAS Verordnung) oder einzelner EU-Mitglied- oder Drittstaaten möglich bleibt. Zur Umsetzung wären Staatsverträge notwendig.

### 1.5.2 Entwicklungen in den letzten fünfzehn Jahren

In einer ersten Phase gingen die meisten Staaten davon aus, dass eine EI-D auf existierenden Identitätskarten-Konzepten aufbauen würden. Die Fragen, die sich stellten, waren in erster Linie technischer Natur und befassten sich mit Problemen der technischen Modalitäten. In der Folge führten viele europäische Staaten in den letzten fünfzehn Jahren eine mit der Identitätskarte verbundene E-ID als Kernstück eines nationalen E-ID-Systems ein. Pionier war Finnland, welches im Jahr 1999 eine Identitätskarte mit E-ID herausgab. Es folgten Estland, Belgien, Spanien und Portugal. Deutschland führte im Jahr 2010 einen elektronischen Personalausweis (ePA) ein. Zudem gaben in den letzten Jahren auch Länder im Nahen Osten und in Asien neue staatliche Identitätskarten mit E-ID-Funktion heraus. Die Lancierung von E-ID-Projekten war oft durch die Absicht getrieben, im internationalen Vergleich auf keinen Fall in Rückstand zu geraten. 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.

Erste E-ID-Lösungen bauten etwa auf Smart-Cards mit kontaktbasierten Chips, die im Wesentlichen auf der Technologie der Signaturkarten aufbauten. Beispiele dieser Art waren die finnische, die estnische und die belgische E-ID-Karte sowie übrigens im Kern auch die SuisseID.

Eine weitere verbreitete Lösungsvariante 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-Identifizierung. Schweden, Monaco, Lettland, Finnland (2. Auflage) und die Niederlande haben solche Identitätskarten. Der ECC-Standard ist allerdings nie ganz stabilisiert worden. 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.

Ein wichtiger Repräsentant der beschriebenen Entwicklungsrichtung ist der 2010 von Deutschland eingeführte elektronische Personalausweis (ePA). Er enthält im Wesentlichen die vorstehend erwähnten Komponenten, wurde aber an einigen Punk-

ten 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.

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, aber nur bei rund drei Prozent der Karten ist die E-ID-Funktion aktiviert und wird auch genutzt. Demnach 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. Bürgerinnen und Bürger müssen Infrastrukturkomponenten wie Lesegeräte und Software beschaffen und einsetzen. Zudem muss der Staat konstant Änderungen und Updates bei diesen Komponenten entwickeln und verteilen, was den Betrieb stark verteuert.

Am 22. August 2017 hat die Bundesrepublik Deutschland die Online-Ausweisfunktion des Personalausweises und Aufenthaltstitels auf dem höchstmöglichen Vertrauensniveau gemäss eIDAS-Verordnung an die EU-Kommission notifiziert. Die Notifizierung wurde am 26. September 2017 im Amtsblatt der EU-Kommission veröffentlicht. Neben Deutschland befinden sich fünf weitere Länder in der Phase der Vorbereitung auf die Notifizierung ihrer nationalen E-ID-Dienste: Spanien, Italien (Voranmeldung vorhanden), Frankreich, Dänemark und Grossbritannien.

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 lang ist, und eine staatliche Lösung den sich ausdifferenzierenden Nutzungsbedürfnissen oft nicht hinreichend Rechnung trägt.

Angeführt vom US-amerikanischen Projekt der gemeinsamen Entwicklung eines «Identity Ecosystems»[17] begann man sich in vielen Ländern grundsätzlicher zu

17 National Strategy for Trusted Identities in Cyberspace (NSTIC): Identity Ecosystem

überlegen, wie eine gute Architektur für das gesamte nationale und internationale Ökosystem 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-Ökosystems; 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 Betreiber 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 Anbieterinnen von E-ID für alle Branchen, 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.

Die EU hat in der 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

Setzen staatliche Systeme auf eine feste Verbindung der E-ID mit einem konventionellen Ausweis, beispielsweise mittels Chip auf der IDK, können sie mit der Entwicklung der Technologien nur sehr schwer mithalten und müssen permanent kostspielige Anpassungen in Kauf nehmen. Ausgehend von den Erfahrungen in den Nachbarländern drängt sich deshalb für die Schweiz eine andere Lösung auf.

Die vorgeschlagene Lösung kombiniert die vertrauensbildende Wirkung staatlicher Anerkennung und Aufsicht mit dem technologischen Knowhow und der Dynamik privatwirtschaftlicher Initiative. Sie entlastet den Bund von schwierigen Entscheidungen unter Bedingungen komplexer technologischer Innovationsprozesse und von hohen Entwicklungs- und Implementierungskosten. Gleichzeitig bietet sie Raum für flexible und den Bedürfnissen angepasste innovative Lösungen. Die Rolle des Bundes beschränkt sich dabei auf die Definition notwendiger Rahmenbedingungen und Vorgaben, die im Rahmen der Anerkennung und Aufsicht durchgesetzt werden.

Ein Vergleich des im Gesetzesentwurf umgesetzten Regelungskonzepts mit den Entwicklungen, Erfahrungen und aktuellen Überlegungen im internationalen Umfeld ergibt folgendes Bild:

- Die Schweiz berücksichtigt die Erfahrungen der letzten fünfzehn Jahre und geht mit ihrem Konzept der Anerkennung der IdP einen Weg, der von verschiedenen Stellen als wegweisend beurteilt wird.
- Das schweizerische Konzept gewährleistet ein sicheres E-ID-System durch präzise Vorgaben, ein Anerkennungsverfahren und staatliche Aufsicht.

– 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 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 Verpflichtung zur Übernahme der EU-Verordnung. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern wird aber davon ausgegangen, dass die Schweiz ein Interesse daran hat, früher oder später in das europäische System für die Interoperabilität von elektronischen Identitäten eingebunden zu sein. 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 Gesetzentwurf wird u. a. ein Rechts- und Standardisierungsrahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der IdP geschaffen. Dieser ermöglicht zudem eine spätere gegenseitige Anerkennung des schweizerischen E-ID-Systems einerseits und andererseits der nach eIDAS-Verordnung notifizierten E-ID-Systeme oder auch der E-ID-Systeme von einzelnen EU-Mitglied- oder Drittstaaten.

## 1.6 Umsetzung

Das vorliegende Gesetz regelt allgemein die Grundsätze und Anforderungen für die Ausstellung von E-ID durch anerkannte IdP und die Verwendung dieser E-ID. Damit die beantragten Bestimmungen umgesetzt werden können, müssen sie per Verordnung des Bundesrates und per Departementsverordnung präzisiert werden. In den Verordnungen sollen namentlich folgende Punkte geregelt werden:

- die Verfahren für die Überprüfung der Ausweise von Schweizerinnen und Schweizern und für die Überprüfung der Ausweise sowie der Identität von Ausländerinnen und Ausländern;
- die verschiedenen Sicherheitsniveaus, insbesondere die Mindestanforderungen an die Identifizierung, unter Berücksichtigung des jeweiligen Stands der Technik;
- die näheren Vorschriften zum Ausstellungsprozess;
- die näheren Vorschriften zur Sperrung und zum Widerruf einer E-ID;
- die Sorgfaltspflichten der Inhaberinnen und Inhaber einer E-ID;
- die Voraussetzungen für die Anerkennung;
- die näheren Vorschriften zu den verschiedenen im Gesetz vorgesehenen Meldungen;
- die technischen Standards für die Sicherstellung der Interoperabilität und die Schnittstellen;
- das Verfahren zum Entzug der Anerkennung;
- die für die Übermittlung der Daten anwendbaren Standards und technischen Protokolle und wie vorzugehen ist, falls verschiedene Personenregister widersprüchliche Daten übermitteln;
- die technischen und organisatorischen Massnahmen zur sicheren Bearbeitung und Weitergabe der Personenidentifizierungsdaten;
- die näheren Vorschriften zu den Ausstellungsverfahren gemäss den Übergangsbestimmungen.

Ebenfalls in einer Verordnung regeln wird der Bundesrat die Erhebung der Gebühren nach Artikel 46*a* des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[18] (RVOG).

Schliesslich lehnt sich das vorliegende Gesetz an die technischen und organisatorischen Massnahmen an, die im Bereich der elektronischen Signatur und des elektronischen Patientiendossiers gelten. In den Ausführungsbestimmungen zum vorliegenden Gesetz, sei dies in den Verordnungen oder den Weisungen, wird diesen Standards Rechnung getragen werden.

18 SR **172.010**

## 1.7 Erledigung parlamentarischer Vorstösse

Die E-ID war bisher Gegenstand eines überwiesenen parlamentarischen Vorstosses:

– Motion FDP-Liberale Fraktion 17.3083 «Digitalisierung. Eine elektronische Identität für den landesweiten Bürokratieabbau». Die Motion wurde vom Bundesrat zur Annahme empfohlen. Die Motion verlangt eine Priorisierung des Vorhabens unter Berücksichtigung der Interoperabilität und der Sicherstellung von Sicherheitsstandards und deren Kontrolle. Mit der Vorlage dieser Botschaft werden die Anliegen der Motion erfüllt. Die Motion wurde im Nationalrat am 20.9.2017 und im Ständerat am 28.2.2018 angenommen.

Der Bundesrat beantragt, diesen Vorstoss mit dieser Botschaft abzuschreiben.

# 2 Erläuterungen zu einzelnen Artikeln

## 2.1 Struktur

Der erste Abschnitt des Gesetzesentwurfs enthält die allgemeinen Bestimmungen sowie Begriffe. Im zweiten Abschnitt wird die Ausstellung der E-ID geregelt, so die persönlichen Voraussetzungen für Bezügerinnen und Bezüger, die Sicherheitsniveaus, der Ausstellungsprozess, die Personenidentifizierungsdaten, die Aktualisierung der Personenidentifizierungsdaten, die systematische Verwendung der Versichertennummer zum Datenaustausch, Datenbearbeitung und -haltung, das subsidiäre E-ID-System des Bundes sowie Sperrung und Widerruf. Der dritte Abschnitt führt die Pflichten der Inhaberinnen und Inhaber einer E-ID auf. Im vierten Abschnitt werden die Anforderungen an Anbieterinnen von Identitätsleistungen (IdP) geregelt: die Pflichten der Anbieterinnen von Identitätsleistungen (IdP), die Anerkennungsverfahren, die Datenweitergabe, der Zugang zu einer E-ID, die Interoperabilität sowie die Aufsichtsmassnahmen und der Entzug der Anerkennung. Die Anforderungen an Betreiberinnen von E-ID-verwendenden Diensten werden im fünften Abschnitt bestimmt. In den Abschnitten sechs und sieben werden die Organisation und die Aufgaben von fedpol (Identitätsstelle) und dem ISB (Anerkennungsstelle) festgelegt. Die Kompetenz zur Regelung der Gebühren wird im achten Abschnitt geregelt, und der neunte Abschnitt enthält die Haftungsregeln. Im zehnten Abschnitt befinden sich die Schluss- und Übergangsbestimmungen. In einem Anhang wird die Änderung anderer Erlasse geregelt.

## 2.2 Ingress

Die Kompetenz zur Regelung von elektronischen Identifizierungseinheiten (E-ID) ergibt sich aus der Bundesverfassung (BV)[19]. Erwähnt werden insbesondere Artikel 95 Absatz 1 BV, der den Bund ermächtigt, wirtschaftspolizeiliche Vorschriften

19 SR **101**

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.

Artikel 96 Absatz 1 BV verleiht dem Bund die Kompetenz, Vorschriften gegen volkswirtschaftlich oder sozial schädliche Auswirkungen von Kartellen und anderen Wettbewerbsbeschränkungen zu erlassen. Mit dem vorliegenden Gesetz werden Massnahmen gegen schädliche Auswirkungen der Wirtschaftstätigkeit marktmächtiger IdP sowie gegen entsprechende Missbräuche verankert.

Im Weiteren stützt sich das Gesetz auf Artikel 97 Absatz 1 BV. Dieser weist dem Bund die Kompetenz zu, den Schutz der Konsumentinnen und Konsumenten zu regeln. Durch den Entwurf wird ein System zur Anerkennung und Beaufsichtigung der IdP geschaffen, das auch Konsumentinnen und Konsumenten schützen soll.

Soweit die Vertragsverhältnisse zwischen den Identitätsdienstleistern, Inhaberinnen und Inhabern sowie Betreiberinnen von E-ID-verwendenden Diensten betroffen sind, werden im vorliegenden Bundesgesetz zivilrechtliche Aspekte geregelt. Da diesem Aspekt keine zentrale Bedeutung zukommt, wird auf die Aufführung von Artikel 122 Absatz 1 BV, der dem Bund die Kompetenz zur Regelung des Zivilrechts gibt, verzichtet.

## 2.3 Allgemeine Bestimmungen

*Art. 1* Gegenstand und Zweck

*Abs. 1*

Das Gesetz regelt neben der staatlichen Identifizierung der Inhaberinnen und Inhaber einer E-ID, der Anerkennung und Aufsicht 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. Weiter werden Inhalt, Ausstellung, Verwendung, Sperrung und Widerruf der E-ID geregelt.

*Abs. 2*

Das BGEID trägt dazu bei, Sicherheit und Vertrauen im elektronischen Geschäftsverkehr (E-Business und E-Government) aufzubauen. Zudem soll der Datenschutz gewährleistet werden: Buchstabe b übernimmt deshalb den Zweckartikel des DSG.

