



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

Bern, Juni 2022

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise

(E-ID-Gesetz, BGEID)

**Erläuternder Bericht
zur Eröffnung des Vernehmlassungsverfahrens**

Inhaltsverzeichnis

Übersicht	3
Erläuternder Bericht	4
1 Ausgangslage	4
1.1 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates	4
1.2 Erledigung parlamentarischer Vorstösse	5
2 Rechtsvergleich, insbesondere mit dem europäischen Recht	5
3 Grundzüge der Vorlage	5
3.1 Beantragte Neuregelung	5
3.2 Abstimmung von Aufgaben und Finanzen	6
3.3 Umsetzung	6
4 Erläuterungen zu den einzelnen Artikeln	6
5 Auswirkungen	20
5.1 Finanzielle und personelle Auswirkungen auf den Bund	20
5.2 Auswirkungen auf die Kantone und Gemeinden	20
5.3 Auswirkungen auf die Volkswirtschaft	21
5.4 Auswirkungen auf die Gesellschaft	21
6 Rechtliche Aspekte	22
6.1 Verfassungsmässigkeit	22
6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz	22
6.3 Erlassform	22
6.4 Unterstellung unter die Ausgabenbremse	22
6.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz	23
6.6 Delegation von Rechtssetzungsbefugnissen	23
6.7 Datenschutz	23

Übersicht

Die Digitalisierung der Gesellschaft schreitet voran. Die Möglichkeit, sich zu identifizieren, stellt eine wichtige Säule dieses Wandels dar. Mit diesem Vorentwurf soll für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises ein staatlicher elektronischer Identitätsnachweis (E-ID) eingeführt werden, der auf einer vom Bund betriebenen Infrastruktur beruht. Diese Infrastruktur ermöglicht, ganz unterschiedliche elektronische Nachweise zu erstellen und zu verwalten und so deren Verbreitung und Verwendung zu fördern. Gleichzeitig erlaubt sie, die Entwicklungen auf europäischer und internationaler Ebene zu verfolgen und die Anforderungen an den Schutz der Personendaten einzuhalten.

Ausgangslage

Am 7. März 2021 wurde das Bundesgesetz über elektronische Identifizierungsdienste (BGEID)¹ mit knapp 65 Prozent Nein-Stimmen deutlich abgelehnt. Am 10. März 2021 wurden in der Frühlingssession der Eidgenössischen Räte von Vertreterinnen und Vertretern aller Fraktionen sechs inhaltlich identische Motionen eingereicht, mit denen eine vertrauenswürdige staatliche E-ID verlangt wurde (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129).

Am 26. Mai 2021 beauftragte der Bundesrat das Eidgenössische Justiz- und Polizeidepartement (EJPD), zusammen mit dem Eidgenössischen Finanzdepartement (EFD) und der Bundeskanzlei (BK) die Arbeiten zur Schaffung eines staatlichen elektronischen Identitätsnachweises (E-ID) rasch an die Hand zu nehmen. In einem ersten Schritt hat das EJPD unter Einbezug von Spezialisten aus Kantonen und Wissenschaft ein Diskussionspapier erarbeitet. Diese Auslegeordnung sieht drei technische Lösungsansätze vor und legt insbesondere auch deren Einbettung ins wirtschaftliche und gesellschaftliche Umfeld dar und beleuchtet verschiedene Einsatzmöglichkeiten einer staatlichen E-ID.

Vom 2. September bis am 14. Oktober 2021 fand dazu eine informelle öffentliche Konsultation statt. Es gingen sechzig Stellungnahmen von Privatpersonen, kantonalen Verwaltungen, Wissenschaft, Wirtschaftsorganisationen und Firmen ein. Am 14. Oktober 2021 organisierte das EJPD zum Abschluss der Konsultation eine Konferenz mit einer öffentlichen Diskussion, an der fünfzig Vertreterinnen und Vertreter von Kantonen, Politik, Wissenschaft, Zivilgesellschaft und Wirtschaft sowie interessierte Privatpersonen teilnahmen.

Die Konsultationsteilnehmenden sprachen sich für einen Self-Sovereign-identity-Ansatz (SSI) aus. Sie waren zudem der Ansicht, dass mit einer umfassenden Vertrauensinfrastruktur die Ausstellung und Verwendung unterschiedlicher elektronischer Nachweise möglich ist. Dieses Vorgehen steht im Einklang mit den Forderungen der Motionen, die im Nationalrat am 14. September 2021 und im Ständerat am 13. Juni 2022 angenommen wurden. Im Rahmen der künftigen Arbeiten ist es angezeigt, diesem Willen sowie den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung Rechnung zu tragen. Zudem möchte das EJPD enger mit den Ämtern und Kantonen zusammenarbeiten, die in diesem Bereich entsprechende Pilotprojekte durchführen.

Am 17. Dezember 2021 hat der Bundesrat gestützt auf die Ergebnisse dieser Konsultation einen Richtungsentscheid getroffen und die Grundsätze für die Ausgestaltung eines künftigen staatlichen Identitätsnachweises festgelegt.

Nutzerinnen und Nutzer der E-ID sollen grösstmögliche Kontrolle über ihre Daten haben (Self-Sovereign Identity). Der Datenschutz wird unter anderem durch das System selber (Grundsatz des Schutzes der Privatsphäre durch Technik), aber auch durch die Beschränkung der nötigen Datenflüsse auf das Minimum (Prinzip der Datensparsamkeit) sowie eine dezentrale Datenspeicherung gewährleistet.

Die E-ID soll auf einer staatlich betriebenen Infrastruktur beruhen, die nicht nur zur Ausstellung der E-ID verwendet werden soll, sondern staatlichen und privaten Stellen auch zur Verfügung gestellt werden kann, um andere elektronische Nachweise, wie Strafregisterauszüge, Führerausweise, Hochschuldiplome oder ärztliche Rezepte, auszustellen. Der Ausbau dieses Ökosystem der elektronischen Nachweise kann schrittweise erfolgen.

Inhalt der Vorlage

Der Vorentwurf sieht für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises die Einführung eines staatlichen elektronischen Identitätsnachweises vor. In diesem Rahmen überprüft der Staat die Identität der antragstellenden Person und stellt ihr einen elektronischen Identitätsnachweis aus. Die neue Vorlage verfolgt einen Ansatz, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung beruht. Der Bezug und die Verwendung der E-ID bleiben freiwillig.

Zudem soll mit dem Vorentwurf eine umfassende staatliche Vertrauensinfrastruktur geschaffen werden, die es den Akteuren des öffentlichen und privaten Sektors ermöglicht, elektronische Nachweise zu verwenden und interessierten Personen solche auszustellen. In diesem Rahmen wird der Staat eine staatliche elektronische Brieftasche anbieten, die die E-ID und weitere elektronische Nachweise enthalten kann. Die Inhaberinnen und Inhaber der Brieftasche können ihre E-ID und andere elektronische Nachweise sicher und transparent beantragen, beziehen und vorweisen. Mit einer solchen Öffnung des Systems kann eine grössere Verbreitung und eine häufigere Nutzung der elektronischen Nachweise sichergestellt werden. Der Vorentwurf 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. Er sieht auch die Kompetenz für den Bundesrat vor, internationale Abkommen abzuschliessen um eine internationale Anerkennung der E-ID zu erreichen und ausländische E-ID in der Schweiz zu anerkennen.

¹ BBl 2019 6567

Erläuternder Bericht

1 Ausgangslage

Am 7. März 2021 wurde das Bundesgesetz über elektronische Identifizierungsdienste an der Urne mit 64 Prozent Nein-Stimmen abgelehnt. Am 10. März 2021 sind sechs inhaltlich identische Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» von allen Fraktionen eingereicht worden (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129). Zudem wurden innerhalb von drei Monaten nach der Abstimmung die Interpellation 21.3310 Andrey «Identitätskarte als Teil einer zukünftigen E-ID-Lösung» und die Interpellation 21.3718 Graf-Litscher «Selbstbestimmte elektronische Identitäten» eingereicht. Die sechs Motionen wurden am 14. September 2021 im Erstrat angenommen und die Diskussion über die Interpellation 21.3310 Andrey wurde verschoben. Zudem hat der Nationalrat beschlossen, die Interpellation 21.3718 Graf-Litscher zu erledigen.

An seiner Sitzung vom 26. Mai 2021 empfahl der Bundesrat dem Parlament, die sechs Motionen anzunehmen. Weiter erklärte er, dass er rasch eine neue Lösung für den elektronischen Identitätsnachweis vorlegen wolle, der den Anliegen der Motionärinnen und Motionären Rechnung trägt. Er hat daher das EJPD beauftragt, bis Ende Jahr zusammen mit dem Eidgenössischen Finanzdepartement (EFD) und der Bundeskanzlei (BK) und in enger Absprache mit den Kantonen und den beiden Eidgenössischen Technischen Hochschulen Zürich und Lausanne ein Grobkonzept zu erarbeiten. Es geht insbesondere darum, die verschiedenen technischen Lösungsansätze für die E-ID zu prüfen und die jeweiligen Kosten zu beziffern.

Das EJPD hat das «Zielbild E-ID» (im Folgenden «Diskussionspapier») unter Einbezug der Kantone und der Wissenschaft erarbeitet. Diese Auslegeordnung enthält verschiedene Begriffsbestimmungen der E-ID und der entsprechenden Vertrauensinfrastruktur. Zudem werden drei technische Lösungsansätze präsentiert: Self-Sovereign Identity (SSI), Public-Key-Infrastruktur (PKI) und zentraler staatlicher Identitätsprovider (IdP). Die Auslegeordnung legt insbesondere auch deren Einbettung ins wirtschaftliche und gesellschaftliche Umfeld dar und beleuchtet verschiedene Einsatzmöglichkeiten einer staatlichen E-ID.

Vom 2. September bis am 14. Oktober 2021 fand dazu eine informelle öffentliche Konsultation statt. Es gingen sechzig Stellungnahmen von kantonalen Verwaltungen sowie von Vertreterinnen und Vertretern aus Wissenschaft, Wirtschaftsorganisationen und Firmen ein. Am 14. Oktober 2021 organisierte das EJPD zum Abschluss der Konsultation eine Konferenz mit einer öffentlichen Diskussion, an der fünfzig Vertreterinnen und Vertreter von Kantonen, Politik, Wissenschaft, Zivilgesellschaft und Wirtschaft sowie interessierte Privatpersonen teilnahmen. Die informelle öffentliche Konsultation hatte zum Ziel, die Meinungen zu den wichtigsten Anforderungen an eine E-ID, den wichtigsten Einsatzbereichen und den erwarteten Vorteilen zusammenzutragen. Zudem ging es darum, die Meinungen der interessierten Personen zum Umfang des E-ID-Ökosystems in Erfahrung zu bringen. Die zusammengetragenen Informationen erlaubten es dem Bundesrat, einen Grundsatzentscheid für die neue Stossrichtung der E-ID zu treffen.

Die Konsultationsteilnehmenden sprachen sich für einen Self-Sovereign-Identity-Ansatz (SSI) aus. Sie waren zudem der Ansicht, dass eine Vertrauensinfrastruktur mit einem Ambitionsniveau 3 (vgl. Diskussionspapier Kap. 4.2) erforderlich ist. Dieses Vorgehen steht im Einklang mit den Forderungen der Motionen, die im Nationalrat am 14. September 2021 und im Ständerat am 13. Juni 2022 angenommen wurden. Im Rahmen der künftigen Arbeiten ist es angezeigt, diesem Willen sowie den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung Rechnung zu tragen. Zudem möchte das EJPD enger mit den Ämtern und Kantonen zusammenarbeiten, die in diesem Bereich entsprechende Pilotprojekte durchführen.

Gestützt auf die Ergebnisse der informellen öffentlichen Konsultation hat der Bundesrat am 17. Dezember 2021 über die neue Stossrichtung der E-ID entschieden. Demnach soll die E-ID-Vorlage einen Ansatz verfolgen, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung sowie auf einer staatlichen Vertrauensinfrastruktur beruht, mit der ein Ökosystem für elektronische Nachweise eingeführt werden kann, die von Akteuren des öffentlichen und des privaten Sektors ausgestellt werden. Der Bundesrat hat die Frist für die Unterbreitung des Vorentwurfs für die Vernehmlassung um einen Monat verlängert. Ferner wurde dem EJPD, in Zusammenarbeit mit dem EFD (Digitale Verwaltung Schweiz DVS) und der BK (Digitale Transformation und IKT-Lenkung DTI), die Verantwortung für die Sicherstellung des Informationsflusses und für die Koordination der Abhängigkeiten zwischen dem Vorentwurf und verwandten Projekten von Bund und Kantonen übertragen.

1.1 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 zur Legislaturplanung 2015–2019² und im Bundesbeschluss vom 14. Juni 2016³ über die Legislaturplanung 2015–2019 angekündigt. Aufgrund der Ablehnung dieser Vorlage in der Abstimmung vom 7. März 2021 entschied der Bundesrat, die Gesetzgebungsarbeiten im Bereich der E-ID wiederaufzunehmen und neu auszurichten. Diese Vorlage wurde weder in der Botschaft vom 29. Januar 2020 zur Legislaturplanung 2019–2023⁴ noch im Bundesbeschluss vom 21. September 2020 über Legislaturplanung 2019–2023⁵ angekündigt.

² BBl 2016 1105

³ BBl 2016 5183

⁴ BBl 2020 1777

⁵ BBl 2020 8385

1.2 Erledigung parlamentarischer Vorstösse

Dieser Vorentwurf setzt die folgenden parlamentarischen Vorstösse um:

- Motionen aller Fraktionen 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129 «Vertrauenswürdige staatliche E-ID». Die Motionen verlangen, dass der Staat ein elektronisches Identifikationsmittel zum Nachweis der eigenen Identität (Authentifizierung) in der virtuellen Welt, vergleichbar mit Identitätskarte oder Pass in der physischen Welt, schafft. Dabei sollen insbesondere die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) eingehalten werden. Diese Motionen wurden im Nationalrat am 14. September 2021 gemäss dem Antrag des Bundesrates angenommen. Im Zweitrat wurden sie noch nicht behandelt.

Bei der Erarbeitung der Vorlage wurde auch folgenden parlamentarischen Vorstössen Rechnung getragen:

- Interpellation 21.3310 Andrey «Identitätskarte als Teil einer zukünftigen E-ID-Lösung». Der Bundesrat hat am 26. Mai 2021 die Fragen der Interpellation beantwortet. Die Diskussion wurde verschoben, da die Antworten nicht befriedigend waren.
- Interpellation Graf-Litscher 21.3718 «Selbstbestimmte elektronische Identitäten». Am 18. August 2021 hat der Bundesrat die Fragen beantwortet. Am 1. Oktober 2021 hat der Nationalrat beschlossen, die Interpellation zu erledigen.

