



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Zentrale Dienste

Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz)

Bericht über das Ergebnis des
Vernehmlassungsverfahrens

Inhaltsverzeichnis

1	Gegenstand des Vernehmlassungsentwurfs	4
2	Durchführung des Vernehmlassungsverfahrens	4
3	Eingereichte Stellungnahmen	5
3.1	Teilnahme	5
3.2	Darstellung der Ergebnisse im Vernehmlassungsbericht	5
4	Allgemeine Würdigung des Entwurfs	5
4.1	Allgemeine Anmerkungen	5
4.2	Bemerkungen zu Konzept und zur Aufgabenteilung Staat – Markt	5
5	Einzelfragen	8
5.1	Interoperabilität	8
5.2	E-ID-Registrierungsnummer	8
5.3	Personenidentifizierungsdaten	9
6	Bemerkungen zu den einzelnen Artikeln	10
6.1	1. Abschnitt: Allgemeine Bestimmungen	10
6.1.1	Art. 1 Gegenstand und Zweck	10
6.1.2	Art. 2 Begriffe	11
6.2	2. Abschnitt: Ausstellung von E-ID	11
6.2.1	Art. 3 Persönliche Voraussetzungen	11
6.2.2	Art. 4 Anerkennung von IdP	13
6.2.3	Art. 5 Sicherheitsniveaus	14
6.2.4	Art. 6 Ausstellungsprozess	15
6.2.5	Art. 7 Personenidentifizierungsdaten	17
6.2.6	Art. 8 Aktualisierung der Personenidentifizierungsdaten	18
6.2.7	Art. 9 Systematische Verwendung der Versichertennummer zum Datenaustausch	19
6.2.8	Art. 10 Datenbearbeitung und Datenweitergabe	20
6.2.9	Art. 11 Erlöschen der Anerkennung und Art. 12 Aufsichtsmaßnahmen und Entzug der Anerkennung	22
6.2.10	Art. 13 Subsidiäres E-ID-System des Bundes	23
6.3	3. Abschnitt Inhaberinnen und Inhaber von E-ID, Art. 14 Pflichten	23
6.4	4. Abschnitt Betreiberinnen von E-ID-verwendenden Diensten	24
6.4.1	Art. 15 Vereinbarung mit IdP	24
6.4.2	Art. 16 Behörden als Betreiberinnen von E-ID-verwendenden Diensten ...	24
6.5	5. Abschnitt	25
6.5.1	Art. 17 Pflichten	25
6.5.2	Art. 18 Interoperabilität	26
6.6	6. Abschnitt: Schweizerische Stelle für elektronische Identität	26
6.6.1	Art. 19 Organisation	26
6.6.2	Art. 20 Aufgaben und Pflichten	26
6.7	7. Abschnitt: Anerkennungsstelle für IdP	27
6.7.1	Art. 21 Zuständigkeit	27
6.7.2	Art. 22 Liste der anerkannten IdP	27
6.8	8. Abschnitt: Gebühren Art. 23	27
6.9	9. Abschnitt: Haftung Art. 24	28
6.10	10. Abschnitt: Schlussbestimmungen	28
6.11	Änderung anderer Erlasse	28
6.12	Erläuterungen	29

7 Einsichtnahme..... 30

Anhang / Annexe / Allegato..... 31

1 Gegenstand des Vernehmlassungsentwurfs

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

Der Vorentwurf geht von einer Aufgabenteilung zwischen Staat und Markt aus. Die notwendige Akzeptanz für die E-ID soll mit vertrauenswürdigen rechtlichen und organisatorischen Rahmenbedingungen – verbunden mit der Leistungsfähigkeit und Dynamik des Marktes – erreicht werden. Geeignete IdP werden vom Bund zur Ausstellung von anerkannten E-ID und zum Betrieb von anerkannten E-ID-Systemen ermächtigt.

2 Durchführung des Vernehmlassungsverfahrens

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

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

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

Das Vernehmlassungsverfahren zum Vorentwurf des Bundesgesetzes über elektronische Identifizierungsdienste (E-ID-Gesetz) (bis November 2017 Bundesgesetz über anerkannte elektronische Identifizierungseinheiten) dauerte vom 22. Februar 2017 bis zum 29. Mai 2017. Zur Teilnahme eingeladen wurden die Kantone, die in der Bundesversammlung vertretenen politischen Parteien, die gesamtschweizerischen Dachverbände der Gemeinden, Städte und Berggebiete und der Wirtschaft sowie weitere interessierte Organisationen.

3 Eingereichte Stellungnahmen

3.1 Teilnahme

Von den 65 zur Stellungnahme eingeladenen Adressatinnen und Adressaten haben 48 geantwortet. Stellung genommen haben 26 Kantone, 8 politische Parteien und 54 Organisationen und weitere Teilnehmende. Insgesamt gingen damit 88 Stellungnahmen ein.

Es sind 40 unaufgeforderte Stellungnahmen eingegangen. Sie stammen zum einen von Verbänden aus der Wirtschaft, insbesondere den Branchen ICT und Finanzdienstleistungen, und dem Bereich E-Government und E-Health, zum anderen von Privatpersonen.

Santésuisse hat ausdrücklich keine Bemerkungen zur Vorlage gemacht und der Schweizerische Arbeitgeberverband hat auf eine Stellungnahme verzichtet.

3.2 Darstellung der Ergebnisse im Vernehmlassungsbericht

Zur Darstellung der Ergebnisse in diesem Bericht sind die Teilnehmenden in mehrere Kategorien unterteilt worden: Kantone; politische Parteien; Dachverbände der Gemeinden, Städte und Berggebiete und Gebietskörperschaften; Dachverbände der Wirtschaft; Vereinigungen im IKT-Bereich; andere Vereinigungen, Unternehmen sowie weitere Interessierte und Privatpersonen.

Den Auflistungen im Anhang lassen sich die in den jeweiligen Kategorien enthaltenen Stellungnahmen entnehmen (siehe Anhang 1).

Der vorliegende Bericht beschränkt sich auf die Darstellung der zentralen und wichtigen Fragen zur Vernehmlassungsvorlage, wie sie nachfolgend ausgeführt werden. Sämtliche Stellungnahmen sind zusammen mit diesem Bericht integral veröffentlicht unter Startseite BJ > Staat & Bürger > Laufende Rechtsetzungsprojekte > E-ID-Gesetz.

4 Allgemeine Würdigung des Entwurfs

4.1 Allgemeine Anmerkungen

Die Vernehmlassungsteilnehmenden sind einheitlich der Meinung, dass es eine schweizerische E-ID braucht und begrüßen – mit Ausnahme der SVP – den Erlass einer gesetzlichen Regelung. Es ist unbestritten, dass möglichst bald eine sichere Identifizierungslösung für Online-Dienste eingerichtet werden soll und dass diese Lösung international, insbesondere mit den EU-Nachbarländern, kompatibel sein soll.

In keiner der Vernehmlassungsantworten findet sich eine Forderung nach einer rein schweizerischen E-ID; die Lösung soll sich an der eIDAS-Verordnung¹ der EU und deren Durchführungsverordnungen orientieren, so dass eine spätere Notifizierung möglich ist.

4.2 Bemerkungen zu Konzept und zur Aufgabenteilung Staat – Markt

Ein wiederkehrendes Thema in den Stellungnahmen ist die Rolle des Staates bei der Herausgabe der E-ID. Hauptsächlich thematisiert ist die Frage, ob der Staat oder Private eines oder mehrere elektronische Systeme für die Ausstellung, Verwaltung und Anwendung der E-

¹ 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

ID (E-ID-Systeme) betreiben sollen. Die Vernehmlassungsantworten bringen kein klares Resultat zur Frage, ob staatlich anerkannte private Anbieterinnen von Identitätsdienstleistungen (Identity Provider, IdP) (z.B. die Post, ein Telekomanbieter oder eine Bank) in einem detailliert vorgeschriebenen und regelmässig überprüften Prozess den Herausgabeprozess der E-ID übernehmen und die Identifizierung der antragsstellenden Person durchführen oder ob eine staatliche Stelle (z.B. die kantonalen Passstellen) dies tun sollen.

Einundzwanzig Kantone sprechen sich für die vorgeschlagene Aufgabenteilung aus², AI und AR lehnen das Konzept der Aufgabenteilung ab und befürworten eine Abgabe der E-ID durch den Staat, vergleichbar mit der Abgabe von Pass und ID-Ausweis. TG ist nur teilweise einverstanden; ZG bevorzugt die Herausgabe einer E-ID durch den Staat, allenfalls unter Beizug von Privaten für Support und Helpdesk. ZH regt an, unter der Leitung des Bundes eine Trägerschaft bestehend aus Bund, Kantonen und Gemeinden als Identitätsdienstleister einzusetzen. VD schlägt vor, die Herausgabe der E-ID an den Verwendungszweck zu knüpfen und je nach dem eine private oder staatliche Stelle mit der Herausgabe zu betrauen. BS beantragt zu prüfen, ob die Herausgabe der E-ID nicht doch eine staatliche Aufgabe darstelle.

Die Parteien äussern sich unterschiedlich: Für die BDP soll der staatliche elektronische Identitätsnachweis (staatliche E-ID) eine Staatsaufgabe sein; die E-ID soll vom Staat alleine herausgegeben werden oder durch maximal einen mit dieser hoheitlichen Aufgabe beauftragten Dritten. Die CVP begrüsst grundsätzlich, dass der Bundesrat mit dem vorliegenden Entwurf die Rahmenbedingungen für die Anerkennung von E-ID bereitstellt, stellt aber die Frage, ob die Bereitstellung der E-ID, zumindest bei E-Government-Diensten, bei welchen ein erhöhtes Sicherheitsniveau notwendig ist, nicht eher Sache des Bundes sein sollte. Die FDP unterstützt die Stossrichtung des vorgeschlagenen Konzeptes, denn der Staat solle keine eigenen Anwendungen vertreiben, sondern lediglich die Rahmenbedingungen so setzen, dass die Wirtschaft und die Bürger die Chancen der Digitalisierung bestmöglich nutzen können; Private seien aufgrund der technologischen Dynamik geeigneter als der Staat, um derartige Systeme herzustellen und anzubieten. Die GLP unterstützt das Konzept des Bundesrates, wonach das E-ID-Ökosystem in einer Aufgabenteilung zwischen Staat und Markt geschaffen werden soll und sprechen sich für das Konzept der Herausgabe der E-ID durch staatlich anerkannte private IdP aus. Aus Sicht der Grünen Partei ist die elektronische Identität (E-ID) notwendig, doch verfolgt die Vorlage die falsche Stossrichtung: Die Erteilung einer Identität, eines digitalen «Passes» müsse eine Aufgabe der öffentlichen Hand bleiben. Die Piratenpartei unterstützt im Grundsatz die Entwicklung und Einführung einer E-ID zur staatlich anerkannten Identifizierung von Personen im digitalen Raum sieht aber im Identitätsnachweis, egal ob auf Papier oder elektronisch, eine Staatsaufgabe. Die SP lehnt die Vorlage in der vorliegenden Form ab, anerkennt aber ausdrücklich den Handlungsbedarf und bittet den Bundesrat, einen Kompromissvorschlag zwischen einer derart vollständigen Auslagerung und einer rein staatlichen Lösung zu erarbeiten; sie bevorzugt eine Lösung, bei der die Hauptverantwortung für den Prozess und das technische Design der E-ID stärker als bei der jetzt vom Bundesrat vorgeschlagenen Lösung bei der öffentlichen Hand bleibt, ohne dass deshalb die Privatwirtschaft ausgeschlossen bliebe und deren technisches Know-How und Innovationsfähigkeit nicht berücksichtigt würde. Die SVP kann dem Vorentwurf zwar nicht zustimmen, ist jedoch einverstanden damit, dass der Staat auf die Herausgabe der E-ID verzichte. Sie sieht es angezeigt, dass der Bund bei der E-ID von jeglicher staatlichen Verantwortung absehen würde. Vielmehr solle es dem Markt überlassen werden, ob und welches System sich durchsetzen kann.

² AG, BE, BL, BS, FR, GE, GL, GR, JU, LU, NE, NW, OW, SH, SG, SO, SZ, TI, UR, VS, ZH

Bei den Gebietskörperschaften gehen die Meinungen auseinander. Pfäffikon ZH ist für die vorgeschlagene Aufgabenteilung und schlägt gleichzeitig vor, unter der Leitung des Bundes eine Trägerschaft bestehend aus Bund, Kantonen und Gemeinden als Identitätsdienstleister einzusetzen. Der Gemeindeverband und eine Mehrheit im SSV sind gegen die vorgeschlagene Aufgabenteilung und ziehen eine staatliche E-ID vor. Der SSV beantragt daher, dass der Bund die Vorlage überarbeite und mit einer Variante ergänzt, in der die Lösung mit einer einheitlichen staatlich abgegebenen E-ID konkretisiert wird.

Die Dachverbände der Wirtschaft, namentlich CP, Economiesuisse, FER, SBV, SGV, SwissHoldings und VSKB haben sich für die vorgeschlagene Aufgabenteilung ausgesprochen.

Von den Vereinigungen im IKT-Bereich haben sich Digitalswitzerland, IG ICT ZH, KARTAC, SFTI, SPA und SwissICT für das Konzept und die Aufgabenteilung ausgesprochen, ASUT und ISSS schlagen vor, dass der Staat ergänzend zu privaten IdP eine staatliche E-ID anbietet. Für SDA und Swico ist der staatliche Nachweis der elektronischen Identität eine hoheitliche Aufgabe, welche der Staat selbst wahrnehmen soll und die SWITCH schlägt vor, auf das Marktmodell zugunsten einer Umsetzung durch den Bund oder einer Vergabe durch den Bund an einen Dritten zu verzichten.

Von den anderen Vereinigungen sprechen sich SAV und VZGV für die vorgeschlagene Aufgabenteilung aus, der VSED unterstützt einerseits Ablaufoptimierungen und medienbruchfreie Prozesse, zieht andererseits nach wie vor ganz klar eine staatliche E-ID dem nun vorgesehenen Modell vor. Die Vereinigungen DJS, eGov-Schweiz, ParlDigi und SKS sehen im staatlichen Nachweis der elektronischen Identität eine hoheitliche Aufgabe, welche vom Staat selbst oder allenfalls im Auftrag des Staates durch maximal einen Dritten wahrgenommen werden sollte. Privatim enthält sich zur Frage, ob die Ausstellung einer E-ID nicht gleich wie die Ausstellung amtlicher Ausweise in der analogen Welt eine staatliche Aufgabe sei, die auch durch staatliche Stellen zu erfüllen wäre.

Die Unternehmen Coop, Post, SBB, Swisscom, SwissSign AG, UBS begrüssen die vorgeschlagene Aufgabenteilung. Swisscom und SwissSign AG schlagen als Massnahme zur Förderung der Verbreitung einer E-ID vor, dass der Antrag zur Ausstellung auch bei einer Passstelle oder kantonalen Migrationsbehörde gestellt werden kann, wobei die Ausstellung einer E-ID daneben auch direkt bei einem IdP möglich sein sollte. Die UBS schlägt vor, bereits durchgeführte Identifizierungsprozesse, z.B. bei Banken, Telekommunikationsunternehmen etc., als Basis für die Ausstellung der E-ID zu nutzen. Für Coop ist auf einen "Swiss Finish" unbedingt und zwar in jeder Form zu verzichten.

Eine Privatperson spricht sich uneingeschränkt für die vorgeschlagene Aufgabenteilung aus (R. Hauser). NüGlarus unterstützt die vorgeschlagene Aufgabenteilung und schlägt vor, dass der Staat ergänzend zu privaten IdP eine staatliche E-ID anbietet. Die Digitale Gesellschaft und Open Geneva Hackathons sehen im Identitätsnachweis und in der Ausgabe von entsprechenden Ausweisen eine zentrale Staatsaufgabe, deren Ausgestaltung nicht Privaten überlassen werden sollte. BFH, Grundrechte.ch, DJS und drei Privatpersonen (S. Häusler, B. Lehmann, und F. Scotoni) sprechen sich gegen die vorgeschlagene Aufgabenteilung aus und sehen in der Herausgabe einer E-ID eine staatliche Aufgabe.

5 Einzelfragen

5.1 Interoperabilität

Die Vernehmlassungsvorlage sieht in Art. 18 vor, dass die E-ID-Systeme interoperabel sind, so dass jede E-ID bei jedem E-ID-verwendenden Dienst eingesetzt werden kann. Zudem soll die Interoperabilität im internationalen Kontext die spätere Notifizierung ermöglichen. Die Vernehmlassungsteilnehmenden, die sich zu diesem Punkt geäußert haben, begrüßen diese Vorgabe grundsätzlich, und fordern zudem einen Identitätsvermittlungsdienst – auch E-ID-Broker genannt.

VS, GR, BE und SH weisen auf die grosse Bedeutung der Interoperabilität hin, wobei GR und TI zudem zur Klärung der Rolle des Identitätsverbunds Schweiz IDV auffordern.

Von den Parteien erwähnen CVP, Grünliberale und FDP die Bedeutung der Interoperabilität. Die zentrale Forderung der FDP ist die Interoperabilität zwischen den E-ID-Systemen verschiedener Anbieter und der Sicherstellung der Schnittstelle zwischen dem IDV Schweiz und den IdP und verlangt diesbezüglich ergänzende Bestimmung im Gesetz.

Von den Gebietskörperschaften fordert der SSV die Bezugnahme auf den Identitätsverbund IDV Schweiz.

Auch die Dachverbände der Wirtschaft FER und VSKB sehen die Interoperabilität als unabdingbare Voraussetzung für die Verbreitung der E-ID. Um die Interoperabilität zu garantieren, befürwortet die SBV einen E-ID-Broker, der als Vermittler zwischen IdP untereinander und zwischen IdP und E-ID-verwendenden Diensten fungiert.

Von den Vereinigungen im IKT-Bereich sprechen sich ASUT, Digitalswitzerland, KARTAC, SFTI, SWITCH und SwissICT ausdrücklich für die Interoperabilität, auch im internationalen Bereich, aus. Digitalswitzerland befürwortet eine Vermittlerplattform, durch welche Identitäts-Attribute zwischen den IdP transferiert werden können.

Coop, Post, SBB, SwissSign AG und UBS sehen Regelungsbedarf für die internationale Interoperabilität, d.h. die Anerkennung von ausländischen elektronischen Identifizierungsmitteln. Darüber hinaus soll im Gesetz die finanzielle Abgeltung zwischen den IdP festgelegt werden. Die Swisscom schlägt vor, einen Identitäts-Broker als Bindeglied der IdP untereinander und zwischen IdP und E-ID-verwendenden Diensten einzusetzen.

NüGlarus spricht sich für die Sicherstellung der Interoperabilität der schweizerischen E-ID mit üblichen EU-Identitäten aus.