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 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 erfüllt damit eine wichtige Funktion im Rahmen der Digitalisierung von Wirtschaft, Staat und Gesellschaft in der Schweiz.

*Art. 2* Begriffe

*Bst. a*

Ein 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 13 Absatz 2 BGEID 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 resp. deren Erlöschen oder Entzug finden sich in den Artikeln 14 und 19 BGEID.

*Bst. b*

Ein E-ID-verwendender Dienst ist eine von der Betreiberin angebotene Informatikanwendung, der es den Inhaberinnen und Inhaber einer E-ID ermöglicht, diese Dienstleistung nach Identifizierung über ein E-ID-System zu nutzen. Dazu gehören beispielsweise Online-Anbieterinnen, bei denen über das Internet Güter oder Dienstleistungen bezogen werden können und die bei der Geschäftsabwicklung ein E-ID-System einsetzen.

## 2.4 Ausstellung, Arten und Inhalt sowie Sperrung und Widerruf von E-ID

*Art. 3* Persönliche Voraussetzungen

*Vorbemerkung*

Ein IdP kann grundsätzlich nicht verpflichtet werden, eine E-ID auszustellen, nur weil jemand die Voraussetzungen dazu erfüllt. Durch die Kann-Formulierung in Absatz 1 wird dies sichergestellt. Von diesem Grundsatz wird in Artikel 17 dann abgewichen, wenn der Markt nicht funktioniert, da IdP eine marktbeherrschende Stellung missbrauchen.

Durch den Bezug einer E-ID werden die antragstellenden Personen zu Inhaberinnen und Inhabern einer E-ID.

*Minderjährige*

Für Minderjährige und für Personen, deren Handlungsfähigkeit teilweise oder vollständig entzogen worden ist, können E-ID ausgestellt werden. Allerdings hat die vertretungsberechtigte Person diese im Namen der vertretenen Person zu beantragen: Die vertretene Person wird Inhaberin oder Inhaber der E-ID. Die Anwendung hat dann aber unter Aufsicht der vertretungsberechtigten Person zu erfolgen. Für die

vertretene Person muss ein entsprechender Ausweis ausgestellt sein. Die entsprechende Regelung wird auf Verordnungsstufe erfolgen.

*Abs. 1*

*Ausweis als Identitätsnachweis*

Für die Beantragung einer E-ID genügt ein gültiger Schweizer Ausweis (Bst. a), ein gültiges, nach Artikel 13 Absatz 1 des Ausländergesetzes vom 16. Dezember 2005[20] (AuG) anerkanntes Ausweispapier oder eine gültige Legitimationskarte nach der Gaststaatgesetzgebung (Bst. b Ziff. 1). Zudem können auch Ausländerinnen und Ausländer, die nicht im Besitz eines Ausweispapiers sind, aber deren Identität zum Zeitpunkt der Ausstellung in einem besonderen Identifizierungsverfahren verlässlich festgestellt werden konnte, eine E-ID beantragen (Bst. b Ziff. 2).

*Anforderungen an Ausländerinnen und Ausländer*

Damit auch Ausländerinnen und Ausländer mit einer E-ID Zugang zu E-ID-verwendenden Diensten – auch zu E-Government-Anwendungen – erhalten können, ist vorgesehen, dass alle Ausländerinnen und Ausländer, die über einen Ausländerausweis verfügen, der eine Aufenthaltsbewilligung enthält (Art. 41 Abs. 1 AuG i.V.m. Art. 71 Abs. 1 der Verordnung vom 24. Oktober 2007[21] über Zulassung, Aufenthalt und Erwerbstätigkeit [VZAE]; Ausweis L, B, C), Ausländerinnen und Ausländer, die über eine Legitimationskarte verfügen (Art. 17 Abs. 1 der Gaststaatverordnung vom 7. Dezember 2007[22] i.V.m. Art. 71a Abs. 1 VZAE), sowie die Grenzgängerinnen und Grenzgänger (Art. 71*a* VZAE, Ausweis G) sich eine E-ID ausstellen lassen können.

Die E-ID und die mögliche Nutzung von E-Government-Anwendungen sollen damit Ausländerinnen und Ausländern offenstehen, deren Identität bei der Ausstellung einen gültigen Ausländerausweis gemäss Artikel 41 AuG verlässlich festgestellt werden konnte. Da Ausländerinnen und Ausländer gemäss Artikel 89 AuG während ihres Aufenthaltes in der Schweiz im Besitz eines gültigen, nach Artikel 13 Absatz 1 AuG anerkannten Ausweispapiers sein müssen, ist dies der Fall bei Ausländerausweisen C, B, L und G. Die entsprechende Regelung wird auf Verordnungsstufe erfolgen (vgl. Absatz 2).

Die Kategorien N, F, S und Ci von Ausländerausweisen berechtigen nicht ausnahmslos zum Bezug einer E-ID, weil nicht davon ausgegangen werden kann, dass die Identität der betroffenen Personen verlässlich festgestellt werden konnte.

Für die übrigen Ausländerinnen und Ausländer, insbesondere die mit N-, F- und S-Ausweisen wird derzeit darauf verzichtet, 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 Gesuche um Änderung oder Berichtigung von Personendaten eingereicht, wobei diese Gesuche nicht

20 SR **143.1**
21 SR **142.201**
22 SR **192.121**

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.

*Abs. 2*

Um flexibel auf neueste Technologien reagieren zu können, werden die Verfahren für die Überprüfung der Ausweise von Schweizerinnen und Schweizer und für die Überprüfung der Ausweise sowie der Identität von Ausländerinnen und Ausländer auf Verordnungsebene geregelt. Die Identifizierungsprozesse können allenfalls den zulässigen Identifizierungsmethoden im Bankenbereich nachgebildet werden. Die Geldwäschereigesetzgebung schreibt zum Beispiel genau vor, welche Methoden für die Identifizierung von Neukundinnen und Neukunden zulässig sind. In diesem Zusammenhang wird eine E-ID als Identitätsnachweis gelten.

Eine Übersicht über die Delegation von Rechtsetzungsbefugnissen findet sich unter Ziffer 5.7.

*Art. 4* Sicherheitsniveaus

*Abs. 1*

Nicht alle Geschäftsprozesse erfordern dasselbe Sicherheitsniveau. Oft führt eine höhere Sicherheit zu mehr Aufwand beim Bezug, zu einer reduzierten Benutzerfreundlichkeit und zu höheren Kosten. Aus diesem Grund sollen IdP E-ID-Systeme 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. 20 BGEID).

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 (Abwärtskompatibilität).

Je nach Sicherheitsniveau des Systems wird durch die E-ID ein unterschiedliches Mass an Vertrauen vermittelt. Das Sicherheitsniveau «*niedrig*» bezweckt eine Minderung der Gefahr des Identitätsmissbrauchs und Identitätsveränderung. Beim Niveau «*substanziell*» wird ein hoher Schutz gegen Identitätsmissbrauchs und Identitätsveränderung bezweckt. Das Niveau «*hoch*» bietet den höchstmöglichen Schutz gegen Identitätsmissbrauch und Identitätsveränderung.

*Abs. 2*

Die verschiedenen Sicherheitsniveaus unterscheiden sich durch die übermittelten Personenidentifizierungsdaten, den Prozess, wie die E-ID ausgestellt wird, und die Regeln für deren Anwendung sowie den Betrieb des E-ID-Systems (insbesondere die Aktualisierung der Personenidentifizierungsdaten). Die Anforderungen sind auf

Gesetzesstufe möglichst technologieneutral umschrieben und werden auf Verordnungs- oder Weisungsstufe im Detail und für verschiedene E-ID-Trägerformen genauer bestimmt.

*Abs. 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.

*Abs. 4*

Der Bundesrat regelt die verschiedenen Sicherheitsniveaus, insbesondere die Mindestanforderungen an die Identifizierung. Er berücksichtigt dabei den jeweiligen Stand der Technik.

*Art. 5* Personenidentifizierungsdaten

*Abs. 1, 2 und 3*

Welche und wie viele Personenidentifizierungsdaten einer E-ID zugeordnet werden, hängt von deren Sicherheitsniveau ab. Während für eine E-ID des Niveaus niedrig nur grundlegende Identifizierungsdaten verlangt werden (E-ID-Registrierungsnummer, amtlicher Name, Vornamen und Geburtsdatum), werden für eine E-ID des Sicherheitsniveaus substanziell oder hoch zusätzliche Daten (Geschlecht, Geburtsort und Staatsangehörigkeit) gefordert. Für das Sicherheitsniveau hoch ist überdies ein Gesichtsbild notwendig.

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

*Abs. 4*

Soweit dies für die Erfüllung seiner Aufgaben nach dem BGEID erforderlich ist, können die Personenidentifizierungsdaten durch fedpol mit Informationen über die letzte Aktualisierung der Daten im Informationssystem nach Artikel 24 versehen werden.

Private IdP, die zusätzliche Dienstleistungen anbieten, dürfen auch Daten bearbeiten, die im vorliegenden Gesetz nicht vorgesehen sind, wie beispielsweise die Lieferadresse oder Bezahlinformationen. Sie müssen dafür jedoch die Zustimmung der Inhaberin oder des Inhabers der E-ID einholen. Ein öffentlicher IdP (im Sinne von Art. 10) darf solche Daten nur dann bearbeiten, wenn dafür eine gesetzliche Grundlage besteht.

*Art. 6* Ausstellungsprozess

*Vorbemerkung*

Der Ausstellungsprozess wird zwischen der antragstellenden Person und dem fedpol initiiert. Je nach Sicherheitsniveau ist eine persönliche Vorsprache beim IdP oder eine gleichwertige Identifizierung Voraussetzung für die Ausstellung. Der Bundesrat regelt den Ausstellungsprozess je Sicherheitsniveau; die entsprechenden Delegationen finden sich in verschiedenen Bestimmungen der Vorlage (vgl. insbesondere Art. 3 Abs. 2, Art. 4 Abs. 4 und Art. 6 Abs. 5).

*Abs. 1*

Es besteht keine Pflicht, eine E-ID zu beziehen. Wenn eine Person eine E-ID erhalten will, muss sie über einen IdP fedpol kontaktieren. Der Antrag muss von der späteren Inhaberin oder dem späteren Inhaber der E-ID ausgehen (antragstellende Person). Der IdP darf nicht von sich aus eine E-ID ausstellen, selbst wenn ihm die Person bereits durch bestehende Kundenbeziehungen bekannt ist.

Obwohl sich die antragstellende Person zur Beantragung einer E-ID an einen IdP wenden muss, wird sie sich direkt bei fedpol identifizieren müssen. Es ist vorgesehen, dass sie zum Beispiel während des Identifizierungsprozesses von der Website des IdP auf die Website von fedpol weitergeleitet wird, um dort die nötigen Angaben zu machen. So kann die antragstellende Person ihren Identifizierungsantrag direkt über das Informationssystem von fedpol einreichen.

*Abs. 2*

Fedpol überprüft, ob die antragstellende Person die persönlichen Voraussetzungen nach Artikel 3 erfüllt. Wenn dies der Fall ist, identifiziert fedpol sie mithilfe der Informationen, die für das betreffende Sicherheitsniveau erforderlich sind. Diese stammen aus den Registern des Bundes nach Artikel 22 Absatz 3. In der Folge teilt fedpol dem IdP mit, ob das Ergebnis des Identifizierungsprozesses erfolgreich war oder nicht. Wenn die Person entsprechend dem beantragten Sicherheitsniveau identifiziert wurde und in die Übermittlung der Daten eingewilligt hat, übermittelt fedpol die Personenidentifizierungsdaten nach Artikel 5 dem IdP.

*Abs. 3*

Fedpol protokolliert die Datenübermittlungen im Zusammenhang mit dem Ausstellungsprozess. Die Protokolle bieten Gewähr dafür, dass die Vorgänge rückverfolgt werden und bei Streitigkeiten zwischen den betroffenen Parteien als Nachweis dienen können. Fedpol ist ausserdem aufgrund der Auskunftspflicht gegenüber den Inhaberinnen und Inhabern der E-ID zur Protokollierung verpflichtet.

*Abs. 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 antragstellenden Person verwendet und in deren Gerät eingesetzt wird. Je nach Sicherheitsniveau werden unterschiedli-

che 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.

*Abs. 5*

Der Bundesrat wird in einer Verordnung detailliertere Vorschriften zum Ausstellungsprozess erlassen. Er wird insbesondere den genauen Ablauf regeln sowie im Detail bestimmen, welche zusätzlichen Personendaten, die nur der antragstellenden Person bekannt sind, für deren verlässliche Identifizierung verwendet werden dürfen.

*Art. 7* Aktualisierung der Personenidentifizierungsdaten

Einige der Identitätsattribute sind veränderbar. Dies gilt insbesondere für den Namen. Dieser Tatsache wird durch die Pflicht zur regelmässigen Aktualisierung Rechnung getragen.

Das Vertrauen in die E-ID wird durch regelmässige Aktualisierung der Personenidentifizierungsdaten bei den staatlichen Informationssystemen erhöht. Es wird vorgeschrieben, in welchen maximalen Abständen für jedes Sicherheitsniveau dieser Abgleich zu erfolgen hat. Zuständig für die Aktualisierungsabfrage ist der IdP; dazu nimmt er bei fedpol eine automatisierte Abfrage anhand der E-ID-Registrierungsnummer vor. Für die regelmässigen Aktualisierungen werden Gebühren erhoben.