2 Rechtsvergleich, insbesondere mit dem europäischen Recht

In der Europäischen Union sind im Bereich der E-ID Reformen im Gange. Der Bundesrat ist der Ansicht, dass diese Entwicklungen in die Überlegungen auf nationaler Ebene einbezogen werden sollten. Am 3. Juli 2021 verabschiedete die Europäische Kommission einen Vorschlag⁶ zur Änderung der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung)⁷ und zur Schaffung eines rechtlichen Rahmens für eine europäische digitale Identität. Im Rahmen dieser neuen Verordnung stellen die Mitgliedstaaten den Bürgerinnen und Bürgern sowie Unternehmen innerhalb von 12 Monaten nach dem Inkrafttreten elektronische Brieffaschen zur Verfügung, in denen diese ihre nationale elektronische Identität mit den Nachweisen anderer persönlicher Attribute (z. B. Führerschein, Abschlusszeugnisse, Bankkonto) verknüpfen können. Die Brieffaschen können von Behörden oder privaten Einrichtungen bereitgestellt werden, sofern diese von den Mitgliedstaaten anerkannt sind. Auf parlamentarischer Ebene ist Ende Juni 2022 eine Diskussion im zuständigen Ausschuss (ITRE) vorgesehen. Die Abstimmung im Ausschuss soll im Oktober 2022 und jene im Plenum im November 2022 stattfinden.

Damit der Vorschlag in nützlicher Frist umgesetzt werden kann, wird er durch eine Empfehlung ergänzt. Die Kommission fordert die Mitgliedstaaten auf, bis Oktober 2022 ein gemeinsames Instrumentarium zu schaffen und unverzüglich mit den erforderlichen Vorarbeiten zu beginnen. Dieses Instrumentarium wird die technische Architektur, Normen, Leitlinien und bewährte Verfahren umfassen.

Der von der Kommission vorgegebene Rahmen basiert auf den Grundsätzen von Self-Sovereign Identity (SSI). Er ist aber technologisch neutral, wenn es um die genaue Umsetzung dieser Grundsätze geht. Die Mitgliedstaaten verhandeln untereinander die technischen Standards seit September 2021.

Die Schweiz ist rechtlich nicht verpflichtet, die EU-Verordnung und die dazu gehörenden Änderungen zu übernehmen. In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten Mitgliedsländern der Europäischen Union hat die Schweiz jedoch ein Interesse daran, ihr System für den elektronischen Identitätsnachweis so zu gestalten, dass es interoperabel mit jenem der Europäischen Union ist. Der Vorentwurf sieht vor, dass der Bundesrat internationale Abkommen abschliessen kann, um eine internationale Anerkennung der E-ID zu erreichen und ausländische E-ID zu anerkennen (Art. 25). So wird es in Zukunft möglich sein, eine gegenseitige Anerkennung, insbesondere mit der EU, zu erlangen. Dazu strebt die staatliche E-ID der Schweiz das Sicherheitsniveau «substanzial» an. Der Vorentwurf wurde so formuliert, dass er mit dem europäischen Recht vereinbar ist.

3 Grundzüge der Vorlage

3.1 Beantragte Neuregelung

Der Vorentwurf sieht für Inhaberinnen und Inhaber eines von den Schweizer Behörden ausgestellten Ausweises die Einführung eines kostenlosen und freiwilligen staatlichen elektronischen Identitätsnachweises vor. Dabei nimmt der Staat weiterhin seine zentrale Aufgabe der Überprüfung der Identität einer Person und der Ausstellung des entsprechenden elektronischen Nachweises wahr. Wie in den im Nationalrat eingereichten Motionen gefordert, verfolgt die neue Vorlage einen Ansatz, der auf den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung beruht.

⁶ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM (2021) final, 3. Juni 2021.

⁷ 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/CE, EG, ABl. L 257 vom 28.8.2014, S. 73.

Zudem sieht der Vorentwurf die Schaffung einer staatlichen Vertrauensinfrastruktur vor, die es Akteuren des öffentlichen und privaten Sektors ermöglicht, elektronische Nachweise auszustellen und zu verwenden. Der Staat wird das erforderliche Basissystem betreiben (Basisregister, System zur Bestätigung von Identifikatoren⁸) und eine staatliche elektronische Brieftasche zur Verfügung stellen, die die E-ID und weitere elektronische Nachweise enthalten kann. Die Inhaberinnen und Inhaber der Brieftasche können ihre E-ID und andere elektronische Nachweise sicher und transparent vorweisen. Mit einer solchen Öffnung des Systems kann die Verbreitung der elektronischen Nachweise verbessert und ihre Nutzung erhöht werden. Gleichzeitig kann so das Vertrauen der Bevölkerung in die elektronischen Prozesse gestärkt werden.

Die Einführung einer elektronischen Vertrauensinfrastruktur durch den Staat ist eine wichtige und neue Entwicklung. Zudem basiert diese Vorlage auf einem neuartigen partizipativen Verfahren, das eine informelle Konsultation, öffentliche Diskussionen und ein Online-Forum für fachliche Diskussionen umfasst. Auch Erfahrungen aus Pilotprojekten mit anderen Ämtern und der Austausch mit anderen Ländern fliessen in diese Vorlage ein.

Die Frage der Verwendung der E-ID in verschiedenen Bereichen ist im Vorentwurf nur exemplarisch geregelt (vgl. Änderungen anderer Erlasse: SchKG und EPDG). Die Möglichkeit, die E-ID in anderen Bereichen einzusetzen, wird im Rahmen der Vernehmlassung geprüft.

3.2 Abstimmung von Aufgaben und Finanzen

Die Fragen zur Abstimmung von Aufgaben und Finanzen werden nach der Vernehmlassung eingehend analysiert. Es wurde eine erste Schätzung der Kosten vorgenommen (vgl. Kap. 5.1 Finanzielle und personelle Auswirkungen auf den Bund).

3.3 Umsetzung

Die Ausführungsbestimmungen für die Umsetzung dieses Gesetzes werden auf Verordnungsstufe geregelt (vgl. Art. 27 und entsprechende Erläuterungen).

4 Erläuterungen zu den einzelnen Artikeln

Ingress

Der Vorentwurf stützt sich auf die Artikel 38 Absatz 1, 81 und 121 Absatz 1 der Bundesverfassung (BV).

Für den staatlichen elektronischen Identitätsnachweis beruht er auf den Artikeln 38 Absatz 1 und 121 Absatz 1 BV. Gemäss Artikel 38 Absatz 1 BV ist der Bund dafür zuständig, Erwerb und Verlust der Bürgerrechte durch Abstammung, Heirat und Adoption zu regeln. Weiter ist die Gesetzgebung über die Ein- und Ausreise, den Aufenthalt und die Niederlassung von Ausländerinnen und Ausländern sowie über die Gewährung von Asyl gemäss Artikel 121 Absatz 1 BV ebenfalls Sache des Bundes. Obwohl die beiden Artikel nicht ausdrücklich die Ausweise regeln, muss der Bund die Kompetenz haben, die erforderlichen Ausweise zu regeln. Dies selbst dann, wenn diese nicht ausschliesslich dem Nachweis der Staatsangehörigkeit der Schweizer Bürgerinnen und Bürger und des Aufenthaltsstatus der Ausländerinnen und Ausländer dienen. Gestützt auf diese beiden Artikel ermächtigen das Ausweisgesetz vom 22. Juni 2001 (AwG)⁹ und das Ausländer- und Integrationsgesetz vom 16. Dezember 2005 (AIG)¹⁰ den Bund, den Schweizer Bürgerinnen und Bürgern Identitätsausweise und den Ausländerinnen und Ausländern Ausländerausweise auszustellen. Da die staatliche E-ID zum Nachweis der Identität in der virtuellen Welt dient, ist es gerechtfertigt, diesen Vorentwurf für den amtlichen Nachweis der Identität, der Staatsangehörigkeit und des Aufenthaltsstatus der Ausländerinnen und Ausländer auf die gleiche Verfassungsgrundlage zu stützen.

Die Kompetenz zur Schaffung einer Vertrauensinfrastruktur für die E-ID ergibt sich aus Artikel 81 BV, gemäss dem der Bund im Interesse des ganzen oder eines grossen Teils des Landes öffentliche Werke errichten und betreiben oder ihre Errichtung unterstützen kann. Die Unterstützung für den Betrieb und den Unterhalt von Werken Dritter kann sich hingegen nicht auf Artikel 81 stützen; sie könnte sich höchstens auf eine Bundeskompetenz stützen. Ein «öffentliches Werk» nach dieser Bestimmung ist herkömmlicherweise physischer Art, im Sinne eines Bauwerks, wie beispielsweise ein Tunnel. Das Rechtsgutachten des BJ für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen¹¹ hält jedoch Folgendes fest: «Zusammengefasst wäre es nach einem in der Lehre teilweise befürworteten Ansatz möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Artikel 81 BV zu subsumieren»¹². Gemäss der zeitgemässen und teleologischen Auslegung von Lendi¹³ und von Biaggini¹⁴ können «öffentliche Werke» auch immateriell oder nicht fest sein, wie ein im Interesse der Schweiz entwickeltes Informatik- oder Kommunikationssystem. Der Bundesrat schliesst sich dieser Lehrmeinung an und hält es daher für zulässig, Artikel 81 BV als Grundlage für einen Vorentwurf zur Schaffung einer Vertrauensinfrastruktur heranzuziehen, mit der unterschiedliche elektronische Nachweise (einschliesslich der E-ID) ausgestellt, verwendet und überprüft werden

⁸ Gemäss Art. 18 Abs. 2 kann der Bundesrat den Bund mit der Bestätigung der Identifikatoren und den kryptografischen Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen beauftragen.

⁹ SR 143.1

¹⁰ SR 142.20

¹¹ Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, BPB 1712 vom 1. Mai 2012.

¹² Ibid, S. 8.

¹³ Ibid; Lendi, Martin, in St. Galler Kommentar, 2. Aufl. 2008, Art. 81 Rz. 6.

¹⁴ Ibid.; Biaggini, Giovanni in BV-Kommentar, Zürich 2007, Art. 81 Rz. 2, kritisiert von Markus Kern im Basler Kommentar, Rz. 6 und 9.

können. In diesem Zusammenhang ist darauf hinzuweisen, dass Artikel 81 BV dem Bund nicht die Kompetenz verleiht, verbindliche technische und organisatorische Standards für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen zu erlassen und durchzusetzen.¹⁵

Der vorliegende Vorentwurf regelt bestimmte zivilrechtliche Aspekte im Zusammenhang mit den Beziehungen zwischen den Ausstellerinnen und den Inhaberinnen und Inhabern einer E-ID sowie den Verifikatorinnen und den Inhaberinnen und Inhabern einer E-ID. Angesichts deren untergeordneter Bedeutung wird im Ingress Artikel 122 Absatz 1 BV nicht erwähnt, der die Kompetenz des Bundes in zivilrechtlicher Hinsicht begründet.

1. Abschnitt Gegenstand und Zweck

Art. 1

Abs. 1

Der Vorentwurf schafft den rechtlichen Rahmen für die elektronischen Nachweise in der Schweiz, einschliesslich des staatlichen elektronischen Identitätsnachweises. Er regelt zudem die Anforderungen, die die Vertrauensinfrastruktur zum Ausstellen, Widerrufen, Überprüfen, Aufbewahren und Vorweisen von elektronischen Nachweisen erfüllen muss. Weiter regelt der Vorentwurf die Rollen und Kompetenzen für den Betrieb der Vertrauensinfrastruktur.

Abs. 2

Bst. a

Mit diesem Vorentwurf soll ein sicherer staatlicher elektronischer Identitätsnachweis (E-ID) eingeführt werden, der unter Privaten und mit Behörden verwendet werden kann. Die E-ID ermöglicht den Inhaberinnen und Inhabern, sich bei Geschäftsprozessen in der digitalen Welt einfacher zu identifizieren. So können die bestehenden (Online)-Identifizierungsprozesse, die viel komplexer sind, ersetzt werden. Die E-ID kann auf dem Smartphone installiert und so ebenfalls in der physischen Welt verwendet werden.

Bst. b.

Da der Datenschutz gewährleistet sein muss, übernimmt dieser Buchstabe den in Artikel 1 des Bundesgesetzes vom 25. September 2020 über den Datenschutz (nDSG)¹⁶ festgelegten Zweck. Er hält fest, dass bei der Bearbeitung von Personendaten im Zusammenhang mit dem Bezug und der Verwendung der E-ID die Datenschutzanforderungen eingehalten werden müssen. Dieses Ziel wird insbesondere durch die Umsetzung der Anforderungen der sechs inhaltlich identischen Motionen «Vertrauenswürdige staatliche E-ID» (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129) erreicht, die nach der Ablehnung der früheren Vorlage in der Abstimmung vom 7. März 2021 von allen Fraktionen eingereicht worden sind. Gemäss den Motionärinnen und Motionären muss der staatliche elektronische Identitätsnachweis insbesondere den Grundsätzen «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) entsprechen. In diesem Buchstaben werden diese Anforderungen als spezifische Zwecke formuliert, die im Zusammenhang mit dem Schutz der Personendaten umgesetzt werden müssen.

Das nDSG gilt für die Bearbeitung der Personendaten, die im Rahmen der Umsetzung dieses Vorentwurfs durchgeführt wird. Um Wiederholungen zu vermeiden und das Verständnis zu erleichtern, verweisen die Bestimmungen des Vorentwurfs nicht auf die einschlägigen Artikel des nDSG (vgl. Kap. 6.8 Datenschutz).

Bst. c

Mit diesem Buchstaben soll sichergestellt werden, dass die Ausgestaltung der E-ID und der Vertrauensinfrastruktur dem aktuellen Stand der Technik entspricht.¹⁷ Der Gesetzgeber strebt mit diesem Begriff ein hohes Niveau der Datensicherheit und des Datenschutzes dank fortschrittlicher Verfahren an. Zu diesem Zweck ist die regelmässige Überprüfung der umgesetzten Sicherheitsmassnahmen auf ihre Wirksamkeit hinsichtlich der geforderten Schutzziele, ihrer Aktualität sowie ihres Innovationsgrads zu fördern. So sind die Sicherheitsmassnahmen auch mit den Sicherheitsprodukten auf dem Markt zu vergleichen.¹⁸

Bst. d

Um den Bezug und die Verwendung der E-ID zu fördern, legt der Vorentwurf neue Standards fest oder harmonisiert bestehende Standards über die Ausstellung, die Überprüfung und den Widerruf der E-ID. Auch die Sicherheit der Infrastruktur und der Prozesse zur Ausstellung und Überprüfung der anderen elektronischen Nachweise soll gewährleistet werden. Um diese Ziele zu erreichen, darf jedoch der technische Fortschritt nicht eingeschränkt werden. Daher wird die Wahl der technischen Lösung im Vorentwurf nur geregelt, wenn dies für die Erreichung der gesetzgeberischen Ziele absolut erforderlich

¹⁵ Ibid; Biaggini, G., ebd., Art. 81 Rz. 3.