5.2 E-ID-Registrierungsnummer

Der Vorentwurf geht davon aus, dass die heutige Praxis der Nutzung der AHVN13 bestehen bleibt, und führt deshalb zusätzlich eine E-ID-Registrierungsnummer ein, die für die E-ID aber auch für andere Anwendungen zur Verfügung stehen soll.

BE, BL, LU, NE, SH, UR, VD, ZH und ZG würden es begrüßen, wenn die AHVN13 auch für die E-ID verwendet werden könnte. AG, BS und VS sind mit der gewählten Lösung und der Einführung einer nicht-sprechenden Identifikationsnummer einverstanden.

Die Parteien BDP, GPS und Piratenpartei sprechen sich gegen die Einführung einer E-ID-Registrierungsnummer aus und schlagen transaktionsbezogene einmal verwendbare Authentisierungs-codes vor.

Pfäffikon ZH begrüsst die vorgeschlagene Möglichkeit der Verwendung der AHVN13.

Von den Dachverbänden der Wirtschaft schlägt der VSKB die Herausgabe der E-ID-Registrierungsnummer mit der Ausstellung einer Identitätskarte oder eines Passes vor.

Von den Vereinigungen im IKT-Bereich sprechen sich SDA und Swico für transaktionsbezogene einmal verwendbare Authentisierungscode aus und erachten es als falsch, die E-ID als neue permanente zentrale Personennummer einzuführen. Der ISSS befürwortet die Schaffung einer eindeutig identifizierenden jedoch auf die AHV-Versichertennummer nicht rückführbare numerischen Kennzeichnung.

Von den anderen Vereinigungen sprechen sich Privatim für die Verwendung eines nicht-sprechenden eindeutigen Identifikators aus, der von der Versichertennummer unabhängig ist. Der VZGV begrüsst die angedachte Erweiterung des Kreises der Berechtigten zur Verwendung der AHV-Versichertennummer. Für FMH und IG eHealth gilt es darauf zu achten, dass keine Inkompatibilität entsteht, die dann die Nutzung der E-ID für ein Patientendossier verunmöglichen würde. Eine Verknüpfung der E-ID-Registrierungsnummer mit der Patientenidentifikationsnummer soll möglich sein. eGov-Schweiz schlägt vor, dass die E-ID mit einem eindeutigen eGovernment-Identifikator für alle natürlichen und juristischen Personen erweitert werde. Aus Sicht des Vereins besteht auch die Möglichkeit der Verwendung der AHVN13.

Für die UBS sollte es möglich sein, dass eine Person verschiedene E-ID mit je unterschiedlichen Registrierungsnummern unterhalten kann.

Von den weiteren Interessierten sind Open Geneva Hackathons und eine Privatperson (B. Lehmann) für die Verwendung eines nicht-sprechenden eindeutigen Identifikators der von der Versichertennummer unabhängig ist.

5.3 Personenidentifizierungsdaten

Eine staatlich anerkannte E-ID bestätigt die Existenz und Identität einer natürlichen Person aufgrund der Personenidentifizierungsdaten, die in staatlich geführten und gepflegten Registern hinterlegt sind. Da nur Daten bestätigt werden können, die in den Informationssystemen des Bundes (Informationssystem Ausweisschriften [ISA]; Zentrales Migrationsinformationssystem [ZEMIS]; elektronisches Personenstandsregister Infostar; Zentralregister der zentralen Ausgleichsstelle der AHV [ZAS-UPI]) geführt werden, ist die Aufzählung in Art. 7 der Vernehmlassungsvorlage abschliessend.

AG, BS und GR schlagen eine Verringerung der Anzahl der bestätigten Personenidentifizierungsdaten vor und verweisen auf den Grundsatz, dass im Rahmen von staatlichen E-Dienstleistungen nicht mehr Personendaten bearbeitet werden dürfen, als in der physischen Welt; TG empfiehlt ein Verbot der Zuordnung weiterer Daten zur E-ID.

Piratenpartei und GPS halten fest, dass die relevanten Daten der E-ID denen der analogen Identitätspapiere entsprechen sollen, d.h. nur die Parameter Name(n), Vorname(n) und Geburtstag (eventuell noch Nationalität, Heimatort) als Basisdaten enthalten sollen.

Von den Gebietskörperschaften äussert sich der Gemeindeverband mit dem Wunsch, weniger Personenidentifizierungsdaten zu bestätigen.

Von den Dachverbänden der Wirtschaft begrüsst es die SBV, dass Informationen, welche über die staatlich geführten Personenidentifizierungsdaten hinausgehen, Teil einer E-ID sein können.

Einige Vereinigungen im IKT-Bereich schlagen Varianten bezüglich Bestätigung oder Umgang mit zusätzlich zugeordneten Daten vor. Für die IG ICT ZH gibt es keinen Grund, die Personenidentifizierungsdaten abschliessend und einschränkend zu nennen. Für die KAR-

TAC soll es den beteiligten Personen überlassen bleiben, unter welchem Sicherheitsniveau die einzelnen Attribute verfügbar gemacht werden, während die SPA vorschlägt, die von der Identitätsstelle einer E-ID zuzuordnenden Personenidentifizierungsdaten für jedes Sicherheitsniveau auf Gesetzesstufe verbindlich zu definieren. Der ISSS schlägt vor, weitere mögliche biometrische Attribute und persönliche Zusatzparameter in einer Verordnung zu präzisieren.

Auch die anderen Vereinigungen sind sich nicht einig. Während die DJS ablehnt, dass Personendaten auf Vorrat gesammelt und den privaten Anbietern zur Verfügung gestellt werden sollen und Privatim in der Anzahl der bestätigten Daten eine unverhältnismässige Datenbekanntgabe sieht, schlägt die FMH vor, dass die E-ID darüber hinaus auch mit der Patientenidentifikationsnummer gemäss Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015 (EPDG, SR 816.1) verknüpft werden kann. Der KFS schlägt vor, den Inhabern die Möglichkeit zu geben zusammen mit der E-ID (freiwillig) weitere persönliche Daten abzuspeichern. Der SAV sieht bei einzelnen Attributen (Zivilstand und Staatsangehörigkeit) keine Erhöhung der Sicherheit und beantragt darauf zu verzichten. Für den VZGV ist die abschliessende Aufzählung der Personenidentifizierungsdaten nicht notwendig, es könnten zukünftig durchaus weitere Identifizierungsdaten in den Bundessystemen aufgenommen werden. Der VSED unterstützt wiederum die Einschränkung von Personenidentifizierungsdaten durch den Inhaber bei einer konkreten Anwendung einer E-ID, die vom IdP an eine Betreiberin von E-ID verwendenden Diensten übermittelt werden.

Von den Unternehmen schlägt die UBS vor, die Aufzählung in Artikel 7 Absatz 2 der Vernehmlassungsvorlage für weitere Attribute zu öffnen.

Von den weiteren Interessierten schlägt die BFH vor, privaten Anbietern zu ermöglichen, zusätzliche Attribute mit einer E-ID zu verknüpfen. Die Digitale Gesellschaft hingegen möchte auf die Verwendung von biometrischen Merkmalen zur Identifizierung verzichten. Grundrechte.ch geht die Vorlage bezüglich der zu verarbeitenden Daten für eine E-ID viel zu weit. Es sei nicht ersichtlich, weshalb derart viele Personendaten quasi auf Vorrat gesammelt und den privaten Anbietern zur Verfügung gestellt werden sollen.

6 Bemerkungen zu den einzelnen Artikeln

6.1 1. Abschnitt: Allgemeine Bestimmungen

6.1.1 Art. 1 Gegenstand und Zweck

Von den Dachverbänden der Wirtschaft schlagen SBV und VSKB vor, die weite Verbreitung und die Orientierung an internationalen Standards im Zweckartikel zu erwähnen.

Bei den Vereinigungen im IKT-Bereich schlagen KARTAC und SPA vor, die weite Verbreitung und Nutzung und die Sicherstellung der nationalen und internationalen Interoperabilität in den Zweckartikel aufzunehmen.

Die Unternehmen äussern sich wie folgt: Die UBS schlägt vor, die Sicherstellung der weiten Verbreitung der E-ID und die Orientierung an internationalen Standards in den Zweckartikel aufzunehmen. Die Post begrüsst es, dass die Verwendung der E-ID als Regelungszweck aufgeführt wird. Zusätzlich solle in Art. 1 die Rolle des Bundes als Herausgeberin der elektronischen Identifizierungseinheiten beschrieben werden und der Begriff „herausgeben“ sei entsprechend zu verwenden; der Begriff der Interoperabilität soll sich auch auf die internationale Interoperabilität beziehen. Aus Sicht der Swisscom sollte das subsidiäre E-ID-System des Bundes gemäss Art. 13 VE nicht eine Möglichkeit, sondern eine Pflicht auf den Zeitpunkt des Inkrafttretens des Gesetzes sein. Falls der Markt die staatlich anerkannte E-ID nicht von

Anfang an fördern, dann müsse es der Bund selbst machen und ein System mindestens für den eGov-Bereich anbieten. Demnach sollte auch in Art. 1 Abs. 2 VE als Zweck die Sicherstellung der Verbreitung der E-ID im eGov-Bereich aufgenommen werden. Die SBB schlägt unter anderem vor, zusätzlich die Rolle des Bundes zu beschreiben: „die Rechte und Pflichten des Bundes als Herausgeber der elektronischen Identifizierungseinheiten sowie als Träger der Identitäts- und Anerkennungsstelle.“

6.1.2 Art. 2 Begriffe

FR sieht es als zwingend an, eine Legaldefinition der Inhaberin und des Inhabers einer E-ID aufzunehmen. ZH regt an, eine Definition der Identitätsstelle aufzunehmen.

Die Dachverbände der Wirtschaft nehmen wie folgt Stellung: Die SBV regt an, im ganzen Erlass „Identitätsdienstleistung“ durch „Identifizierungsdienstleistung“ zu ersetzen, schlägt vor, die Erweiterung des Kreises der IdP um staatliche Stellen im ganzen Erlass entsprechend anzupassen und regt die Aufnahme der Bezeichnung „E-ID-Broker“ und „Identitätsattribute“ in die Legaldefinitionen an. SwissHoldings erscheint es vor allem wichtig, keine „eigenen“ Schweizer Begriffe zu definieren, sondern wenn immer möglich die eIDAS Terminologie zu verwenden.

Von den Vereinigungen im IKT-Bereich schlägt der ISSS vor, weitere Begriffe in die Liste der Legaldefinitionen aufzunehmen und die Begriffe „Sperrung“ im gesamten Erlass durch „Aussetzung“ und „E-ID-verwendende Dienste“ durch „vertrauende Beteiligte“ zu ersetzen (eIDAS Begriffe). Die KARTAC schlägt vor, den Begriff „Attribute“ bei den Legaldefinitionen aufzuführen.

Von den anderen Vereinigungen bemerkt die FMH, dass die Bedürfnisse der sicheren und effizienten Patientenbehandlung nicht identisch mit denjenigen des sicheren elektronischen Geschäftsverkehrs seien. Die für die Schweiz im VE E-ID-Gesetz vorgeschlagene Beschränkung auf die Herausgabe an natürliche Personen überzeuge nicht. So müsse zum Beispiel der Patient wissen können, ob er mit dem richtigen Patientendossier verbunden ist. Die Authentizität des Servicebetreibers sicherzustellen sei mindestens so wichtig wie die Authentifizierung der Gesundheitsfachperson, die auf das EPD zugreifen können soll. Weiter verlangt die FMH die Klärung der Frage nach der Rechtsnatur der anerkannten elektronischen Identifizierungseinheit (Urkunde, Zertifikat, etwas Drittes?) bei den Legaldefinitionen.

Die UBS schlägt vor, die Legaldefinitionen um die Begriffe „Attribute“ und „Broker“ zu erweitern. Post und SBB beantragen die Aufnahme der Identitätsstelle in die Legaldefinitionen. Die SBB schlägt zudem weitere Ergänzungen bei den Legaldefinitionen vor.

Eine Privatperson (D. Muster) erachtet die Aussagen als nicht vollständig und fragt sich, wieso der Bezug einer E-ID auf natürliche Personen beschränkt sei und regt an, für juristische Personen und WebServer auch eine E-ID auszustellen und so die sichere Identifikation zu ermöglichen. Eine Privatperson (B. Oldani) würde die Herausgabe einer E-ID für juristische Personen begrüssen und regt an den Begriff „Person“ durch „Personeneinheit (juristische oder natürliche Person)“ zu ersetzen.

6.2 2. Abschnitt: Ausstellung von E-ID

6.2.1 Art. 3 Persönliche Voraussetzungen

AG beantragt, den Wortlaut von Art. 3 Abs. 1 Bst. b E-ID-Gesetz so zu ergänzen, dass die E-ID für Ausländerinnen und Ausländer, die zum Zeitpunkt der Ausstellung über einen gültigen biometrischen Ausländerausweis verfügen, ausgestellt werden kann. BE regt an, die

persönlichen Voraussetzungen so anzupassen, dass sie nicht voraussetzen, dass die Person schon über einen bestimmten Ausweis für Schweizer Staatsangehörige verfüge, sondern dass sie die Voraussetzungen für die Erlangung eines solchen erfülle. BL sieht in der „kann-Formulierung“ einen Verstoss gegen die Rechtsgleichheit. BL möchte eine Regelung in Bezug auf die Verwendung der E-ID durch Personen, denen die Handlungsfähigkeit entzogen wurde. GE remarque qu'il conviendrait de prévoir des procédures d'identification propres aux cantons, notamment pour une reconnaissance forte du personnel administratif et policier. ZG schlägt vor, im Gesetz zu regeln, wie sich Organe einer juristischen Person elektronisch ausweisen können. ZH regt an, die Vertragsfreiheit der IdP sinnvoll einzuschränken, so dass keine Personengruppen willkürlich von staatlichen Leistungen ausgeschlossen werden, die sie allenfalls nur mit einer E-ID beziehen können.

Aus Sicht der SVP sollte nicht der Bundesrat, sondern der Gesetzgeber abschliessend bestimmen, welche Kategorien von Ausländerausweisen nicht zur Ausstellung einer E-ID berechtigen.

Economiesuisse und SwissHoldings betonen, dass alle Einwohnerinnen und Einwohner der Schweiz die Möglichkeit erhalten sollen, eine E-ID zu beziehen und zu verwenden. Hier dürfe es nicht zu behindernden Ausschlusskriterien kommen wie z.B. die Beschränkung auf Bürgerinnen und Bürger, hohe Kosten für den Nutzer oder eine komplizierte Anwendung.

Von den Vereinigungen im IKT-Bereich regt der ISSS eine Erweiterung der bezugsberechtigten Personengruppen an (Jede Person mit einer Versichertennummer, Ausländer ohne Aufenthaltsberechtigung, Unternehmen mit UID-Nummer, Juristische Personen mit Domizil im Ausland). Die SPA beantragt einen weitgehenden Kontrahierungszwang für IdP vorzusehen.

Die FMH verlangt, dass die E-Identität für Patienten mit der Patientenidentifikationsnummer gemäss EPDG verknüpft werden könne und beantragt die Schaffung einer E-ID für Personen, die weder Schweizer sind noch eine Aufenthaltsbewilligung haben, analog zur Handhabung im Gesundheitsbereich, um die Bedürfnisse von eHealth-Anwendungen abzudecken. Die KAZ und der Schweizerische Verband für Zivilstandswesen beantragen eine Anpassung der Voraussetzungen für die Herausgabe an Ausländerinnen und Ausländer. Der SAV schlägt vor, anstelle von «kann» das Verb «dürfen» zu wählen, da das Gesetz keinen Kontrahierungszwang der IdP vorsehe und in Art. 3 Abs. 1 Bst. a und b den Kreis derjenigen Personen bestimmt sei, denen der IdP eine E-ID ausstellen darf. Der Verein e-Gov-Schweiz regt an, eine E-ID ebenfalls für juristische Personen auf der selben gesetzlichen Basis umzusetzen.

Die UBS regt an, dass die Delegationsnorm in Art. 3 Abs. 3 ergänzt wird um den Begriff „Entsperrung“. Die Post sieht Gründe für und gegen einen Kontrahierungszwang, wobei Post und SBB vorschlagen, im Falle eines Kontrahierungszwangs eine angemessene Abgeltung der dadurch entstehenden Kosten durch die öffentliche Hand vorzusehen. Die SBB möchten den Anwenderkreis möglichst breit fassen und E-ID abgeben an ausländische Eigentümer von Grundstücken in der Schweiz, die eine elektronischen Identität zum Ausfüllen der Steuerklärung verwenden oder an Touristen, die ihre elektronische Identität im Bereich E-Health oder für touristische Zwecke einsetzen möchten.

Inclusion Handicap bemerkt, dass einer Person mit Behinderung nicht das Erstellen einer E-ID und das Eingehen des damit verbundenen Vertrags verweigert werden könne, mit Begründungen wie der Umstand, dass der betreffende IdP nicht über die nötigen technischen Möglichkeiten verfügt, um die Kommunikation mit der Person mit Behinderung sicherstellen zu können oder damit, dass der IdP nicht über ein barrierefrei zugängliches Gebäude verfüge und somit die Person mit Behinderung nicht zur persönlichen Vorsprache empfangen werden kann. Zudem verlangt Inclusion Handicap, dass der Akt der Antragsstellung bei allen

Sicherheitsstufen für alle Personen barrierefrei möglich zu sein habe. Eine Privatperson (D. Muster) sieht Fälle, in denen ein Kontrahierungszwang des IdP angebracht wären und schlägt eine Umkehr vor, nämlich ein Kontrahierungszwang mit gesetzlich geregelten Ausnahmen; er schlägt die Regelung der Anerkennung ausländischer E-ID vor. Eine Privatperson (B. Oldani) schlägt eine Ergänzung für die Herausgabe von E-ID an juristische Personen vor.

6.2.2 Art. 4 Anerkennung von IdP

BL sieht eine Lücke bezüglich des geforderten Sicherheitsberichts und beantragt die Ergänzung von Art. 4 Abs. 2. FR erachtet die Erneuerung der Anerkennung nach 3 Jahren als erhebliches Erschweris sowohl für die Bundesverwaltung als auch für die IdP und verlangt, dass bei den Prozessen auf Einfachheit und Kosteneffizienz geachtet werde. GE möchte auf Gesetzes- oder Verordnungsebene verankern, dass auch Kantone als IdP agieren können. SH regt an zu prüfen, ob zusätzlich ein Kriterium bezüglich der Beherrschung durch ausländische Investoren aufgenommen werden solle. TG verlangt eine Ergänzung bezüglich Datenhaltung „ausschliesslich in der Schweiz“.

Die GLP begrüsst die Regelung, dass IdP die E-ID-System-Daten in der Schweiz nach schweizerischem Recht halten und bearbeiten müssen, hat aber Zweifel an der Praktikabilität der Regelung. Für die SVP sollten IdP als Anerkennungsvoraussetzung nicht nur ihren Sitz in der Schweiz haben müssen, sondern auch mehrheitlich von Schweizer Staatsangehörigen kontrolliert werden.