*Art. 8* Systematische Verwendung der Versichertennummer zum Datenaustausch

*Vorbemerkung*

Die AHVN13 gemäss AHVG soll nicht breitflächig und unkontrolliert bekannt gegeben werden können, da dies – im Ergebnis – auch den Kreisen eine systematische Nutzung ermöglichen würde, die dazu nicht befugt sind. Artikel 8 der Vorlage enthält die gesetzliche Grundlage und Bearbeitungsgrundsätze im Zusammenhang mit der systematischen Nutzung der AHVN13 für die E-ID durch fedpol. Die Regelung sieht im Einzelnen wie folgt aus:

*Abs. 1*

Fedpol ist berechtigt, beim elektronischen Datenaustausch mit den Personenregistern nach Artikel 24 Absatz 3 die AHVN13 für die Identifizierung der Personen systematisch zu verwenden. Die AHVN13 dient als eindeutiger Identifikator bei der Abfrage von anderen Datenbanken, die die Versichertennummer ebenfalls systematisch verwenden. Die Versichertennummer ist unerlässlich, um Daten unter 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. Durch Veränderung des Namens kann die ursprüngliche Identität verändert und auf legale Weise eine neue aufgebaut werden, da mit der Namensänderung auch die amtlichen Aus-

weisschriften neu ausgestellt werden, die keine Rückschlüsse auf die alte Identität zulassen. Die Versichertennummer ermöglicht jedoch eine eindeutige Zuordnung.

*Abs. 2*

Fedpol darf zur Identifizierung von Personen die AHVN13 durch ein Abrufverfahren nur den Betreiberinnen von E-ID-verwendenden Diensten zugänglich machen, die selbst AHVN13-nutzungsberechtigt sind. Die AHVN13 soll im Rahmen der Verwendung der E-ID nur den 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 technisch unterbunden werden.

Da die Sozialversicherungsnummer (AHVN13) nicht direkt als E-ID-Registrierungsnummer verwendet werden soll, muss ein zusätzlicher Dienst geschaffen werden. Organisationen, welche zur systematischen Nutzung der AHVN13 berechtigt sind, sollen über diesen Dienst die zu einer E-ID-Registrierungsnummer gehörige AHVN13 abfragen können.

*Art. 9* Datenbearbeitung und -haltung

*Vorbemerkung*

Datenbearbeitung, Datenhaltung und Datenweitergabe bilden 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 den Inhaber der E-ID. Die IdP stehen als Vermittler dazwischen. Umso wichtiger ist die Regelung des Datenschutzes. Das DSG sowie untergeordnete Erlasse gelten für alle Beteiligten. Der Artikel hält den Zweck und die spezifischen Bedingungen für die Bearbeitung und Haltung der Daten durch die IdP fest. Er präzisiert namentlich die Anforderungen des DSG an die Datenbearbeitung und verschärft sie in Bezug auf die zu ergreifenden Sicherheitsmassnahmen.

*Abs. 1 und 2*

Die in den Absätzen 1 und 2 formulierten Datenschutzbestimmungen orientieren sich an der Datenschutzgesetzgebung. Bei der Anwendung der E-ID kann die Inhaberin oder der Inhaber jeweils 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. Die Daten dürfen vom IdP nur bearbeitet und gehalten werden, bis die E-ID widerrufen wird. Zudem dürfen sie ausschliesslich für Identifizierungen nach dem vorliegenden Gesetz verwendet werden. Für E-ID des Sicherheitsniveaus substanziell darf der IdP das Gesichtsbild der Inhaberin oder des Inhabers (das im Informationssystem nach Art. 24 gespeichert ist) nur während des Ausstellungsprozesses verwenden.

*Abs. 3*

Dieser Absatz fordert von den IdP besondere Sicherheitsmassnahmen. Damit geht er über die Bestimmungen des DSG hinaus. Es wird sichergestellt, dass die Personenidentifizierungsdaten, Nutzungsdaten sowie übrige Daten sicher bearbeitet und aufbewahrt werden. Die Personenidentifizierungsdaten, die Daten über die Nutzung einer E-ID sowie die übrigen Daten sind sowohl physisch als auch organisatorisch getrennt zu halten. Die Trennung erfolgt gemäss der Kategorie der Daten und dem Bearbeitungszweck. Mit dieser zusätzlichen Sicherheitsmassnahme soll vermieden werden, dass Unbefugte Zugang zu sämtlichen Daten über die Inhaberin oder den Inhaber einer E-ID erhalten. So sollen namentlich die negativen Folgen eines unerlaubten Zugriffs auf das System beschränkt werden.

*Art. 10* Subsidiäres E-ID-System des Bundes

Das vorliegende Gesetz geht 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 die Möglichkeit vor, ein eigenes E-ID-System für dieses Sicherheitsniveau betreiben zu dürfen. Die mit dem Betrieb eines E-ID-Systems beauftragte Verwaltungseinheit wird in Bezug auf die Anwendung des vorliegenden Gesetzes gleich behandelt wie die IdP: Die Bestimmungen über IdP sind in diesen Fällen auf die betreffende Verwaltungseinheit anwendbar.

Der Bundesrat kann aber nur eine Verwaltungseinheit mit dieser Aufgabe betrauen, die über eine Ermächtigung zur Erbringung von gewerblichen Leistungen für Dritte gemäss Artikel 41*a* des Finanzhaushaltgesetzes vom vom 7. Oktober 2005[23] (FHG) verfügt. In Frage kommen dafür das Informatik-Service-Center des EJPD, das Bundesamt für Bauten und Logistik oder das Bundesamt für Informatik und Telekommunikation (vgl. Art. 41*a* Abs. 1 FHG).

*Art. 11* Sperrung und Widerruf

*Abs. 1–4*

Fedpol ermöglicht die systematische Überprüfung der Gültigkeit der E-ID-Registrierungsnummer in einem gebräuchlichen Verfahren (vgl. Art. 23 Abs. 2 BGEID). Derzeit ist dies durch die Führung einer elektronischen Liste vorgesehen. 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. Die Abfrage des IdP bei fedpol erhöht das Vertrauen in nach diesem Gesetz ausgestellte E-ID und ist deshalb kostenlos. IdP sind verpflichtet, ebenfalls eine Möglichkeit zur kostenlosen Abfrage einzurichten, die sich auf die von ihnen herausgegebenen E-ID beschränkt (Art. 15 Abs. 1 Bst. c BGEID).

23 SR **611.0**

Je nach Ergebnis der Abfrage ist die E-ID zu sperren oder zu widerrufen. Es ist notwendig, 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. Um Missbrauch zu verhindern, prüft der IdP vor der Sperrung der E-ID die Herkunft der Meldung.

Die E-ID kann nach dem Wegfall des Grundes der Sperrung wieder aktiviert und weiter verwendet werden. Widerrufen werden alle einer E-ID-Registrierungsnummer zugeordneten E-ID, wenn eine E-ID-Registrierungsnummer dauerhaft nicht mehr verwendet werden darf, beispielsweise beim Tod der Inhaberin oder des Inhabers (Abs. 3). Eine widerrufene E-ID kann nicht wieder aktiviert werden, eine vorübergehend gesperrte jedoch schon. Der IdP informiert die Inhaberin oder den Inhaber einer E-ID unverzüglich über die Sperrung.

*Abs. 5*

Der Bundesrat regelt die Sperrung und den Widerruf einer E-ID. Er bestimmt insbesondere, in welchen Fällen die E-ID widerrufen wird.

## 2.5 Inhaberinnen und Inhaber von E-ID

*Art. 12* Pflichten

*Abs. 1 und 2*

Die hier den Inhaberinnen und Inhabern von E-ID auferlegten Pflichten entsprechen etwa den Sorgfaltspflichten, die üblicherweise für eine Kredit- oder Bankkontokarte angewendet werden müssen. Beispielsweise ist es notwendig und zumutbar, die allenfalls notwendige PIN nicht offenzulegen und nicht 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.

Trotz aller Vorsichtsmassnahmen kann ein Identitätsmissbrauch nie völlig ausgeschlossen werden. Entsprechend sollten angemessene Strafbestimmungen zur Sanktionierung eines solchen Verhaltens eingeführt werden. Im Entwurf des Bundesgesetzes vom 15. September 2017[24] über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz wird das Strafgesetzbuch mit einem Artikel 179decies ergänzt, der den Identitätsmissbrauch mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht. Zur Vermeidung von Doppelspurigkeiten enthält das vorliegende Gesetz keine Bestimmungen zur Bestrafung desselben Verhaltens.

24 BBl **2017** 7193

*Abs. 3*

Im Rahmen der deliktischen Haftung stellt Artikel 12 der Vorlage 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 Verordnungsebene vorgeschrieben wird beispielsweise, dass Fehler in den Personenidentifizierungsdaten unverzüglich dem IdP anzuzeigen sind, ebenso jeder Verlust oder der Verdacht auf Missbrauch einer E-ID.

## 2.6 Anbieterinnen von Identitätsdienstleistungen

*Art. 13* Anerkennung

*Vorbemerkung*

Im Rahmen der Anerkennungsverfahren werden die IdP einer vertieften Prüfung unterzogen. Dabei werden Prüfungen des Strafregisters und der Finanzen sowie Audits durchgeführt, um das geforderte Funktionieren der IdP festzustellen. Mit der Anerkennung der IdP werden auch deren E-ID-Systeme geprüft und anerkannt. Die technischen Anforderungen an die E-ID-verwendenden Systeme 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[25].

*Abs. 1*

Will ein IdP nach diesem Gesetz E-ID ausstellen, muss er verschiedene organisatorische und technische Vorgaben einhalten. Die Einhaltung der Vorgaben wird durch das ISB 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.

*Bst. a*

Natürliche oder juristische Personen ohne Eintrag im Handelsregister können keine Anerkennung erlangen. Da sich auch Behörden ins Handelsregister eintragen[26] können, ist es ihnen grundsätzlich möglich, E-ID-Systeme nach diesem Gesetz zu betreiben.

25 National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Cybersecurity Framwork; der Text kann auf der Webseite des NIST abgerufen werden: www.nist.gov.

26 vgl. Artikel 2 Buchstabe a Ziffer 13 der Handelsregisterverordnung vom 17. Oktober 2007 (mit Verweis auf Artikel 2 Buchstabe d des Fusionsgesetzes vom 3. Oktober 2003).

*Bst. b und c*

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, 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, 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.

*Bst. d*

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

*Bst. e*

Der IdP hat sicherzustellen, dass die Datenbearbeitung und Datenhaltung ausschliesslich in der Schweiz erfolgt. Jeglicher unerlaubte Zugriff aus dem Ausland und von Dritten auf die Daten ist zu verhindern. Der Begriff Datenbearbeitung umfasst jeden Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Archivieren oder Vernichten von Daten. 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.

*Bst. f*

Der IdP muss sich gegen die Haftungsrisiken versichern. Die Haftung richtet sich nach dem Obligationenrecht (OR[27];vgl. Art. 28).

*Bst. g*

Es versteht sich von selbst, dass der IdP nur anerkannt werden kann, wenn er sich an das anwendbare Recht hält. Im Vordergrund stehen dabei die Regeln dieses Gesetzes und seiner Ausführungsbestimmungen. Dazu gehören aber auch andere relevante Regelwerke, so etwa das DSG.

*Abs. 3*

Die technischen Entwicklungen im Bereich elektronische Identifizierung und Authentifizierung unterliegen einem stetigen Wandel. Deshalb muss die Anerkennung in regelmässigen Abständen erneuert werden. Form und Inhalt der Prüfung werden durch den Bundesrat in einer Verordnung festgelegt. Es könnte dort bei-

27 SR **220**

spielweise vorgesehen werden, dass ein IdP jährlich einen Sicherheitsbericht erstellen und an das ISB übermitteln soll.

*Abs. 4*

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

Auf Verordnungs- und Weisungsebene werden nähere Vorschriften zu den Voraussetzungen der Anerkennung erlassen, insbesondere betreffend die fachlichen und sicherheitsbezogenen Anforderungen, die anwendbaren Standards und technischen Protokolle für die E-ID-Systeme sowie die notwendigen Versicherungsdeckung. Diese Vorgaben werden durch das ISB regelmässig geprüft. Dadurch wird auch eine Anerkennung der E-ID-Systeme erreicht.

*Art. 14* Erlöschen der Anerkennung

*Abs. 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. Die Anerkennung erlischt auch, wenn der IdP seine Geschäftstätigkeit aufgibt.

*Abs. 2 und 3*

Die Absätze 2 und 3 sollen den Erhalt einmal aufgebauter E-ID-Netze sichern. Dadurch, dass der Erlös aus der Übernahme gegebenenfalls in die Konkursmasse fällt, erhalten E-ID-Systeme als Ganzes einen wirtschaftlichen Wert, selbst wenn die einzelnen Daten nicht handelbar sind.

*Abs. 4*

Bei Erlöschen der Anerkennung ist der Wille der Inhaberin oder des Inhabers der E-ID zu respektieren. Wenn diese oder dieser nicht in die Übernahme ihrer bzw. seiner Daten durch einen anderen IdP oder den Bund eingewilligt hat, so dürfen die Daten nicht übermittelt werden und müssen vernichtet werden.

*Abs. 5*

Falls kein IdP die E-ID-Systeme eines anderen IdP übernehmen kann, soll diese Bestimmung sicherstellen, dass die aufgebauten E-ID-Netzwerke trotzdem weiterbetrieben werden können. Dies ist sowohl für die Nutzerinnen und Nutzer als auch für die Wirtschaftspartnerinnen, die diese verwenden und sich auf diese verlassen, von grosser Bedeutung. In einer solchen Situation ordnet das ISB entweder an, dass der Bund die E-ID-Systeme ohne Entgelt übernimmt, oder dass die darin enthaltenen Daten vernichtet werden, wenn die E-ID-Systeme nicht weiterbetrieben werden.