¹⁶ BBl 2020 7639

¹⁷ Der Begriff «aktueller Stand der Technik» unterscheidet sich konzeptuell von anderen ähnlichen Begriffen wie den «anerkannten Regeln der Technik» und dem «aktuellen Stand der Wissenschaft und der Forschung». Einfach ausgedrückt verweist der Begriff «aktueller Stand der Technik» auf innovativere Methoden als der Begriff «anerkannte Regeln der Technik» und auf ältere Methoden als der Begriff «Stand der Wissenschaft und der Forschung». Diese Unterscheidung ist bei der Bestimmung des erforderlichen Sicherheitsniveaus wesentlich. Nach Artikel 7 Absatz 2 nDSG müssen ebenfalls Massnahmen ergriffen werden, die dem «Stand der Technik» entsprechen, doch es werden keine Kriterien aufgestellt, die Aufschluss über den Inhalt des Begriffs «Stand der Technik» geben. Daraus darf jedoch nicht geschlossen werden, dass das, was im Gesetz nicht konkret bestimmt ist, nicht überprüft und folglich nicht angewendet werden kann.

¹⁸ Was heute als «Stand der Technik» gilt, kann morgen aufgrund der innovationsbedingten Verschiebung, also der Alterung der Sicherheitsmassnahme, im Vergleich mit anderen verfügbaren Sicherheitsmassnahmen eher den «anerkannten Regeln der Technik» zugeordnet werden.

ist. Die Vorlage sieht insbesondere eine dezentrale Datenverwaltung vor und schliesst somit jede technische Lösung aus, bei der eine Anbieterin von Identifizierungsdienstleistungen zwischen die Inhaberin oder den Inhaber und die Verifikatorin eines elektronischen Nachweises geschaltet wird. So kann verhindert werden, dass bei einer solchen Anbieterin Spuren hinterlassen werden, und die Inhaberinnen und Inhaber haben auf diese Weise eine grössere Kontrolle über ihre Daten. Die Mehrheit der Fragen im Zusammenhang mit der Wahl der Technologie ist jedoch auf nicht auf Gesetzesstufe geregelt. Angesichts der raschen technischen Fortschritte sollte sichergestellt werden, dass dieser Vorentwurf nach dem Inkrafttreten in demjenigen technologischen Kontext umgesetzt werden kann, der dann vorliegt und heute nicht bekannt ist. Verschiedene Aspekte, die auf Verordnungsstufe geregelt werden müssen, sind in technologischer Hinsicht noch nicht abschliessend bekannt, oder sogar abhängig von der Technologie. Die Verordnung muss die Interoperabilität aller in die Kommunikation involvierter Systeme gewährleisten. Dazu muss sie namentlich die Datenformate und die Schnittstellen sehr genau festlegen. Dabei sollte der Grundsatz beachtet werden, dass nur absolut notwendige technologische Entscheide getroffen werden sollten. Soweit wie möglich sollte es den beteiligten Akteuren überlassen werden, die Technologie zu wählen, die sie für die Formatierung, Speicherung und Bearbeitung der Daten auf ihrer Seite der Schnittstelle verwenden wollen.

2. Abschnitt E-ID

Art. 2 Form und Inhalt

Abs. 1

Der Bund stellt eine Vertrauensinfrastruktur zur Verfügung (vgl. 5. Abschnitt), die staatlichen und privaten Akteuren ermöglicht (vgl. Einschränkung in Art. 18 Abs. 3), unterschiedliche Nachweise in elektronischer Form auszustellen, die zum Nachweis der Identität, eines Sachverhalts oder eines Ereignisses verwendet werden können (elektronischer Nachweis). Die E-ID ist ein elektronischer Nachweis, der von fedpol mittels der staatlichen Vertrauensinfrastruktur ausgestellt wird.

Abs. 2

Eine E-ID enthält die folgenden Personenidentifikationsdaten: den amtlichen Namen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, die Nationalität und das Gesichtsbild aus dem Informationssystem Ausweisschriften (ISA) oder dem zentralen Migrationsinformationssystem (ZEMIS). Diese Daten sind in den amtlichen Registern des Staates verfügbar, auf die fedpol nach Artikel 11 Absatz 3 Zugriff hat. Verlangt eine Verifikatorin einen Nachweis, so kann die Inhaberin oder der Inhaber ihr alle diese Daten oder gewisse davon übermitteln.

Abs. 3

Neben den Personenidentifikationsdaten enthält eine E-ID zusätzliche Informationen. Es handelt sich um folgende Daten: die AHV-Nummer; die E-ID-Nummer; ihr Ausstellungsdatum; ihr Ablaufdatum; Angaben zum Ausweis, der im Ausstellungsprozess verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises; und Angaben zum Ausstellungsprozess (diese werden auf Verordnungsstufe ausführlicher geregelt).

Art. 3 Persönliche Voraussetzungen

Vorbemerkung

Mit der Kann-Formulierung von Absatz 1 wird sichergestellt, dass die antragstellenden Personen nicht verpflichtet sind, eine E-ID zu beziehen oder zu verwenden. Wenn jedoch die persönlichen Voraussetzungen erfüllt sind, ist fedpol verpflichtet, der antragstellenden Person eine E-ID auszustellen. Durch den Bezug einer E-ID werden die antragstellenden Personen zu Inhaberinnen und Inhabern einer E-ID.

Bst. a

Um die Ausstellung einer E-ID zu beantragen, genügt für Schweizer Bürgerinnen und Bürger ein gültiger Ausweis nach dem AwG. Juristische Personen, die immer durch ihr Organ, also durch natürliche Personen, handeln, können nicht Inhaberinnen und Inhaber einer E-ID sein und werden mittels der einheitlichen Unternehmens-Identifikationsnummer (UID)¹⁹ identifiziert.

Bst. b

Alle Ausländerinnen und Ausländer, die eine gültige Bewilligung nach dem Bundesgesetz vom 16. Dezember 2005 über die Ausländerinnen und Ausländer und über die Integration (AIG)²⁰ und der Verordnung vom 24. Oktober 2007 über Zulassung, Aufenthalt und Erwerbstätigkeit (VZAE)²¹ besitzen, können eine E-ID beziehen. Es handelt sich um folgende Ausweise:

- Ausweis L: Kurzaufenthaltsbewilligung (Art. 32 AIG und Art. 71 Abs. 1 VZAE)
- Ausweis B: Aufenthaltsbewilligung (Art. 33 AIG und Art. 71 Abs. 1 VZAE)
- Ausweis C: Niederlassungsbewilligung (Art. 34 AIG und Art. 71 Abs. 1 VZAE)
- Ausweis Ci: Aufenthaltsbewilligung mit Erwerbstätigkeit (Art. 30 Abs. 1 Bst. g und 98 Abs. 2 AIG und Art. 45 und 71a Abs. 1 Bst. e VZAE)

¹⁹ Vgl. www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer.html.

²⁰ SR 142.20

²¹ SR 142.201

- Ausweis N: Ausweis für Asylsuchende (Art. 42 AsylG und Art. 71a Abs. 1 Bst. b VZAE)
- Ausweis F: Ausweis für vorläufig aufgenommene Ausländerinnen und Ausländer (Art. 41 Abs. 2 AIG und Art. 71a Abs. 1 Bst. c VZAE)
- Ausweis S: Ausweis für Schutzbedürftige (Art. 74 AsylG und Art. 71a Abs. 1 d VZAE)
- Ausweis G: Grenzgängerbewilligung (Art. 35 AIG und Art. 71a Abs. 1 Bst. a VZAE)

Es gibt keinen grundlegenden Unterschied zwischen der E-ID für Schweizer Bürgerinnen und Bürger und jener für Ausländerinnen und Ausländern. Die E-ID kann grundsätzlich von Schweizer Bürgerinnen und Bürgern und von Ausländerinnen und Ausländern gleich verwendet werden. Der Bezug einer E-ID bietet jedoch den Inhaberinnen und Inhabern keine Garantie für einen Zugang zu allen damit verbundenen Diensten. Es ist beispielsweise nicht sicher, dass sie damit alle Online-Dienste nutzen können. Gewisse Anbieterinnen können – aus Sicherheitsgründen im Zusammenhang mit der Zuverlässigkeit der Überprüfung der Identität von Ausländerinnen und Ausländern – entscheiden, den Zugang zu ihren Diensten auf Inhaberinnen und Inhaber einer bestimmten Aufenthaltsbewilligung zu beschränken. Der vorliegende Vorentwurf sieht keine Beschränkung des Zugangs zu den Online-Diensten vor und lässt den betreffenden Dienstanbieterinnen diesbezüglich einen gewissen Spielraum.

Für bestimmte Ausweiskategorien (z. B. Ausweise N, F, S und Ci) kann nicht davon ausgegangen werden, dass die Identität der betreffenden Personen verlässlich festgestellt werden konnte. 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 Personenidentifikationsdaten eingereicht, wobei diese Gesuche nicht selten mit nicht tauglichen Dokumenten untermauert werden. Aus diesem Grund scheint es gerechtfertigt, die Möglichkeit zur Anerkennung der den Ausländerinnen und Ausländern ausgestellten E-ID vorzusehen: Jede E-ID enthält Angaben zum Ausweis, der für die Ausstellung verwendet wurde. Sofern dies gerechtfertigt und im Gesetz ausdrücklich vorgesehen ist, kann der Zugang zu gewissen Diensten für Inhaberinnen und Inhaber eines Ausländerausweises, deren Identität nicht verlässlich festgestellt werden konnte, eingeschränkt werden.

Um die Effizienz und die Geschwindigkeit des Antragsverfahrens für die E-ID zu steigern, beruht dieses auf einem gültigen Schweizer Ausweis. Es wurde auch erwogen, die Identität der antragstellenden Person erneut zu prüfen. Von dieser Möglichkeit wurde jedoch aus Kosten-, Benutzerfreundlichkeits- und Geschwindigkeitsgründen abgesehen. Ein solches Vorgehen wäre kostspieliger gewesen als der Bezug eines Ausweises.

Art. 4 Ausstellung

Vorbemerkung

Die antragstellende Person stellt einen Antrag bei fedpol, das den Ausstellungsprozess einleitet, wenn die persönlichen Voraussetzungen nach Artikel 3 erfüllt sind.

Abs. 1

Es besteht keine Pflicht, eine E-ID zu beziehen. Wenn eine Person eine E-ID erhalten will, muss sie diese bei fedpol beantragen. Der Antrag muss von der späteren Inhaberin oder dem späteren Inhaber der E-ID (antragstellende Person) oder deren oder dessen gesetzlicher Vertretung ausgehen (s. Abs. 2 für Minderjährige und Personen unter umfassender Beistandschaft). Die antragstellende Person oder ihre gesetzliche Vertretung kann die Ausstellung einer E-ID direkt über das Informationssystem von fedpol oder über die elektronische Brieftasche beantragen.

Abs. 2

Gemäss diesem Absatz benötigen Minderjährige unter 14 Jahren und Personen unter umfassender Beistandschaft für den Bezug einer E-ID die Einwilligung ihrer gesetzlichen Vertretung. Die vorgesehene Altersgrenze stützt sich auf Artikel 8 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG²², wonach «[...] die Verarbeitung der personenbezogenen Daten des Kindes rechtmässig [ist], wenn das Kind das sechzehnte Lebensjahr vollendet hat» (Abs. 1). Weiter können «[d]ie Mitgliedstaaten [...] durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf». Die Schweiz ist rechtlich nicht verpflichtet, die Anforderungen von Artikel 8 einzuhalten. Ausserdem wurde der Inhalt dieses Artikels bei der Reform des Datenschutzgesetzes nicht übernommen. Das Spezialgesetz im Bereich der elektronischen Identifizierung kann jedoch den Zugang für Kinder und Personen unter umfassender Beistandschaft einschränken. Diese Personen benötigen einen besonderen Schutz, da sie sich der Risiken, Folgen, Garantien und ihrer Rechte im Zusammenhang mit der Bearbeitung von Personendaten weniger bewusst sind. Diese Altersbegrenzung für den Bezug einer E-ID ist weniger hoch als jene für den Bezug von Schweizer Identitätsausweisen (18 Jahre; Art. 5 Abs. 1 AwG). Da Jugendliche für die Erledigung ihrer alltäglichen Aufgaben und Aktivitäten hauptsächlich das Internet verwenden, sieht der Vorentwurf vor, dass sie ab dem Zeitpunkt, wo sie die Folgen der Bearbeitung ihrer Personendaten verstehen, eine E-ID beziehen können. Der Hauptzweck dieses Absatzes besteht darin, die betreffenden Personen zu schützen, aber auch, ihre Aktivitäten in der digitalen Welt nicht in ungerechtfertigter Weise einzuschränken.

Abs. 3

Fedpol prüft, ob die antragstellende Person die Voraussetzungen nach Artikel 3 erfüllt. Wenn dies der Fall ist, überprüft es ihre Identität mithilfe der erforderlichen Informationen. Dazu vergleicht es die von der antragstellenden Person bereitge-

²² Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 119 vom 4.5.2016, S. 1–88.

stellten Informationen mit jenen aus den Registern des Bundes nach Artikel 11 Absatz 3. Wenn die Überprüfung der Identität der antragstellenden Person erfolgreich war, übermittelt ihr fedpol eine E-ID mit den Daten nach Artikel 2 Absätze 2 und 3.

Abs. 4

Der vorliegende Absatz setzt die Anforderungen von Artikel 34 Absatz 2 Buchstabe a nDSG um. Gemäss diesem Artikel ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich, damit Bundesorgane besonders schützenswerte Daten bearbeiten dürfen. Gemäss Artikel 5 Buchstabe c Ziffer 4 nDSG stellen «biometrische Daten, die eine natürliche Person eindeutig identifizieren», besonders schützenswerte Daten dar. Unter biometrischen Daten sind «Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen».²³ Mit dem vorliegenden Absatz wird eine gesetzliche Grundlage im formellen Sinn geschaffen, die den Bundesrat ermächtigt, in einer Verordnung die Verwendung eines Gesichtsbildes nach Artikel 2 Absatz 2 Buchstabe g und der im Ausstellungsprozess erhobenen biometrischen Daten vorzusehen. Dieser Schritt ist nötig zur Überprüfung, ob das von der antragstellenden Person im Rahmen des Ausstellungsprozesses erfasste Gesichtsbild demjenigen entspricht, welches in den Registern des Bundes (ISA oder ZEMIS) enthalten ist.

Abs. 5

Der Bundesrat regelt die Einzelheiten des Ausstellungsprozesses in einer Verordnung oder legt insbesondere den Ablauf des Prozesses sowie die technischen Standards und Protokolle für die Übermittlung der Daten fest.

Art. 5 Widerruf

Der Vorentwurf sieht die Möglichkeit vor, eine E-ID in den Fällen nach den Buchstaben a–e zu widerrufen. Aus technischer Sicht ist es aufgrund der dezentralen Art des Systems zur Ausstellung der E-ID nicht möglich, eine E-ID direkt durch die Inhaberin oder den Inhaber zu sperren oder zu deaktivieren. Die Inhaberin oder der Inhaber oder die gesetzliche Vertretung von Minderjährigen unter 14 Jahren oder von Personen unter umfassender Beistandschaft kann den Widerruf der eigenen E-ID oder der I-ID der Person, die sie vertritt, verlangen. Zudem widerruft fedpol die E-ID, wenn der begründete Verdacht auf deren Missbrauch besteht. Bevor es eine E-ID widerruft, überprüft es die Informationen, die ihm übermittelt wurden. Es widerruft die E-ID auch, wenn es informiert wird, dass die Inhaberin oder der Inhaber einer E-ID verstorben ist, der im Ausstellungsprozess der E-ID verwendete Ausweis entzogen wurde oder sich die Personenidentifikationsdaten nach Artikel 2 Absatz 2 geändert haben. Ausserdem wird die E-ID widerrufen, wenn eine neue E-ID für dieselbe Person ausgestellt wird. Eine widerrufene E-ID kann nicht mehr aktiviert werden: Die betroffene Person kann bei fedpol einen neuen Ausstellungsantrag gemäss Artikel 4 Absatz 1 einreichen.