Von den Dachverbänden der Wirtschaft sehen die FER und SwissHoldings die Regelung, dass mögliche IdP ihren Sitz in der Schweiz haben müssen, als Hindernis für die spätere Notifikation der schweizerischen E-ID bei der EU. Die SBV bemerkt, dass falls im Gesetzestext definiert wird, auch staatliche Stellen als IdP anerkannt werden können, für diese die Anerkennungsvoraussetzung des Art. 4 Abs. 2 Bst. b VE-E-ID-Gesetz entfalle und macht diesbezüglich einen Formulierungsvorschlag für einen neuen Abs. 3.

Von den Vereinigungen im IKT-Bereich macht der ISSS Formulierungsvorschläge und Anmerkungen und verlangt Konkretisierungen. KARTAC und SPA schlagen vor, auf gesetzlicher Ebene sicherzustellen, dass bei Geschäftsaufgabe eines IdP, die von diesem IdP ausgestellten E-ID im Geschäftsverkehr und im Verkehr mit Verwaltungseinheiten ohne Unterbruch weiter genutzt bzw. nahtlos durch eine neue E-ID abgelöst werden können. KARTAC und SPA schlagen vor, die Datenhaltung ausserhalb der Schweiz zuzulassen, sofern Datensicherheit und Datenschutz adäquat nach Schweizer Recht sichergestellt ist. KARTAC und SPA verlangen, dass gleichwertige Anerkennungsverfahren, die bereits nach einem anderen Gesetz durchgeführt wurden, als hinreichend zuzulassen sind.

Die FMH regt an zu verlangen, dass die Server, auf denen E-ID-Daten gespeichert werden, zudem in europäischen Händen sein müssten und nicht einer US-Firma gehören dürften. Der SAV regt an, auf den zweiten Satzteil von Abs. 2 Bst. g. und Abs. 4 Bst. b «...oder gleichwertige finanzielle Sicherheiten nachweisen» zu verzichten. Die Regelung würde nur dann Sinn machen, wenn das Vorhandensein der finanziellen Mittel (durch die Behörde) auch regelmässig geprüft würde und die Mittel dem Zugriff von Dritten entzogen wären.

Die UBS sieht in der Voraussetzung zur Datenhaltung in der Schweiz und nach schweizerischem Recht eine nicht zeitgemässe Voraussetzung und regt eine grössere Flexibilität an, soweit die entsprechenden Sicherheitsanforderungen garantiert werden können. Zudem sollten auch Betreiber von E-ID-verwendenden Diensten im Ausland zugelassen sein, was zwangsläufig einen gewissen Datenverkehr ins Ausland mit sich bringen würde. Nur so kön-

ne auch die grenzüberschreitende Interoperabilität genutzt werden. Das Gesetz sollte daher lediglich voraussetzen, dass das vom schweizerischen Recht vorgegebene Niveau an Datensicherheit und Datenschutz einzuhalten ist. SBB und UBS regen an, verschiedene Anerkennungsverfahren von Anbietern anderer anerkannter Dienste, z.B. Signaturen oder Zustellplattformen, jeweils auch für den anderen Bereich gelten zu lassen, sofern eine gewisse Gleichwertigkeit vorliegt. Die Post stellt fest, dass die Anerkennungsvoraussetzungen für IdP, für anerkannte Zertifizierungsdiensteanbieter (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03), für anerkannte Zustellplattformen (Anerkennungsverordnung Zustellplattformen, SR 272.11) und für zertifizierte Gemeinschaften (EPDG) voneinander abweichen und dass die Gemeinsamkeiten der genannten Stellen eine Harmonisierung der materiellen und formellen Anerkennungsvoraussetzungen rechtfertigen. Post und SBB sehen Unklarheiten bezüglich der Auswirkungen der Pflicht zur Erneuerung der Anerkennung, vor allem im Fall der Nicht-Erneuerung.

Inclusion Handicap regt an, als zusätzliche Voraussetzung aufzuführen, dass die zugelassenen IdP sicherzustellen haben, dass für Menschen mit Behinderung keine Benachteiligungen bei der Antragstellung für eine E-ID bestehen. Eine Privatperson (B. Oldani) regt an, auf die ausreichende Versicherung zur Deckung der Haftpflicht des IdP zu verzichten. Eine Privatperson (D. Muster) schlägt vor, die Aufzählung in Art. 4 Abs. 4 abschliessend zu gestalten und auf den Begriff „insbesondere“ zu verzichten. Eine Privatperson (B. Oldani) vermutet, dass die Gesetzesartikel von reinen Juristen mit Null Verständnis in Informatik formuliert wurden und schlägt vor, auf die Delegationsnorm in Abs. 4 und damit auf den Erlass von technischen Vorschriften zu verzichten sowie eventuelle Probleme mit technischer Innovation und nicht mit Vorschriften zu lösen.

6.2.3 Art. 5 Sicherheitsniveaus

FR und ZH begrüssen die Festlegung von drei verschiedenen Sicherheitsniveaus. TG wünscht für jedes Sicherheitsniveau eine eigene E-ID erstellen zu können, die Ausstellung einer einzelnen, hochsicheren E-ID, die dann gemäss Art. 5 Abs. 3 des Entwurfs auch auf einem tieferen Sicherheitsniveau Verwendung finden kann, ist nicht erwünscht. NW äussert sich eher kritisch zu den Sicherheitsniveaus, da es für den Anwender verwirrend sein dürfte, welche Sicherheit er mit den Stufen „niedrig“, „substanziell“ und „hoch“ erhält. GR bemerkt, dass es fürs E-Voting sehr vorteilhaft wäre, wenn die Benutzergeräte von anerkannten E-ID-Systemen die nötigen Eigenschaften für die verifizierbare medienbruchfreie elektronische Stimmabgabe mitbringen. Es sei deshalb darauf zu achten, dass Sicherheitsniveau „hoch“ auch die Anforderungen für E-Voting abdecke.

SBV und VSKB regen an, die Ausführungsbestimmungen der Mindestanforderungen für jede der drei Sicherheitsstufen (niedrig, substanziell, hoch) auf Verordnungsebene konsequent prinzipienbasiert zu entwickeln, damit sie den dynamischen Entwicklungen in diesem Bereich Rechnung tragen.

Der ISSS macht Formulierungsvorschläge sowie Anmerkungen und verlangt Konkretisierungen; insbesondere sollen die Anforderungen an Identifizierung und Authentifizierung mit dem ZertES identisch sein. KARTAC und SPA schlagen vor, dass die E-ID die Anforderungen nach der Geldwäschereigesetzgebung und nach den einschlägigen Standesregeln erfülle und dass eine bereits vorgenommene Identifikation nach Geldwäschereigesetzgebung zu akzeptieren sei. KARTAC und SPA schlagen die freie Zuordnung von zusätzlichen Attributen unabhängig vom Sicherheitsniveau vor; Art. 5 soll um eine entsprechende Formulierung ergänzt werden. KARTAC und SPA schlagen eine Ergänzung von Art. 5 Abs. 4 vor (Der Bundesrat regelt, ... insbesondere die *massvollen* Mindestanforderungen ...), um sicherzustel-

len, dass der Ausstellungsprozess in Bezug auf die Identifizierung und Authentifizierung zwar sicher, aber auch zweck- bzw. verhältnismässig ausgestaltet wird. Digitalswitzerland sieht das Vertrauen der Bevölkerung in die E-ID-Lösungen sowie die einfache, flexible und kostengünstige Handhabung als wichtigste Merkmale für eine breite Anwendung in der Schweiz. Die Bewertung der Daten nach Sicherheitsniveaus sei entsprechend von zentraler Bedeutung.

Die FMH bemerkt, dass für unterschiedliche Behandlungen im Gesundheitswesen unterschiedliche Sicherheitsniveaus der Patientenidentifikation und im eHealth-Bereich unterschiedliche Sicherheitsniveaus der Authentifizierung angemessen wären.

Die UBS schlägt eine Ergänzung von Art. 5 Abs. 4 vor („Der Bundesrat regelt..., insbesondere die *angemessenen* Mindestanforderungen ..), damit die Identifizierung und Authentifizierung zwar sicher, aber auch zweckmässig ausgestaltet würden. Die Post erachtet es als sinnvoll, dass in Art. 5 Abs. 1 die Namensgebung der eIDAS Verordnung verwendet werde, sieht hingegen keinen Mehrwert in Abs. 2 und beantragt dessen Streichung. Die Swisscom regt an, bereits im Gesetz festzuhalten, dass Verfahren, die eine gleichwertige Sicherheit zum persönlichen Erscheinen bieten, von IdP verwendet werden könnten. Für die Swisscom erscheint es zudem als sehr wichtig, dass eine bereits erfolgte Identifikation, die als gleichwertig anzusehen sei, nicht ein zweites Mal durchgeführt werden muss. Die SBB sieht keinen Mehrwert in Abs. 2 und beantragt Streichung.

Eine Privatperson (D. Muster) regt an, bei der Sorgfalt der Identifikation und beim korrekten Erfassen der Personenangaben im Zusammenhang mit einer E-ID keine unterschiedlichen Sicherheitsniveaus einzuführen und zu akzeptieren. Eine Privatperson (R. Hauser) weist auf die Wichtigkeit der Ausführungsgesetzgebung hin und insbesondere, dass es für das Sicherheitsniveau «hoch» immer auch eine technische Umsetzungsvariante geben müsse, bei der die «Private Keys» (oder deren Äquivalent) sich physisch im Kontrollbereich des Nutzers befinden. Eine weitere Privatperson (B. Oldani) regt an, den ganzen Artikel zu streichen; es gäbe keinen Grund, verschiedene Sicherheitsniveaus zu haben, ein Ausweis sei gültig oder ungültig – nicht teilgültig.

6.2.4 Art. 6 Ausstellungsprozess

FR unterstreicht, dass beim Einsatz der E-ID im Bereich des E-Government nicht mehr Personenidentifizierungsdaten betroffen sein sollen, als in der realen Welt und dass diese Daten angemessenen Sicherheitsbestimmungen unterliegen sollen. FR sieht in der fehlenden qualifizierten oder anerkannten elektronischen Signatur eine wesentliche Einschränkung für die Entwicklung im E-Government. GE remarque que le processus d'établissement fédéral de l'e-ID, tel que proposé par l'avant-projet, omet une pratique reconnue à Genève dans le cadre de l'AeL, à savoir l'identification par courrier postal recommandé. SZ ist der Meinung, dass sich im gegenwärtigen technischen Umfeld einzig die Einwohnerämter für die persönliche Vorsprache beim "Aussteller", eignen. ZG regt an, das zentrale E-Mail-Verzeichnis des EJPD für die elektronische Zustellung über eine anerkannte Zustellplattform mit dem Verzeichnis der Identitätsstelle zu verknüpfen.

Der Gemeindeverband regt an, die persönliche Vorsprache zur Identitätsprüfung als unabdingbar im Gesetz zu verankern. Der SGV möchte Klärung, ob der zukünftige Inhaber einer E-ID auch die durch die Identitätsstelle zu übermittelnden Daten an den IdP oder durch den IdP abzurufende Daten einschränken kann. Weiter soll zwingend gewährleistet sein, dass die Bevölkerung eine Wahlfreiheit habe und der Antrag für eine E-ID an keine Bedingungen geknüpft werden kann, die dem Interesse der Bevölkerung im Wesentlichen entgegensteht.

Das heisse, dass weder ein E-ID-Anbieter eine Monopol-Stellung erhält, noch, dass Absprachen zwischen E-ID-Anbietern stattfinden.

Economiesuisse betont, dass alle Einwohnerinnen und Einwohner der Schweiz die Möglichkeit erhalten sollen, eine E-ID zu beziehen und zu verwenden; es dürfe nicht zu störenden Ausschlusskriterien kommen wie z.B. die Beschränkung auf Bürgerinnen und Bürger, hohe Kosten für den Nutzer oder eine komplizierte Anwendung.

ISSS und KARTAC schlagen vor im Gesetz zu erwähnen, dass eine Person mehr als eine E-ID haben könne (Erwähnung von Pseudonymen) und dass die E-ID auch auf in der Schweiz üblicherweise verwendeten Mobilgeräten verwendet werden könne. KARTAC und SPA regen an, dass der Prozess der Identitätsprüfung im Gesetz ausdrücklich geregelt wird und insbesondere sei die persönliche Vorsprache zu erwähnen. ISSS und KARTAC schlagen vor, dass anerkannte IdP die Prüfung der Identität der antragstellenden Person an Dritte delegieren können (Registrierungsstellen); IdP müssten für die korrekte Ausführung der Aufgabe durch die Registrierungsstelle haften. Digitalswitzerland hält fest, dass der Identifikationsprozess bei den IdP bereits im Gesetz festgehalten werden sollte und dass Verfahren, die eine gleichwertige Sicherheit zum persönlichen Erscheinen bieten, von IdP verwendet werden können (Videoidentifikation). Digitalswitzerland betrachtet es als wichtig, dass eine bereits erfolgte Identifikation, die als gleichwertig anzusehen sei, nicht ein zweites Mal durchgeführt werden muss. Der ISSS schlägt die Einführung der E-ID für juristische Personen vor und formuliert den Ausstellungsprozess. Die IG ICT ZH beantragt die Aufführung des Zweckes der Protokollierung. Die SPA beantragt, dass im Gesetz verankert wird, dass eine Person mehrere E-ID von einem oder mehreren IdP besitzen kann und dass die Identifizierungseinheit zentral geführt werden kann.

Der VZGV beantragt die Aufführung des Zweckes der Protokollierung. Für die FMH ist die Schnittstelle zum EPDG bezüglich der Erneuerung der Identitätsprüfung zu klären. IG eHealth würde es begrüssen, wenn das Erstellen einer E-ID auch durch die staatlichen Ausweis-Ausstellungsprozesse gefördert würde. Der SAV regt an, den technischen Ablauf so zu gestalten, dass eine Nachfrage der Identitätsstelle bei der antragstellenden Person nicht notwendig sei. Aus Sicht des VSED ist in jedem Fall eine persönliche Vorsprache für die Beantragung einer E-ID zwingend; mit den heutigen Mitteln erachtet er eine reine virtuelle Identifikation als relativ leicht manipulierbar für Personen mit dem nötigen technischen Wissen. Für den VSED muss ebenfalls zwingend gewährleistet sein, dass die Merkmale je nach Anforderungsniveau der gewünschten E-ID durch den Inhaber eingeschränkt werden können.

Die UBS schlägt vor im Gesetz zu erwähnen, dass eine Person mehr als eine E-ID haben kann; sie regt an, dass der Prozess der Identitätsprüfung im Gesetz ausdrücklich geregelt wird und insbesondere die persönliche Vorsprache und die Videoidentifikation zu erwähnen sei; zudem sei im Gesetz zu regeln, dass bereits identifizierte Personen nicht noch einmal identifiziert werden müssen, sofern die Identifikation für die Erstellung einer E-ID bereits ausreichend gewesen war. Post und SBB sind der Ansicht, dass man im Gesetz nicht den Prozess mit seinen Schritten definieren soll, sondern die zentralen Anforderungen an diesen. Die Post macht Formulierungsvorschläge, die neben dem IdP eine „Ausweise ausstellende Behörde“ implizieren. Die SBB regt an, nebst der Ausstellung der E-ID durch IdP auch die bestehenden staatlichen Prozesse, bzw. die bei der Ausstellung der physischen Ausweise erfolgte Identitätsprüfung für einen leichten Zugang zur E-ID zu nutzen. Sollte der Gesetzgeber diesen Vorschlag nicht aufnehmen, wäre jedenfalls eine Ausgleichszahlung zwischen den IdP vorzusehen: IdP, welche keine kostspieligen Identifikationen vornehmen, müssten jene IdP entschädigen, welche die damit verbundenen Kosten getragen haben.

Die BFH schlägt vor, Ausstellungs- und Abgabeverfahren des elektronischen Identifizierungsmittels nach denjenigen der staatlichen Ausweise (Identitätskarte und Pass) auszurich-

ten. Eine Privatperson (D. Muster) regt an, den Inhalt von Art. 6 (Ausstellungsprozess) dem Art. 3 (Persönliche Voraussetzungen) zuzuordnen. Eine weitere Privatperson (B. Oldani) regt an, den Artikel so zu formulieren, dass juristische Personen ebenfalls eine E-ID beantragen können. Für eine Privatperson (F. Scotoni) scheint dieses Vorgehen für alle Beteiligten nachteilig.

6.2.5 Art. 7 Personenidentifizierungsdaten

AG und BE regen an, in Art. 7 Abs. 1 Bst. b und c «amtlicher Name» bzw. «Vorname» zu ersetzen durch «Name gemäss dem elektronischen Personenstandsregister (Infostar)» bzw. «Vorname gemäss Infostar» und Art. 7 Abs. 2 so zu ändern, dass die Identitätsstelle der E-ID die angegebenen Daten nicht zuordnen *kann*, sondern zuordnen *muss* – differenziert nach dem jeweiligen Sicherheitsniveau. BL sieht in der Möglichkeit der Zuordnung verschiedener Personenidentifizierungsdaten ein erhöhtes Risiko der Fragmentierung und für die Gewährleistung der Interoperabilität. BS beantragt die Reduktion der Menge der einer E-ID zuzuordnenden Personendaten, allenfalls aber eine einschränkende Regelung der Verwendung bzw. der Bekanntgabe der Daten. FR weist auf die Bedeutung des Datenschutzes hin. SO regt die Prüfung der Berücksichtigung von Wohnsitz und Wohnadresse als spezifisches Element der elektronischen Identifizierung an und die Ergänzung der Liste der konsultierten Register in Art. 20 Abs. 2 E-ID-Gesetz durch die kantonal betriebenen Einwohnerregisterplattformen. GL regt an, die Schutzniveaus und die damit verknüpften Personenidentifizierungsdaten deutlicher zu umschreiben. TG will den Geburtsort durch den Heimatort ersetzen. TG verlangt die Zuordnung von weiteren Daten zur E-ID nicht zu erlauben, sondern ausdrücklich zu verbieten. SZ sieht es als unerlässlich für die Polizeiarbeit an, Zugriff auf bestimmte Attribute der E-ID zu erhalten. Der Miteinbezug der Polizeilandschaft bei der Lösungsfindung zu dieser Thematik sei dringend notwendig.

Les Verts constatent, que l'art. 7 al. 2 et 4 décrit un catalogue relativement important de données qui peuvent être utilisées (et de données sensibles, telles que les données biométriques) mais sans préciser toutefois à quelles fins et dans quel cadre ces données pourront être utilisées. C'est pourquoi les Verts soutiennent un système qui ne se base pas sur un « super-registre », mais sur un système d'accès différencié aux différents registres sous contrôle du citoyen.