*Art. 15* Pflichten

*Abs. 1*

*Bst. 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.

*Bst. 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. Der Ausstellungsprozess umfasst drei Schritte und kann je nach Sicherheitsniveau unterschiedlich ausgestaltet sein:

1. Der IdP ordnet die von fedpol übermittelten Personenidentifizierungsdaten (Art. 5 BGEID) mit der E-ID-Registrierungsnummer eindeutig der E-ID mit dem zugehörigen Authentizierungsmittel zu, das die Inhaberin oder den Inhaber authentifiziert. Zumindest auf höheren Sicherheitsniveaus ist das Authentifizierungsmittel meist direkt in eine Trägereinheit integriert (z.B. Chip auf Karte oder SIM-App in einem 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 lautet).
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 Authentifizierungsmittel an die richtige Person gebunden werden muss.

*Bst. 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 ZertES entspricht. So kann fedpol beispielsweise eine Liste mit E-ID-Registrierungsnummern führen und publizieren, die vorübergehend oder dauerhaft für den Bezug oder den Einsatz einer E-ID ungültig sind. 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.

*Bst. d*

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

*Bst. e*

Die Aktualisierung der Personenidentifizierungsdaten führt zu mehr Sicherheit. Die Periodizität ist je nach Sicherheitsniveau unterschiedlich und wird in Artikel 7 Absatz 1 festgelegt.

*Bst. f und g*

Damit gewährleistet ist, dass das E-ID-System gut funktioniert, ist der IdP verpflichtet, den betreffenden Behörden bestimmte Informationen zu melden, von denen er Kenntnis erlangt hat. So muss er fedpol Fehler in den Personenidentifizierungsdaten und dem ISB sicherheitsrelevante Vorkommnisse im E-ID-System oder beim Einsatz der E-ID melden, die ihm zur Kenntnis gebracht wurden oder die er selbst entdeckt.

*Bst. h*

Sobald beim Einsatz einer E-ID Personenidentifizierungsdaten übermittelt werden, muss der IdP das Einverständnis der Inhaberin oder des Inhabers einholen. Sie oder er muss explizit zustimmen, welche Personenidentifizierungsdaten bei einer konkreten Anwendung der E-ID vom IdP an eine Betreiberin von E ID-verwendenden Diensten übermittelt werden.

*Bst. i*

Das BGEID stärkt den Auskunftsanspruch gemäss Artikel 8 DSG. Der IdP wird verpflichtet, auf Anfrage Auskunft zu allen Daten zu geben, die er über eine Person bearbeitet. Aus Transparenz- und Vertrauensgründen soll E-ID-Inhaberinnen und -Inhabern online Zugang zu ihren Personenidentifizierungs- sowie Nutzungsdaten gewährt werden. Buchstabe i sieht deshalb eine Auskunftspflicht seitens des IdP vor, soweit er die Protokolldaten gemäss Buchstabe j nicht bereits vernichtet hat.

*Bst. j*

Protokolldaten über den Einsatz der E-ID, die der IdP hat, sind nach einer Frist von sechs Monaten zu vernichten. Diese Frist ist u.a. auch im Bereich der Fernmeldeüberwachung vorgesehen (vgl. Art. 26 Abs. 5 des Bundesgesetzes vom 18. März 2016[28] betreffend die Überwachung des Post- und Fernmeldeverkehrs). Die Protokolldaten werden gebraucht für die Erteilung von Auskunft nach Buchstabe i und für die Nachvollziehbarkeit von Transaktionen im Streitfall.

Durch diese Vorschrift nicht betroffen sind Protokoll, Registrierungs- und Transaktionsdaten beim E-ID-verwendenden Dienst.

*Bst. k*

Der EDÖB kann zu den Mustern für die Vereinbarungen der IdP mit den E-ID-verwendenden Diensten Stellung nehmen. Diese sind ihm zur Überprüfung zu unterbreiten.

28 SR **780.1**

*Bst. l*

Da die Anerkennung spätestens nach drei Jahren erneuert werden muss, muss der IdP alle geplanten Änderungen an seinem E-ID-System und an seiner Geschäftstätigkeit melden. Demnach müssen Änderungen, die während dieses Zeitraums vorgenommen wurden, vom ISB separat genehmigt werden. Denn es ist möglich, dass die Anerkennung während dieses Zeitraums nicht aufrechterhalten werden kann, wenn die Anerkennungsvoraussetzungen nach Artikel 13 Absatz 2 aufgrund dieser Änderungen nicht mehr erfüllt sind.

*Abs. 2*

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.

*Abs. 3*

Schliesslich erlässt der Bundesrat nähere Vorschriften zu den verschiedenen Meldungen nach dem vorliegenden Gesetz. Dabei geht es um die Meldung der geplanten Aufgabe der Geschäftstätigkeit des IdP, die Meldung von Fehlern in den Personenidentifizierungsdaten, der sicherheitsrelevanten Vorkommnisse im E-ID-System oder beim Einsatz der E-ID sowie der Muster für die Vereinbarungen mit den E-ID-verwendenden Diensten.

*Art. 16* Datenweitergabe

*Abs. 1*

Die IdP dürfen Betreiberinnen von E-ID-verwendenden Diensten Personenidentifizierungsdaten im Sinne von Artikel 5 nur weitergeben, soweit sie für die Identifizierung der betreffenden Person notwendig sind und dem geforderten Sicherheitsniveau entsprechen. Zudem muss die Inhaberin oder der Inhaber der E-ID in deren Übermittlung eingewilligt haben.

Die Übermittlung ist erforderlich, damit das E-ID-System seine Funktion erfüllen kann und die Ansprüche der Nutzerinnen und Nutzer an den Komfort, die Flexibilität und Einfachheit erfüllt werden können. Dabei wird der Grundsatz der Verhältnismässigkeit gewahrt, denn die vorgesehene Beeinträchtigung der Privatsphäre geht nicht über das hinaus, was für die Erfüllung dieses Zwecks nötig ist. Bei den übermittelten Personendaten handelt es sich im Übrigen nicht um besonders schützenswerte Daten im Sinne von Artikel 3 Buchstabe c DSG.

*Abs. 2*

Es wird sowohl dem IdP als auch der Betreiberin von E-ID-verwendenden Diensten untersagt, die staatlich bestätigten Personenidentifizierungsdaten nach Artikel 5 ausserhalb eines E-ID-Einsatzes 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 zudem auch nicht unentgeltlich weitergegeben werden dürfen, z. B. zur kommerziellen Nutzung durch eine andere Unternehmung innerhalb eines Konzerns.

*Art. 17* Zugang zu einer E-ID

Mit diesem Artikel sollen Personen, die die persönlichen Voraussetzungen für eine E-ID erfüllen, sowie die Inhaberinnen und Inhaber einer E-ID vor den schädlichen Auswirkungen bewahrt werden, die daraus resultieren könnten, dass ein oder zwei IdP eine marktbeherrschende Stellung einnehmen. Dies könnte namentlich eintreffen, wenn ein IdP beschliesst, einem Teil der Bevölkerung keine E-ID auszustellen oder sie nicht zu denselben Bedingungen anzubieten wie breiten Bevölkerungskreisen.

Nach Absatz 1 müssen aber konkrete Hinweise dafür vorliegen, dass der betreffende IdP wiederholt nicht allen Personen, die die persönlichen Voraussetzungen dafür erfüllen, Zugang zu einer E-ID gewährten oder nicht zu denselben Bedingungen anbieten würden. Es wird jedoch nicht präzisiert, wer glaubhaft machen muss, dass ein solcher Fall vorliegt. Demnach könnten die berechtigten Personen, die Inhaberinnen und Inhaber einer E-ID, andere IdP, die Betreiberinnen von E-ID-verwendenden Diensten oder Konsumentenschutzorganisationen eine solche Ungleichbehandlung geltend machen. Wenn die Voraussetzungen nach Absatz 1 erfüllt sind, muss das ISB oder IdP tätig werden.

Zur Erleichterung der Auslegung und Anwendung des Artikels wurden die Kriterien, die bei der Beurteilung eines Falls zu berücksichtigen sind, möglichst konkret formuliert. Der Ermessensspielraum des ISB und des IdP ist folglich beschränkt. So können die entsprechenden Entscheide effizienter gefällt werden.

*Art. 18* Interoperabilität

Interoperabilität unter den E-ID-Systemen ist eine wichtige Voraussetzung für die Verbreitung von E-ID. Deshalb wird hier festgehalten, dass IdP ihre E-ID-Systeme des entsprechenden Sicherheitsniveaus gegenseitig akzeptieren müssen. Die Interoperabilität wird durch technische Standards und definierte Schnittstellen ermöglicht, die auf dem Verordnungs- oder Weisungsweg erlassen werden.

Inhaberinnen und Inhaber sollen 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 wird realisiert durch die Einhaltung von Interoperabilitätsstandards und -regeln, die durch alle IdP einzuhalten sind.

Vgl. dazu auch die Ausführungen unter Ziffer 1.2.6.6.

*Art. 19* Aufsichtsmassnahmen und Entzug der Anerkennung

*Abs. 1*

Das ISB wird aktiv, wenn es bei den regelmässigen Kontrollen oder aufgrund einer Meldung feststellt, dass ein IdP Vorgaben missachtet oder die Voraussetzungen für die Anerkennung (Art. 13 Abs. 2 BGEID) nicht mehr erfüllt sind. Als notwendige Massnahmen kommen insbesondere technische Vorgaben, z.B. Einhaltung der neuesten Standards, oder organisatorische Massnahmen, z.B. Auflagen zur Schulung von Mitarbeitenden, in Frage. Das ISB setzt eine Frist zur Behebung der festgestellten Mängel.

*Abs. 2*

Werden die Mängel innert der angemessenen Frist nicht behoben, kann die Anerkennung durch das ISB entzogen werden. Ein Entzug muss in jedem Fall verhältnismässig sein.

*Abs. 3*

Der Bundesrat regelt auf Verordnungsstufe das Verfahren zum Entzug der Anerkennung.

## 2.7 Betreiberinnen von E-ID-verwendenden Diensten

*Art. 20* Vereinbarung mit einem 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.

*Art. 21* Verwendung der E-ID-Registrierungsnummer

Diese Bestimmung schafft die Rechtsgrundlage für die Identifizierung von Personen anhand der E-ID-Registrierungsnummer durch die E-ID-verwendenden Dienste. In den meisten Fällen wird es sich bei den von der Bestimmung erfassten Betreiberinnen voraussichtlich um private Akteure handeln. Es ist jedoch möglich, dass auch Behörden E-ID-verwendende Dienste im Sinne des Gesetzes anbieten. Sie könnten namentlich eine E-Government-Anwendung anbieten, die sich auf einen E-ID-verwendenden Dienst stützt, um eine Aufgabe von öffentlichem Interesse zu erfüllen. Damit die Behörden in diesem Fall befugt sind, die E-ID-Registrierungsnummer zur Identifizierung zu verwenden, muss eine gesetzliche Grundlage geschaffen werden.

*Art. 22* Zu akzeptierende E-ID

Betreiberinnen von E-ID-verwendenden Diensten und Behörden oder andere Stellen, die Verwaltungsaufgaben erfüllen, müssen jede E-ID, die für das entsprechende Si-

cherheitsniveau ausgestellt wurde, akzeptieren. Für Behörden und andere Stellen, die Verwaltungsaufgaben erfüllen gilt diese Pflicht nur, sofern sie beim Vollzug von Bundesrecht eine elektronische Identifizierung vornehmen. Demnach müssen auch Behörden von Kantonen und Gemeinden sowie andere Stellen mit Verwaltungsaufgaben beim Vollzug von Bundesrecht jede nach diesem Gesetz ausgestellte E-ID auf dem entsprechenden Sicherheitsniveau akzeptieren. Dies schliesst nicht aus, dass heute eingesetzte elektronische Identifizierungsmittel weiterhin verwendet werden können.

Diese Bestimmung unterstreicht die Bedeutung und Akzeptanz einer E-ID nach diesem Gesetz, 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 E-ID Kosten nach diesem Gesetz einsparen können, sondern auch alle Einwohnerinnen und Einwohner der Schweiz.

## 2.8 Funktion des Bundesamtes für Polizei

*Art. 23* Aufgaben und Pflichten

*Abs. 1*

Fedpol weist die Personenidentifizierungsdaten einer eindeutigen E-ID-Registrierungsnummer zu und übermittelt sie an den IdP. Der Umfang der übermittelten Personenidentifizierungsdaten variiert je nach Sicherheitsniveau (vgl. Art. 6 BGEID).

*Abs. 2*

Fedpol ermöglicht die systematische Überprüfung der Gültigkeit der E-ID-Registrierungsnummer in einem gebräuchlichen Verfahren. 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 fedpol erhöht das Vertrauen in die vom betreffenden IdP ausgestellten E-ID und ist deshalb kostenlos. IdP sind verpflichtet, ebenfalls eine kostenlose Abfragemöglichkeit einzurichten, die sich aber auf die von ihnen ausgestellten E-ID beschränkt (Art. 15 Abs. 1 Bst. c BGEID).

Vgl. Erläuterungen zu Artikel 11 Absätze 1 bis 4.