Art. 6 Gültigkeitsdauer

Aus Sicherheitsgründen hat die E-ID eine zeitlich befristete Gültigkeit. Der Bundesrat regelt die Anforderungen an diese Dauer in einer Verordnung. In diesem Rahmen sollte geklärt werden, ob die Gültigkeitsdauer der E-ID jener des Dokuments entsprechen muss, das für ihre Ausstellung verwendet wurde. Die Gültigkeitsdauer wird in der E-ID angegeben (Art. 2 Abs. 3 Bst. d). Wird der für die Ausstellung der E-ID verwendete Ausweis von den Behörden entzogen, so widerruft fedpol die E-ID, sobald es über den Entzug informiert wird (Art. 5 Bst. d Ziff. 1).

Nach Ablauf der Gültigkeit bleibt die E-ID weiterhin auf dem Gerät der Inhaberin oder des Inhabers bestehen als authentischer aber abgelaufener digitaler Nachweis.

Art. 7 Sorgfaltspflicht

Abs. 1

Die im Vorentwurf den Inhaberinnen und Inhabern einer 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 nDSG wird das Strafgesetzbuch mit einem Artikel 179^{decies} ergänzt, der den Identitätsmissbrauch mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bedroht. Zur Vermeidung von Doppelspurigkeiten enthält der vorliegende Vorentwurf keine Bestimmungen zur Bestrafung desselben Verhaltens.

Abs. 2

Die Inhaberin oder der Inhaber einer E-ID muss fedpol unverzüglich jeden Verdacht auf Missbrauch ihrer oder seiner E-ID melden. Dabei kann es sich beispielsweise um Ereignisse, die nach dem Verlust des E-ID-Trägers stattfinden, oder um Informationen von Dritten über eine unübliche Verwendung der E-ID handeln.

Art. 8 Anlaufstellen der Kantone

²³ Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, 7020.

Der digitale Wandel ist auf Bundes-, Kantons- und Gemeindeebene bereits im Gange. Mit der E-ID hat man Zugriff auf verschiedene digitalisierte Prozesse, die die Ausführung von elektronischen Geschäftsprozessen erleichtern. Da gewisse Aufgaben oder Aktivitäten von zuhause aus ausgeführt werden können, ist die physische Präsenz der betreffenden Person nicht mehr erforderlich. Trotz dieses Trends zur Digitalisierung der Gesellschaft sind gewisse Bevölkerungsgruppen nicht bereit, sich diesem Wandel zu stellen. Es ist ihnen lieber, eine Behörde in der physischen Welt aufzusuchen, weil sie Unterstützung benötigen. Daher sieht dieser Artikel die Schaffung von kantonalen Stellen vor, die den betreffenden Personen Hilfestellungen bieten. Es wird Sache der Kantone sein, die Anlaufstellen und deren Organisation zu bestimmen. Diese Anlaufstellen der Kantone leisten allgemeine Unterstützung bei verschiedenen E-Government-Anwendungen. Diese Unterstützung ist ergänzend zum technischen Support des fedpol bei der Ausstellung, der Verwendung oder dem Widerruf der E-ID.

Die meisten dieser Hilfestellungen im Zusammenhang mit der Digitalisierung dürften auf kantonomer Ebene benötigt werden. Daher sieht diese Bestimmung vor, die Anlaufstellen in der Nähe der Personen zu schaffen, die diese benötigen könnten. Ausserdem haben einige Kantone bereits ähnliche Stellen eingerichtet. Im Kanton Jura beispielsweise bietet ein Netz von Anlaufstellen Hilfe vor Ort im Zusammenhang mit kantonalen E-Government-Diensten. Auf internationaler Ebene hat sich Dänemark ebenfalls für ein solches Vorgehen entschieden.

Auf Bundesebene unterstützt der Bund die Anlaufstellen der Kantone bei Aspekten im Zusammenhang mit der Vertrauensinfrastruktur (Second-Level-Support).

Art. 9 Pflicht zur Akzeptanz der E-ID

Behörden und andere Stellen, die Verwaltungsaufgaben erfüllen, müssen die staatliche E-ID gemäss dem vorliegenden Vorentwurf akzeptieren, wenn sie eine elektronische Identifizierung vornehmen. Demnach sind auch die Behörden von Kantonen und Gemeinden Adressaten dieser Norm. Dies ist angezeigt, weil die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet wird und damit vergleichbar ist mit Identitätskarte oder Pass in der physischen Welt, die auch bei jeder Identifizierung von allen Behörden akzeptiert werden. Diese Verpflichtung gilt nur für Identifizierungsprozesse, bei denen ein persönliches Erscheinen die Vorlage eines Identitätsdokuments erforderlich sind. Sie betrifft nicht die bestehenden kantonalen und kommunalen Login-Lösungen.

Die staatliche E-ID kann zusammen mit den bestehenden Mitteln für den Zugang zu E-Government-Diensten verwendet werden. Diese Bestimmung unterstreicht die Bedeutung und Akzeptanz einer E-ID nach diesem Gesetz, wie sie sowohl in der Strategie «Digitale Schweiz»²⁴ als auch in der «E-Government Strategie Schweiz 2020–2023»²⁵ definiert ist. Nicht zuletzt sollen so die vom Bund für die E-ID zu tätigen 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, die damit mittelfristig Kosten einsparen können, sondern auch alle Einwohnerinnen und Einwohner der Schweiz.

Die Fragen im Zusammenhang mit der Verwendung der E-ID sowie die diesbezüglichen rechtlichen Folgen sind im Vorentwurf nicht geregelt. Diese Fragen müssen für jeden Sektor einzeln geregelt werden. Der Vorentwurf trägt insbesondere dem elektronischen Patientendossier sowie dem Bereich Schuldbetreibung und Konkurs Rechnung. In der Vernehmlassung werden andere Fälle untersucht und gegebenenfalls in den Vorentwurf aufgenommen.

Art. 10 Vorweisen einer E-ID

Mit dem vorliegenden Artikel soll sichergestellt werden, dass die Inhaberinnen und Inhaber einer E-ID nicht verpflichtet sind, bei Interaktionen in der physischen Welt ihre E-ID vorzuweisen. Trotz der Vorteile der E-ID geht es darum, die Möglichkeit, (physische) Ausweise vorzuweisen, nicht zu ersetzen oder auszuschliessen. Wenn die Identifizierung einer Person in einem physischen Prozess anhand eines Ausweises erfolgen kann, darf das Vorweisen der E-ID (oder Bestandteilen davon) nur als Option angeboten werden.

Art. 11 Informationssystem zur Ausstellung und zum Widerruf der E-ID

Abs. 1

Fedpol betreibt ein Informationssystem, mit dem die Personendaten nach Artikel 2 bearbeitet werden. Das Informationssystem ermöglicht die Entgegennahme der Anträge der antragstellenden Personen und die Erfüllung der Aufgaben von fedpol bei der Ausstellung und dem Widerruf von E-ID.

Abs. 2

Das Informationssystem beinhaltet die zusätzlichen Daten gemäss Artikel 2 Absatz 3 sowie die Daten zum Widerruf der E-ID. Weiter werden auch die sogenannten Randdaten gespeichert, die während des Prozesses zur Überprüfung der Identität und zur Ausstellung der E-ID generiert werden und die zu Statistik- und Supportzwecken sowie zur Missbrauchsverhinderung erforderlich sind. Die Personendaten werden direkt in den Registern des Bundes aufgerufen und nicht im System gespeichert (vgl. Abs. 3).

Abs. 3

Das Informationssystem kann für die Ausstellung einer E-ID auf die folgenden Personenregister zugreifen, die auf Bundesebene geführt werden:

²⁴ Vgl. www.uvek.admin.ch/uvek/de/home/kommunikation/digitale-schweiz.html.

²⁵ Vgl. www.digitale-verwaltung-schweiz.ch/application/files/3016/3636/7600/E-Government-Strategie-Schweiz-2020-2023_D_def.pdf.

- das Informationssystem Ausweisschriften (ISA);
- das Zentrale Migrationsinformationssystem (ZEMIS);
- das elektronische Personenstandsregister (Infostar) gemäss Artikel 39 des Zivilgesetzbuches (ZGB)²⁶ und Artikel 6a der Zivilstandsverordnung vom 28. April 2004 (ZStV)²⁷;
- das zentrale Versichertenregister der Zentralen Ausgleichsstelle der AHV (ZAS/UPI) nach Artikel 71 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG)²⁸.

Somit kann fedpol seine Aufgaben bei der Ausstellung der E-ID automatisiert erfüllen. Auf dieser Grundlage kann fedpol die Identität der antragstellenden Person überprüfen und ihr die Daten nach Artikel 2 Absatz 3 über eine sichere Verbindung übermitteln. Die aufgerufenen Daten werden weder dupliziert noch im Informationssystem von fedpol gespeichert.

Abs. 4

Der Bundesrat regelt die Aufbewahrungsfristen der verschiedenen Arten von Daten auf Verordnungsstufe. Die Daten nach den Absätzen 2 und 3 dürfen bis fünf Jahre nach Ablauf der E-ID aufbewahrt werden. Die Aufbewahrung der Daten hat zum Zweck, allfällige Fälle von Missbrauch untersuchen zu können.

3. Abschnitt Andere elektronische Nachweise

Art. 12 Ausstellung

Abs. 1

Behörden und Private (vgl. Einschränkung von Art. 18 Abs. 3) können die Vertrauensinfrastruktur des Bundes gemäss dem 5. Abschnitt nutzen, um elektronische Nachweise auszustellen (andere als die staatliche E-ID, die nur von fedpol ausgestellt wird). Es handelt sich um eine Kann-Bestimmung, so dass Behörden und Private nicht zu deren Nutzung verpflichtet sind. Die Arten von elektronischen Nachweisen, die ausgestellt werden können, werden zudem in diesem Absatz nicht beschränkt; die Vertrauensinfrastruktur soll verschiedenen Akteuren zur Verfügung stehen und ihnen ermöglichen, elektronische Nachweise unterschiedlichster Art auszustellen.

Abs. 2

Die elektronischen Nachweise enthalten unterschiedliche Daten. Neben dem von der Ausstellerin festgelegten Basisinhalt müssen sie deren Identifikator und das Ausstellungsdatum des elektronischen Nachweises enthalten.

Art. 13 Widerruf

Der vorliegende Artikel widerspiegelt die gängige Praxis, wonach Ausstellerinnen die von ihnen ausgestellten elektronischen Nachweise selber widerrufen. Dritte, also Behörden oder natürliche Personen, sind nicht befugt, die von anderen Akteuren ausgestellten elektronischen Nachweise zu widerrufen. Zudem übernimmt dieser Artikel bestimmte Anforderungen, die für den Widerruf der E-ID gelten. Er bezweckt die Einführung gemeinsamer Mindestanforderungen, um die Inhaberinnen und Inhaber von elektronischen Nachweisen beim Vertragsabschluss mit der Ausstellerin zu schützen; das kantonale Recht und das Obligationenrecht sehen keine vergleichbaren Anforderungen vor. So ermöglicht er der Inhaberin oder dem Inhaber oder der gesetzlichen Vertretung von Minderjährigen unter 14 Jahren oder von Personen unter umfassender Beistandschaft, den Widerruf des elektronischen Nachweises zu verlangen. Zudem ist die Ausstellerin verpflichtet, einen elektronischen Nachweis zu widerrufen, wenn der begründete Verdacht auf dessen Missbrauch besteht. Bevor die Ausstellerin einen elektronischen Nachweis widerruft, überprüft sie die Informationen, die ihr übermittelt wurden. Ein widerrufener elektronischer Nachweis kann nicht mehr aktiviert werden: Die betroffene Person kann bei einer Ausstellerin einen neuen Ausstellungsantrag einreichen.

4. Abschnitt Nutzung von elektronischen Nachweisen

Art. 14 Form und Aufbewahrung von elektronischen Nachweisen

Die Inhaberin oder der Inhaber erhält den elektronischen Nachweis als Datenpaket. Dieses Datenpaket ist auf einem technischen Träger gespeichert, der der Inhaberin oder dem Inhaber gehört und in ihrer oder seiner alleinigen Kontrolle ist. (Dritte haben keinen Zugriff). Der Vorentwurf enthält keine Anforderungen an die technischen Mittel, die zur Aufbewahrung des elektronischen Nachweises verwendet werden müssen. Der technische Träger kann von der Inhaberin oder dem Inhaber des elektronischen Nachweises gewählt werden.

Art. 15 Übertragbarkeit von elektronischen Nachweisen

Abs. 1

Dieser Absatz legt fest, dass ein persönlicher (für eine natürliche Person ausgestellter) elektronischer Nachweis nicht einer Drittperson übertragen werden darf.²⁹ Er widerspiegelt eine zunehmende Praxis der Ausstellerinnen, mit der verhindert werden soll, dass mit der Ausstellung von persönlichen elektronischen Nachweisen Missbräuche betrieben werden. Ein

²⁶ SR 210

²⁷ SR 211.112.2

²⁸ SR 831.10

²⁹ Für das Vorweisen von elektronischen Nachweisen siehe Art. 16.

solcher Schutz der Nutzerinnen und Nutzer ist im Rahmen einer vom Bund bereitgestellten Vertrauensinfrastruktur besonders wichtig.

Abs. 2

Nach einem Wechsel des technischen Trägers (Smartphone, Computer usw.) kann die Inhaberin oder der Inhaber die Applikationen, die auf dem alten Träger installiert waren, normalerweise wiederherstellen. Der Bund kann den Inhabenden und Inhabern von elektronischen Nachweisen diese Möglichkeit ebenfalls bieten, indem er ein System für Sicherungskopien nach Artikel 21 bereitstellt. So können die elektronischen Nachweise, die die Inhaberin oder der Inhaber auf einem alten technischen Träger gespeichert hatte, mit geringem Aufwand auf einem neuen Träger wiederhergestellt werden. Mit der Übertragung von elektronischen Nachweisen in das System für Sicherungskopien nach Artikel 21 kann den Inhabenden und Inhabern diese Möglichkeit zur raschen Wiederherstellung angeboten werden. Dieser Absatz überträgt dem Bundesrat die Kompetenz, die technischen Vorgaben zu regeln, die für eine solche Übertragung von elektronischen Nachweisen erforderlich sind.