Der Gemeindeverband unterstützt die Möglichkeit der Einschränkung von Personenidentifizierungsdaten, die vom IdP an eine Betreiberin von E-ID verwendeten Diensten übermittelt werden. Äusserst heikel erachtet der Gemeindeverband es deshalb, wenn zusätzliche Daten, wie die Adresse, Mobile-Nr. oder E-Mail-Adresse ohne Einwilligung der Person oder sogar in Unkenntnis des Inhabers hinzugefügt und diese Daten privaten Dritten bekannt gegeben würden. Oft seien Personen, die eine Adress- und Datensperre z.B. in den Einwohnerregistern beantragt haben an Leib und Leben bedroht.

Der VSKB regt an, Art. 7 Abs. 4 VE E-ID-Gesetz mit dem Zusatz „..., insbesondere eine Adresse, Telefon- oder Kundennummer.“ zu ergänzen. Die SBV schlägt für den gleichen Absatz die Aufnahme eines Einverständniserfordernisses vor.

Der ISSS schlägt die Erwähnung des Bürgerortes (bei Schweizer Staatsangehörigen) und der Nationalität (bei ausländischen Staatsangehörigen) vor, während KARTAC und SPA den Heimatort als zusätzlichen Inhalt einer E-ID aufführen wollen. Der ISSS schlägt vor, die Aufzählung durch „weitere biometrische Attribute“ oder „persönliche Zusatzparameter“ zu ergänzen, dies als sinnvolle Offenheit für die Zukunft der Digitalisierung. KARTAC und SPA schlagen vor, die von der Identitätsstelle einer E-ID zuzuordnenden Personenidentifizierungsdaten für jedes Sicherheitsniveau auf Gesetzesstufe verbindlich zu definieren. Die IG

ICT ZH sieht keine Notwendigkeit der Beschränkung der Anzahl der Personenidentifizierungsdaten. Für SWITCH soll die Nutzung der durch den Inhaber der E-ID freigegebenen Basis-Attribute durch E-ID-verwendende Dienste für letztere grundsätzlich kostenlos und möglichst ohne weitere Hindernisse erfolgen.

Die KAZ und der Schweizerische Verband für Zivilstandswesen regen an, in Art. 7 Abs. 1 Bst. b und c «amtlicher Name» bzw. «Vorname» zu ersetzen durch «Name gemäss dem elektronischen Personenstandsregister (Infostar)» bzw. «Vorname gemäss Infostar». Privatim sieht mit der nicht abschliessenden Aufzählung und der Möglichkeit, noch weitere Personendaten zuzuordnen, eine Unvereinbarkeit mit dem datenschutzrechtlichen Verhältnismässigkeitsgrundsatz. Es würden damit Daten auf Vorrat gesammelt und miteinander verknüpft. Für den VZGV ist das Argument der abschliessenden Aufzählung der Personenidentifizierungsdaten nicht nachvollziehbar, es könnten zukünftig durchaus weitere Identifizierungsdaten in den Bundessystemen aufgenommen werden. Eine Beschränkung bzw. abschliessende Aufzählung sei daher nicht notwendig. Für den SAV tragen weder Zivilstand noch Staatsangehörigkeit, bzw. Aufenthaltsstatus dazu bei, das Sicherheitsniveau zu erhöhen, es sei deshalb darauf zu verzichten. Der SAV regt an, in Abs. 3 eine Delegationsnorm zugunsten des Bundesrates zu schaffen, die offene gesetzliche Norm lasse im Grundsatz alles zu. Der VSED unterstützt die Einschränkung von Personenidentifizierungsdaten durch den Inhaber bei einer konkreten Anwendung einer E-ID, die vom IdP an eine Betreiberin von E-ID-verwendenden Diensten übermittelt werden; er schlägt vor, dass der E-ID-Inhaber Einfluss auf die zusätzlich vom IdP hinzugefügten Daten haben solle, insbesondere um diese einzuschränken.

Die UBS regt an, die Aufzählung in Art. 7 Abs. 2 durch Einfügung des Begriffs „insbesondere“ für weitere Personenidentifizierungsdaten zu öffnen; sie regt an, die weiteren Daten gemäss Abs. 4 als „Attribute“ zu bezeichnen und dem IdP die Möglichkeit einzuräumen, diese Daten den verschiedenen Sicherheitsniveaus zuzuteilen. Post und SBB regen an, den „Heimort“ aufzunehmen.

Die BFH unterstützt klar die Weiterverwertung der E-ID-Funktionalitäten und -Daten für privatwirtschaftliche Zwecke, anders als die privatwirtschaftliche Erbringung des hoheitlichen Identitätsnachweises. Um eine Einbindung von Zusatzattributen von privater Seite zu ermöglichen und so die Einsatzmöglichkeiten der E-ID qualitativ zu erweitern, sei es privaten Anbietern zu ermöglichen, zusätzliche Attribute mit einer E-ID zu verknüpfen. Für eine Privatperson (B. Lehmann) wird in der Erfassung des Gesichtsbildes bzw. weiterer biometrischer Merkmale in den von den IdP für natürliche Personen ausgestellten E-ID's der Sicherheitsniveaus "substanziell" oder "hoch" zweifellos ein zusätzlicher Schutz gegen deren Unterschiebung, Fälschung und Imitation geschaffen. Die Erfassung biometrischer Daten greife jedoch in die grundrechtlich geschützte Privatsphäre und das informationelle Selbstbestimmungsrecht der betroffenen Personen als InhaberInnen der E-ID ein. Eine Privatperson (B. Oldani) regt an, nur E-ID der höchsten Sicherheitsstufe anzubieten und für juristische Personen u.a. die Attribute „HR-Name“, „Gründungsdatum“, „Firmenregisternummer“ und „Gründungsort“ einzuführen.

6.2.6 Art. 8 Aktualisierung der Personenidentifizierungsdaten

BE regt an, Art. 8 Abs. 1 so zu ändern, dass die Identitätsstelle den IdP Änderungen der Personenidentifizierungsdaten laufend und kostenlos (oder allenfalls gegen eine geringe Pauschalgebühr) meldet. BS beantragt eine Regelung zum Ablauf, zur Erneuerung oder Ungültigkeit usw. und zur Sperrung oder zum Widerruf einer E-ID. GL und ZH erachten die quartalsweise Übermittlung für das Sicherheitsniveau „substanziell“ als ungenügend und ZH

regt an, dem Bundesrat die Kompetenz zur Verkürzung der minimalen Aktualisierungszeiten zu erteilen. ZG verlangt, im Gesetz sei sicherzustellen, dass IdP Informationen über Todesfälle so rasch als möglich erhalten, damit sie E-ID mit hohem Sicherheitsniveau zeitnah sperren könnten.

Der Gemeindeverband betont, dass auch hier sichergestellt sein müsse, dass ein zertifizierter IdP Anbieter bei der Identitätsstelle lediglich diejenigen Daten von Personen abrufen bzw. aktualisieren kann, welche für das Sicherheitsniveau der E-ID benötigt werden und für welche der E-ID-Inhaber sein Einverständnis gegeben hat.

Der VSKB regt an, dass aus der Gesetzesnorm klar hervorgehen sollte, dass es in der Verantwortung der Identitätsstelle liegt, umgehend eine Meldung an die IdP zu machen, sobald sie eine E-ID-Registrierungsnummer sperrt. Die SBV regt die Klarstellung an, dass es sich bei der Sperrung lediglich um die Deaktivierung der Datensätze unter Wahrung der gesetzlichen Aufbewahrungspflicht von 10 Jahren handeln könne und dass analog den bewährten Prozessen bei Kredit- und Debitkarten zu verfahren sei.

Der ISSS macht Formulierungsvorschläge bezüglich der Ausstellung von E-ID für juristische Personen.

Die FMH hält fest, dass der Begriff „berufliche Qualifikation“, anders als im neuen ZertES (für geregelte Zertifikate gemäss Art. 7 ZertES), im vorliegenden Erlass nicht erwähnt wird. Wenn E-Identitätsausweise nach diesem Gesetz im Rahmen von eHealth-Anwendungen eingesetzt werden sollen, sei die Koordination des Ausgabe- und Widerrufprozesses mit der Stelle, die die Qualifikation als Gesundheitsfachperson bestätigt, von zentraler Bedeutung. Privatim beantragt die Ergänzung des Gesetzes durch Regelungen zum Ablauf, zur Erneuerung oder Ungültigkeit, zur Sperrung oder zum Widerruf einer E-ID.

Die UBS regt an im Gesetz zu regeln, dass IdP eine E-ID im Zweifel sperren kann, ohne dafür haftbar gemacht zu werden. Post, SBB und SwissSign AG erachten die regelmässige Aktualisierung von stabilen Daten nicht als zweckmässig und bevorzugen eine Aktualisierung, die jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID steht. Die Swisscom regt an, die Pflichten der IdP im Zusammenhang mit der Sperrung oder dem Widerruf von E-ID bereits auf Gesetzesstufe klarer zu regeln. SBB lehnt die vorgesehene periodische Aktualisierung der Personenidentifizierungsdaten ab, weil bei den in Art. 8 enthaltenen Aktualisierungsvorgaben bis zu einem Jahr alte Daten verwendet würden. Stattdessen sei eine Regelung vorzusehen, wonach die IdP die Daten bei der Identifizierungsstelle ausschliesslich zum Zeitpunkt der Nutzung der E-ID abfragen.

Eine Privatperson (B. Oldani) sieht es als nicht praktikabel an, dass der IdP für die Sperrung oder den Widerruf der E-ID verantwortlich sei und schlägt vor, „die Hinterlegung der E-ID so [zu] organisieren, wie das zentrale Einwohnerregister des Bundes“.

6.2.7 Art. 9 Systematische Verwendung der Versichertennummer zum Datenaustausch

BS beantragt die Prüfung der Verwendung der AHV-Versichertennummer. Allenfalls könne diese durch einen bereichsspezifischen Identifikator ersetzt werden. BS und SH empfehlen von der Schaffung einer zusätzlichen eindeutigen Identifikationsnummer wie der E-ID Registrierungsnummer abzusehen und dazu die AHVN13 zu verwenden. LU würde eine einheitliche und für alle Stellen zur Erfüllung ihrer gesetzlichen Aufgaben zugängliche eindeutige Personennummer als Grundlage für eine effiziente Bearbeitung von Daten und deren Austausch begrüßen. NE déplore que l'utilisation et la gestion du n°AVS ne soient pas clairement définies. UR beantragt, die Nutzung der AHV-Nummer von Privatpersonen möglichst

freizugeben. VD Le Conseil d'Etat vaudois soutient la proposition visant à utiliser le NAVS 13 comme identificateur de personnes, même si cette solution suscite les réticences des préposés à la protection des données personnelles. ZG begrüsst es, dass die neue, nicht sprechende Sozialversicherungsnummer als eindeutige Nummer zur Antragstellung dient und als Attribut in der Identitätsstelle weiterverwendet wird. Im Kanton Zug werde die Sozialversicherungsnummer im Rahmen der kantonalen Identifikationslösung bereits heute zur Antragstellung und als Attribut verwendet. ZH begrüsst die Möglichkeit der Verwendung der AHV-Nummer.

Die Gemeinde Pfäffikon ZH begrüsst ausdrücklich die vorgesehene Verwendung der AHVN13, die für ein effizientes und reibungsloses Funktionieren des Systems unumgänglich sei.

Die IG ICT ZH begrüsst die angedachte Erweiterung des Kreises der Berechtigten zur Verwendung der Versichertennummer. Die SDA bemerkt, dass systembedingte Strukturierungsnummern nicht zu kommunizieren seien: Der Vorentwurf gehe deswegen mit der „E-ID-Registrierungsnummer“ in die falsche Richtung. Ein neues Register, falls tatsächlich benötigt, müsse wohl über eine Nummer erschlossen werden und zwar für jeden neu anzulegenden Eintrag, der über die AHVN13 gespiesen würde. Für die SIK ist es essentiell, dass die Identitätsstelle die Versichertennummer für den im Vorentwurf vorgesehenen Zweck systematisch verwenden darf.

Der SAV sieht die AHVN13 als notwendig für eine eindeutige Zuordnung der E-ID an. Der VZGV begrüsst die angedachte Erweiterung des Kreises der Berechtigten zur Verwendung der Versichertennummer. Der Verein eGov-Schweiz schlägt vor, dass die E-ID mit einem eindeutigen eGovernment-Identifikator für alle natürlichen und juristischen Personen erweitert wird. Aus Sicht des Vereins besteht auch die Möglichkeit der Verwendung der AHVN13. Auf den Aufbau neuer Register sollte soweit möglich verzichtet werden.

Post und SBB regen an, darauf zu achten, dass keine Inkompatibilität entsteht, die dann die Nutzung der E-ID für Patientendossiers erschwert.

Privatim spricht sich dagegen aus, die AHV-Versichertennummer durch einzelne gesetzliche Regelungen faktisch zu einem allgemein gebräuchlichen administrativen Personenidentifikator auszuweiten. Die Verwendung eines einheitlichen Personenidentifikators in allen Bereichen erhöhe die Risiken einer Persönlichkeitsverletzung für die betroffenen Personen. Auf die Verwendung der AHV-Versichertennummer durch zahlreiche Behörden sowie auch Private im Bereich der E-ID sei deshalb zu verzichten. Eine Privatperson (B. Lehmann) äussert gegenüber der Verwendung der unveränderten Versichertennummer nach 50c AHVG („AHV- oder Sozialversicherungsnummer“) als Bestandteil der Personenidentifizierungsdaten aus datenschutzrechtlicher Sicht erhebliche Bedenken und schlägt vor eine den Inhaber einer E-ID eindeutig identifizierende aber nicht rückrechenbare Personennummer zu erzeugen.

6.2.8 Art. 10 Datenbearbeitung und Datenweitergabe

BL bemerkt, dass die Notwendigkeit zur Freigabe der Datenbekanntgabe nicht dazu führen darf, dass verbeiständete Personen für den vertrauenden Nutzer nicht mehr als beschränkt handlungsfähig erkennbar sind, weil sie den Zusatz der beschränkten Handlungsfähigkeit nicht freigeben. FR exige une interdiction stricte de l'utilisation des données à d'autres fins. JU und VS möchten auch keine Weitergabe der Daten des niedrigen Sicherheitsniveaus ohne ausdrückliche Einwilligung der Inhaberin oder des Inhabers der E-ID. JU regt an, die Weitergabe von Daten von Minderjährigen besonders zu regeln.

Die GLP begrüsst, dass die Inhaberin oder der Inhaber darüber entscheidet, welche Personenidentifizierungsdaten der IdP an die Betreiberinnen von E-ID-verwendenden Diensten übermitteln darf und dass der IdP das ausdrückliche Einverständnis der Inhaberin oder des Inhabers der E-ID zur Erstübermittlung von Personenidentifizierungsdaten einholen muss. Die GLP regt an zu präzisieren, dass nur die staatlich bestätigten Daten vom Weitergabeverbot nach Abs. 3 erfasst werden, nicht aber der beim IdP bereits bestehende Datenbestand, der keinen Bezug zum E-ID-System aufweist. Auf den letzteren Datenbestand sollte für die GLP nur das gewöhnliche Datenschutzrecht anwendbar sein.

Der Gemeindeverband sieht Klärungsbedarf in verschiedenen Fragen, insbesondere zum Umfang des Handelsverbots, bzw. der Erlaubnis des Handels mit den Personenidentifizierungsdaten nach Art. 7 Abs. 1 und Abs. 4. Die E-ID-Inhaberin und der E-ID-Inhaber müsse sich auf jeden Fall bewusst sein, welche Daten an Dritte weitergegeben werden und welche nicht. Der Gemeindeverband schlägt vor, Art. 10 Abs. 3 wie folgt zu ergänzen: *Für die Bekanntgabe der Daten nach Art. 7 Abs. 1 und 4 an Dritte ist das Einverständnis des E-ID-Inhabers einzuholen.*

Die FER begrüsst die Erwähnung des Einverständnisses der Inhaberin oder des Inhabers der E-ID zur Datenübermittlung und die Einschränkung der Datenbearbeitung durch den Staat und die IdP. Der VSKB regt an, Kongruenz der Sicherheitsniveaus von E-ID-verwendenden Diensten und übermittelten Personendaten zu schaffen: Daten von bestimmten Sicherheitsniveaus sollten nur an E-ID-verwendende Dienste (bspw. Online-Shops) weitergegeben werden können, wenn diese nachgewiesenermassen ein ausreichendes Sicherheitsniveau implementiert haben. SBV und VSBK regen an, zur Stärkung des Datenschutzes den Geltungsbereich von Art. 10 Abs. 3 auf sämtliche Absätze von Art. 7 zu Personenidentifizierungsdaten auszuweiten. Der VSKB sieht die aktuelle Eingrenzung der Datenbearbeitung als zu restriktiv und schlägt vor, diese Vorgabe hinsichtlich möglicher künftiger Entwicklungen abzuschwächen. Die SBV sieht in der vorgeschlagenen Regelung der Datenweitergabemöglichkeiten einen Widerspruch zu den grundsätzlichen Anforderungen an einen vernünftigen Datenschutz.

Das Verbot der Weitergabe von Personenidentifizierungsdaten in seiner absoluten Form erachten KARTAC und SPA als zu weitgehend, nicht kompatibel mit der Geldwäschereigesetzgebung und nicht praktikabel. KARTAC und SPA regen an, das in Art. 10 Abs. 3 VE E-ID-Gesetz vorgesehene absolute Verbot der Weitergabe von Personenidentifizierungsdaten und darauf basierenden Nutzungsprofilen durch den IdP oder den Betreiber von E-ID-verwendenden Diensten zu ersetzen und an dessen Stelle einen Ansatz zu wählen, welcher einerseits nicht im Widerspruch zu (bewährten) rechtlichen Mechanismen der Geldwäschereibekämpfung steht und andererseits der E-ID-Inhaberin/dem E-ID-Inhaber ein Mitspracherecht bei der Verwendung der Daten zubillige. Der ASUT geht davon aus, dass die Vorschriften des Datenschutzgesetzes (in Revision) vollumfänglich Anwendung finden werden. Die SPA erachtet das vorgesehene Verbot der Weitergabe der Daten innerhalb eines Konzerns als nicht praktikabel und nicht der heutigen Realität entsprechend. Der SFTI sieht die explizite Eingrenzung der Datenbearbeitung für den IdP auf die zwei Anwendungsfälle „Identifizierung“ und „Authentifizierung“ möglicherweise mit Blick auf die Herausforderungen und Bedürfnisse des praktischen Alltags als zu einschränkend an und empfiehlt deshalb eine offenere Formulierung.