*Abs. 3*

Die verschiedenen Informationssysteme werden durch unterschiedliche Quellen mit Daten versorgt. Infostar ist das zentrale Personenstandsregister 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.

*Art. 24* Informationssystem

*Abs. 1 und 2*

Fedpol führt ein Informationssystem zur Bearbeitung der Personendaten nach Artikel 5. Bearbeitet werden die AHV-Nummer und die Protokolldaten des Prozesses zur Ausstellung der E-ID nach Artikel 6 Absatz 5. Die Liste ist abschliessend.

Der Zweck der Datenbearbeitung ist abschliessend in Absatz 2 geregelt. Das Informationssystem ermöglicht die Entgegennahme der Anträge und Einverständniserklärungen der antragstellenden Personen, die automatisierte Erfüllung der Aufgaben von fedpol bei der Ausstellung von E-ID, der Aktualisierung der Personenidentifizierungsdaten sowie die Prüfung der Gültigkeit einer E-ID-Registrierungsnummer.

*Abs. 3*

Das Informationssystem unterhält Schnittstellen zu folgenden Personenregistern, die auf Bundesebene geführt werden und zum Bezug und Abgleich der Personenidentifizierungsdaten verwendet werden:

- das Informationssystem Ausweisschriften (ISA) gemäss Artikel 11 des Ausweisgesetzes vom 22. Juni 2001[29] und Artikel 10 der Ausweisverordnung vom 20. September 2002[30];
- das Zentrale Migrationsinformationssystem (ZEMIS) gemäss Artikel 101 ff. des Ausländergesetzes und der ZEMIS-Verordnung vom 12. April 2006[31];
- das elektronische Personenstandsregister Infostar gemäss Artikel 39 des Zivilgesetzbuches (ZGB)[32] und Artikel 6a der Zivilstandsverordnung vom 28. April 2004[33];
- das Informationssystem Ordipro der EDA nach Artikel 5 des Bundesgesetzes vom 24. März 2000[34] über die Bearbeitung von Personendaten im Eid-

29 SR **143.1**
30 SR **143.11**
31 SR **142.513**
32 SR **210**
33 SR **211.112.2**

genösischen Departament für auswärtige Angelegenheiten (Ordipro) und Artikel 2 der Verordnung vom 7. Juni 2004[35] über das Informationssystem Ordipro des Eidgenössischen Departements für auswärtige Angelegenheiten; sowie

– das Zentralregister der zentralen Ausgleichsstelle der AHV (ZAS-UPI) gemäss Artikel 71 AHVG.

Der IdP ist zur Zusammenarbeit mit fedpol verpflichtet. Aus diesem Grund wird das System des IdP mit dem Informationssystem von fedpol verknüpft werden müssen, damit die Personenidentifizierungsdaten übermittelt werden können. Entsprechend wird fedpol dem IdP über eine Schnittstelle Zugang zu seinem Informationssystem gewähren, damit dieser die Personenidentifizierungsdaten der Inhaberinnen und Inhaber einer E-ID speichern und den E-ID-verwendenden Diensten weitergeben kann. Der IdP seinerseits wird ein eigenes Informationssystem betreiben, in dem er die von fedpol erhaltenen Personenidentifizierungsdaten sowie die Daten über die Nutzung der E-ID durch die Inhaberin oder den Inhaber speichert. Nach Artikel 15 Absatz 1 Buchstabe i muss er den Inhaberinnen und Inhabern einer E-ID online Zugang zu diesen Daten gewähren. Der IdP wird auf keinen Fall Zugriff auf die Personenregister nach Artikel 24 Absatz 3 haben. Darüber hinaus muss er für die Erstübermittlung der Personenidentifizierungsdaten an Betreiberinnen von E-ID-verwendenden Diensten das ausdrückliche Einverständnis der Inhaberin oder des Inhabers der E-ID einholen (Art. 15 Abs. 1 Bst. h). Die Artikel 9 und 16 umfassen noch weitere Anforderungen in Bezug auf die Bearbeitung, Haltung und Weitergabe von Daten durch den IdP.

## 2.9 Funktion des Informatiksteuerungsorganes des Bundes

*Art. 25* Zuständigkeit

*Abs. 1*

Die Anerkennungsstelle für Identitätsdienstleister (Anerkennungsstelle) wird durch das ISB geführt. Das Verfahren zur Anerkennung von IdP ist dem Verfahren zur Anerkennung von Zustellplattformen nachgebildet (vgl. Ziff. 1.3.2).

*Abs. 2*

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 der Liste mit anerkannten Zustellplattformen nachgebildet.

34 SR **235.2**
35 SR **235.21**

*Art. 26* Informationssystem

Zur Erfüllung der gesetzlichen Aufgaben führt das ISB ein eigenes Informationssystem, das folgende Informationen umfasst: die im Anerkennungsprozess von den IdP gelieferten Daten, Unterlagen und Nachweise, die Meldungen über die geplante Aufgabe der Geschäftstätigkeit der IdP (Art. 14 Abs. 2), die Meldungen über sicherheitsrelevante Vorkommnisse im E-ID-System oder beim Einsatz der E-ID (Art. 15 Abs. 1 Bst. g), die Meldungen über alle geplanten Änderungen am E-ID-System und Änderungen an der Geschäftstätigkeit (Art. 15 Abs. 1 Bst. l) sowie Informationen über die Aufsichtsmassnahmen. Das Informationssystem wird für die Anerkennung von IdP und für die Aufsicht über sie geführt.

## 2.10 Gebühren

*Art. 27*

Fedpol und ISB erheben von den IdP für Verfügungen und Dienstleistungen Gebühren. Für Abfragen zur Gültigkeit der E-ID-Registrierungsnummer werden keine Gebühren erhoben. Für die Bemessung der Gebühren 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 bei fedpol, verzichtet werden soll. Ermässigte Gebühren für den Fall, dass ein IdP die E-ID den Bezügerinnen und 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.

## 2.11 Haftung

*Art. 28*

*Vorbemerkung*

Die Haftung für Schäden, die bei der Verwendung der E-ID entstehen könnten, unterliegt den bekannten und bewährten Haftungsregeln nach dem Obligationenrecht resp. dem Verantwortlichkeitsgesetz vom 14. März 1958[36] und den kantonalen Staatshaftungserlassen.

Die Bestimmungen haben deklaratorischen Charakter und dienen der Klarstellung, dass sämtliche Haftungsregeln, z. B. in Bezug auf den Schadensbegriff, die Entlas-

36 SR **170.32**

tungsmöglichkeiten 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 Signaturschlüsselinhaberinnen und -inhabern 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 Identifizierung von Teilnehmerinnen und Teilnehmern im elektronischen Geschäftsverkehr.

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

*Abs. 1*

Die Haftpflicht der Inhaberin oder des Inhabers, der E-ID-verwendenden Diensten und der IdP – oder kurz gesagt: die Haftung der privaten Akteurinnen und Akteure – richtet sich nach dem Obligationenrecht. Ob es sich dabei um eine vertragliche Haftung oder eine ausservertragliche Haftung (Art. 41 ff. OR) handelt, ist im Einzelfall zu beurteilen.

*Abs. 2*

Als Verwaltungseinheiten des Bundes unterstehen fedpol und das ISB dem Verantwortlichkeitsgesetz.

## 2.12 Schlussbestimmungen

*Art. 29* Übergangsbestimmung

Mit dieser Übergangsbestimmung soll die Anerkennung elektronischer Identifizierungseinheiten, die vor dem Inkrafttreten des vorliegenden Gesetzes ausgestellt worden sind, erleichtert werden. In den meisten Fällen haben die Inhaberinnen und Inhaber einer elektronischen Identifizierungseinheit beim IdP oder einem ähnlichen Organ bereits einen strengen Ausstellungsprozess durchlaufen.

Während einer Übergangsphase von zwei Jahren anerkennt das ISB demnach auf Antrag eines IdP von diesem ausgestellte elektronische Identifizierungseinheiten als E-ID des Sicherheitsniveaus niedrig. Ausserdem anerkennt das ISB von einem IdP ausgestellte elektronische Identifizierungseinheiten als E-ID des Sicherheitsniveaus substanziell, wenn zusätzlich eine Identifizierung in einem gesetzlich geregelten und beaufsichtigten Verfahren durchgeführt wurde, das eine vergleichbare Sicherheit bietet wie die nach dem vorliegenden Gesetz vorgesehenen Verfahren. Auch wer ein gültiges qualifiziertes Zertifikat nach Artikel 2 Buchstabe h des Bundesgesetzes über die elektronische Signatur besitzt, kann sich damit von einem IdP ohne weitere

Identifizierung eine E-ID des Sicherheitsniveaus substanziell ausstellen lassen. In allen drei Fällen müssen die Anforderungen nach Absatz 1 Buchstabe a erfüllt sein: Die Inhaberin oder der Inhaber muss die persönlichen Voraussetzungen nach Artikel 3 erfüllen, sie oder er muss sich mit der Ausstellung der E-ID einverstanden erklärt haben und die Personenidentifizierungsdaten (wie Nummer der Identitätskarte, Name, Vorname und Geburtsdatum) müssen mit den Daten im Informationssystem nach Artikel 24 übereinstimmen.

Der Bundesrat wird in einer Verordnung nähere Vorschriften zu den Ausstellungsverfahren erlassen. Er wird namentlich die Anforderungen an das Verfahren, die verschiedenen Verfahrensschritte und die Kompetenzen des für die Anerkennung zuständigen Organs festlegen.

Er wird dabei insbesondere auch zu bestimmen haben, wie die E-ID-Registrierungsnummer den vom IdP vor Inkrafttreten dieses Gesetzes ausgestellten elektronischen Identifizierungseinheiten zugeordnet wird.

*Art. 30* Änderung anderer Erlasse

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

*Art. 31* 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.

## 2.13 Änderung anderer Erlasse

*Vorbemerkungen*

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. Verschiedene Verordnungen und Weisungen müssen deshalb bei der Erarbeitung der Ausführungsbestimmungen zum E-ID-Gesetz geändert werden, beispielweise die Verordnung vom 6. Juni 2014[37] über die Informationssysteme für den öffentlichen Veterinärdienst (ISVet-V) oder die Verordnung vom 23. Oktober 2013[38] über Informationssysteme im Bereich der Landwirtschaft (ISLV).

37 SR **916.408**
38 SR **919.117.71**

## 1. Bundesgesetz vom 20. Juni 2003[39] über das Informationssystem für den Ausländer- und den Asylbereich

*Art. 9 Abs. 1 Bst. c und Abs. 2 Bst. c Ziff. 3 (neu)*

In Artikel 9 Absatz 1 werden die Behörden aufgezählt, denen das SEM die von ihm oder in seinem Auftrag im Informationssystem nach dem BGIAA bearbeiteten Daten des Ausländerbereichs durch ein Abrufverfahren zugänglich machen kann. Buchstabe c hält fest, zu welchen Zwecken den Bundesbehörden im Bereich des Polizeiwesens Zugang zu den Daten gewährt werden darf. Mit dem vorliegenden Gesetz wird dieser Liste ein weiterer Zweck angefügt: die Personenidentifizierung sowie die Zuordnung und Aktualisierung von Personenidentifizierungsdaten gemäss BGEID.

In Artikel 9 Absatz 2 werden die Behörden aufgezählt, denen das SEM die von ihm oder in seinem Auftrag im Informationssystem nach dem BGIAA bearbeiteten Daten des Asylbereichs zugänglich machen kann. Buchstabe c hält fest, zu welchen Zwecken den Bundesbehörden im Bereich des Polizeiwesens Zugang zu diesen Daten gewährt werden darf. Mit dem Gesetzesentwurf wird der Liste ein neuer Zweck angefügt: die Erfüllung ihrer Aufgaben nach dem BGEID.

## 2. Ausweisgesetz vom 22. Juni 2001[40]

*Art. 1 Abs. 3 zweiter Satz*

Grundsätzlich werden Schweizer Diplomaten- und Dienstpässe nur 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 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 fremdländische Ehe- oder Lebenspartner haben, 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, Fachleute 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

39 SR **142.51**
40 SR **143.1**

Rubrik Nationalität entsprechend auch der Heimatstaat der Person aufgeführt und der Heimatort mit «***» ersetzt.

*Art. 11 Abs. 1 Bst. k und Abs. 2*

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.

*Art. 12 Abs. 2 Bst. g*

Nicht nur fedpol (Bst. a), sondern auch das EDA (Konsularische Direktion) soll die für 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.

*Art. 14*

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

## 3. Zivilgesetzbuch (ZGB)[41]

*Art. 43a Abs. 4 Ziff. 5*

Artikel 43*a* 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 fedpol erweitert.

## 4. Bundesgesetz vom 20. Dezember 1946[42] über die Alters- und Hinterlassenenversicherung (AHVG)

*Art. 50a Abs. 1 Bst. b^quater^*

In Artikel 50*a* AHVG wird geregelt, welchen Stellen in Abweichung von Artikel 33 des Bundesgesetzes vom 6. Oktober 2000[43] über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) Daten, insbesondere die AHVN13, bekannt gegeben

41 SR **210**
42 SR **831.10**
43 SR **830.1**

werden dürfen. Fedpol wird neu als eine dieser Stellen erwähnt. Die formalgesetzliche Voraussetzung für die systematische Nutzung der AHVN13 durch fedpol und IdP wird in Artikel 8 Absatz 1 BGEID geschaffen.