Art. 16 Vorweisen von elektronischen Nachweisen

Abs. 1

Die Inhaberin oder der Inhaber kann frei entscheiden, welche Bestandteile des Nachweises oder davon abgeleitete Aussagen sie oder er der Verifikatorin vorweist. Die Verifikatorin legt jedoch fest, welche Daten für den Zugang zu ihren Diensten erforderlich sind. Der Vorentwurf enthält keine Anforderungen an die Art von Daten, die bei der Überprüfung der elektronischen Nachweise übermittelt werden müssen; für diesen Entscheid ist die Verifikatorin zuständig. Der Handlungsspielraum der Inhaberin oder des Inhabers wird somit durch die Anforderungen begrenzt, die die Verifikatorinnen für den Überprüfungsprozess festlegen. Beschliesst die Inhaberin oder der Inhaber, die erforderlichen Elemente nicht zu übermitteln, kann sie oder er den elektronischen Nachweis nicht erbringen. Es gibt jedoch Grenzen dafür, was die Verifikatorinnen von einer Inhaberin oder einem Inhaber eines elektronischen Nachweises verlangen dürfen; sie müssen den Grundsatz der Beschränkung der Datenbearbeitung auf das strikte Minimum beachten, der besagt, dass die Personendaten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Bearbeitung notwendige Mass beschränkt sein müssen. Dabei handelt es sich um einen allgemeinen Grundsatz zum Schutz von Personendaten, der im Vorentwurf nicht erwähnt werden muss.

Abs. 2

Die im 5. Abschnitt geregelten Systeme erlauben es der Ausstellerin nicht, auf die Informationen im Zusammenhang mit dem Vorweisen und Überprüfen eines elektronischen Nachweises zuzugreifen. Sie sind so gestaltet, dass ein solcher Zugang technisch nicht möglich ist.

Abs. 3

Die Systeme nach dem 5. Absatz sind so gestaltet, dass die Betreiberin keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise hat. Soweit wie möglich sind die Systeme so zu gestalten, dass keine Rückschlüsse über die Verwendung der elektronischen Nachweise und die beteiligten Behörden und Privaten gezogen werden können.

5. Abschnitt Vertrauensinfrastruktur

Vorbemerkungen

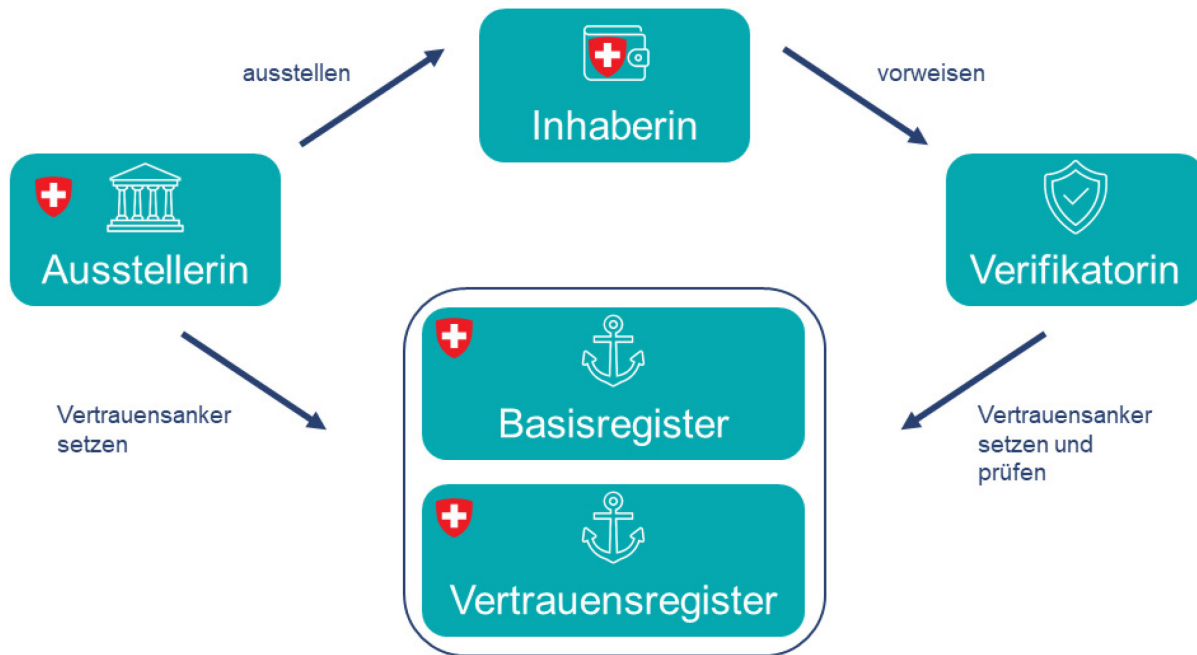
Der Bund hat die Kompetenz, eine Informatikinfrastruktur zu entwickeln und zu betreiben, mit welcher elektronische Nachweise ausgestellt, verwendet, verwaltet, bestätigt und widerrufen werden können. Es handelt sich um eine Reihe von Normen und Standards, Prozessen, Konzepten und Infrastrukturelementen, die das Vertrauen in die digitalen Prozesse herstellen, deren Konformität gewährleisten und von einem breiten Publikum akzeptiert und verwendet werden. In diesem Rahmen errichtet und betreibt der Bund die Informatikinfrastruktur im Interesse des Landes nach Artikel 81 BV. Dieser Abschnitt weicht somit von einer strengen Auslegung von Artikel 81 BV ab, wonach es sich bei öffentlichen Werken um materielle oder physische Werke handelt, wie ein Gebäude oder einen Tunnel. Aufgrund der technischen und wirtschaftlichen Fortschritte ist es angezeigt, das Konzept der «öffentlichen Werke» in einer Weise auszulegen, die die jüngsten Entwicklungen widerspiegelt³⁰, also als immaterielles oder nicht festes Werk, wie ein grösseres, mit der geplanten Vertrauensinfrastruktur vergleichbares Informatik- oder Kommunikationssystem.

Mit der Vertrauensinfrastruktur sollen die Ausstellung und die Verwendung der E-ID und anderer elektronischer Nachweise ermöglicht werden. Eine solche Öffnung des Systems ist angesichts der technischen und wirtschaftlichen Entwicklungen auf internationaler und europäischer Ebene nötig.

Noch nicht bestimmt ist, welche Stellen innerhalb der Bundesverwaltung für Aufbau und Betrieb der verschiedenen Elemente der Vertrauensinfrastruktur zuständig sein werden. Deshalb wird im 5. Abschnitt noch ganz allgemein von «Bund» gesprochen. Gestützt auf die Erfahrungen mit den Pilotprojekten wird dies zu klären und mit der Erarbeitung der Botschaft festzulegen sein.

³⁰ Vgl. Kap. 3.1

Die Vertrauensinfrastruktur besteht aus folgenden Akteuren und Elementen:



Art. 17 Basisregister

Abs. 1

Der Bund stellt interessierten Behörden und Privaten ein Basisregister zur Verfügung. Dieses stellt ein zentrales Element der Vertrauensinfrastruktur dar und bildet den ersten Teil des Vertrauensankers des Systems: Es ermöglicht, die Ausstellerinnen zu identifizieren und die Authentizität und Integrität der vorgewiesenen elektronischen Nachweise zu überprüfen.

Das Register kann in verteilter Form («distributed ledger technology», DLT), beispielsweise mithilfe von Blockchain, bereitgestellt werden. Die Wahl der technischen Lösung ist jedoch im Vorentwurf nicht geregelt, der soweit möglich technologieneutral sein soll (vgl. Erläuterungen zur Art. 1 Bst. c).

Abs. 2

Die im Basisregister erfassten Daten umfassen die Identifikatoren aller Ausstellerinnen; die kryptografischen Schlüssel der Ausstellerinnen, die erforderlich sind, um deren Identifikatoren zu kontrollieren und um die Authentizität und Integrität der elektronischen Nachweise zu überprüfen; und die Daten über widerrufenen elektronischen Nachweise. Diese Daten sind als alphanumerische Zeichenfolgen im Basisregister enthalten und lassen keine Rückschlüsse auf die Identität der Ausstellerinnen und Verifikatorinnen zu. Die Adressen, Telefonnummern, E-Mail-Adressen oder sonstige Kontaktangaben der Ausstellerinnen sowie die Personendaten der Inhaberrinnen und Inhaber werden im Basisregister nicht erfasst.

Abs. 3

Die Ausstellerinnen und Verifikatorinnen tragen ihre Daten selber in das Basisregister ein. Es handelt sich um einfache Erklärungen, die von keiner Drittperson überprüft werden. Die Daten werden beim Eintragen durch einen kryptografischen Algorithmus gesichert und gelten als fälschungssicher.

Ausstellerinnen und Verifikatorinnen, welche ihre Identifikatoren durch den Mechanismus zur Bestätigung des Identifikators bestätigen lassen möchten, müssen einen Eintrag im Basisregister machen. Dabei wird auf eine Verifizierung der Identität der Ausstellerinnen oder Verifikatorinnen verzichtet, bevor diese sich im Basisregister eintragen können. Dies würde ein ressourcenintensives Zulassungsverfahren voraussetzen, was zu einem teuren und unnötigen Flaschenhals führen würde. Zwar besteht damit ein Risiko, dass Ausstellerinnen oder Verifikatorinnen mit vorgetäuschter Identität elektronische Beweismittel ausstellen können. Dies wird aber durch die Veröffentlichung von Informationen über Fälle von begründetem Verdacht auf Missbrauch der Vertrauensinfrastruktur gemäss Artikel 22 gemildert und durch das System zur Bestätigung von Identifikatoren gemäss Artikel 18 ausgeschlossen. Der Ausschluss von registrierten Ausstellerinnen oder Verifikatorinnen ist technisch im Basisregister nicht möglich, jedoch im System zur Bestätigung von Identifikatoren gemäss Artikel 18.

Abs. 4

Das Basisregister enthält keine Daten über die elektronischen Nachweise, wie persönliche oder materielle Daten, oder Spuren der Ausstellung der elektronischen Nachweise. Behörden und Private, die das Basisregister verwenden, haben keinen Zugang zu den Personendaten, die bei der Ausstellung der elektronischen Nachweise bearbeitet werden.

Art. 18 System zur Bestätigung von Identifikatoren

Abs. 1

Der Bund stellt einen staatlichen Mechanismus zur Verfügung, mit dem überprüft werden kann, ob ein Identifikator und ein kryptografischer Schlüssel einer im Basisregister eingetragenen Ausstellerin oder einer bestimmten Verifikatorin gehört. Dieser bildet den zweiten Teil des Vertrauensankers des Systems: Es ermöglicht den Inhaberinnen und Inhabern von elektronischen Nachweisen und den Verifikatorinnen in Erfahrung zu bringen, mit wem sie effektiv zu tun haben. Der Bund könnte beispielsweise ein Vertrauensverzeichnis oder Zertifikate einsetzen, die von einer zuständigen Behörde ausgestellt werden.

Mit einem Mechanismus zur Bestätigung des Identifikators soll eine Verbindung zwischen der virtuellen und der physischen Welt hergestellt werden: Damit kann ein technischer Identifikator, der im Basisregister eingetragen ist, einer Organisation, Einheit oder einer Privatperson zugeordnet werden, die in der physischen Welt existiert. Dieser Mechanismus ist für die Nutzerinnen und Nutzer und die Verifikatorinnen von grosser Bedeutung. Da eine Verifikatorin nicht unbedingt eine direkte Beziehung zu einer Ausstellerin hat, kann sie diesen Mechanismus einsetzen, um nur die elektronischen Nachweise von verlässlichen Ausstellerinnen zu akzeptieren. Die E-ID beispielsweise wird von fedpol ausgestellt und der technische Identifikator der Ausstellerin erscheint in der E-ID. Eine Verifikatorin verwendet den Mechanismus zur Bestätigung des Identifikators, um sich zu vergewissern, dass der Identifikator und die kryptografischen Schlüssel der Ausstellerin der E-ID effektiv von fedpol stammen.

Der Bund stellt sicher, dass alle interessierten Behörden und Private Zugang zum Mechanismus zur Bestätigung des Identifikators haben. Über diesen Zugang können sie sicherstellen, dass es sich bei ihrem Gegenüber in der virtuellen Welt tatsächlich um die Organisation, Einheit oder die Person handelt, für die sie sich ausgibt. So kann die Authentizität der an einem Geschäftsprozess Beteiligten überprüft werden.

Die Einführung des Systems zur Bestätigung der Identifikatoren der Ausstellerinnen und der Verifikatorinnen erfolgt etappenweise. Von Anfang an wird dem Bund die Kompetenz übertragen, die Identität der Bundes-, Kantons- und Gemeindebehörden zu bestätigen, die sowohl als Ausstellerinnen als auch als Verifikatorinnen handeln. Er beauftragt eine Stelle in der Bundesverwaltung mit dem Betrieb und dem Unterhalt des Systems zur Bestätigung der Identität. Diese Stelle führt eine Liste der als Ausstellerinnen und Verifikatorinnen handelnden Behörden, die sie auf ihrer Website veröffentlicht und regelmässig aktualisiert.

Abs. 2

Der Bundesrat kann allenfalls vorsehen, dass der Bund auch den Identifikator und die kryptografischen Schlüssel von privaten Ausstellerinnen und Verifikatorinnen bestätigt. Dies könnte nötig werden, wenn das Ökosystem der E-ID sich genügend entwickelt und die Nachfrage des privaten Sektors genug gross ist. So kann auch das Vertrauen, das die Vertrauensinfrastruktur im Bereich der elektronischen Identifizierung genießt, gestärkt werden. Der Bundesrat kann dann die Anforderungen für die Bestätigung des Identifikators dieser Organisationen, Einheiten und Personen in einer Verordnung festlegen. Die technischen und organisatorischen Massnahmen, die in diesem Zusammenhang ergriffen werden müssen, sind ebenfalls vorzusehen.

Es ist möglich, dass die Akteure des privaten Sektors entscheiden, selber und separat einen nicht staatlichen (privaten) Mechanismus zur Bestätigung der Identifikatoren bereitzustellen; Absatz 2 schränkt ihre Aktivitäten in diesem Bereich nicht ein.

Abs. 3

Alle interessierten Behörden und Privaten können die vom System bestätigten Zuordnungen der Identifikatoren im Rahmen der Überprüfung elektronischer Nachweise abrufen.

Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Der Bund stellt den Personen, die dies beantragen, eine Anwendung zur Aufbewahrung und Vorweisung der elektronischen Nachweise, eine sogenannte staatliche elektronische Brieftasche, zur Verfügung. Es handelt sich um eine Software-Anwendung, mit der elektronische Nachweise sicher beantragt und bezogen sowie in einer für die Nutzerinnen und Nutzer transparenten und nachvollziehbaren Weise aufbewahrt, ausgewählt, kombiniert und geteilt werden können. Darin können die E-ID sowie viele andere elektronische Nachweise enthalten sein. Die Einführung der staatlichen elektronischen Brieftasche richtet sich soweit wie möglich nach den Standards, die zurzeit von der Europäischen Union erarbeitet werden.