Der SAV ist der Meinung, dass der Handel mit Daten auf das Notwendige zu beschränken und im vorliegenden Gesetz zu bestimmen sei, welche Daten gehandelt werden dürfen, um alle Personen gleich zu behandeln. Der VSED beantragt eine Ergänzung des Abs. 3 mit einem Erfordernis einer Einverständniserklärung für die Bekanntgabe der Daten nach Art. 7 Abs. 1 und 4 an Dritte.

Swisscom und UBS regen an im Gesetzestext klarzustellen, dass eine Weitergabe von Daten mit Zustimmung des Inhabers ebenfalls möglich sein sollte. Soweit es um Themen geht, die bereits von den Bestimmungen des Datenschutzgesetzes abgedeckt sind, ist die Swisscom der Ansicht, dass auf datenschutzrechtliche Bestimmungen im E-ID-Gesetz zu verzichten sei. Für Post und SBB ist es unklar, ob ein IdP Personenidentifizierungsdaten gemäss Art. 7 Abs. 2 an Betreiberinnen von E-ID-verwendenden Diensten weitergeben darf (Abs. 2) oder nicht (Abs. 3). Die Abs. 1, 2 und 3 sollten besser abgestimmt und präzisiert werden. Weiter empfehlen Post und SBB, dem Ergebnis der Revision des DSG ist bei der Schlussfassung des Art. 10 angemessen Rechnung zu tragen.

Für die BFH reichen die bestehenden Datenschutzregulierungen der EU und der Schweiz (wo strikter) aus, um die staatliche Vergabe einer nationalen E-ID wirksam zu regeln.

6.2.9 Art. 11 Erlöschen der Anerkennung und Art. 12 Aufsichtsmassnahmen und Entzug der Anerkennung

AG regt an, Vorgaben zum Vorgehen bei einer geplanten Geschäftsaufgabe zu machen und eine Regelung zum Ablauf, zur Erneuerung oder Ungültigkeit usw. einer E-ID einzuführen. BL regt an, dass E-ID-Systeme, welche nicht ohne Unterbruch von einem anderen IdP übernommen werden, subsidiär vom Bund betrieben werden müssten. BS beantragt den Vorentwurf um die klare Regelung zu ergänzen, was im Falle der Geschäftsaufgabe der zertifizierten Stellen mit den Daten zu geschehen habe. BL regt die genaue Regelung des abzuliefernden Sicherheitsberichts in Art. 12 an. FR weist darauf hin, dass die Rechte der betroffenen Personen, der Inhaberinnen und Inhaber einer E-ID, nicht erwähnt werden. Die betroffene Person sollte Zugang zu ihren Daten erhalten und ihre Zustimmung jederzeit entziehen können. So sollte sie im Fall eines Konkurses oder der Geschäftsaufgabe eines IdP oder der Übernahme des Systems durch einen anderen IdP informiert werden.

Die FER fragt sich, ob die Kontinuität der Haftung der IdP mit der vorliegenden Formulierung ausreichend bestimmt sei und schlägt vor, eine Solidarhaftung des „aufgebenden IdP“ mit dem die E-ID übernehmenden IdP einzurichten. Die FER begrüsst es, dass keine Kausalhaftung vorgesehen ist und regt an, neben dem Konkurs weitere Auflösungsgründe zu nennen. Der VSKB regt an zu präzisieren, zu welchem Zeitpunkt eine Meldung der geplanten Geschäftsaufgabe zu machen sei. FER und SBV regen eine Verschärfung des Art. 12 Abs. 3 Bst. d an.

Privatim beantragt die Ergänzung des Gesetzes durch klare Regelungen, was im Falle der Geschäftsaufgabe einer IdP mit den Daten zu geschehen habe. Der SAV regt an, zu bestimmen, welche Stelle im Fall des Konkurses über das Schicksal der Daten verfügen könne bzw. an wen die Daten anheimfallen, wenn sie im Zuge der Konkursliquidation nicht verkauft werden können; zudem erachtet er die Einschränkung auf Internetkriminalität als nicht notwendig und zu eng gefasst.

Post und SBB regen eine gesetzliche Regelung an, welche IdP verpflichtet, Inhaberinnen und Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc“ (gegen entsprechende Entschädigung durch den Bund) zu übernehmen.

Eine Privatperson (B. Lehmann) regt an zu überlegen, ob angesichts der Bedeutung der elektronischen Identität für die digitale Wirtschaft und Gesellschaft nicht in Analogie zu Art. 13 E-ID-G der Bund das aufgegebene E-ID-System und die damit zusammenhängenden Rechtspflichten übernehmen und weiterführen solle.

6.2.10 Art. 13 Subsidiäres E-ID-System des Bundes

AG bevorzugt die Bezeichnung einer Verwaltungseinheit durch den Bundesrat. Durch die durch den Bund definierte Verwaltungseinheit könnte eine möglichst kostenneutrale sowie funktional den Bedürfnissen der öffentlichen Verwaltung entsprechende Dienstleistung geschaffen werden. TG begrüsst dass der Bund befugt sein soll, für die Bedürfnisse von Behörden ein E-ID-System betreiben zu können. ZG regt an, statt eines subsidiären E-ID Systems eine zentrale Herausgabe von E-ID mit substanziellem oder hohem Sicherheitsniveau durch den Bund vorzusehen (analog der Ausgabe von Pass und Identitätskarte).

Die GLP regt an, den Bund gesetzlich zu verpflichten, E-ID der Sicherheitsniveaus „substanziell“ und „hoch“ anzubieten, falls sich auf dem schweizerischen Markt kein IdP dafür findet.

Die FER wünscht eine Auflistung der Kosten für ein subsidiäres E-ID-System des Bundes, für den Fall, dass aus Rentabilitätsgründen kein privater IdP ein solches betreiben wolle. SBV und VSBK schlagen vor, dass ein subsidiäres E-ID-System für den im Vorentwurf aufgeführten Fall im Sinne der Systemkontinuität zwingend betrieben werden müsse, und es grundsätzlich allen Marktteilnehmern (nicht nur Behörden) dauerhaft zugänglich sein sollte.

Der SAV regt an, dass sich der Bund eine generelle Kompetenz vorbehält, eigenständig tätig zu werden.

Aus Sicht der Swisscom sollte das subsidiäre E-ID-System des Bundes gemäss Art. 13 VE nicht eine Möglichkeit, sondern eine Pflicht auf den Zeitpunkt des Inkrafttretens des Gesetzes sein. Falls der Markt die staatlich anerkannte E-ID nicht von Anfang an fördert, dann müsse es der Bund selbst machen und ein System mindestens für den eGov-Bereich anbieten. Demnach sollte auch in Art. 1 Abs. 2 VE als Zweck die Sicherstellung der Verbreitung der E-ID im eGov-Bereich aufgenommen werden.

Inclusion Handicap regt an, die Voraussetzungen zum Entzug der Anerkennung dadurch zu ergänzen, dass auch ein Verstoß gegen Art. 8 Abs. 2 BV sowie der UNO-Konvention über die Rechte von Menschen mit Behinderungen (UNO-BRK; SR 0.109) zum Entzug der Anerkennung führen könne.

6.3 3. Abschnitt Inhaberinnen und Inhaber von E-ID, Art. 14 Pflichten

LU regt an, Strafbestimmungen aufzunehmen für die Fälle, in denen rechtmässige Inhaber ihre E-ID pflichtwidrig an Dritte weitergeben. ZG regt an, im Gesetz klar zu regeln, ob eine Person nur eine oder mehrere E-ID besitzen könne. ZG würde es zur Vereinfachung der Prozesse begrüssen, wenn pro Person nur eine einzige E-ID gelöst werden könnte.

Der ISSS macht Formulierungsvorschläge und Anmerkungen und macht Konkretisierungen in Bezug auf die Herausgabe der E-ID an juristische Personen. Die IG ICT ZH bemerkt, dass die notwendigen Massnahmen abhängig von der Sicherheitsstufe seien.

Der VZGV bemerkt, dass die notwendigen Massnahmen abhängig von der Sicherheitsstufe seien und regt eine Präzisierung an.

Swisscom und UBS regen an in Art. 14 VE die Pflicht der Inhaberin oder des Inhabers der E-ID aufzunehmen, wann diese dem IdP Meldung zu erstatten haben zwecks Sperrung oder Widerruf der E-ID, insbesondere bei Vorliegen von Anhaltspunkten für Missbrauch der E-ID.

Eine Privatperson (F. Scotoni) sieht in der Delegationsnorm einen direkten Gegensatz zu Art. 164 Abs. 1 lit. c BV und regt eine genauere Umschreibung der Sorgfaltspflichten der Inhaberinnen und Inhaber an.

6.4 4. Abschnitt Betreiberinnen von E-ID-verwendenden Diensten

6.4.1 Art. 15 Vereinbarung mit IdP

BL schlägt vor, für sämtliche staatlichen Stellen und ausgelagerten Verwaltungsbetriebe eine effiziente staatliche Lösung vorzusehen oder aber zumindest die Möglichkeit zu schaffen, in einem einzigen Vertrag die Zusammenarbeit mehrerer Gemeinwesen mit einem IdP zu regeln. BL regt an sicherzustellen, dass die Kantone vor der Überwälzung von Wuchergebühren geschützt werden, namentlich weil die Kantone alle E-ID akzeptieren müssen. SZ empfiehlt, einen (eCH-)Standard zu schaffen, welcher schweizweit sicherstellt, dass gleiche bzw. gleichartige Online-Services das gleiche Sicherheitsniveau verlangen.

Die GLP schlägt eine Präzisierung des Textes vor, um klarzustellen, dass die Betreiberin eines E-ID-verwendenden Dienstes nicht mit allen IdP eine solche Vereinbarung abschliessen muss.

Die SBV regt an, eine Meldepflicht bei Anhaltspunkten für einen Missbrauch einzuführen.

Die UBS schlägt vor, einen Broker einzusetzen und dementsprechend den Gesetzestext anzupassen. Coop begrüsst die schlanke Formulierung des Gesetzesentwurfs und verlangt auch eine entsprechend schlanke Umsetzung auf Verordnungsebene. Wie für die Konsumentinnen und Konsumenten seien auch für die Betreiberinnen die Einfachheit und Flexibilität eines E-ID-Systems entscheidende Voraussetzungen für dessen Nutzung.

Eine Privatperson (D. Muster) stellt Fragen zur Kontrolle der Einhaltung der Vereinbarungen, und den Sorgfaltspflichten und Befugnissen bei der Kontrolle. Eine weitere Privatperson (B. Oldani) beantragt die Streichung dieses Artikels, da er impraktikabel sei.

6.4.2 Art. 16 Behörden als Betreiberinnen von E-ID-verwendenden Diensten

BE regt eine Ergänzung dahingehend an, dass die Verwendungspflicht auch die Unternehmen umfasse, die im Rahmen eines bundesrechtlichen Leistungsauftrags oder der bundesrechtlichen Regulierung grosse Teile der Bevölkerung bedienen. VS weist darauf hin, dass die betroffenen Verwaltungen ihre Identifizierungsumgebungen in einer Übergangsphase an das vorgeschlagene Gesetz anpassen können sollten. UR hält fest, dass für elektronische Behördendienstleistungen das Schutzniveau in der jeweiligen gesetzlichen Grundlage festgelegt werden sollte, ein Gesichtsbild und die Unterschrift nur für die höheren Schutzniveaus nötig seien und die Erfassung weiterer biometrischer Daten nicht vorgesehen sei. ZH sieht in der Verpflichtung jede anerkannte E-ID zu akzeptieren eine mögliche Marktverzerrung, da ein im Vergleich zu anderen Produkten teures und wenig wirtschaftliches E-ID-Produkt trotzdem Verbreitung finden würde, weil seine Nutzung nicht durch die Inhaberin oder den Inhaber, sondern aufgrund der gebrauchsbasierten Abgeltung mit staatlichen Mitteln finanziert würde. TG würde es begrüssen, wenn Musterverträge zur Verfügung gestellt würden.

Für economiesuisse und SwissHoldings soll die E-ID auch im Behördenverkehr als vollwertige - aber freiwillige - Alternative zu materiellen Identifikations- und Authentifikationsmitteln, wie Identitätskarte und Pass, akzeptiert werden.

Post und SBB fordern eine zentrale Akzeptanznorm, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt und machen einen Formulierungsvorschlag. Die UBS schlägt vor, den Artikel umfassender zu formulieren und einen Auftrag an die Gemeinden und Kantone auf Gesetzesstufe einzufügen. Die Swisscom regt an, überall, wo man sich staatlichen Stellen gegenüber elektronisch identifizieren und authentisieren muss (sei es bundesintern mit Angestellten der Bundesverwaltung oder im

Kontakt von natürlichen Personen mit der Bundesverwaltung), die staatlich anerkannte E-ID als einzige Möglichkeit zwingend vorzuschreiben.

6.5 5. Abschnitt

6.5.1 Art. 17 Pflichten

BL sieht es im Interesse des Kindes- und Jugendschutzes sowie um beschränkt handlungsfähige Menschen zu schützen angebracht, das Alter bis 18 Jahre und die Einschränkung der Handlungsfähigkeit stets zu übermitteln. Für BL ist zu klären, durch wen die Überprüfung gemäss Abs. 1 Bst. c gewährleistet werden muss. TG sieht es als sinnvoll an, in Art. 17 den Begriff „antragstellende Person“ zu verwenden. TG regt an, Regelungen zur Entsperrung der E-ID in das Gesetz aufzunehmen. ZH regt an, dass die Inhaberin oder der Inhaber der E-ID zusätzlich die Möglichkeit haben sollte, auf eigenes Begehren hin die Aufbewahrungszeit der Daten über die Anwendung der E-ID zu verlängern. Überdies soll die Inhaberin oder der Inhaber auf Wunsch die Daten einsehen und allenfalls selbstverantwortlich zu einem späteren Zeitpunkt (d. h. nach Ablauf der Frist von sechs Monaten) löschen können. ZH erachtete es als sinnvoll, den IdP zu verpflichten, die Sperrliste auch der Identitätsstelle nach Art. 19 E-ID-Gesetz zu melden; Zudem sei zu prüfen, ob auch den Strafverfolgungsbehörden Zugriff auf diese Sperrliste gewährt werden sollte.

Der FER erscheint es mit Blick auf die betroffenen Unternehmen nicht realistisch, dass die IdP jederzeit die Gültigkeit aller E-ID, die sie ausstellen, nachweisen können müssen und dass deren Überprüfung kostenlos möglich sein muss. Der Verweis auf die Kostenlosigkeit sollte gemäss der FER aus der Bestimmung gestrichen werden. Der VSKB regt Klärung und Anpassung von Abs. 1 Bst. g an, damit Konformität mit anderen gesetzlichen Aufbewahrungspflichten erreicht wird.

Die FMH stellt fest, dass die Frage einer Publikation oder einer Zugänglichmachung des Widerrufs oder der Sperrung an E-ID-Anwender wie z.B. an das Patientendossier nicht geregelt ist.

Post und SBB schlagen vor, das Wort „periodisch“ wegzulassen oder durch „ordnungsgemäss“ zu ersetzen. Die UBS hält fest, dass nur die Identitätsstelle die Überprüfung der Gültigkeit der E-ID jederzeit durchführen sollen könne; gegenüber Dritten, insbesondere gegenüber E-ID betreibenden Diensten, kann diese Pflicht des IdP nicht uneingeschränkt gelten. UBS und Swisscom schlagen vor, Bst. g zu streichen, da einerseits die Grundsätze des Datenschutzes gelten und es andererseits regulatorische Anforderungen geben könne, welche eine längere Aufbewahrung erfordern. Die UBS schlägt für das Teilen von Attributen, die über die Personenidentifizierungsdaten hinausgehen, vor, bei jedem Ereignis das ausdrückliche Einverständnis des E-ID-Inhabers vorzuschreiben; sie erachtet es als wichtig, dass Meldungen über Störungen oder den Verlust gemeldet und bearbeitet werden können. Wie dies organisiert ist, soll hingegen dem IdP überlassen bleiben.

Inclusion Handicap fordert, dass die benötigten technischen Mittel zur Einholung des Einverständnisses von den IdP so ausgestaltet werden, dass auch Menschen mit Behinderungen ihr Einverständnis schnell und auf unkomplizierte Weise geben und den Kundendienst in gleicher Weise benützen können, wie Menschen ohne Behinderungen. Dabei sollen mehrere verschiedene barrierefreie Kanäle zur Verfügung gestellt werden.

6.5.2 Art. 18 Interoperabilität

Der VSKB erachtet es als wichtig, dass die neu zu schaffende Identitätsstelle, welche die Standards der Schnittstellen für die Interoperabilität der E-ID-Systeme festlegt, dies prioritär angeht. In einem zweiten Schritt soll der Bundesrat die Interoperabilität mit dem Ausland prüfen und sicherstellen.

KARTAC und SPA regen an, die Orientierung an internationalen Standards bei der (technischen) Verordnungsgebung im Gesetz zu verankern. Für Digitalswitzerland ist die Interoperabilität zentraler Bestandteil für die erfolgreiche Einführung der E-ID-Lösung und befürwortet eine Vermittlerplattform; wie eine solche Vermittlerplattform zu gestalten ist, soll durch den Bund gefördert und abschliessend geklärt werden. SWITCH regt an, das am Markt nicht erprobte "Roaming" zwischen den verschiedenen Anbietern zu klären, so dass die Eckwerte vor der Akkreditierung und deutlich vor der Markteinführung vorliegen.

Privatim sieht eine unverhältnismässige Datenbekanntgabe, selbst wenn dafür das Einverständnis der betroffenen Personen erforderlich ist.

Post, SBB und SwissSign AG sehen es als zwingend an, die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer Roaming Gebühr zu regeln, da andernfalls eine Diskriminierung von IdP drohe, die über einen grossen E-ID Stamm verfügen. Des Weiteren wäre es für Post und SBB sinnvoll, die internationale Interoperabilität ebenfalls zu beachten und z.B. den Aufbau und Betrieb von STORK-Servern durch den Bund vorzuschreiben. Swisscom und UBS schlagen die Einführung eines Brokers und dessen Verankerung auf gesetzlicher Ebene vor.

Die BFH regt an, für den Identitätsverbund IDV Schweiz eine aktive Rolle im E-ID-Ökosystem innerhalb der Schweiz, wie auch zwischen der Schweiz und dem Ausland zu definieren.

6.6 6. Abschnitt: Schweizerische Stelle für elektronische Identität

6.6.1 Art. 19 Organisation

BL sieht den Aufbau von Wissen und Synergiepotenziale ungenutzt, wenn die Umsetzung dieses Gesetzes auf EFD und EJPD verteilt werden und beantragt die Umsetzung des E-ID-Gesetzes in einem Departement. LU erachtet es für notwendig, dass die Strafverfolgungsbehörden bei einer zentralen Anlaufstelle Informationen über erteilte E-ID einholen und Hinweise auf eine missbräuchliche Verwendung melden können. UR begrüsst, dass die Identitätsstelle wie von Ihnen vorgeschlagen im EJPD aufgebaut wird.