### 5. Bundesgesetz vom 18. März 2016[44] über die elektronische Signatur (ZertES)

*Art. 9 Abs. 1bis*

Im Ausgabeprozess für eine elektronische Signatureinheit ist die persönliche Vorsprache vorgeschrieben. Diese entfällt, wenn der Identitätsnachweis durch eine E-ID des Sicherheitsniveaus substanziell erbracht werden kann.

## 3 Auswirkungen

### 3.1 Finanzielle und personelle Auswirkungen

Aufgrund der Wichtigkeit des strategischen Projekts elektronische Identität werden die finanziellen und personellen Auswirkungen getrennt nach Aufbau und Betrieb dargestellt. Im Aufbau enthalten ist auch das Vorprojekt, welches bis Ende 2017 dauerte.

#### 3.1.1 Aufbau

##### 3.1.1.1 Vorprojekt (bis 2017)

Im Rahmen eines Vorprojekts wurden bis Ende 2017 mögliche konzeptionelle Varianten für staatlich anerkannte E-ID analysiert und der Rechtsetzungsentwurf erarbeitet. Zudem wurde ein E-ID-Demonstrator aufgebaut. Der E-ID-Demonstrator wird einerseits bei Präsentationen des Projektes und andererseits für die Erarbeitung der Spezifikationen der technischen Anforderungen in der Verordnung und den Ausführungsbestimmungen genutzt. Er dient so als Entwicklungs- und Testwerkzeug für diese Regelwerke. Für das Vorprojekt sind Kosten von insgesamt 390 000 Franken angefallen. Davon wurden 290 000 Franken vom EJPD und 100 000 Franken durch E-Government Schweiz finanziert.

##### 3.1.1.2 Organisation

Die Identitätsstelle beim fedpol und die Anerkennungsstelle beim ISB müssen in den Jahren 2018–2020 aufgebaut werden. Der Aufwand für den Aufbau umfasst die Personalgewinnung und die Etablierung der Prozesse und Schnittstellen. Die Identi-

44 SR **943.03**

tätsstelle ist einerseits für die technische Infrastruktur und den zugehörigen Support (Fachsupport und Kundenhotline), andererseits für die Pflege der Vorgaben für die Anerkennung zuständig. Die Anerkennungsstelle vollzieht das E-ID-Gesetz im Bereich der Anerkennung der IdP, führt die vorgegebenen Kontrollen durch und überwacht die Compliance.

| Aufwand in PT | 2018 | 2019 | 2020 | Summe |
|---|---|---|---|---|
| Aufbau Identitätsstelle | – | 150 | 75 | 225 |
| Aufbau Anerkennungsstelle | – | 50 | 25 | 75 |
| Summe | – | 200 | 100 | 300 |
| Kosten | – | 160 000 | 80 000 | **240 000** |

PT = Personentage (Berechnungsgrundlage 220 Projekttage pro Person und Jahr)

Bei einem Kostensatz von 800 Fr,/ PT ergibt sich ein Aufwand für den Aufbau der Identitätsstelle und der Anerkennungsstelle von total 240 000 Franken.

#### 3.1.1.3 Systeme

Der Betrieb der Identitätsstelle soll so weit als sinnvoll automatisiert werden. Dazu muss eine neue Fachanwendung geschaffen werden, welche Schnittstellen zu den IdP und den verwaltungsinternen Registern (ISA, ZEMIS, Infostar und ZAS-UPI) hat. Über die Schnittstelle zu den IdP werden die staatlich anerkannten Identitätsdaten geliefert. Ein weiterer Teil dieser Fachanwendung ist eine Webseite des Bundes, auf welcher die Antragstellenden ihre Identität und ihr Einverständnis bestätigen müssen, um eine E-ID zu erhalten. Zudem muss als Teil der Fachanwendung über eine öffentlich und kostenlos zugängliche Schnittstelle abgefragt werden können, ob E-ID-Registrierungsnummer gültig ist und welche IdP staatlich anerkannt sind.

Da die Sozialversicherungsnummer (AHVN13) nicht direkt als E-ID-Registrierungsnummer verwendet werden soll, muss ein zusätzlicher Dienst geschaffen werden. Organisationen, welche zur systematischen Nutzung der AHVN13 berechtigt sind, sollen über diesen Dienst die zu einer E-ID-Registrierungsnummer gehörige AHVN13 abfragen können.

Sonstige Aufwände umfassen u. a. externe IT-Sicherheitsfachleute, welche für spezielle Fragestellungen, zum Beispiel im Bereich der Informatiksicherheit, zugezogen werden.

Die Kosten für den Aufbau der Informatiksysteme (2018–2020) sowie die Gesamtkosten einschliesslich Finanzierung sind in Ziffer 3.1.1.4 dargestellt.

#### 3.1.1.4 Gesamtkosten und Finanzierung Aufbau

| | Vorprojekt | | | Umsetzung | Summe |
|---|---|---|---|---|---|
| Aufwand in CHF | 2015–2017 | 2018 | 2019 | 2020 | |
| Personalaufwand (inkl. Projektmanagement) | 200 000 | 240 000 | 320 000 | 250 000 | 1 010 000 |
| Systementwicklung (E-ID-Demonstrator) | 180 000 | 110 000 | 100 000 | 50 000 | 440 000 |
| Systementwicklung (Fachanwendung/Datenbank) | – | 260 000 | 2 580 000 | 1 950 000 | 4 790 000 |
| Systementwicklung (AHVN13 Schnittstelle) | – | 50 000 | 400 000 | 300 000 | 750 000 |
| Sonstiger Aufwand (IT-Sicherheitsexperten) | 10 000 | 150 000 | 240 000 | 270 000 | 670 000 |
| Aufbau Organisation Identitätsstelle und Anerkennungsstelle | – | – | 160 000 | 80 000 | 240 000 |
| **Gesamtkosten** | **390 000** | **810 000** | **3 800 000** | **2 900 000** | **7 900 000** |
| ./. Zentrale IKT-Mittel | – | 700 000 | 800 000 | – | 1 500 000 |
| ./. eGovernment Schweiz | 100 000 | 450 000 | 900 000 | – | 1 450 000 |
| ./. Eigenmittel EJPD | 290 000 | – | 1 660 000 | 1 920 000 | 3 970 000 |
| ./. Zweckgebundene Reserve | | –340 000 | 340 000 | – | – |
| **Mehrbedarf einmalige Projektausgaben** | – | – | **100 000** | **880 000** | **980 000** |
| ./. Zentrale IKT-Mittel | – | – | – | 880 000 | 880 000 |
| ./. eGovernment Schweiz | – | – | 100 000 | – | 100 000 |

Die Finanzierung des Projektaufwands ist bis zu einem Betrag von 6 920 000 Franken durch beim EJPD vorhandene Mittel bereits sichergestellt (einschliesslich Anteile zentrale IKT-Mittel und Beteiligung eGovernment Schweiz).

Aufgrund der Ergebnisse zur Vernehmlassung des E-ID-Gesetzes muss ein zusätzlicher Dienst zur Abfrage der AHVN13 aufgebaut und implementiert werden. Die dazu notwendigen Mittel von 750 000 Franken fallen zusätzlich an und müssen ergänzend beantragt werden. Ebenfalls muss der E-ID-Demonstrator weiterentwickelt und gepflegt werden. Dies wird zusätzliche Kosten von 230 000 Franken auslösen und führt 2018–2020 zu einem Zusatzaufwand von insgesamt 980 000 Franken, welcher ebenfalls ergänzend beantragt werden muss. Da 100 000 Franken aus Mitteln von eGovernment Schweiz stammen, müssen insgesamt 880 000 Franken aus den zentralen IKT-Mitteln beantragt werden.

Die Ausgaben gegenüber Dritten werden über den Verpflichtungskredit V0224.00 «Erneuerung Schweizerpass und Identitätskarte» von 19,6 Millionen bei fedpol abgerechnet.

### 3.1.2 Betrieb (ab 2020)

Auf Seiten der Identitäts- und der Anerkennungsstelle werden ab 2020 voraussichtlich bis zu acht zusätzliche Stellen benötigt.

Die Informatikbetriebskosten werden momentan mit 15 Prozent der getätigten Investitionen resp. mit rund einer Million Franken veranschlagt. Die Betriebskosten fallen ab dem Jahr 2020 an. Projekt und Betrieb überlappen sich im ersten Jahr zu einem gewissen Teil. Weitere Aufwände umfassen Mittel im Bereich der Kommunikation der E-ID-Lösung, externe Beratungen sowie Unvorhergesehenes.

Der mit der Umsetzung des vorliegenden Gesetzesentwurfs zu finanzierende Betriebsaufwand wird auf maximal 2,4 Millionen Franken geschätzt (1,4 Mio. für bis zu 8 Stellen und 1 Mio. für den Sachaufwand). Der Ressourcenbedarf wird mit der Erarbeitung der Ausführungsverordnungen und in Kenntnis des Ergebnisses der parlamentarischen Beratung nochmals genauer evaluiert und zusammen mit der Inkraftsetzung des E-ID-Gesetzes dem Bundesrat beantragt. Dabei wird auch die Nachfrage nach E-ID bei möglichen E-ID-Anbietern näher abgeklärt.

### 3.1.3 Langfristige Erfolgsrechnung

Mit dem Bundesratsbeschluss vom 22. Februar 2017 «Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz); Eröffnung des Vernehmlassungsverfahrens» wurde das EJPD beauftragt, dem Bundesrat mit der Botschaft zum E-ID-Gesetz ein grundsätzlich haushaltsneutrales Finanzierungskonzept für den Betrieb der Identitätsstelle und der Anerkennungsstelle einschliesslich Stellenbedarf zu beantragen. Das Szenario geht von konservativen Annahmen und einem kontinuierlichen Anwachsen der E-ID-Anzahl aus, beginnend mit Null.

Die Kosten wurden gemäss der vorgehenden Angaben zusammengestellt. Bei den Erträgen geht das Szenario von folgenden Annahmen aus:

Für die Anerkennung der IdP und ihrer E-ID-Systeme durch die Anerkennungsstelle werden Gebühren erhoben. Die Gebühren hängen vom anzuerkennenden Sicherheitsniveau ab. Die Anerkennung muss alle drei Jahre erneuert werden. Davon ausgehend, dass mittelfristig jedes Jahr eine Anerkennung mit einer durchschnittlichen Gebühr von 50 000 Franken stattfindet, kann eine ebenso hohe jährliche Einnahme budgetiert werden.

Für die Dienstleistungen der Identitätsstelle werden Gebühren erhoben. Die Gebühreneinnahmen hängen stark von der Verbreitung der E-ID ab. Die Gebühren für die Abfrage der Personenidentifizierungsdaten durch den IdP werden rund 26 Rappen betragen (Abruf niedrig: 1× pro Jahr, substanziell: 1× pro Quartal, hoch 1× pro Woche). Dies ergibt im Mix Gebühreneinnahmen von rund 1 Franken pro E-ID und Jahr, dies unter der Annahme, dass 24 Prozent das Sicherheitsniveau *«niedrig»*, 75 Prozent das Sicherheitsniveau *«substanziell»* und 1 Prozent das Sicherheitsniveau *«hoch»* nutzen. Weiter geht das Szenario davon aus, dass die Erstübermittlung der Attribute kostenlos erfolgt, da die IdP ihre E-ID ebenfalls kostenlos abgeben.

Zusammengefasst ergibt sich folgendes Bild:

| Aufwand | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 |
|---|---|---|---|---|---|---|---|
| Personalkosten | 1 400 000 | 1 400 000 | 1 400 000 | 1 400 000 | 1 400 000 | 1 400 000 | 1 400 000 |
| IKT-Betriebskosten | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 | 1 000 000 |
| Total Aufwand | 2 400 000 | 2 400 000 | 2 400 000 | 2 400 000 | 2 400 000 | 2 400 000 | 2 400 000 |
| **Ertrag** | | | | | | | |
| Anzahl E-ID | – | 400 000 | 800 000 | 1 200 000 | 1 600 000 | 2 000 000 | 2 400 000 |
| Ertrag aus Anerkennung | 50 000 | 50 000 | 50 000 | 50 000 | 50 000 | 50 000 | 50 000 |
| Ertrag aus Datenübermittlung | – | 400 000 | 800 000 | 1 200 000 | 1 600 000 | 2 000 000 | 2 400 000 |
| Total Ertrag | 50 000 | 450 000 | 850 000 | 1 250 000 | 1 650 000 | 2 050 000 | 2 450 000 |
| **Erfolg** | –2 350 000 | –1 950 000 | –1 550 000 | –1 150 000 | –750 000 | –350 000 | 50 000 |

Das Vorhaben generiert für sich isoliert betrachtet voraussichtlich nach rund sechs Jahren schwarze Zahlen. Sollte die Verbreitung der E-ID wesentlich schneller vonstatten gehen, etwa da ein IdP mit einem grossen Kundenstamm die Anerkennung erlangt, wird dieser Punkt deutlich rascher erreicht.

Die Kostenneutralität der E-ID kann aber nicht isoliert auf das E-ID-Projekt betrachtet werden. Zusätzliche Kostenvorteile und Einsparungen werden insbesondere im Zusammenhang mit der weitergehenden Digitalisierung der Verwaltungsabläufe beim Bund, den Kantonen und den Gemeinden erzielt werden. Diese zum jetzigen Zeitpunkt nicht quantifizierbare Kostenersparnis muss für eine korrekte Kosten-Nutzen-Gesamtbetrachtung der Erfolgsrechnung der E-ID angerechnet werden. Eine aussagekräftige Kosten-Nutzen-Rechnung ist deshalb erst einige Jahre nach der Einführung der E-ID unter Einbezug aller am E-ID-Ökosystem Beteiligten möglich. Erst dann wird sich zeigen, wie viele Betreiberinnen von E-ID-verwendenden Diensten sich auf die E-ID abstützen und auf eine eigene kostenintensive Identitätsmanagement-Lösung verzichten.