Die Inhaberin oder der Inhaber der Brieftasche bewahrt den elektronischen Nachweis in einer elektronischen Brieftasche auf einem Träger seiner Wahl, beispielsweise einem Smartphone, auf. Die Verifikatorin kann die Inhaberin oder den Inhaber bitten, ihr die Daten über einen sicheren Kommunikationskanal vorzuweisen. Die Inhaberin oder der Inhaber kann in diesem Fall entscheiden, welche Daten aus seiner elektronischen Brieftasche sie oder er der Verifikatorin effektiv übermittelt.

Die Verwendung von elektronischen Brieftaschen, die von privaten Akteuren ausgestellt werden, ist im Gesetz nicht geregelt. Neben der staatlichen elektronischen Brieftasche können die Nutzerinnen und Nutzer auch andere Anwendungen für die Aufbewahrung und Vorweisung ihrer elektronischen Nachweise verwenden. Der Bund kann die Anbieterinnen von elektronischen Geldbörsen einem Bewertungs- und Zertifizierungsprozess nach Artikel 13 nDSG unterstellen. Es ist daher nicht nötig, die Zertifizierungsmöglichkeit im Vorentwurf zu regeln.

Art. 20 Anwendung zur Prüfung von elektronischen Nachweisen

Mit dieser Kann-Bestimmung kann der Bundesrat den Bund beauftragen, eine Anwendung bereitzustellen, mit der elektronische Nachweise auf ihre Gültigkeit überprüft werden können. Dabei handelt es sich um eine zusätzliche Sicherheitsmassnahme, die nötigenfalls ergriffen werden kann. Sie kann insbesondere dazu dienen, das Vertrauen, das die Vertrauensinfrastruktur in der Bevölkerung geniesst, zu stärken.

Art. 21 System für Sicherungskopien

Abs. 1

Nach dem Verlust eines Smartphones oder dem Kauf eines neuen Smartphones hat es sich bei den Nutzerinnen und Nutzer eingebürgert, die installierten Anwendungen aus einem Backup wiederherzustellen. So können die Funktionalitäten des alten Systems bei einem Wechsel des Smartphones rasch wieder verfügbar gemacht werden. Die gleiche Möglichkeit kann den Inhaberinnen und Inhabern von elektronischen Nachweisen angeboten werden. Dieser Absatz gibt dem Bundesrat die Kompetenz, ein Informatiksystem vorzusehen, in dem die Inhaberinnen und Inhaber Kopien ihrer elektronischen Nachweise speichern können. Nach einem Wechsel des technischen Trägers (Smartphone, Computer usw.) können sie die gespeicherten elektronischen Nachweise rasch wiederherstellen. Eine solche Sicherung der elektronischen Nachweise kann auf einer Cloud oder lokal auf einem technischen Träger der Inhaberin oder des Inhabers vorgesehen werden.

Die Nutzung des Systems für Sicherungskopien ist freiwillig. Allen Inhaberinnen und Inhabern steht es frei, die Möglichkeit zur Sicherung der elektronischen Nachweise zu nutzen.

Abs. 2

Nur die Inhaberinnen und Inhaber können auf die geschützten Sicherungskopien zugreifen. Das System erlaubt es Dritten nicht, darauf zuzugreifen.

Abs. 3

Die Sicherungskopien können auf Verlangen der Inhaberin oder des Inhabers oder der gesetzlichen Vertretung von Minderjährigen unter 14 Jahren oder von Personen unter umfassender Beistandschaft vernichtet werden.

Art. 22 Missbrauch der Vertrauensinfrastruktur

Mit dem Bereitstellen einer Vertrauensinfrastruktur verpflichtet sich der Bund auch, die erforderlichen Sicherheitsmassnahmen einzuführen, um das Missbrauchsrisiko möglichst gering zu halten. Da der Ausschluss von Ausstellerinnen aus dem Basisregister technisch nicht möglich ist, sieht das Vorprojekt diese Massnahme vor, um allfälligen Missbrauch entgegenzuwirken. Mit diesem Artikel wird der Bund beauftragt, eine Plattform zu betreiben, die dazu dient, schlechte Praktiken bekannt zu machen und die Bevölkerung vor möglichen Risiken zu warnen. Es ist jedoch nicht anzunehmen, dass Inhaberinnen und Inhaber, die die veröffentlichten Informationen möglicherweise nicht zur Kenntnis genommen haben, automatisch ihre Sorgfaltspflicht nach Artikel 7 Absatz 1 verletzen. Ausserdem darf die Plattform nur Fälle erwähnen, bei denen ein hinreichend begründeter Verdacht auf Missbrauch der Vertrauensinfrastruktur besteht. Diese Massnahme bezweckt also, die Nutzerinnen und Nutzer zu schützen und die Transparenz der Funktionsweise der Vertrauensinfrastruktur sicherzustellen.

Der Vorentwurf definiert den Begriff «Missbrauch» nicht, um mögliche Missbrauchsfälle nicht ungebührlich einzuschränken oder auszuschliessen. Ausserdem soll keine Verwirrung in Bezug auf Missbrauchsfälle entstehen, die bereits gesetzlich geregelt sind, wie z. B. der Identitätsdiebstahl (Art. 179^{decies} StGB, eingeführt durch das nDSG). Der von diesem Artikel erfasste Missbrauch umfasst Fälle der Nutzung der Vertrauensinfrastruktur, die nicht mit den im Vorentwurf vorgesehenen Zielen und Anforderungen übereinstimmen.

Art. 23 Quellcode der Vertrauensinfrastruktur

Der Bund veröffentlicht den Quellcode der Elemente der Vertrauensinfrastruktur nach dem 5. Abschnitt im Internet. Interessierte Personen können sich dort informieren. Die Entwicklung des Codes und die anderen dazu gehörenden Rechte sind nicht in diesem Artikel geregelt; sie fallen unter Artikel 9 des Entwurfs des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG)³¹.

Art. 24 Betrieb der Vertrauensinfrastruktur

Der Betrieb der Elemente der Vertrauensinfrastruktur wird durch einen Dienstleister innerhalb der Bundesverwaltung sichergestellt. Dieser Artikel ermöglicht es, die Anforderungen der sechs gleichlautenden Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129) zu gewährleisten. Zudem wird damit auch sichergestellt, dass der Bund nicht die gesamte Vertrauensinfrastruktur ausserhalb der Bundesverwaltung betreiben kann.

Art. 25 Technische Entwicklung

Abs. 1

Die technische Entwicklung schreitet rasch voran und wird sich auch nach dem Inkrafttreten dieses Vorentwurfs fortsetzen. Um sicherzustellen, dass dieser Entwicklung Rechnung getragen werden kann, gibt dieser Artikel dem Bundesrat die

³¹ BBL 2022 805

Kompetenz, auf Verordnungsstufe ergänzende Bestimmungen zu erlassen, damit die Vertrauensinfrastruktur an die technische Entwicklung angepasst werden kann und die in diesem Gesetz definierten Ziele weiterhin erreicht werden können.

Abs. 2

Aus verschiedenen Gründen kann für die ergänzenden Bestimmungen die Schaffung einer formellen gesetzlichen Grundlage erforderlich sein. Nach Artikel 34 Absatz 2 Buchstabe a nDSG reicht es beispielsweise nicht, die Bearbeitung von besonders schützenswerten Personendaten in einer Verordnung zu regeln; hierfür ist eine Grundlage in einem Gesetz im formellen Sinn erforderlich. In diesem Fall tritt die Verordnung des Bundesrates in folgenden Fällen ausser Kraft: wenn der Bundesrat zwei Jahre nach ihrem Inkrafttreten der Bundesversammlung keinen Entwurf einer gesetzlichen Grundlage unterbreitet hat; mit der Ablehnung des Entwurfs des Bundesrates durch die Bundesversammlung; mit Inkrafttreten der gesetzlichen Grundlage.

6. Abschnitt Gebühren

Art. 26

Abs. 1

Bei den Ausstellerinnen und Verifikatorinnen werden für die Eintragung der Daten (Identifikator, kryptografisches Material und Widerruf der elektronischen Nachweise) im Basisregister und im System zur Bestätigung von Identifikatoren Gebühren erhoben.

Die Höhe der Gebühren, die im Gesetz nicht vorgesehen ist, wird auf Verordnungsstufe festgelegt. Dabei wird sich der Gesetzgeber an praxisüblichen Beträgen orientieren.³²

Abs. 2

Wenn der Bundesrat beschliesst, ein System für Sicherungskopien nach Artikel 21 bereitzustellen, kann er in einer Verordnung Gebühren für dessen Nutzung vorsehen.

Abs. 3

Ebenfalls in einer Verordnung regeln wird der Bundesrat die Erhebung der Gebühren nach Artikel 46a des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG)³³.

Abs. 4

Für übrigen Dienstleistungen gemäss diesem Gesetz erhebt der Bund keine Gebühren. So werden für die Ausstellung der E-ID sowie für deren Nutzung und Überprüfung keine Gebühren erhoben. Auch die Verwendung der elektronischen Brieftasche des Bundes, das Aufrufen des Basisregisters und die Verwendung des Mechanismus zur Bestätigung des Identifikators sind gebührenfrei.

Durch den teilweisen Verzicht auf eine Gebührenerhebung soll die Nutzung und Verbreitung der E-ID gefördert werden. Der Bund hat ein grosses Eigeninteresse an einem möglichst verbreiteten Einsatz der E-ID, um den Austausch mit Behörden und Privaten zu vereinfachen.

7. Abschnitt Internationale Abkommen

Art. 27

In Anbetracht der hohen geschäftlichen und gesellschaftlichen Verflechtung mit den meisten EU-Mitgliedsländern hat die Schweiz ein Interesse daran, die Möglichkeit zu schaffen, früher oder später in das europäische System für die Interoperabilität von elektronischen Identitäten eingebunden zu sein. Dafür braucht es ein bilaterales oder internationales Abkommen. Dieser Artikel ermächtigt den Bundesrat, internationale Abkommen abzuschliessen, um die Verwendung und Anerkennung der E-ID auf internationaler Ebene zu erleichtern. Zudem kann er die erforderlichen Ausführungsvorschriften erlassen. Mit einem solchen Abkommen kann künftig die gegenseitige Anerkennung des schweizerischen Identifizierungssystems und derjenigen, die gemäss der eIDAS-Verordnung notifiziert oder von bestimmten EU-Mitgliedstaaten oder Drittstaaten eingeführt worden sind, sichergestellt werden.

8. Abschnitt Schlussbestimmungen

Art. 28 Ausführungsbestimmungen

Die Ausführungsbestimmungen dieses Gesetzes regeln die Umsetzung der technischen und organisatorischen Aspekte im Zusammenhang mit der Kommunikation der elektronischen Nachweise sowie die Funktionsweise der Bestandteile der Vertrauensinfrastruktur. Dabei soll insbesondere Folgendes geregelt werden: das Format der elektronischen Nachweise; die Standards und Protokolle für die Kommunikationsvorgänge beim Ausstellen und Vorweisen elektronischer Nachweise;

³² Siehe zum Beispiel die Angaben welche von der Sovrin Foundation geliefert werden: <https://sovrin.org/issue-credentials/>.
³³ SR 172.010

die Bestandteile und die Funktionsweise des Basisregisters, des Systems zur Bestätigung von Identifikatoren, der Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen und des Systems für Sicherungskopien; die Nachweise, die bei der Aufnahme in das System zur Bestätigung von Identifikatoren vorgelegt werden müssen; die Schnittstellen, Elemente und Funktionsweise des Informationssystems für die Ausstellung und den Widerruf von E-ID sowie die Rollen und Zuständigkeiten der Akteure, die an der Bereitstellung und Nutzung der Vertrauensinfrastruktur beteiligt sind. Ferner wird auch die Kompetenz an den Bundesrat delegiert, technische und organisatorische Massnahmen für den Datenschutz und die Datensicherheit beim Betrieb und der Nutzung der Vertrauensinfrastruktur in einer Verordnung zu regeln.

Mit diesen Ausführungsbestimmungen sollen insbesondere neue Standards festgelegt sowie die internationalen und europäischen Standards in diesem Bereich harmonisiert werden, um die Umsetzung dieses Gesetzes zu erleichtern. Aus Gründen der Klarheit und Transparenz werden sie in einer Bestimmung zusammengefasst.

Art. 29 Änderung anderer Erlasse

Im Anhang zum Vorentwurf wird die Änderung anderer Erlasse vorgeschlagen. Insbesondere wird fedpol ermächtigt, auf die Informationssysteme ISA, Infostar und ZEMIS zuzugreifen. Mit den vorgeschlagenen Änderungen wird auch die Verwendung der E-ID in bestimmten Bereichen, wie dem elektronischen Patientendossier sowie Schuldbetreibung und Konkurs, exemplarisch geregelt. In der Vernehmlassung ist zu prüfen, ob weitere Bundesgesetze angepasst werden müssen (oder ob die Änderungen auf Verordnungsstufe erfolgen können).

Art. 30 Referendum und Inkrafttreten

Wie jedes Bundesgesetz untersteht auch der Vorentwurf dem fakultativen Referendum und der Bundesrat wird das Datum des Inkrafttretens bestimmen.

Änderung anderer Erlasse

Vorbemerkung

Die bisherigen Abklärungen haben ergeben, dass die Anforderungen an die Identifizierung und Authentifizierung für E-Government-Anwendungen, sofern erforderlich, auf Verordnungs- oder Weisungsebene geregelt werden müssen. Verschiedene Verordnungen und Weisungen müssen deshalb im Hinblick auf die Umsetzung des E-ID-Gesetzes geändert werden. Dies erfolgt aber erst mit dem Erlass der Ausführungsbestimmungen zum E-Gesetz. Nachfolgend wird deshalb nur die Änderung anderer Bundesgesetze erläutert.

1. Bundesgesetz vom 20. Juni 2003³⁴ über das Informationssystem für den Ausländer- und den Asylbereich

Art. 9 Abs. 1 Bst. c und 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. Diese Liste soll mit einem neuen Zweck ergänzt werden: der Erfüllung der Aufgaben, für die sie gemäss diesem Vorentwurf zuständig sind.

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 durch ein Abrufverfahren 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 Vorentwurf wird der Liste ein neuer Zweck angefügt: der Erfüllung ihrer Aufgaben nach dem E-ID-Gesetz.

2. Ausweisgesetz vom 22. Juni 2001³⁵

Art. 11 Abs. 2

In Artikel 11 Absatz 2 wird aufgezählt, zu welchen Zwecken fedpol im Rahmen der Führung des ISA Daten bearbeiten darf. Mit dieser Vorlage wird die Aufzählung der Zwecke nach Buchstaben gegliedert. Zudem wird ein neuer Zweck der Datenbearbeitung hinzugefügt: die Erfüllung der Aufgaben nach dem E-ID-Gesetz.

³⁴ SR 142.51

³⁵ SR 143.1

3. Zivilgesetzbuch³⁶

Art. 43a Abs. 4 Ziff. 9

Artikel 43a ZGB regelt den Zugang im Abrufverfahren zu den elektronischen Registern zur Führung des Personenstandes. Die Auflistung der Stellen, die Zugriff auf Infostar haben, wird um fedpol erweitert.