Da in Art. 19 und Art. 21 zwei unterschiedliche Departemente (EDF und EJPD) bezeichnet werden, regen Post und SBB an, Regeln zur Koordination zwischen der Identitätsstelle und der Anerkennungsstelle zu schaffen.

6.6.2 Art. 20 Aufgaben und Pflichten

SO beantragt die Prüfung der Berücksichtigung von Wohnsitz und Wohnadresse als spezifisches Element der elektronischen Identifizierung. Allenfalls sei die Liste in Art. 20 Abs. 2 E-ID-Gesetz durch die kantonal betriebenen Einwohnerregisterplattformen zu ergänzen.

SFIT empfiehlt einen zusätzlichen Absatz, der die Eindeutigkeit der E-ID-Registrierungsnummer sicherstellen soll.

6.7 7. Abschnitt: Anerkennungsstelle für IdP

6.7.1 Art. 21 Zuständigkeit

Der ISSS schlägt vor, die Anerkennungsstelle für IdP gemäss E-ID-Gesetz und die Akkreditierungsstelle für anerkannte Anbieterinnen von Zertifizierungsdienstleistungen gemäss ZertES zu vereinigen.

Post und SBB regen an, Abs. 1 zu einer Delegationsnorm umzugestalten und damit den Bundesrat zu ermächtigen, die Zuständigkeiten betreffend die Anerkennungsstelle zu bestimmen. Dies vereinfache die Zuständigkeiten und Aufsichten für verschiedene Trust Service Provider zu harmonisieren.

Eine Privatperson (D. Muster) wünscht eine Aufsichtsbehörde und ein Abgleich der Bestimmung mit dem ZertES betreffend Anerkennungsstelle.

6.7.2 Art. 22 Liste der anerkannten IdP

Keine Bemerkungen zu diesem Artikel.

6.8 8. Abschnitt: Gebühren Art. 23

In Bezug auf die Zugänglichkeit und die Kosten ist der Kanton FR der Auffassung, dass die Kosten im Hinblick auf einen verbreiteten Einsatz der elektronischen Identifikation für die Benutzerinnen und Benutzer möglichst tief sein sollten und die Verwendung möglichst einfach sein sollte. Betreffend die Finanzierung empfiehlt FR die Einführung eines jährlichen Kostendachs, damit das Budget unter Kontrolle bleibt. ZG sieht einen Widerspruch zwischen Art. 20 Abs. 4 und Art. 23 Abs. 1 im Bereich der Gebührenpflicht für Dienstleistungen der Identitätsstelle, der zu beseitigen sei.

Die GLP hält fest, dass es zu verhindern gilt, dass die IdP durch zu hohe Gebühren daran gehindert werden, die E-ID erfolgreich am Markt zu betreiben.

Digitalswitzerland begrüsst die geplante kostenlose Erstübermittlung von Personenidentifizierungsdaten im Herausgabeprozess. Die SPA regt an, bei der Gebühren-Festsetzung eine sachgerechte Abwägung zwischen den Interessen des Bundes an der Finanzierung seiner Verwaltungseinheiten und den überwiegenden volkswirtschaftlichen Interessen an einer weiten Verbreitung und Nutzung der E-ID in der Bevölkerung vorzunehmen.

Der VSKB begrüsst die im Erläuterungsbericht (S. 34) aufgeführte Option auf einen Verzicht der vollständigen Kostendeckung des Verwaltungsaufwands. IG eHealth schlägt vor, eine bedarfsgerechte Aktualisierung der Personenidentifizierungsdaten vorzusehen. Das vorgesehene Gebührenmodell wirke kontraproduktiv auf eine bedarfsgerechte Aktualisierung.

Post, SBB und SwissSign AG führen aus, dass Aufbau und Betrieb der staatlichen Identitätsstelle durch den Bund finanziert werden solle. Auf die Gebühren für die Dienstleistungen der Identitätsstelle sei zu verzichten. Die Daten der Identitätsstelle sollen den IdP kostenlos zur Verfügung stehen. Wird dem Antrag auf Gebührenverzicht nicht stattgegeben, sei zumindest eine Gleichbehandlung zwischen privatwirtschaftlichen IdP und solchen der öffentlichen Hand sicherzustellen.

Für NüGlarus sollten grundsätzlich keine Kosten bei der Nutzung einer E-ID eines Identitätsproviders durch einen Diensteanbieter anfallen, um die Verbreitung von neuen Technologien nicht zu verlangsamen. Eine Privatperson (B. Oldani) hält fest, dass die Identitätsstelle und die Anerkennungsstelle auf Gebühren verzichten sollen, denn falls Gebühren erhoben wer-

den, dienen sie zur Deckung des Aufwandes; Einsparungen des Aufwandes durch technische Weiterentwicklungen würden eine Gebührensenkung bewirken. Weiter würden die Behörden (Bund, Kantone, Gemeinden) wegen der E-ID vermehrt per E-Mail kommunizieren und ersparten sich gesamthaft Kosten für Briefpapier, Kuvert, Porto in Millionenhöhe. Diese Minderausgaben seien ein Gewinn zur Finanzierung der durch die E-ID anfallenden Anwendungskosten.

6.9 9. Abschnitt: Haftung Art. 24

BE, SO und GL weisen darauf hin, dass E-ID-verwendende Dienste oder IdP auch staatliche Stellen sein können, für die ein anderes Staatshaftungsrecht gelte, als das erwähnte Verantwortlichkeitsgesetz des Bundes (Verantwortlichkeitsgesetz, VG, SR 170.32). ZG hält fest, dass zumindest E-ID mit hohem Sicherheitsniveau so zu konzipieren seien, dass mit ihnen auch Rechtsgeschäfte abgeschlossen werden können.

Die FMH regt an festzuhalten, dass ähnlich wie im ZertES, auch im E-ID-Gesetz der IdP die Haftung weder für eigenes Verhalten noch für jenes ihrer Hilfspersonen wegbedingen könne.

Die Post regt an zu beachten, dass nicht Haftungsvorschriften zu einem Standortnachteil für Schweizer Akteure führen.

Inclusion Handicap erachtet eine barrierefreie Nutzung der E-ID als sehr wichtig, da für allfällige Fehler bei der Benutzung der E-ID, welche einen Schaden anrichten, die betroffenen E-ID-NutzerInnen eintreten müssten. Der Exkulpationsbeweis dürfte – wie generell im Cyberspace/im Internet - nicht einfach sein. Eine Privatperson (D. Muster) regt an, die Haftung der jeweiligen Partei klarer zu regeln; wie Z.B. in der EU-Verordnung. Eine Privatperson (F. Scotoni) sieht die vorgeschlagene Haftung als weitaus nachteiliger als eine Staatshaftung bei einer staatlichen Lösung an. Eine weitere Privatperson (B. Oldani) regt an diesen Artikel zu streichen, weil er nicht praktikabel sei; Weltweit hafte kein Softwarehersteller für eine Software.

6.10 10. Abschnitt: Schlussbestimmungen

Digitalswitzerland fordert den Bundesrat auf, das Inkrafttreten des E-ID-Gesetzes und der damit fallende Startschuss für eine breite anerkannte E-ID-Lösungen zu forcieren.

6.11 Änderung anderer Erlasse

BL schlägt eine Änderung in Art. 41 Abs. 6 AuG (Ausländergesetz, SR 142.20) vor: „Das SEM legt die Form und den Inhalt der Ausweise fest. Für Ausweise, welche nicht zum Bezug einer anerkannten elektronischen Identifizierungseinheit (E-ID) nach dem Bundesgesetz über anerkannte elektronische Identifizierungseinheiten berechtigen, legt das SEM Inhalt, Ausstellung, Verwendung, Sperrung und Widerruf zur elektronischen Identifizierung fest. Es kann die Ausfertigung der Ausweise und die Ausstellung der elektronischen Identifizierung teilweise oder ganz Dritten übertragen.“ TG bemerkt zur vorgesehenen Anpassung des ZertES, dass vom Verzicht der Vorsprache zur Erstellung einer elektronischen Signatur abzusehen sei.

Der VSKB fordert dazu auf, an geeigneter Stelle die Anforderungen an ein angemessenes Sicherheitsniveau bei den E-ID-verwendenden Diensten zu verankern und insbesondere im ZertES zu präzisieren, dass die Pflicht zur persönlichen Vorsprache nur entfalle, wenn eine E-ID der Sicherheitsniveaus „hoch“ oder „substanziell“ verwendet werde.

Der ASUT begrüsst die vorgesehene Ergänzung des Bundesgesetzes über die elektronische Signatur, allerdings sollte – analog Art. 24 Ziff. 1 Bst. b eIDAS-Verordnung – zusätzlich das Sicherheitsniveau "substanziell" oder „hoch“ gefordert werden; er schlägt vor, wo immer möglich bei Prozessen, in denen die Identität einer natürlichen Person durch persönliches Erscheinen mit Vorweisen eines Ausweisdokuments oder einer sonstigen qualifizierten Prüfung (z.B. Identifikation von Bankkunden) geprüft werden müsse, eine digitalisierte Variante mit Einsatz der E-ID zwingend vorzuschreiben. Der ISSS schlägt vor, im ZertES das Sicherheitsniveau der E-ID festzuhalten und im Ausweisgesetz verschiedene Anpassungen bezüglich Herausgabe von Ausweisen an Ausländer und der Führung der AHVN13 einzuführen. Der SFTI bemerkt, dass die von Art. 9 Abs. 1^{bis} ZertES angeordnete Rechtsfolge sich einerseits nur auf die Sicherheitsniveaus „substanziell“ und „hoch“, nicht aber auf das tiefste Sicherheitsniveau „niedrig“ erstrecken dürfe und andererseits mit der Bestimmung von Art. 7 VZertES (Verordnung über die elektronische Signatur, SR 943.032) koordiniert werden müsse.

Die FMH sieht in der vorgeschlagenen Anpassung des ZertES Inkompatibilität mit den verschiedenen Sicherheitsniveaus gemäss Art. 5 Abs. 1 des vorliegenden Gesetzesentwurfs. Der KFS regt eine Anpassung des Bundesgesetzes über den Konsumkredit (KKG) an, insbesondere die Art. 9, 11 und 12 KKG könnten dergestalt geändert werden, dass es ausreichend sei, wenn die Verträge sich durch Text nachweisen lassen.

Post und SBB regen an, im Minimum für EPDG, ZertES, VELeS (Verordnung der BK über die elektronische Stimmabgabe, SR 161.116), diverse Finanzmarktregulierungen, VeÜ-ZSSV (Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren, SR 272.1) VeÜ-VwV (Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens, SR 172.021.2), usw. die E-ID ausdrücklich als Referenz für elektronische Identitäten und deren Sicherheitsniveaus zu verankern. Die SBB regt an, im ZertES das Sicherheitsniveau der einsetzbaren E-ID zu präzisieren. Die Post regt an, im ZertES das Niveau so zu wählen, dass mit einer zu niedrigen E-ID (UserName/Password) kein qualifiziertes Zertifikat ausgestellt werden kann. Die Swisscom begrüsst die vorgesehene Ergänzung des Bundesgesetzes über die elektronische Signatur, und bemerkt, dass – analog zu Art. 24 Ziff. 1 Bst. b eIDAS-Verordnung – zusätzlich das Sicherheitsniveau "substanziell" oder „hoch“ gefordert werden sollte. Coop regt an, durch eine ergänzende Revision des Obligationenrechts den eCommerce zusätzlich zu unterstützen, indem die elektronische Übermittlung, die eine dauerhafte Aufzeichnung einer Vereinbarung ermöglicht, mit der heute geforderten Schriftlichkeit gleichgesetzt wird.

6.12 Erläuterungen

AG, BE, BL, GL, SH, SZ, ZH regen an, die finanziellen Folgen für die Kantone und die Gemeinden detaillierter auszuführen.

Für den SSV besteht eine Reihe weiterer Unklarheiten betreffend Folgekosten, insbesondere welches die Aufwände und Kosten für die Betreiber eines E-ID-verwendenden Dienstes wären, die durch das komplexe System der Zertifizierungen ausgelöst würden.

Die SIK bemerkt, dass der geplante Einführungszeitpunkt einer E-ID Ende 2019 bzw. im Verlauf des Jahres 2020 aufgrund dringend benötigter IAM-Lösungen sehr spät sei. Für laufende E-Government-Projekte sei es wichtig, dass in diesem Bereich eine gemeinsame Umsetzung angegangen wird. Es muss sichergestellt werden, dass die Vorhaben des Bundes wie der IDV sehr eng mit der Gesetzgebung der E-ID abgestimmt werden. In der Botschaft sind die Zusammenhänge und Abhängigkeiten dieser Projekte zur E-ID aufzuzeigen.

7 Einsichtnahme

Gemäss Art. 9 des Bundesgesetzes vom 18. März 2005 über das Vernehmlassungsverfahren (SR 172.061) sind die Vernehmlassungsunterlagen, nach Ablauf der Vernehmlassungsfrist die Stellungnahmen der Vernehmlassungsteilnehmer, und nach Kenntnisnahme durch den Bundesrat der Ergebnisbericht, öffentlich zugänglich. Sämtliche Stellungnahmen sind integral veröffentlicht unter Startseite BJ > Staat & Bürger > Laufende Rechtsetzungsprojekte > E-ID-Gesetz.

Verzeichnis der Eingaben
Liste des organismes ayant répondu
Elenco dei partecipanti

Kantone / Cantons / Cantoni

AG	Aargau / Argovie / Argovia
AI	Appenzell Innerrhoden / Appenzell Rh.-Int. / Appenzello Interno
AR	Appenzell Ausserrhoden / Appenzell Rh.-Ext. / Appenzello Esterno
BE	Bern / Berne / Berna
BL	Basel-Landschaft / Bâle-Campagne / Basilea-Campagna
BS	Basel-Stadt / Bâle-Ville / Basilea-Città
FR	Freiburg / Fribourg / Friburgo
GE	Genf / Genève / Ginevra
GL	Glarus / Glaris / Glarona
GR	Graubünden / Grisons / Grigioni
JU	Jura / Giura
LU	Luzern / Lucerne / Lucerna
NE	Neuenburg / Neuchâtel
NW	Nidwalden / Nidwald / Nidvaldo
OW	Obwalden / Obwald / Obvaldo
SG	St. Gallen / Saint-Gall / San Gallo
SH	Schaffhausen / Schaffhouse / Sciaffusa
SO	Solothurn / Soleure / Soletta
SZ	Schwyz / Svitto
TG	Thurgau / Thurgovie / Turgovia
TI	Tessin / Ticino
UR	Uri
VD	Waadt / Vaud
VS	Wallis / Valais / Vallese
ZG	Zug / Zoug / Zugo
ZH	Zürich / Zurich / Zurigo

Parteien / Partis politiques / Partiti politici

BDP	Bürgerlich-Demokratische Partei BDP Parti bourgeois-démocratique PBD Partito borghese democratico PBD
CVP	Christlichdemokratische Volkspartei CVP Parti Démocrate-Chrétien PDC Partito Popolare Democratico PPD
FDP	FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali PLD. Ils Liberals
GPS	Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES
GLP	Grünliberale Partei glp Parti vert'libéral pvl
Piratenpartei	Piratenpartei Parti Pirate Partito Pirata
SP	Sozialdemokratische Partei der Schweiz SP Parti Socialiste Suisse PS Partito Socialista Svizzero PS
SVP	Schweizerische Volkspartei SVP Union Démocratique du Centre UDC Unione Democratica di Centro UDC

Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete sowie Gebietskörperschaften / Associations faîtières des communes, des villes et des régions de montagne qui oeuvrent au niveau national et collectivités locales / Associazioni mantello nazionali dei Comuni delle città e delle regioni di montagna e autorità territoriali

Gemeindeverband	Schweizerischer Gemeindeverband Association des Communes Suisses Associazione dei Comuni Svizzeri Associaziun da las Vischnancas Svizras
SSV	Schweizerischer Städteverband Union des villes suisses Unione delle città svizzere
Pfäffikon ZH	Gemeinde Pfäffikon ZH

Gesamtschweizerische Dachverbände der Wirtschaft / Associations faîtières de l'économie qui oeuvrent au niveau national / Associazioni mantello nazionali dell'economia

CP	Centre patronal
Economiesuisse	Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation
FER	Fédération des Entreprises Romandes
SBV	Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association
SGV	Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)
SwissHoldings	Verband der Industrie- und Dienstleistungskonzerne in der Schweiz Fédération des groupes industriels et de services en Suisse Federation of Industrial ans Service Groups ins Switzerland
VSKB	Verband Schweizerischer Kantonalbanken Union des Banques Cantonales Suisses Unione delle Banche Cantionali Svizzere

Vereinigungen im IKT-Bereich / Associations du domaine informatique et télécommunications

ASUT	Verband der Telekommunikationsbranche in der Schweiz Association du secteur des télécommunications en Suisse
Digitalswitzerland	Schweizer Verein für die Digitale Innovation association Suisse pour l'innovation digitale Associazione svizzera per lo sviluppo digitale
IG ICT ZH	Interessengemeinschaft der Zürcher Gemeinden für Information and Communications Technology
ISSS	Information Security Society Switzerland Fachverband in der Schweiz für ICT-Sicherheit
KARTAC	Interessengemeinschaft der Zahlkartenindustrie
SDA	Swiss Data Alliance
SFTI	Swiss Fintech Innovations Verband schweizerischer Finanzinstitute zur Förderung von digitalen Innovationen
SIK	Schweizerische Informatikkonferenz Conférence suisse sur l'informatique Conferenza svizzera sull'informatica Conferenza svizra d'informatica

SPA	Swiss Payment Association Branchenorganisation der Schweizer Herausgeber (Issuer) von Kreditkarten der internationalen Kartenorganisationen
Swico	Wirtschaftsverband für die digitale Schweiz
swissICT	Schweizerischer Verband der Informations- und Kommunikationstechnologie
SWITCH	Stiftung neutrale Technologie- und Dienstleistungsplattform der Schweizer Hochschulen