## 3.2 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 möglich, aber nur nach Eingabe eines Passwortes, das auf dem Postweg zugestellt wird und mit Einsendung eines handschriftlich unterschrie-

benen 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.

Der Finanzbedarf für allfällige Anpassungen der E-Government-Lösungen, die von Kantonen, Städten oder Gemeinden angeboten werden, ist schwer abzuschätzen. Je nach Art der IT-Lösung ist die Einführung eines E-ID-basierten Identifizierungsprozesses mehr oder weniger aufwendig. Es ist jedoch vorgesehen, dass die Kantone, Städte und Gemeinde, die einen E-ID-verwendenden Dienst betreiben, die Kosten für die Nutzung der vom IdP weitergebenen Identifizierungsdaten übernehmen. Die Kantone, Städte und Gemeinde werden dank der Einführung eines E-ID-Identifizierungsprozesses aber auch Ersparnisse erzielen, die diese Kosten aufwiegen.

## 3.3 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.

## 3.4 Auswirkungen auf die Gesellschaft

Die sichere Identifizierung 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 las-

sen 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 könnte in vielen Fällen die Notwendigkeit entfallen, den Namen, Vornamen und das Geburtsdatum offenzulegen. Die E-ID-Registrierungsnummer wäre 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.

### 3.5 Auswirkungen auf die Umwelt

Die Vorlage hat keine direkten Auswirkungen auf die Umwelt. Grundsätzlich sollte ein vermehrter Wechsel von physischer zu elektronischer Abwicklung von Geschäften per Saldo Ressourcen einsparen und sich entsprechend vorteilhaft für die Umwelt auswirken. So können zum Beispiel persönliche Vorsprachen und die damit verbundenen Belastungen der Verkehrsinfrastruktur und Emissionen vermieden werden.

### 3.6 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.

## 4 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[45] zur Legislaturplanung 2015–2019 und im Bundesbeschluss vom 14. Juni 2016[46] 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

45 BBl **2016** 1105, hier 1171 und 1222
46 BBl **2016** 5183, hier 5185

Schweiz» 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 Identifizierungsmittel 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 setzt im Schwerpunktplan die Etablierung einer national und international gültigen elektronischen Identität als operatives Ziel. 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.

# 5 Rechtliche Aspekte

## 5.1 Verfassungsmässigkeit

Die Kompetenz zur Regelung von E-ID ergibt sich 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.

Des Weiteren müssen marktmächtige IdP mit einer marktbeherrschenden Stellung sicherstellen, dass sie den berechtigten Personen die E-ID zu denselben Bedingungen anbieten wie breiten Bevölkerungskreisen. Damit dient die Vorlage der Bekämpfung volkswirtschaftlich schädlicher Auswirkungen der Tätigkeit bestimmter bedeutender, namentlich marktmächtiger IdP. Denn die Vorlage unterstellt deren E-ID-Angebot Bedingungen und bildet einen Rahmen für deren Tätigkeit. Die Vorlage stützt sich folglich auf Artikel 96 Absatz 1 BV, der dem Bund die Kompetenz verleiht, Vorschriften gegen volkswirtschaftlich oder sozial schädliche Auswirkungen von Kartellen und anderen Wettbewerbsbeschränkungen zu erlassen.

Das vorliegende Gesetz enthält Bestimmungen zur Gewährleistung, dass die berechtigten Personen besser Zugang zu einer E-ID erhalten. Er umfasst auch ein System für die Anerkennung, Beaufsichtigung und Sanktionierung der IdP. Damit dient die Vorlage dem verstärkten Konsumentenschutz. Demnach stützt sie sich auf Artikel 97 Absatz 1 BV, der dem Bund die Kompetenz zuweist, Massnahmen zum Schutz der Konsumentinnen und Konsumenten zu treffen.

Soweit die Vertragsverhältnisse zwischen den Identitätsdienstleistern, Inhaberinnen und Inhabern sowie Betreiberinnen von E-ID-verwendenden Diensten betroffen sind, werden im vorliegenden Bundesgesetz zivilrechtliche Aspekte geregelt. Da diesem Aspekt keine zentrale Bedeutung zukommt, wird auf die Aufführung der von

Artikel 122 Absatz 1 BV, der dem Bund die Kompetenz zur Regelung des Zivilrechts gibt, verzichtet.

## 5.2 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. Zum Umsetzung wären Staatsverträge notwendig.

## 5.3 Erlassform

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

## 5.4 Unterstellung unter die Ausgabenbremse

Da die Vorlage neue wiederkehrende Ausgaben von mehr als 2 Millionen Franken nach sich zieht, bedarf sie der Zustimmung der Zustimmung der Mehrheit der Mitglieder beider Räte nach Artikel 159 Absatz 3 Buchstabe b der Bundesverfassung.

## 5.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Die Einführung der E-ID ist unumstritten. Die vorgesehene Aufgabenteilung und Aufgabenerfüllung tangiert weder das Subsidiaritätsprinzip noch das Prinzip der fiskalischen Äquivalenz. Die finanziellen Auswirkungen auf Bund oder Kantone beträgt weniger als 10 Millionen Franken. Die beiden genannten Prinzipien sind von der Vorlage nicht betroffen.

## 5.6 Einhaltung der Grundsätze des Subventionsgesetzes

Das E-ID-Gesetz sieht keine Finanzhilfen oder Abgeltungen vor. Die Umsetzung der Vorlage soll auf dem freien Markt geschehen. Entsprechende Geschäftsmodelle sind bereits vorhanden. Auf weitere Ausführungen wird deshalb verzichtet.

## 5.7 Delegation von Rechtssetzungsbefugnissen

*Verfahren zur Überprüfung der Identität und der Ausweise*

Der Bundesrat legt auf Verordnungsstufe die Verfahren fest für die Überprüfung der Ausweise von Schweizerinnen und Schweizern und für die Überprüfung der Ausweise sowie der Identität von Ausländerinnen und Ausländern. Der Zweck dieser Verfahren besteht darin, die spezifische Situation der betroffenen Personen im Einzelfall beurteilen zu können. Der Bundesrat wird damit nicht ermächtigt, bestimmte Personenkategorien auszuschliessen. Vielmehr soll er Verfahren einführen können, mit denen im Einzelfall objektiv überprüft werden kann, ob die betreffende Person zuverlässig identifiziert werden kann und ob sie die Voraussetzungen für eine E-ID erfüllt. Die entsprechende Kompetenz findet sich in Artikel 3 Absatz 2 BGEID.

*Technische und organisatorische Vorgaben*

Um möglichst zeitnah auf technische Entwicklungen reagieren zu können, werden die Voraussetzungen für die Prozesse (Anerkennung von IdP und Sicherheitsniveaus) und technische Vorgaben und Standards auf Verordnungs- und Weisungsebene geregelt.

Nach Artikel 4 Absatz 4 regelt der Bundesrat die verschiedenen Sicherheitsniveaus, insbesondere die Mindestanforderungen an die Identifizierung; er berücksichtigt dabei den jeweiligen Stand der Technik.

Artikel 6 Absatz 5 verleiht dem Bundesrat die Kompetenz, nähere Vorschriften zum E-ID-Ausstellungsprozess sowie zu den für die Identifizierung zu verwendenden Personenidentifizierungsdaten zu erlassen. Aufgrund der Komplexität und des Detaillierungsgrads der zu regelnden Materie sind diese eher in einer Verordnung als in einem Gesetz zu regeln. Ausserdem wird der Bundesrat, ebenfalls per Verordnung, nähere Vorschriften zu den E-ID-Ausstellungsverfahren für Personen erlassen, die eine gültige und gemäss Artikel 29 bundesrechtskonforme Identifizierungseinheit besitzen. 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 BGEID).

Voraussetzungen für die Anerkennung kann der Bundesrat aufgrund von Artikel 13 Absatz 4 insbesondere in Bezug auf die fachlichen und sicherheitsbezogenen Anforderungen und deren Überprüfung, die notwendige Versicherungsdeckung (bzw. zu den gleichwertigen finanziellen Sicherheiten), die auf die E-ID-Systeme anwendbaren Standards und technischen Protokollen sowie die regelmässige Überprüfung dieser Systeme regeln. 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.

Adressat einer Verordnung über die neuesten anwendbaren Standards und technischen Protokolle für die Übermittlung der Personenidentifizierungsdaten ist fedpol.

Für den Fall, dass verschiedene Personenregister abweichende Daten liefern, regelt der Bundesrat das Vorgehen zur Bereinigung (Art. 23 Abs. 3 BGEID).

Schliesslich wird der Bundesrat gestützt auf Artikel 24 Absatz 4 die technischen und organisatorischen Massnahmen zur sicheren Bearbeitung und Weitergabe der Personenidentifizierungsdaten festlegen. Die Massnahmen müssen rasch an die technischen Entwicklungen angepasst werden können. Es ist deshalb sinnvoller, sie in einer Verordnung zu regeln.

*Subsidiäres E-ID-System des Bundes*

Falls sich kein IdP findet, der für die Ausstellung von E-ID der Sicherheitsniveaus substanziell oder hoch anerkannt ist, kann der Bundesrat eine Verwaltungseinheit beauftragen, die ein E-ID-System für dieses Sicherheitsniveau betreibt und E-ID ausstellt (Art. 10 Abs. 1).

*Haftpflichtrechtliche Schutznormen für Inhaberinnen und Inhaber*

Der Bundesrat kann die einzuhaltenden Sorgfaltspflichten für Inhaberinnen und Inhaber einer E-ID (Art. 12 Abs. 3 BGEID) sowie die Sperrung und den Widerruf einer E-ID (Art. 11 Abs. 5 BGEID) 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 27.

## 5.8 Datenschutz

### 5.8.1 Allgemeine Anmerkungen

Das Gesetz hat auch den Zweck, in seinem Regelungsbereich den Datenschutz zu fördern. Artikel 1 Absatz 2 Buchstabe b übernimmt den Zweckartikel des DSG. Die Regeln des Datenschutzrechts (DSG und die zugehörigen Verordnungen) gelten für alle Beteiligten. Insbesondere unterstehen IdP und Betreiberinnen von E-ID-Diensten den Vorschriften, die Privatpersonen betreffen. Fedpol und ISB unterstehen den Bestimmungen, die für Bundesorgane gelten. Aus Gründen der Transparenz werden im vorliegenden Gesetz bestimmte Anforderungen des DSG übernommen und präzisiert. In einigen Fällen geht das Gesetz über diese Anforderungen hinaus und verschärft sie.

In Bezug auf das Einwilligungserfordernis werden ausdrückliche Regelungen im Gesetz eingefügt. Zudem wird die Bearbeitung der staatlich bestätigten Personenidentifizierungsdaten eingeschränkt. IdP dürfen sie nur bearbeiten, um Identifizierungen nach diesem Gesetz zu erbringen (Art. 9 Abs. 1 BGEID). Im Übrigen dürfen Personenidentifizierungsdaten, die Daten, die bei der Anwendung der E-ID entstehen, und darauf basierende Nutzungsprofile nicht bekannt gegeben werden (Art. 16 Abs. 2 BGEID).

### 5.8.2 Einwilligung in die Übermittlung

Überall, wo Personenidentifizierungsdaten im Spiel sind, müssen die Voraussetzungen des Datenschutzes eingehalten bzw. erforderlichen Sicherheitsvorkehrungen getroffen werden. Die Inhaberinnen und Inhaber der E-ID geben jeweils ihr ausdrückliches Einverständnis zur Übermittlung von Personenidentifizierungsdaten. Bei Ausstellung der E-ID wird der IdP ermächtigt, die Daten bei fedpol abzurufen (Art. 6 Abs. 2 Bst. c BGEID) und bei der Anwendung bei einem E-ID-verwendenden Dienst wird in jedem Einzelfall das Einverständnis der Inhaberin oder des Inhabers zur Übermittlung der Daten durch den IdP an die Betreiberin von E-ID-verwendenden Diensten eingeholt (Art. 16 Abs. 1 Bst. c BGEID).

### 5.8.3 Trennung von Personenidentifizierungsdaten und Nutzungsdaten

Das vorliegende Gesetz umfasst spezifische Sicherheitsmassnahmen, die in Bezug auf die Gewährleistung der Datensicherheit über die Anforderungen des DSG hinausgehen. Artikel 9 Absatz 3 verlangt, dass der IdP die Personenidentifizierungsdaten nach Artikel 5, die Daten zur Nutzung der E-ID und die übrigen Daten getrennt voneinander hält. Die physische und organisatorische Trennung nach Datenkategorie und Bearbeitungszweck stellt eine zusätzliche Sicherheitsmassnahme dar, mit der verhindert wird, dass Unbefugte auf alle Daten über die Inhaberin oder den Inhaber einer E-ID zugreifen können. Dadurch sollen namentlich die negativen Folgen eines unbefugten Zugangs zum System beschränkt werden. Mit der Trennung kann gewährleistet werden, dass die Daten der einen Kategorie auch dann sicher sind, wenn die Sicherheit einer anderen Kategorie kompromittiert ist.