4. Bundesgesetz vom 11. April 1889³⁷ über Schuldbetreibung und Konkurs

Wie bereits in den Erläuterungen zu Artikel 9 resp. 28 ausgeführt, können Fragen wie die Verpflichtung zur Anerkennung oder die Rechtsfolgen des Einsatzes einer E-ID nicht generell im E-ID-Gesetz geregelt werden, sondern sollen exemplarisch in ausgewählten Rechtsbereichen aufgezeigt werden. Im Rahmen der Vernehmlassung ist weiter zu prüfen, ob analoge Regelungen auch in anderen Rechtsbereichen erforderlich sind.

Art. 8a Abs. 2^{bis}

Für das Einreichen eines Gesuchs um Auskunft aus dem Betreibungsregister bestehen verschiedene Möglichkeiten: Vorsprache am Schalter des Betreibungsamtes, Einreichen eines schriftlichen Gesuchs per Post oder elektronisch via eine der verschiedenen Portallösungen, welche Bund, Kantone oder die Privatwirtschaft anbieten. Betrifft das Gesuch eine Drittperson, muss gemäss Artikel 8a Absatz 1 SchKG ein Interesse glaubhaft gemacht werden, bei sog. Eigenauszügen ist ein Identifikationsnachweis erforderlich, welcher in der Regel durch das Mitsenden einer Kopie einer Identitätskarte oder eines Passes erbracht werden kann. Gerade bei den Portallösungen kann der Bestellprozess für alle Beteiligten vereinfacht werden, wenn die Identifizierung der Gesuchstellerin oder des Gesuchstellers durch das Vorweisen einer E-ID erfolgen kann. Zudem wird die Qualität der Identifizierung – im Vergleich zu einer mehr oder weniger lesbaren (und leicht fälschbaren) Kopie einer Identitätskarte oder eines Passes – deutlich gesteigert.

Art. 33a Abs. 2^{bis}

Gemäss Artikel 33a Absatz 1 SchKG können Eingaben bei den Betreibungs- und Konkursämtern und den Aufsichtsbehörden elektronisch eingereicht werden. Diese sind mit einer qualifizierten elektronischen Signatur zu versehen (Art. 33a Abs. 2 SchKG), womit die Eingabe eindeutig einer natürlichen Person zugeordnet werden kann. Da diese eindeutige Zuordnung auch mit dem Vorweisen einer E-ID sichergestellt werden kann, ist bei den Portallösungen des Bundes oder eines Kantons auf das Anbringen einer qualifizierten elektronischen Signatur zu verzichten. Damit kann der Eingabeprozess für alle Beteiligten vereinfacht werden.

5. Bundesgesetz vom 19. Juni 2015³⁸ über das elektronische Patientendossier

Art. 7

Mit diesem Vorentwurf wird der Begriff «elektronische Identität» in Artikel 7 des EPDG durch «elektronisches Identifikationsmittel» ersetzt. Der Begriff «elektronisches Identifikationsmittel» entspricht dem in diesem Artikel geregelten Konzept besser. Zudem sollen Verwechslungen mit dieser Vorlage vermieden werden, die den rechtlichen Rahmen für den staatlichen elektronischen Identitätsnachweis schafft. Bei letzterem handelt es sich um einen Identitätsnachweis einer Person in elektronischer Form und nicht um ein Identifikationsmittel für die Authentifizierung und den Zugang zu einem Dienst oder einer Anwendung. Aus Klarheitsgründen ist es angezeigt, eine begriffliche Unterscheidung zwischen den beiden Gesetzen beizubehalten und das EPDG zu ändern.

Art. 11 Bst. c

Nach dem heutigen System des EPDG werden die elektronischen Identifikationsmittel für den Zugang zum elektronischen Patientendossier von Privaten herausgegeben, die durch eine anerkannte Stelle zertifiziert sein müssen. Langfristig sollen auch diese Identifikationsmittel vom Bund herausgegeben werden. Damit soll dem politischen Willen des Souveräns mit der Ablehnung des E-ID-Gesetzes in der Volksabstimmung vom 7. März 2021 auch im Bereich des EPDG Nachachtung geschaffen werden, der diese Aufgabe nicht in den Händen der Privatwirtschaft sehen wollte.

Wenn der Bund diese Aufgabe übernimmt, wird er die Anforderungen nach der EPD-Gesetzgebung erfüllen müssen, eine Zertifizierung der zuständigen Bundesstelle ist dafür aber nicht erforderlich, weshalb darauf verzichtet werden soll. Da während einer gewissen Übergangszeit auch weiterhin private Identifikationsmittel für den Zugang zum elektronischen Patientendossier im Einsatz stehen werden, hält Artikel 11 Buchstabe c neu fest, dass private Herausgeber von Identifikationsmitteln weiterhin zertifiziert sein müssen.

³⁶ SR 210

³⁷ SR 210

³⁸ SR 816.1

6. Bundesgesetz vom 18. März 2016³⁹ über die elektronische Signatur

Art. 9 Abs. 4^{bis}

Im Ausgabeprozess für eine elektronische Signatureinheit ist die persönliche Vorsprache vorgeschrieben. Diese entfällt, wenn der Identitätsnachweis durch einen elektronischen Identitätsnachweis nach diesem Gesetz erbracht werden kann. Der Bundesrat kann auf in einer Verordnung vorsehen, dass die betreffende Person nicht persönlich erscheinen muss, wenn der Identitätsnachweis auf anderem Weg mit der erforderlichen Verlässlichkeit erbracht wird.

7. Bundesgesetz vom ...⁴⁰ über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Dieser Vorentwurf schafft den rechtlichen Rahmen für den staatlichen elektronischen Identitätsnachweis. Mit dem elektronischen Identitätsnachweis kann sich die Inhaberin oder der Inhaber identifizieren, aber nicht authentifizieren, um auf einen Online-Dienst oder eine Anwendung zuzugreifen. Aus diesem Grund wird mit diesem Vorentwurf das zukünftige EMBAG geändert und ein Authentifizierungssystem als «IKT-Mittel» im Sinne von Artikel 11 Absätze 1–3 EMBAG eingeführt. Dieses Authentifizierungssystem basiert auf der E-ID und kann Zugang zu einem Dienst oder einer Anwendung gewähren.

Dieses System zur Authentifizierung natürlicher Personen steht als IKT-Mittel auch den Kantonen und Gemeinden zur Verfügung. Zudem kann es genutzt werden von Organisationen und Personen des öffentlichen oder privaten Rechts, soweit sie für den Vollzug von Bundesrecht zuständig sind.

Das EMBAG befindet sich derzeit in der parlamentarischen Beratung und wurde noch nicht vom Parlament verabschiedet. Deshalb wird die vorliegende Änderung nach Abschluss der parlamentarischen Beratungen neu zu beurteilen sein.

5 Auswirkungen

5.1 Finanzielle und personelle Auswirkungen auf den Bund

In der Anfangsphase wird das E-ID-Projekt Kosten für die Gesetzgebungsarbeiten und andere Bereiche generieren, namentlich für die Kommunikation und die Begleitung damit verbundener Projekte. Wenn dem Finanzierungsantrag des EJPD stattgegeben wird, können diese Kosten mit den Geldern zur Verwirklichung der Ambition 3 «Behördenübergreifende digitale Identifikation etablieren» der Agenda der Organisation Digitale Verwaltung Schweiz (DVS) gedeckt werden. Für 2022 wurden die beantragten Mittel (CHF 750'000) durch die Gremien der Organisation DVS genehmigt. Zusätzlich wurden für 2023 1 000 000 Franken in der Finanzplanung der Organisation DVS eingestellt.

Eine erste Schätzung der Projekt- und Betriebskosten wurde gestützt auf die Erfahrungen bei der Ausstellung des Covid-Zertifikats getroffen. Dank den geplanten Pilotversuchen werden die Kosten bei der Ausarbeitung der Botschaft noch genauer bestimmt werden können.

Gemäss dieser Schätzung werden sich die Projektkosten zwischen 25 und 30 Millionen Franken bewegen. Sie umfassen die Entwicklung und die Inbetriebnahme der Vertrauensinfrastruktur. Darin inbegriffen sind die Entwicklung des Informationssystems sowie die Anpassung der Infrastruktur des Identitätsdienstes von fedpol. Von der Lancierung bis zur Inbetriebnahme (go live) der Vertrauensinfrastruktur wird das Projekt zwischen 24 und 36 Monaten dauern.

Die Betriebskosten des Projekts werden sich zwischen 10 und 15 Millionen Franken bewegen. Darüber hinaus muss der Umfang des technischen Supports geschätzt werden, welcher sowohl für die Vertrauensinfrastruktur als auch für die Herausgabe der E-ID gewährleistet werden muss. Die Form und die Dimensionen des Supports können erst nach den Erfahrungen in den Pilotprojekten und nach einer Auswertung potenzieller Synergien zwischen den Ämtern für bestehende und künftige Systeme bestimmt werden.

Zur Finanzierung der Investitionen werden bei der Digitalen Verwaltung Schweiz (DVS) finanzielle Beiträge beantragt, denn die behördenübergreifende digitale Identifikation ist eines der Ziele der DVS. Der Betrieb und die Weiterentwicklung müssen so weit wie möglich durch Gebühren finanziert werden.

5.2 Auswirkungen auf die Kantone und Gemeinden

Kantone und Gemeinden werden verpflichtet die staatliche E-ID zu akzeptieren, wenn sie eine elektronische Identifikation durchführen. Dies ist angezeigt, weil die E-ID als staatliches elektronisches Identifikationsmittel zum Nachweis der eigenen Identität in der virtuellen Welt ausgestaltet wird und damit vergleichbar ist mit Identitätskarte oder Pass in der physischen Welt, die auch bei jeder Identifizierung von allen Behörden akzeptiert werden.

Auf Kantons- und Gemeindeebene sind verschiedene E-Government-Lösungen im Einsatz. Die Prozesse bei der Identifizierung und Authentifizierung, um Zugang zu diesen Systemen zu erhalten, könnten durch die Einführung der E-ID und

³⁹ SR 943.03

⁴⁰ BBL 2022 805

den Einsatz der Vertrauensinfrastruktur erheblich vereinfacht werden. Die Nutzung der E-Government-Dienstleistungen von Städten und Gemeinden wird durch die einfache und sichere Identifizierung gefördert.

Ausserdem werden die Kantone, Gemeinden und Städte bestimmte Aufgaben dank der Vertrauensinfrastruktur effizienter erfüllen können. Sie können zum Beispiel digitale Fischereipatente, Parkkarten und Wohnsitzbescheinigungen ausstellen. Die Ausstellerinnen werden sich weder um die Softwareapplikation für die Nutzerinnen und Nutzer (elektronische Brieftasche) noch um die Sicherheitsmassnahmen kümmern müssen, sondern ausschliesslich um ihre eigenen Prozesse und Verwaltungssysteme. In diesem Sinn wird die Vertrauensinfrastruktur Fortschritte bei der Digitalisierung der Tätigkeiten der öffentlichen Hand auf allen Stufen ermöglichen.

Der Finanzbedarf für allfällige Anpassungen der E-Government-Systeme, die von Kantonen, Städten und Gemeinden angeboten werden, ist schwer abzuschätzen. Die Kosten sollten durch die Einsparungen, welche die Gemeinden, Städte und Kantone mittelfristig dank der Einführung digitaler Prozesse erzielen werden, abgedeckt werden. Ausserdem werden die Kantone durch den Einsatz der Vertrauensinfrastruktur des Bundes Kosten vermeiden können, z. B. müssen sie nicht in ihre eigene Infrastruktur investieren und können sie für die Einführung eines digitalen Führerausweises verwenden. Gemäss dem Gesetz werden sie und die anderen Gebietskörperschaften – wie auch die Privaten – Gebühren für die Eintragung im Basisregister und die Bestätigung der Zugehörigkeit bezahlen. Sie werden so zur Finanzierung des Betriebs der Vertrauensinfrastruktur der E-ID beitragen. Die damit verbundenen Kosten sind jedoch deutlich tiefer als die Kosten einer eigenen Infrastruktur.

Der digitale Wandel ist auf Bundes-, Kantons- und Gemeindeebene bereits im Gange. Trotz dieses Trends zur Digitalisierung der Gesellschaft sind gewisse Bevölkerungsgruppen nicht bereit, sich diesem Wandel zu stellen. Es ist ihnen lieber, eine Behörde in der physischen Welt aufzusuchen, weil sie Unterstützung benötigen. Die Kantone haben bereits verschiedene Angebote und Dienstleistungen für Personen eingerichtet, die Unterstützung oder allgemeine Informationen suchen. Diese bestehenden Anlaufstellen können und sollen auch für die Unterstützung in Zusammenhang mit der E-ID eingesetzt werden.

Es wird Sache der Kantone sein zu bestimmen, wie sie diese Unterstützungsstellen bezeichnen und organisieren. Da diese aber als allgemeine Unterstützung und nicht nur für die E-ID notwendig sind, dürfen die Auswirkungen als gering bezeichnet werden.

5.3 Auswirkungen auf die Volkswirtschaft

Der Bundesrat will den erforderlichen Beitrag zur Digitalisierung der schweizerischen Gesellschaft leisten. Zu diesem Zweck hat er zahlreiche Massnahmen ergriffen, mit denen hauptsächlich der gesetzliche Rahmen angepasst werden soll und die nötigen Infrastrukturen geschaffen werden sollen.

Die Einführung der elektronischen Identifizierung und der Vertrauensinfrastruktur ist ein wichtiger Eckstein in einem umfassenderen Ökosystem elektronischer Nachweise, das Vertrauen und Sicherheit im elektronischen Geschäftsverkehr herstellen kann. Dadurch können anspruchsvolle Geschäfte mit dem Staat wie auch unter Privaten elektronisch und damit effizienter abgewickelt werden.

5.4 Auswirkungen auf die Gesellschaft

Die Digitalisierung der Gesellschaft schreitet voran. Immer mehr Geschäfte können online abgewickelt werden. Es ist immer weniger nötig, persönlich vorzusprechen. Es wird vermehrt erwartet, dass verschiedene Aufgaben elektronisch, vorzugsweise auf einem Smartphone, erledigt werden können. An Kommunikationsmitteln dafür mangelt es zwar nicht. Es ist aber noch nicht möglich, elektronische Nachweise zu schaffen, zu verwalten und vorzuweisen, die einsatzfähig genug sind und von den meisten Anbieterinnen anerkannt werden. Mit der Vertrauensinfrastruktur des Bundes soll diese Lücke geschlossen werden. Sie schafft ein Ökosystem, das es ermöglicht, auf gesicherte Weise verschiedene elektronische Nachweise auszustellen, einzusetzen und vorzuweisen. Es handelt sich um eine Reihe von Normen und Standards, Prozessen, Konzepten und Infrastrukturelementen, die das Vertrauen in die digitalen Prozesse herstellen, deren Konformität gewährleisten und von einem breiten Publikum akzeptiert und verwendet werden. Der elektronische Geschäftsverkehr im öffentlichen und im privaten Sektor kann, unter Beachtung der Anforderungen des nDSG, effizienter und sicherer abgewickelt werden. Durch eine solche Infrastruktur können die Vernetzung zwischen den verschiedenen Akteuren und das Vertrauen in den elektronischen Geschäftsverkehr erhöht werden.