Andere Vereinigungen / Autres associations

DJS	Demokratische Juristinnen und Juristen der Schweiz DJS Juristes démocratiques de Suisse JDS Giuristi e Giuriste Democratici Svizzeri GDS Giuristas e Giurists Democratics Svizzers GDS
eGov-Schweiz	Verein zur Förderung der Innovation im eGovernment Association favorisant la promotion de l'innovation dans la cyberadministration (eGovernment)
FMH	Verbindung der Schweizer Ärztinnen und Ärzte FMH Fédération des médecins suisses FMH Federazione dei medici svizzeri FMH
IG eHealth	Interessengemeinschaft eHealth
Inclusion Handicap	Dachverband der Behindertenorganisationen Association faîtière des organisations suisses de personnes handicapées
KAZ	Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst Conférence des autorités cantonales de surveillance de l'état civil Conferenza delle autorità di vigilanza sullo stato civile
KFS	Verband Konsumfinanzierung Schweiz (KFS) L'association Financement à la consommation Suisse (FCS)
ParlDigi	Parlamentarische Gruppe Digitale Nachhaltigkeit
Privatim	Die schweizerischen Datenschutzbeauftragten Les préposé(e)s suisses à la protection des données Gli incaricati svizzeri della protezione die dati
SAV	Schweizerischer Anwaltsverband SAV Fédération Suisse des Avocats Federazione Svizzera degli Avvocati Swiss Bar Association
Schweizerischer Verband für Zivilstandswesen	Schweizerischer Verband für Zivilstandswesen Association suisse des officiers de l'état civil Associazione svizzera degli ufficiali dello stato civile
SKS	Stiftung für Konsumentenschutz
VSED	Verband Schweizerischer Einwohnerdienste (VSED) Association suisse des services des habitants (ASSH) Associazione svizzera die servizi agli abitanti (ASSA)

Associazioni svizra dals servetschs als abitants (ASSA)

VZGV Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute

Unternehmen / Entreprises /

Coop Coop Genossenschaft

Post Die Post
La poste
La posta
Swiss Post

SBB Schweizerische Bundesbahnen SBB
Chemins de fer fédéraux suisses CFF
Ferrovie federali svizzere FFS

Swisscom Swisscom (Schweiz) AG

SwissSign AG Gemeinschaftsunternehmen der Post und der SBB

UBS UBS Schweiz

Weitere Interessierte und Privatpersonen / Autres milieux intéressés et particuliers / e privati

BFH Berner Fachhochschule
Haute école spécialisée bernoise

Digitale Gesellschaft Digitale Gesellschaft
Société Numérique
Società Digitale
Societad Digitala
Digital Society

Grundrechte.ch grundrechte.ch
droitsfondementaux.ch
dirittifondamentali.ch

NüGlarus Standortinitiative Kanton Glarus

Open Geneva Hackathon Bruno Chanel
Jörn Erbguth
Jean-Henry Morin
Vincent Pignon
Alexis Roussel
Guillaume Saouli

Privatpersonen Ralf Hauser
Stefan Häusler
Beat Lehmann
Daniel Muster
Beat Oldani
Fabio E. R. Scotoni

Auf eine Stellungnahme verzichtet haben:

- Santésuisse
Branchenorganisation der Schweizer Krankenversicherer
Organisation de la branche de l'assurance-maladie sociale
- Schweizerischer Arbeitgeberverband
Union patronale suisse
Unione svizzera degli imprenditori



Loi fédérale sur les services d'identification électronique (LSIE)

Synthèse des résultats de la procédure de consultation

Table des matières

1	Objet de la consultation	4
2	Déroulement de la procédure de consultation	4
3	Avis reçus	5
3.1	Participation	5
3.2	Présentation des résultats dans le rapport	5
4	Appréciation générale de l'avant-projet	5
4.1	Généralités	5
4.2	Remarques relatives au concept et à la répartition des tâches entre l'Etat et les acteurs du marché	6
5	Autres questions	8
5.1	Interopérabilité	8
5.2	Numéro d'enregistrement de l'e-ID	8
5.3	Données d'identification personnelle	9
6	Remarques relatives aux dispositions	10
6.1	Section 1 Dispositions générales	10
6.1.1	Art. 1 Objet et but	10
6.1.2	Art. 2 Définitions	11
6.2	Section 2 Etablissement d'un e-ID	11
6.2.1	Art. 3 Conditions personnelles	11
6.2.2	Art. 4 Reconnaissance des FI	13
6.2.3	Art. 5 Niveau de garantie	14
6.2.4	Art. 6 Procédure d'établissement	15
6.2.5	Art. 7 Données d'identification personnelle	17
6.2.6	Art. 8 Mise à jour des données d'identification personnelle	18
6.2.7	Art. 9 Utilisation systématique du numéro AVS pour l'échange de données	19
6.2.8	Art. 10 Traitement et transmission des données	20
6.2.9	Art. 11 Expiration de la reconnaissance Art. 12 Mesures de surveillance et retrait de la reconnaissance	21
6.2.10	Art. 13 Système e-ID subsidiaire de la Confédération	22
6.3	Section 3 Titulaires d'un e-ID (art. 14)	23
6.4	Section 4 Exploitants d'un service utilisateur	23
6.4.1	Art. 15 Accord avec un FI	23
6.4.2	Art. 16 Autorités en tant qu'exploitants d'un service utilisateur	24
6.5	Section 5	24
6.5.1	Art. 17 Devoirs	24
6.5.2	Art. 18 Interopérabilité	25
6.6	Section 6 Service d'identité électronique suisse	25
6.6.1	Art. 19 Organisation	25
6.6.2	Art. 20 Tâches et devoirs	26
6.7	Section 7 Organisme de reconnaissance des FI	26
6.7.1	Art. 21 Compétence	26
6.7.2	Art. 22 Liste des FI	26
6.8	Section 8 Émoluments (art. 23)	26
6.9	Section 9 Responsabilité (art. 24)	27
6.10	Section 10 Dispositions finales	27

6.11 Modification d'autres actes..... 27

6.12 Rapport explicatif 28

Anhang / Annexe / Allegato..... 30

1 Objet de la consultation

La sécurité juridique et la confiance sont des conditions essentielles pour le développement des transactions. À cet égard, il est indispensable d'établir de façon fiable l'identité des parties prenantes. Dans le monde physique, la Confédération met déjà à disposition des moyens d'identification conventionnels tels que le passeport suisse, la carte d'identité et le titre de séjour. Il sera désormais également possible d'établir l'identité d'une personne physique par voie électronique à l'aide d'une « identité électronique » indépendante de la technologie utilisée ou du support choisi, soit un « moyen d'identification électronique (e-ID) ». Le titulaire d'un e-ID reconnu par l'État pourra s'enregistrer auprès de services en ligne (les services utilisateurs) de manière sécurisée et s'y reconnecter ultérieurement, toujours de manière sécurisée. D'autres services de confiance comme la signature électronique pourront être proposés par les fournisseurs d'identité (FI) mais ne font pas partie intégrante des e-ID.

L'avant-projet prévoit une répartition des tâches entre l'État et les acteurs du marché. L'acceptation de l'e-ID passe par la mise en place de conditions-cadre légales et organisationnelles fiables et dépend de la capacité de fonctionnement et du dynamisme du marché. La Confédération habilitera les FI satisfaisant aux conditions requises à établir des e-ID reconnus et à gérer des systèmes e-ID reconnus.

2 Déroulement de la procédure de consultation

Par décision du 19 décembre 2012, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'élaborer, en collaboration avec la Chancellerie fédérale (ChF), le Département fédéral de l'économie, de la formation et de la recherche (DEFR), le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) et le Département fédéral des finances (DFF), un concept et un projet de loi relatifs à des moyens d'identification électronique officiels qui puissent être proposés conjointement avec la carte d'identité. La première ébauche du concept, présentée dans la note de discussion du 28 février 2014, prévoyait que l'État soit le principal fournisseur d'identité et qu'un e-ID soit remis à tous les Suisses en même temps que la carte d'identité. Elle a fait l'objet d'une consultation auprès des offices et des acteurs du marché en 2014 et 2015.

Compte tenu des avis reçus et des expériences faites dans d'autres pays, le concept a été fondamentalement remanié. Le développement de solutions par l'État lui-même et l'établissement d'e-ID délivrés par l'État engendrent généralement, pour les pouvoirs publics, des coûts informatiques élevés non couverts (par ex. pour le support technique, les systèmes de lecture, les logiciels) car ils n'offrent pas la flexibilité requise pour faire face à l'évolution rapide des besoins et de la technologie. En revanche, le secteur privé développe déjà des moyens d'identification de différents niveaux de garantie (par ex. Apple-ID, Google-ID, Mobile-ID, OpenID, SuisseID, SwissPass, etc.). Il est difficile de déterminer quels e-ID utilisés à l'heure actuelle existeront encore à moyen et à long terme. C'est la raison pour laquelle le nouveau concept prévoit une répartition des tâches entre l'État et le secteur privé.

Le 13 janvier 2016, le Conseil fédéral a pris acte du concept pour des systèmes d'e-ID, chargé le DFJP d'élaborer une loi et fixé le cadre de la législation.

La procédure de consultation relative à l'avant-projet concernant la loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) s'est tenue du 22 février au 29 mai 2017. Le Conseil fédéral a invité les cantons, les partis politiques représentés au sein de l'Assemblée fédérale, les associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national, les associations faîtières

de l'économie qui œuvrent au niveau national ainsi que d'autres organisations intéressées à y prendre part.

3 Avis reçus

3.1 Participation

Sur 65 destinataires consultés, 48 ont répondu. Dans l'ensemble, 88 participants ont donné leur avis, dont 26 cantons, 8 partis politiques et 54 organisations et autres participants.

Quarante participants ont écrit de manière spontanée. Il s'agit d'une part d'associations de l'économie, issues en particulier du domaine de l'informatique et des télécommunications et des services financiers, et d'associations de la cyberadministration et de la cybersanté, et d'autre part de particuliers.

Santésuisse a explicitement indiqué n'avoir aucune remarque à faire sur l'avant-projet et l'Union patronale suisse a renoncé à prendre position.

3.2 Présentation des résultats dans le rapport

Dans le présent rapport, les participants sont classés selon les catégories suivantes : les cantons ; les partis politiques ; les associations faîtières des communes, des villes et des régions de montagne et les collectivités locales ; les associations faîtières de l'économie ; les associations du domaine informatique et télécommunications ; les autres associations ; les entreprises ; les autres milieux intéressés et les particuliers.

La liste en annexe présente les avis reçus en fonction de ces catégories (voir annexe 1).

Le présent rapport se limitera à la description des remarques essentielles relatives à l'avant-projet. Les avis sont publiés dans leur intégralité avec le présent rapport à l'adresse suivante : Accueil OFJ > État & Citoyen > Projets législatifs en cours > Loi e-ID.

4 Appréciation générale de l'avant-projet

4.1 Généralités

Tous les participants estiment qu'il est indispensable d'instaurer les e-ID en Suisse et saluent – à l'exception de l'UDC – l'adoption d'une loi à cet effet. La nécessité de mettre en place un moyen d'identification sécurisé pour les services en ligne le plus rapidement possible n'est pas contestée. La solution choisie devra impérativement être compatible au niveau international, en particulier avec les solutions développées par les États membres de l'UE.

Aucun participant ne demande l'élaboration d'un e-ID dont l'utilisation se limite à la Suisse ; la solution développée doit donc s'appuyer sur le règlement eIDAS de l'UE¹ et ses règlements d'application afin qu'une notification future soit possible.

¹ Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

4.2 Remarques relatives au concept et à la répartition des tâches entre l'État et les acteurs du marché

Un thème récurrent dans les avis est le rôle de l'État lors de l'établissement des e-ID. Il s'agit principalement de déterminer s'il appartient à l'État ou au secteur privé de gérer le ou les systèmes électroniques permettant d'établir, de gérer et d'utiliser les e-ID (les systèmes e-ID). Les participants n'apportent pas de réponse d'ensemble claire à cette question. Certains considèrent que l'établissement des e-ID et l'identification du requérant doivent être pris en charge par les FI (par ex. la Poste, un opérateur téléphonique ou une banque) selon une procédure clairement définie et régulièrement contrôlée ; d'autres estiment que cela devrait relever de la responsabilité d'un service étatique, par exemple le bureau cantonal des passeports.

Vingt-et-un cantons se prononcent en faveur de la répartition prévue par l'avant-projet². AI et AR rejettent la répartition des tâches proposée et souhaiteraient que l'e-ID soit délivré par l'État, comme pour le passeport et la carte d'identité. TG n'approuve que partiellement l'avant-projet sur ce point. ZG préférerait que l'e-ID soit établi par l'État, mais que le secteur privé se charge du support technique et de l'aide aux utilisateurs. ZH suggère de mettre en place une institution tenant lieu de FI et où seraient représentés la Confédération, les cantons et les communes, sous la direction de la Confédération. VD propose que l'e-ID soit établi par un service fédéral ou par le secteur privé, selon le but dans lequel l'e-ID sera utilisé. BS se demande si l'établissement des e-ID ne relève tout de même pas de la souveraineté de l'État.

Les partis politiques sont partagés sur cette question. Pour le PBD, la preuve électronique et officielle de l'identité (e-ID officiel) est une tâche qui appartient à l'État ; l'e-ID ne peut être délivré que par l'État ou tout au plus par un tiers mandaté par l'État. Le PDC approuve le fait que la Confédération prévoit des conditions-cadre pour la reconnaissance des e-ID, mais se demande si la mise à disposition d'e-ID n'est pas plutôt du ressort de l'État, particulièrement en ce qui concerne les services de la cyberadministration qui nécessitent un niveau de garantie élevé. Le PLR approuve l'orientation générale du concept. Selon lui, le rôle de l'État n'est pas de gérer les applications mais seulement de définir les conditions-cadre qui permettront à l'économie et aux citoyens de tirer le meilleur parti de la numérisation ; en raison du développement rapide de la technologie, le secteur privé est plus à même que l'État d'élaborer et de proposer des systèmes e-ID. Le PVL soutient lui aussi le concept de la Confédération et estime que l'écosystème e-ID doit être créé par une répartition des tâches entre l'État et le secteur privé ; il approuve le modèle d'établissement de l'e-ID par des FI du secteur privé soumis à une procédure de reconnaissance officielle. Pour les Verts, si l'identité électronique (e-ID) est nécessaire, ce projet va dans la mauvaise direction : octroyer une identité, un « passeport » digital est une tâche qui doit rester dans les mains de la puissance publique. Le Parti pirate accepte en principe le développement et l'introduction d'un e-ID afin de permettre l'identification officielle et électronique des personnes, mais considère que la preuve de l'identité, qu'elle soit sous forme papier ou électronique, relève de la responsabilité de l'État. Le PS rejette l'avant-projet sous sa forme actuelle mais reconnaît la nécessité de légiférer. Il demande à la Confédération de proposer un compromis entre le transfert complet de la responsabilité au secteur privé et le développement d'une solution entièrement étatique. Pour le PS, il serait préférable d'élaborer une solution qui accorde plus d'importance à l'État au cours de la procédure et de la mise au point technique de l'e-ID, sans que le secteur privé soit exclu ni que son savoir technique et sa capacité d'innovation soient mis de côté pour autant. L'UDC rejette l'avant-projet mais admet que l'État renonce à établir les e-ID. Elle

² AG, BE, BL, BS, FR, GE, GL, GR, JU, LU, NE, NW, OW, SH, SG, SO, SZ, TI, UR, VS, ZH

trouve justifié que la Confédération s'abstienne d'endosser une telle responsabilité et estime qu'il revient aux acteurs du marché de déterminer si un système sera utilisé et lequel.

Les collectivités locales ont des opinions divergentes. Pfäffikon ZH approuve la répartition proposée et suggère également de mettre en place une institution tenant lieu de FI et où seraient représentés la Confédération, les cantons et les communes, sous la direction de la Confédération. L'ACS et une majorité de l'UVS rejettent la répartition proposée et plaident pour l'élaboration d'une solution entièrement étatique. L'UVS demande que la Confédération revoie l'avant-projet et propose une variante dans laquelle les e-ID sont entièrement établis par l'État.

Les associations faîtières de l'économie, c'est-à-dire le CP, Economiesuisse, la FER, l'ASB, l'USAM, SwissHoldings et l'UBCS, se sont déclarées favorables à la répartition des tâches prévue par l'avant-projet.

Quant aux associations du domaine informatique et télécommunications, Digitalswitzerland, l'IG ICT ZH, la KARTAC, la SFTI, la SPA et SwissICT ont approuvé le concept en ce qui concerne la répartition des tâches entre l'État et le secteur privé. L'ASUT et l'ISSS suggèrent que la Confédération propose un e-ID officiel en plus de ceux du secteur privé. Pour la SDA et Swico, la preuve officielle de l'identité électronique est une tâche étatique que la Confédération doit assumer seule. SWITCH propose de renoncer à la solution proposée et suggère de mettre en place une solution établie par la Confédération ou par un tiers mandaté par la Confédération.

Au sein des autres associations, la FSA et le VZGV se déclarent favorables à la répartition proposée. Si le VZGV approuve l'optimisation et la dématérialisation des processus, il favorise toujours explicitement une solution étatique. Les JDS, eGov-Schweiz, ParlDigi et la SKS considèrent que la preuve officielle de l'identité électronique est une tâche souveraine ; elle doit donc être prise en charge par la Confédération, ou par au plus un tiers mandaté par la Confédération. Privativement se demande si l'établissement d'un e-ID ne constitue pas une tâche étatique au même titre que la délivrance des documents d'identité, auquel cas les services fédéraux devraient s'en charger.

Coop, la Poste, les CFF, Swisscom, SwissSign SA et UBS approuvent la répartition proposée. Afin d'encourager la diffusion des e-ID, Swisscom et SwissSign SA proposent que la demande d'établissement d'un e-ID puisse se faire auprès des bureaux des passeports ou des offices de migration cantonaux, et pas seulement auprès d'un FI. UBS suggère d'utiliser les processus d'identification déjà développés par les banques, les entreprises de télécommunications, etc. comme base de l'établissement des e-ID. Pour Coop, il est impératif de renoncer à un « plus » suisse sous quelque forme que ce soit.

R. Hauser se prononce entièrement en faveur de la répartition proposée. NüGlarus approuve la répartition proposée et propose que l'État délivre un e-ID officiel en plus de ceux mis à disposition par les FI. La Société Numérique et Open Geneva Hackathons considèrent que prouver l'identité d'une personne et délivrer des documents d'identité sont des tâches qui relèvent de la souveraineté de l'État et qui ne doivent pas être cédées au secteur privé. La BFH, droitsfondamentaux.ch, les JDS et trois particuliers (S. Häusler, B. Lehmann, et F. Scotoni) critiquent la répartition proposée et considèrent que l'établissement des e-ID constitue une tâche étatique.

5 Autres questions

5.1 Interopérabilité

L'avant-projet prévoit à l'art. 18 que les systèmes e-ID doivent être interopérables, c'est-à-dire que tous les e-ID peuvent être utilisés pour tous les services utilisateurs. Cette interopérabilité doit également être valable sur le plan international de sorte que les systèmes e-ID puissent faire l'objet d'une notification à la Commission européenne. Les participants à la procédure de consultation qui se sont exprimés sur ce point approuvent sur le principe cette disposition. Ils demandent en outre la mise en place d'un service d'intermédiaire, le « broker d'e-ID ».

VS, GR, BE et SH soulignent l'importance de l'interopérabilité. GR et TI demandent également de clarifier le rôle de la Fédération suisse d'identités (FSI).