### 5.8.4 Zugang zu Personenidentifizierungsdaten und Nutzungsdaten

Mit dem vorliegenden Gesetz soll dem Grundsatz in Artikel 4 Absatz 4 DSG, wonach der Zweck der Bearbeitung von Personendaten erkennbar sein muss, sowie dem Anspruch auf Auskunft über die Bearbeitung von Personendaten nach Artikel 8 DSG Nachachtung verschafft werden. Gemäss Artikel 15 Absatz 1 Buchstabe i des vorliegenden Gesetzes gewährt der IdP der Inhaberin oder dem Inhaber der E-ID online Zugang zu den Daten, die bei der Anwendung der E-ID entstehen, sowie zu deren oder dessen Personenidentifizierungsdaten nach Artikel 5. Gleichzeitig soll diese Massnahme zur erhöhten Transparenz des E-ID-Systems beitragen und das Vertrauen der Nutzerinnen und Nutzer in den E-ID-Ausstellungsprozess stärken.

### 5.8.5 Zweck und Einschränkungen

Der Zweck und die Voraussetzungen für die Bearbeitung, Haltung und Weitergabe der Daten sind im vorliegenden Gesetz streng geregelt. Artikel 9 Absatz 1 hält namentlich fest, dass der IdP die von fedpol übermittelten Personenidentifizierungsdaten nur bearbeiten darf, bis die E-ID widerrufen wird, und dies nur für Identifizierungen nach dem vorliegenden Gesetz. Nach Artikel 16 Absatz 1 darf der IdP Betreiberinnen von E-ID-verwendenden Diensten ferner nur die Personenidentifizierungsdaten weitergeben, die dem geforderten Sicherheitsniveau entsprechen, die für die Identifizierung der betreffenden Person im Einzelfall notwendig sind und in deren Übermittlung die Inhaberin oder der Inhaber der E-ID eingewilligt hat. Für die im Informationssystem von fedpol gespeicherten Gesichtsbilder gelten ausserdem besondere Regeln. Für E-ID des Sicherheitsniveaus substanziell dürfen sie nur während des Ausstellungsprozesses verwendet werden. Sie dürfen überdies ausschliesslich den E-ID des Sicherheitsniveaus hoch zugeordnet werden.

Die Datenübermittlung nach dem vorliegenden Gesetz ist erforderlich, damit das E-ID-System seine Funktion erfüllen kann und die Ansprüche der Nutzerinnen und Nutzer an den Komfort, die Flexibilität und Einfachheit erfüllt werden können. Dabei wird der Grundsatz der Verhältnismässigkeit gewahrt, denn die vorgesehene Beeinträchtigung der Privatsphäre geht nicht über das hinaus, was für die Erfüllung dieses Zwecks nötig ist. Bei den übermittelten Personendaten handelt es sich im Übrigen nicht um besonders schützenswerte Daten im Sinne von Artikel 3 Buchstabe c DSG.

Nach den Artikeln 17 Absatz 1 und 19 Absatz 1 DSG dürfen Organe des Bundes Personendaten nur bearbeiten und bekannt geben, wenn dafür eine gesetzliche Grundlage besteht. In Anwendung der Artikel 3 Buchstabe i und 4 Absätze 3 und 4 DSG muss der Zweck des vorgesehenen Systems genau bestimmt werden und für die betroffenen Personen erkennbar sein. Dementsprechend umfasst das vorliegende Gesetz genaue Bestimmungen, die fedpol die Führung eines Informationssystems für die Identifizierung der antragstellenden Personen erlauben. In Artikel 24 werden die Art, der Inhalt und der Zweck des Systems bestimmt. Nach Artikel 24 Absatz 1 enthält das System folgende Daten: die Protokolldaten des E-ID-Ausstellungsprozesses nach Artikel 6 Absatz 5, die Personenidentifizierungsdaten nach Artikel 5 sowie deren Herkunft und Angaben zu deren Aktualisierung und die AHV-Versichertennummern. Artikel 24 Absatz 2 hält fest, welche Zwecke mit dem System verfolgt werden. Das Informationssystem dient: der Entgegennahme der Anträge und Einverständniserklärungen der antragstellenden Person, der automatisierten Erfüllung der Aufgaben von fedpol bei der Ausstellung von E-ID, der Aktualisierung der Personenidentifizierungsdaten nach Artikel 7 sowie der Prüfung der Gültigkeit einer E-ID-Registrierungsnummer nach Artikel 23 Absatz 2.

### 5.8.6 Verbot der Handelbarkeit von Daten

Der Verkauf der im Rahmen des vorliegenden Gesetzes bearbeiteten, gehaltenen und weitergegebenen Daten ist streng beschränkt. Nach Artikel 16 Absatz 3 darf der IdP

die Personenidentifizierungsdaten nach Artikel 5, die Daten, die bei einer Anwendung der E-ID entstehen und darauf basierende Nutzungsprofile nicht bekannt geben. Das Verbot gilt unabhängig vom Sicherheitsniveau der E-ID. Die Daten nach dem vorliegenden Gesetz dürfen folglich nicht Dritten verkauft werden.

Aus diesem Verbot der Handelbarkeit ergibt sich ein verminderter wirtschaftlicher Wert der staatlich bestätigten Personenidentifizierungsdaten. Diese Daten werden deshalb ausdrücklich als nicht pfändbar und von der Konkursmasse ausgenommen erklärt (Art. 14 Abs. 1 BGEID). Um den Fortbestand eines E-ID-Systems nach diesem Gestz und den dazugehörigen E-ID im Fall der finanziellen Krise eines IdP zu sichern, können jedoch solche E-ID-Systeme als Ganzes an andere anerkannte IdP verkauft werden. Der Kaufbetrag fällt dann allenfalls in die Konkursmasse (Art. 14 Abs. 3 BGEID).

## Glossar

| Begriff | Definition |
|---|---|
| Authentifizierung<br>f=authentification<br>i=autentificazione | Prozess der Überprüfung einer behaupteten Identität bei der Verwendung einer E-ID.<br>Hier beweist zum Beispiel eine Inhaberin einer E-ID gegenüber dem IdP, wer sie wirklich ist. Zuerst muss sie sich identifizieren, indem sie dem System Ihren Benutzernamen mitteilt und dann diesen authentifizieren, indem sie dem System das zugehörige Passwort schickt und dieses überprüfen kann, ob sie wirklich die Person ist, als die sie sich ausgibt. |
| Anerkennungsverfahren<br>f=procédure de reconnaissance<br>i=procedura di riconoscimento | In diesem Verfahren werden IdP und ihre E-ID-Systeme durch eine Bundesstelle anerkannt, wenn diese die fachlichen, organisatorischen, technischen sowie sicherheitsbezogenen Voraussetzungen erfüllen. Die Anerkennung wird in regelmässigen Abständen kontrolliert und erneuert. |
| Anerkennungsstelle<br>f=organisme de reconnaissance<br>i=servizio di riconoscimento | Das Informatiksteuerungsorgan des Bundes (ISB) ist gemäss vorliegendem Erlass die Anerkennungsstelle. Es ist insbesondere zuständig für die Entgegennahme und Prüfung der Gesuche um Anerkennung von IdP und deren E-ID-Systemen. |
| anerkannte elektronische Identifizierungseinheit (E-ID)<br>f=moyen d'identification électronique reconnu (e-ID)<br>i=mezzo d'identificazione elettronica riconosciuto | Eine elektronische Identifizierungseinheit, die von einem IdP nach den Vorgaben dieses Gesetzes ausgestellt wird. Trägermittel einer E-ID können z.B. Smartphones oder Chipkarten sein. |
| Betreiberin von E-ID-verwendenden Diensten<br>f=exploitant d'un service utilisateur<br>i=gestori di servizi che utilizzano l'eID | Natürliche oder juristische Person, die für ihre Tätigkeit einen oder mehrere Online-Dienste betreibt, die Vertrauen in die Identität der sie nutzenden Person und in deren Authentizität voraussetzen. Englische Bezeichnung: Relying party. |

| Begriff | Definition |
|---|---|
| eIDAS-Verordnung<br>f=règlement eIDAS<br>i=regolamento eIDAS | Verordnung der EU über elektronische Identifizierung und Vertrauensdienste (electronic IDentification, Authentication and trust Services). Diese bezweckt die Interoperabilität von Identifizierungssystemen und vereinfacht die Identifizierung für grenzüberschreitende Abwicklung von Verwaltungsdienstleistungen auf europäischer Ebene erheblich. |
| E-ID-Registrierungsnummer<br>f=numéro d'enregistrement de l'e-ID<br>i=numero di registrazione eID | Einer Person eindeutig zugeordnete Identifikationsnummer. |
| E-ID-System<br>f=système e-ID<br>i=sistema di eID | Elektronisches System für die Ausstellung, Verwaltung und Anwendung von E-ID. |
| E-ID-verwendender Dienst<br>f=service utilisateur<br>i=servizi che utilizzano l'eID | Eine Informatikanwendung, die ein E-ID-System zur Identifizierung und Authentifizierung nutzt. |
| elektronische Identifizierungseinheit<br>f=moyen d'identification électronique<br>i=mezzo d'identificazione elettronica | eine elektronische Einheit, die zur Identifizierung und Authentifizierung einer natürlichen Person verwendet wird |
| Identity and Access Management (IAM)<br>f=gestion des identités et des accès (GIA)<br>i= Identity and Access Management (IAM) | Alle Prozesse und Anwendungen, die für die Administration von Identitäten und die Verwaltung von Zugriffsrechten auf verschiedene Applikationen, Systeme und Ressourcen zuständig sind. |
| Identity Provider (IdP)<br>f=fournisseur d'identité<br>i= fornitori di servizi d'identificazione elettronica (*identity provider; IdP)* | Nach diesem Gesetz anerkannte Anbieterin von Identitätsdienstleistungen. |

| Begriff | Definition |
|---|---|
| Identitätsstelle<br>f=service d'identité<br>i=servizio delle identità | Das Bundesamt für Polizei fedpol ist gemäss vorliegende Erlass die Identitätsstelle. Es ist insbesondere zuständig für die Überprüfung der Angaben der antragstellenden Personen bei der Identifizierung. |
| Identifizierung<br>f=identification<br>i=identificazione | Prozess der Feststellung der Identität einer Person mit Hilfe von Personenidentifizierungsdaten, die diese Person eindeutig repräsentieren. |
| Interoperabilität<br>f=interopérabilité<br>i=interoperabilità | Die Fähigkeit zur Zusammenarbeit von verschiedenen Systemen, Techniken oder Organisationen. Dazu ist in der Regel die Einhaltung gemeinsamer Standards notwendig. Mobilfunksysteme funktionieren z.B. interoperabel. |
| Personenstandsregister (Infostar)<br>f=registre de l'état civil (Infostar)<br>i=registro informatizzato dello stato civile (Infostar) | Ein elektronisches Personenstandsregister, in welchem alle Zivilstandsereignisse beurkundet werden. Alle schweizerischen Zivilstandsämter sind an Infostar angeschlossen. |
| Informationssystem Ausweisschriften (ISA)<br>f= système d'information relatif aux documents d'identité (ISA)<br>i=servizio d'informazione per documenti d'identità (ISA) | Die bei der Ausstellung eines Ausweises von Schweizer Bürgerinnen und Bürger erfassten Daten sind im ISA gespeichert. |
| National Institute of Standards and Technology (NIST) | Eine Bundesbehörde der Vereinigten Staaten, die zur technologischen Administration des Handelsministeriums gehört und für Standardisierungsprozesse zuständig ist. |
| Ordipro | Ein Informationssystem des Eidgenössischen Departements für auswärtige Angelegenheiten. Ordipro dient insbesondere als Grundlage für die administrative Abwicklung der Akkreditierung und der Ausstellung und Verwaltung der verschiedenen Kategorien von Legitimationskarten für begünstigte Personen nach Artikel 2 Absatz 2 des Gaststaatgesetzes vom 22. Juni 2007 (SR 192.12). |

| Begriff | Definition |
|---|---|
| Personenidentifizierungsdaten<br>f=données d'identification personnelle<br>i=dati d'identificazione personale | Staatlich geführter Datensatz in Infostar, ISA, ZEMIS und Ordipro, der es ermöglicht, die Identität einer Person festzustellen. |
| SuisseID | Eine vom SECO konzipierte elektronische Identifizierungseinheit (basierend auf einer Chipkarte oder einem USB-Stick). Mit der SuisseID können elektronische Dienstleistungen in Anspruch genommen werden, die eine sichere Identifizierung der Nutzerinnen und Nutzer voraussetzen, und eine rechtsgültige elektronische Unterschrift auf einem Dokument angebracht werden. |
| SwissID | Eine elektronische Identifizierungseinheit von SwissSign. Bei der Entwicklung der SwissID wurden die Erfahrungen genutzt, die mit der SuisseID gemacht wurden. Der neue Service wird nach und nach aufgebaut – mittelfristig wird die SuisseID durch die SwissID abgelöst. |
| Unique Person Identification (ZAS-UPI)<br>f=(CdC-UPI)<br>i=(UCC-UPI) | Mit dieser Funktionalität erfolgt die Identifikation der natürlichen Personen und die Verwaltung des Identifikators AHVN13 im zentralen Versichertenregister der Sozialversicherungen des Bundes. |
| Zentrales Migrationsinformationssystem (ZEMIS)<br>f=système d'information central sur la migration (SYMIC)<br>i=sistema d'informazione centrale sulla migrazione (SIMIC) | Ein Informationssystem des Staatssekretariats für Migration SEM. In ZEMIS werden Personendaten aus dem Ausländer- und Asylbereich bearbeitet. |