Einer der wesentlichen Vorteile der E-ID ist die Möglichkeit, die eigenen Daten einem Gegenüber im Internet zu zeigen. Die Inhaberinnen und Inhaber erhalten so nicht nur eine erhöhte Kontrolle über ihre Daten, sondern im Rahmen des elektronischen Geschäftsverkehrs auch mehr Verantwortung, namentlich hinsichtlich der Sorgfaltspflicht. Der Umfang der Verantwortung und deren Auswirkungen werden in einer Verordnung genauer definiert werden. Ausserdem erfordert der Besitz einer E-ID gewisse Kenntnisse über die Funktionsweise des eigenen Systems. Die öffentliche Debatte über den Vorentwurf wird bereits in gewissem Masse zur Förderung der digitalen Kompetenz der Schweizer Bevölkerung in diesem Bereich beitragen.

6 Rechtliche Aspekte

6.1 Verfassungsmässigkeit

Die Kompetenz zur Regelung der E-ID und der Vertrauensinfrastruktur ergibt sich aus den Artikeln 38 Absatz 1, 81, 95 Absatz 1 und 121 Absatz 1 der Bundesverfassung (BV).

Was die staatliche elektronische Identität angeht, stützt sich der Vorentwurf auf Artikel 38 Absatz 1 und 121 Absatz 1 BV. Gemäss Artikel 38 Absatz 1 BV ist der Bund dafür zuständig, Erwerb und Verlust der Bürgerrechte durch Abstammung, Heirat und Adoption zu regeln. Gemäss Artikel 121 Absatz 1 BV ist die Gesetzgebung über die Ein- und Ausreise, den Aufenthalt und die Niederlassung von Ausländerinnen und Ausländern sowie über die Gewährung von Asyl Sache des Bundes. Obwohl die beiden Artikel nicht ausdrücklich die Ausweise regeln, muss der Bund die Kompetenz haben, die erforderlichen Ausweise zu regeln. Dies selbst dann, wenn sie nicht ausschliesslich dem Nachweis der Staatsangehörigkeit der Schweizer Bürgerinnen und Bürger und des Aufenthaltsstatus der ausländischen Einwohnerinnen und Einwohner dienen. Da die staatliche elektronische Identität (E-ID) diese Dokumente in bestimmten Tätigkeitsbereichen ersetzen soll, ist es gerechtfertigt, die künftige Gesetzesvorlage in Bezug auf den amtlichen Nachweis der Identität, der Staatsangehörigkeit und des Aufenthaltsstatus der Ausländerinnen und Ausländer auf diese Verfassungsgrundlage zu stützen.

Die Kompetenz zur Schaffung einer Vertrauensinfrastruktur ist in Artikel 81 BV geregelt, gemäss dem der Bund im Interesse des ganzen oder eines grossen Teils des Landes öffentliche Werke errichten und betreiben oder ihre Errichtung unterstützen kann. Ein «öffentliches Werk» im Sinne dieser Bestimmung ist herkömmlicherweise physischer Art, im Sinne eines Bauwerks wie einem Tunnel. Nach der zeitgemässen und teleologischen Auslegung von Lendi⁴¹ und Biaggini⁴² könnte ein «öffentliches Werk» auch immateriell oder nicht fest sein wie ein grösseres, mit der geplanten Vertrauensinfrastruktur vergleichbares Informatik- oder Kommunikationssystem. So könnte ein Vorentwurf zur Schaffung einer Vertrauensinfrastruktur, mit der verschiedene elektronische Nachweise ausgestellt und bestätigt werden können, auf Artikel 81 BV gestützt werden. In diesem Zusammenhang ist darauf hinzuweisen, dass Artikel 81 BV dem Bund nicht die Kompetenz verleiht, für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen verbindliche technische und organisatorische Standards zu erlassen und durchzusetzen.⁴³

6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Der Vorentwurf ist mit den bestehenden internationalen Verpflichtungen vereinbar. Bei der Erarbeitung der Vorlage wurde darauf geachtet, dass die internationale Interoperabilität grundsätzlich möglich bleibt. Falls zu einem späteren Zeitpunkt gewünscht, kann die in der Schweiz anerkannte E-ID internationale Anerkennung erlangen. Zur Umsetzung wären internationale Abkommen notwendig.

6.3 Erlassform

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

Auf Wunsch der Politik wurde der Vorentwurf unter grossem Zeitdruck ausgearbeitet. Aufgrund der technologieneutralen Ausgestaltung ist er zudem sehr abstrakt und wagt sich mit der Schaffung einer immateriellen öffentlichen Infrastruktur des Bundes (vgl. Art. 81 BV) auf neues Terrain. Je nach den Vernehmlassungsergebnissen wird er noch angepasst werden müssen, insbesondere in Bezug auf die Erfahrungen aus den Pilotversuchen und die von den Behörden geplante sektorielle Verwendung.

6.4 Unterstellung unter die Ausgabenbremse

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

⁴¹ EJPD, Bundesamt für Justiz, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011, VPB 2012.1 (S. 1 - 17), Ausgabe vom 1. Mai 2012, S. 8; Lendi, Martin, in: St. Galler Kommentar, 2. Aufl. 2008, Art. 81 Rz. 6.

⁴² Ibid; Biaggini, Giovanni in BV-Kommentar, Zürich 2007, Art. 81 Rz. 2, kritisiert von Markus Kern im Basler Kommentar, Rz. 6 und 9.

⁴³ Ibid; Biaggini, G., ibid, Art. 81 Rz. 3.

6.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Die Einführung der E-ID und der Vertrauensinfrastruktur ist unumstritten. Die vorgesehene Aufgabenteilung und -erfüllung tangiert weder das Subsidiaritätsprinzip noch das Prinzip der fiskalischen Äquivalenz. Die finanziellen Auswirkungen der Vorlage auf den Bund sind höher als 10 Millionen Franken. Die finanziellen Auswirkungen auf die Kantone können noch nicht beziffert werden.

6.6 Delegation von Rechtssetzungsbefugnissen

Mit dem Vorentwurf werden keine Rechtsetzungsbefugnisse delegiert. In den Artikeln 6, 11 Absatz 4, 25, 26 und 27 wird der Bundesrat lediglich ermächtigt, die nötigen Ausführungsbestimmungen zu erlassen.

6.7 Datenschutz

Die Regeln des Datenschutzrechts (nDSG und die zugehörigen Verordnungen) gelten für alle Beteiligten. Die Einzelpersonen, die Ausstellerinnen und die Verifikatorinnen des privaten Sektors unterliegen den Bestimmungen, die für Privatpersonen gelten. Der Bund (fedpol und andere Behörden), die Ausstellerinnen und Verifikatorinnen des öffentlichen Sektors unterliegen den Bestimmungen, die für Bundesorgane gelten. Im vorliegenden Vorentwurf wird nicht auf die einschlägigen Bestimmungen des nDSG verwiesen. Damit sollen Wiederholungen vermieden und soll Klarheit für die Auslegung sichergestellt werden.

Der Vorentwurf hat auch den Zweck, in seinem Regelungsbereich den Datenschutz zu fördern. Artikel 1 Absatz 2 übernimmt im Übrigen den Zweck nach Artikel 6 nDSG und präzisiert in den Ziffern 1–4, wie er im Kontext der E-ID umgesetzt werden wird. Es geht insbesondere darum, die Anforderungen der sechs inhaltlich identischen Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129) aufzunehmen, die nach der Ablehnung der früheren Vorlage in der Abstimmung vom 7. März 2021 von allen Fraktionen eingereicht worden sind. Gemäss den Motionärinnen und Motionären muss die staatliche elektronische Identität gewissen Grundsätzen entsprechen: Es sollen insbesondere die Grundsätze «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung (wie Speicherung der Ausweisdaten bei den Nutzerinnen und Nutzern) eingehalten werden. In Artikel 1 Absatz 2 Buchstabe b werden diese Anforderungen als spezifische Zwecke formuliert, die im Rahmen des Schutzes der Personendaten zu erfüllen sind.

Artikel 1 Absatz 2 Buchstabe c des Vorentwurfs soll ferner sicherstellen, dass die Ausgestaltung der E-ID und der Vertrauensinfrastruktur dem aktuellen Stand der Technik entspricht. Der Begriff «aktueller Stand der Technik» unterscheidet sich konzeptuell von ähnlichen Begriffen wie «die anerkannten Regeln der Technik» und «der aktuelle Stand der Wissenschaft und der Forschung». Kurz gesagt verweist der Begriff «aktueller Stand der Technik» auf innovativere Methoden als der Begriff «anerkannte Regeln der Technik» und auf ältere Methoden als der Begriff «Stand der Wissenschaft und der Forschung». Diese Unterscheidung ist bei der Bestimmung des erforderlichen Sicherheitsniveaus wesentlich. Nach Artikel 7 Absatz 2 nDSG müssen ebenfalls Massnahmen ergriffen werden, die dem «Stand der Technik» entsprechen, doch es werden keine Kriterien aufgestellt, die Aufschluss über den Inhalt des Begriffs «Stand der Technik» geben. Daraus darf jedoch nicht geschlossen werden, dass das, was im Gesetz nicht konkret bestimmt ist, nicht überprüft und folglich nicht angewendet werden kann. Der Gesetzgeber strebt mit diesem Begriff ein hohes Niveau der Datensicherheit und des Datenschutzes dank fortschrittlicher Verfahren an. Zu diesem Zweck ist die regelmässige Überprüfung der umgesetzten Sicherheitsmassnahmen auf ihre Wirksamkeit hinsichtlich der geforderten Schutzziele, ihrer Aktualität sowie ihres Innovationsgrads zu fördern. So sind die Sicherheitsmassnahmen auch mit den Sicherheitsprodukten auf dem Markt zu vergleichen: Was heute als «Stand der Technik» gilt, kann morgen aufgrund der innovationsbedingten Verschiebung, also der Alterung der Sicherheitsmassnahme, im Vergleich mit anderen verfügbaren Sicherheitsmassnahmen eher den «anerkannten Regeln der Technik» zugeordnet werden.

Aus Gründen der Transparenz werden in Artikel 2 die Daten aufgeführt, die die E-ID enthält. Dabei handelt es sich um Personenidentifizierungsdaten (Abs. 2) und weiteren Daten (Abs. 3). Die Personenidentifizierungsdaten der Inhaberin oder des Inhabers umfassen: den amtlichen Namen, die Vornamen, das Geburtsdatum, das Geschlecht, den Geburtsort, die Nationalität und das Gesichtsbild aus ISA und ZEMIS. Diese Daten sind in den amtlichen Registern des Staates verfügbar, auf die fedpol nach Artikel 11 Absatz 3 Zugriff hat. Nebst den Personenidentifizierungsdaten enthält eine E-ID die AHV-Nummer sowie weitere Daten, welche bei der Ausstellung der E-ID generiert werden: Dabei handelt es sich um die E-ID-Nummer, das Ausstellungsdatum, das Ablaufdatum und die Angaben zum Ausstellungsprozess. Ferner enthält die E-ID Daten zum Ausweis, der zur Ausstellung der E-ID verwendet wurde, insbesondere Typ, Nummer und Gültigkeitsdauer des Ausweises. Details werden in einer Verordnung noch präzisiert werden.

Nach Artikel 34 Absatz 1 nDSG dürfen Bundesorgane Personendaten nur bearbeiten und bekanntgeben, wenn dafür eine gesetzliche Grundlage besteht. In Anwendung von Artikel 6 Absatz 3 nDSG ist der Zweck des vorgesehenen Systems klar und für die betroffene Person erkennbar anzugeben. Dementsprechend umfasst das vorliegende Gesetz genaue Bestimmungen, die fedpol die Führung eines Informationssystems für die Identifizierung der antragstellenden Personen erlauben. In Artikel 11 werden die Art, der Inhalt und der Zweck des Systems bestimmt. Nach Artikel 11 Absatz 2 enthält das System folgende Arten von Daten: die Daten nach Artikel 2 Absatz 3 und die Angaben zum Widerruf einer E-ID. Ausserdem werden darin sogenannte Randdaten aufbewahrt, die in Zusammenhang mit der Identitätsüberprüfung und dem Ausstellungsprozess anfallen und für Support- und Statistikzwecke sowie zur Missbrauchsverhinderung erforderlich sind. Die Personendaten werden direkt in den Registern des Bundes abgefragt und nicht im Informationssystem von fedpol gespeichert

(vgl. Abs. 3). In Artikel 11 Absatz 3 werden die Register des Bundes genannt, auf die fedpol Zugriff hat, damit es die Personendaten abgleichen kann. Das geplante System soll es fedpol ermöglichen, seine Aufgaben bei der Ausstellung und beim Widerruf der elektronischen Nachweise zu erfüllen. Darüber hinaus wird in Absatz 4 eine Frist von längstens fünf Jahren nach Ablauf der E-ID für die Aufbewahrung der Daten im System festgelegt. An den Bundesrat wird die Kompetenz delegiert, in einer Verordnung die Aufbewahrungsfristen für die verschiedenen Datenarten zu regeln.

Die Vertrauensinfrastruktur, die mit dem Vorentwurf eingeführt wird, basiert auf den Prinzipien der Datensparsamkeit, des Schutzes der Privatsphäre durch Technik und mittels datenschutzfreundlicher Konzeption («privacy by design» und «privacy by default») sowie der dezentralen Datenspeicherung. Die Hauptelemente der Infrastruktur werden im 5. Abschnitt geregelt: das Basisregister, das System zur Bestätigung von Identifikatoren und die Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen. Das Basisregister und das System zur Bestätigung von Identifikatoren beinhalten keine Daten über die einzelnen elektronischen Nachweise. Das Basisregister enthält nur Daten über deren Widerruf. Die Daten der Inhaberinnen und Inhaber der E-ID und die elektronischen Nachweise werden ohne zwischengeschaltete Stelle ausschliesslich zwischen der Ausstellerin, dem Inhaber oder der Inhaberin und den Verifikatorinnen übermittelt. Es ist folglich keine gesetzliche Grundlage im Sinn von Artikel 34 Absatz 1 nDSG erforderlich. Die zentrale Idee hinter der Vertrauensinfrastruktur ist, ein System zu schaffen, in dem die Datenflüsse für alle Nutzerinnen und Nutzer direkt und transparent sind, in dem die Ausstellerinnen nicht wissen, wie die ausgestellten elektronischen Nachweise verwendet werden, ohne dabei auf das Recht zu verzichten, sie zu widerrufen, und in dem die Inhaberinnen und Inhaber von den Sicherheitsmassnahmen profitieren können, die dem aktuellen Stand der Technik entsprechen.

Schliesslich wird in Artikel 28 Buchstabe e auch die Kompetenz an den Bundesrat delegiert, in einer Verordnung die technischen und organisatorischen Massnahmen zu regeln, um den Datenschutz und die Datensicherheit beim Betrieb und bei der Nutzung der Vertrauensinfrastruktur zu gewährleisten.