En ce qui concerne les partis politiques, le PDC, le PVL et le PLR mentionnent l'importance de l'interopérabilité. Pour le PLR, il est impératif que les systèmes e-ID des différents fournisseurs soient interopérables et que la mise à disposition d'une interface entre la FSI et les FI soit garantie. Il demande de compléter l'avant-projet à cet effet.

L'UVS demande d'inclure la FSI dans le projet de loi.

La FER et l'UBCS considèrent également que l'interopérabilité est une condition indispensable à la diffusion de l'e-ID. Afin de garantir l'interopérabilité, l'ASB souhaiterait la mise en place d'un intermédiaire entre les différents FI et entre les FI et les services utilisateurs.

Au sein des associations du domaine informatique et télécommunications, l'ASUT, Digitalswitzerland, la KARTAC, la SFTI, SWITCH et SwissICT se prononcent explicitement en faveur de l'interopérabilité au niveau national et international. Digitalswitzerland propose de mettre en place une plateforme de transmission qui permettrait de transférer les attributs d'identité entre les différents FI.

Coop, la Poste, les CFF, SwissSign SA et UBS estiment nécessaire de légiférer en matière d'interopérabilité internationale afin de régler la reconnaissance des moyens d'identification électronique étrangers. Selon ces entreprises, la loi devrait également régler les indemnités entre les FI. Swisscom propose d'instaurer un intermédiaire qui ferait le lien entre les FI et entre les FI et les services utilisateurs.

NüGlarus est favorable à l'interopérabilité des e-ID suisses avec les solutions des États membres de l'UE.

5.2 Numéro d'enregistrement de l'e-ID

L'avant-projet part du principe que la pratique actuelle en matière d'utilisation du n° AVS restera inchangée et introduit de ce fait un numéro d'enregistrement de l'e-ID qui sera utilisable pour l'e-ID mais aussi pour d'autres applications.

BE, BL, LU, NE, SH, UR, VD, ZH et ZG souhaiteraient que le n° AVS puisse aussi être utilisé pour l'e-ID. AG, BS et VS approuvent la solution choisie et l'introduction d'un numéro d'identification neutre.

Le PBD, le PES et le Parti pirate n'approuvent pas l'introduction d'un numéro d'enregistrement de l'e-ID et proposent d'utiliser des codes d'authentification non réutilisables, différents pour chaque transaction.

Pfäffikon ZH approuve la possibilité prévue dans l'avant-projet d'utiliser le n° AVS.

Parmi les associations faitières de l'économie, l'UBCS suggère d'attribuer un numéro d'enregistrement de l'e-ID lors de la délivrance de la carte d'identité ou du passeport.

En ce qui concerne les associations du domaine informatique et télécommunications, la SDA et Swico se prononcent en faveur de l'utilisation d'un code d'authentification non réutilisable, spécifique à chaque transaction. Selon eux, introduire un nouveau numéro personnel central et permanent serait une erreur. L'ISSS préconise l'introduction d'un numéro univoque d'identification qui ne permette pas de retrouver le n° AVS.

Parmi les autres associations, Privatim approuve l'utilisation d'un identificateur univoque non parlant et indépendant du numéro AVS. Le VZGV se félicite que l'avant-projet prévoie la possibilité d'étendre le cercle des personnes habilitées à utiliser le numéro AVS. Pour la FMH et l'IG eHealth, il est nécessaire de veiller à ce qu'aucune incompatibilité ne survienne qui puisse empêcher l'utilisation de l'e-ID pour les dossiers des patients. Le numéro d'enregistrement de l'e-ID doit pouvoir être rattaché au numéro d'identification du patient. eGov-Schweiz propose qu'un identificateur univoque dans le domaine de la cyberadministration soit disponible pour les personnes physiques et morales afin d'étendre le champ d'utilisation de l'e-ID. L'association admet également la possibilité d'utiliser le n° AVS.

UBS estime qu'une personne doit pouvoir disposer de plusieurs e-ID rattachés à des numéros d'enregistrement différents.

Parmi les autres participants, Open Geneva Hackathons et B. Lehmann se déclarent favorables à l'utilisation d'un identificateur univoque non parlant et indépendant du n° AVS.

5.3 Données d'identification personnelle

Un e-ID reconnu par l'État confirme l'existence et l'identité d'une personne physique par le biais des données d'identification personnelle contenues dans des registres tenus et mis à jour par l'État. Comme seules les données gérées par les systèmes d'information de la Confédération (système d'information relatif aux documents d'identité [ISA] ; système d'information central sur la migration [SYMIC] ; registre informatisé de l'état civil [Infostar] ; registre central de la Centrale de compensation de l'AVS [CdC-UI]) peuvent être attestées, la liste à l'art. 7 de l'avant-projet est exhaustive.

AG, BS et GR proposent de réduire le nombre de données d'identification personnelle attestées et rappellent qu'il n'est pas autorisé d'exploiter plus de données personnelles dans le cadre des applications de la cyberadministration que dans le monde réel ; TG recommande d'interdire l'attribution de données supplémentaires à l'e-ID.

Le Parti pirate et le PES estiment que les données attribuées à l'e-ID devraient être les mêmes que celles attribuées aux documents d'identités traditionnels. L'e-ID devrait uniquement contenir les données de base, c'est-à-dire le(s) nom(s), les prénoms, la date de naissance et éventuellement la nationalité et le lieu d'origine.

L'ACS souhaiterait que le nombre de données d'identification personnelle attestées soit réduit.

Au sein des associations faitières de l'économie, l'ASB approuve le fait que d'autres informations que les données d'identification personnelle attestées par l'État puissent être attribuées à un e-ID.

Quelques associations du domaine informatique et télécommunications proposent des variantes relatives à l'attestation et au traitement des données supplémentaires. L'IG ICT ZH ne voit aucune raison de fixer et de circonscrire la liste des données d'identification person-

nelle qui peuvent être attribuées à un e-ID. Pour la KARTAC, il appartient aux personnes concernées de déterminer à quel niveau de garantie attribuer chaque donnée d'identification. À l'inverse, la SPA propose que la loi définisse le niveau de garantie correspondant à chaque donnée d'identification personnelle attribuée à un e-ID par le service d'identité. L'ISSS suggère que l'on précise par voie d'ordonnance quels attributs biométriques et quels paramètres personnels peuvent être ajoutés à l'e-ID.

Les autres associations ne sont pas plus unanimes. Alors que les JDS s'opposent à ce que les données personnelles soient collectées, gardées en réserve et mises à la disposition de fournisseurs privés, et que Privatim estime que le nombre de données attestées constitue une communication de données non conforme au principe de proportionnalité, la FMH souhaiterait que le numéro d'identification du patient au sens de la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP, RS 816.1) puisse être rattaché à l'e-ID. La FCS propose de donner la possibilité aux titulaires de sauvegarder d'autres données personnelles sur leur e-ID. Le FSA considère que certains attributs (l'état civil et la nationalité) n'apportent pas plus de sécurité et conseille de renoncer à les utiliser. Le VZGV estime qu'il n'est pas pertinent de dresser une liste exhaustive des données d'identification personnelles puisque d'autres données d'identification pourront être incluses dans les systèmes d'information de la Confédération à l'avenir. Pour l'ASSH, le titulaire de l'e-ID devrait pouvoir déterminer lui-même, lors de l'utilisation de l'e-ID, le nombre de données d'identification personnelle que le FI transmettra à un service utilisateur.

En ce qui concerne les entreprises, UBS suggère d'ouvrir la liste qui figure à l'art. 7, al. 2, à d'autres attributs.

Parmi les autres participants, la BFH propose de permettre aux fournisseurs privés d'attribuer d'autres données à l'e-ID. La Société numérique souhaiterait quant à elle renoncer à l'utilisation d'éléments biométriques pour l'identification. Pour droitsfondamentaux.ch, l'avant-projet va beaucoup trop loin en ce qui concerne les données qui peuvent être utilisées pour un e-ID ; il est incompréhensible qu'autant de données personnelles puissent être collectées — pour ainsi dire gardées en réserve — et mises à la disposition de fournisseurs privés.

6 Remarques relatives aux dispositions

6.1 Section 1 Dispositions générales

6.1.1 Art. 1 Objet et but

Parmi les associations faîtières de l'économie, l'ASB et l'UBCS proposent de mentionner la large diffusion des e-ID et le respect des normes internationales dans l'article relatif au but.

La KARTAC et la SPA, deux associations du domaine informatique et télécommunications, suggèrent d'intégrer parmi les buts de la loi une large diffusion et utilisation de l'e-ID ainsi que la nécessité de garantir l'interopérabilité nationale et internationale.

Les entreprises se prononcent de la manière suivante : l'UBS propose également d'intégrer la large diffusion et le respect des normes internationales dans cet article. La Poste se félicite que l'utilisation des e-ID soit considérée comme un objet de la loi. Elle souhaiterait que l'art. 1 définisse le rôle de la Confédération en tant qu'autorité de délivrance des moyens d'identification électronique ; en conséquence, le terme « délivrer » devrait être employé par la suite. En outre, l'interopérabilité doit être garantie au niveau national et international. Pour Swisscom, la mise en place d'un système e-ID subsidiaire de la Confédération prévue à

l'art. 13 devrait être une obligation dès l'entrée en vigueur de la loi, et pas seulement une possibilité. Si, dans un premier temps, les acteurs du marché ne favorisent pas la diffusion des e-ID, la Confédération devrait alors s'en charger et proposer un système e-ID applicable tout au moins à la cyberadministration. Ainsi, l'art. 1, al. 2, devrait également garantir la diffusion des e-ID dans la cyberadministration. Les CFF suggèrent entre autres que la loi établisse le rôle de la Confédération selon la formulation suivante : « les droits et les devoirs de la Confédération en tant qu'autorité de délivrance des moyens d'identification électronique et en tant que responsable du service d'identité et de l'organisme de reconnaissance ».

6.1.2 Art. 2 Définitions

FR estime impératif de définir la notion de titulaire d'un e-ID. ZH préconise d'ajouter une définition du service d'identité.

L'ASB recommande de remplacer en allemand le terme « Identitätsdienstleistung » par « Identifikationsdienstleistung » dans l'intégralité de la loi, d'adapter la définition des FI afin d'y inclure les services fédéraux et de reporter ce changement dans l'ensemble de la loi, ainsi que de définir les termes « intermédiaire d'e-ID » et « attribut d'identité ». SwissHoldings estime particulièrement important de n'employer aucun terme qui serait spécifique à la Suisse et d'utiliser la terminologie de l'eIDAS autant que possible.

L'ISSS propose d'ajouter d'autres termes à la liste des définitions et de remplacer « blocage » par « suspension » dans l'intégralité de la loi ainsi que « service utilisateur » par « partie utilisatrice » (termes de l'eIDAS). La KARTAC suggère de définir la notion d'« attribut ».

La FMH fait observer que le traitement sûr et efficace des patients n'implique pas les mêmes besoins que les transactions électroniques sûres. Elle estime problématique de restreindre l'obtention des e-ID en Suisse aux personnes physiques. Par exemple, un patient devrait pouvoir contrôler s'il est rattaché au bon dossier du patient. Pour la FMH, il est tout aussi important de garantir l'authentification des services en ligne que celle des professionnels de la santé qui doivent accéder au dossier électronique du patient. En outre, elle demande que soit précisée la nature juridique des moyens d'identification électroniques reconnus (document officiel, certificat ou autre) dans les définitions.

UBS propose d'ajouter les termes « attribut » et « intermédiaire » dans les définitions. La Poste et les CFF demandent d'ajouter une définition du « service d'identité » et suggèrent quelques compléments aux définitions.

D. Muster estime que les définitions sont incomplètes et se demande pourquoi l'obtention des e-ID est limitée aux personnes physiques. Il recommande de permettre l'établissement d'un e-ID pour les personnes morales et les services en ligne afin de garantir une identification sécurisée. B. Oldani serait favorable à la possibilité d'établir un e-ID pour des personnes morales et souhaiterait remplacer le terme « Person » par « Personeneinheit (juristische oder natürliche Person) ».

6.2 Section 2 Établissement d'un e-ID

6.2.1 Art. 3 Conditions personnelles

AG demande que l'on adapte la formulation de l'art. 3, al. 1, let. b, de façon à ce que les e-ID puissent être délivrés aux étrangers titulaires d'un titre de séjour biométrique valable au moment de l'établissement de l'e-ID. BE suggère une modification des conditions personnelles

afin qu'un e-ID puisse également être établi pour les personnes qui ne sont pas encore titulaires d'un document d'identité suisse mais qui remplissent toutes les conditions pour son obtention. BL estime que la formulation potestative constitue une violation du principe d'égalité juridique. Il recommande en outre d'ajouter une disposition relative à l'utilisation de l'e-ID par des personnes privées de l'exercice des droits civils. GE remarque qu'il conviendrait de prévoir des procédures d'identification propres aux cantons, notamment pour une reconnaissance forte du personnel administratif et policier. ZG souhaiterait que la loi prévoie une solution pour l'identification électronique des organes d'une personne morale. ZH préconise de limiter la liberté contractuelle des FI de manière raisonnable, afin que toute personne qui souhaite bénéficier de prestations de l'État auxquelles il est uniquement possible d'accéder avec un e-ID ne puisse en être exclue arbitrairement.

Selon l'UDC, ce n'est pas au Conseil fédéral mais au législateur de déterminer quels titres de séjour permettent d'obtenir un e-ID.

Economiesuisse et SwissHoldings font observer que tous les habitants de la Suisse devraient pouvoir obtenir et utiliser un e-ID, sans discrimination. Ainsi, ils s'opposent à ce que l'obtention des e-ID soit limitée à certains citoyens, à ce que les coûts soient élevés pour l'utilisateur ou à ce que l'utilisation de l'e-ID soit trop complexe.

L'ISSS suggère d'élargir le cercle des personnes habilitées à obtenir un e-ID pour inclure les personnes disposant d'un n° AVS, les étrangers sans titre de séjour, les entreprises disposant d'un n° IDE et les personnes morales ayant leur siège à l'étranger. La SPA demande l'introduction d'une obligation contractuelle conséquente pour les FI.

La FMH exige que l'identité électronique des patients puisse être rattachée au numéro d'identification des patients au sens de la LDEP et demande la création d'un e-ID pour les personnes qui n'ont ni la nationalité suisse ni un titre de séjour, de manière analogue à ce qui se fait dans le domaine de la santé, afin de répondre aux besoins des applications de la cybersanté. La CEC et l'Association suisse des officiers de l'état civil demandent une modification des conditions d'obtention afin de permettre aux étrangers de disposer d'un e-ID. La FSA propose d'employer le verbe « dürfen » au lieu de « können », étant donné que la loi ne prévoit pas d'obligation contractuelle pour le FI et que l'art. 3, al. 1, let. a et b, définit les groupes de personnes pour lesquelles le FI a le droit d'établir un e-ID. L'association e-Gov-Schweiz recommande de mettre en place un e-ID pour les personnes morales sur la même base légale.

UBS propose d'ajouter le déblocage à la norme de délégation de l'art. 3, al. 3. La Poste présente des arguments pour et contre l'introduction d'une obligation contractuelle. À cet égard, la Poste et les CFF proposent que les pouvoirs publics indemnisent les FI pour les coûts qu'une telle obligation engendrerait. Les CFF souhaiteraient que le cercle des personnes habilitées à obtenir un e-ID soit le plus large possible. Ils voudraient délivrer des e-ID aux propriétaires étrangers d'immeubles en Suisse qui utilisent une identité électronique pour remplir leur déclaration d'impôts, ou aux touristes qui aimeraient utiliser une identité électronique dans le domaine de la cybersanté ou à des fins touristiques.

Inclusion Handicap observe que le fait de ne pas disposer des moyens techniques nécessaires pour établir une communication avec une personne handicapée ou le fait de ne pas disposer d'un accès au bâtiment adapté pour procéder à l'entretien personnel avec une personne handicapée ne constituent pas des raisons valables de refuser l'établissement d'un e-ID et la conclusion du contrat qui y est liée à une personne handicapée. En outre, Inclusion Handicap exige que le fait de demander un e-ID doive être accessible à chacun pour tous les niveaux de garantie. D. Muster estimerait opportun d'obliger les FI à établir un e-ID dans certains cas. En conséquence, il propose de prévoir une obligation contractuelle avec des

exceptions définies par la loi ; il suggère également que l'on règle la reconnaissance des e-ID étrangers. B. Oldani suggère d'étendre l'établissement des e-ID aux personnes morales.

6.2.2 Art. 4 Reconnaissance des FI

BL constate que l'avant-projet ne mentionne pas le rapport de sécurité que le FI doit rédiger et demande à cet effet que l'on complète l'art. 4, al. 2. FR estime que le renouvellement de la reconnaissance après trois ans alourdit considérablement la démarche, tant pour l'administration fédérale que pour les FI ; à ses yeux, le processus de renouvellement doit être aussi simple et économique que possible. GE souhaiterait que soit fixée dans la loi ou par voie d'ordonnance la possibilité pour les cantons de devenir FI. SH se demande s'il ne faudrait pas ajouter un critère relatif aux personnes morales dominées par des investisseurs étrangers. TG recommande de préciser l'art. 4, al. 2, let. f, en ajoutant « uniquement en Suisse ».

Le PVL approuve le fait que les FI doivent conserver et traiter les données des systèmes e-ID en Suisse et conformément au droit suisse, mais doute que ce critère puisse être mis en pratique. Pour l'UDC, les FI doivent non seulement avoir leur siège social en Suisse, mais également être contrôlés en majorité par des ressortissants suisses.

La FER et SwissHoldings considèrent que la restriction aux FI dont le siège social est en Suisse constitue un obstacle pour la notification future des systèmes e-ID suisses à l'UE. L'ASB observe que si les services fédéraux peuvent être reconnus en tant que FI, ils ne sont pas soumis à la condition énoncée à l'art. 4, al. 2, let. b. L'association propose donc un nouvel al. 3.

L'ISSS propose des modifications, fait des remarques et demande des précisions sur l'application de cette disposition. En cas de cessation de l'activité d'un FI, la KARTAC et la SPA suggèrent que les e-ID établis par ce FI puissent continuer à être utilisés sans interruption pour les transactions ou les applications de la cyberadministration ou qu'un nouvel e-ID soit immédiatement établi. Ils proposent également de permettre la conservation des données hors de la Suisse si la sécurité et la protection des données sont garanties conformément au droit suisse. Ils demandent que les procédures de reconnaissance équivalentes qui ont déjà été effectuées en vertu d'une autre base légale puissent être considérées comme suffisantes.

La FMH estime que les serveurs sur lesquels les données sont enregistrées devraient également appartenir à des ressortissants européens et pas à des entreprises américaines. La FSA recommande de ne pas mentionner les « sûretés financières équivalentes » à l'al. 2, let. g, et à l'al. 4, let b. Une telle formulation n'aurait de sens que si les autorités pouvaient contrôler régulièrement la présence de ces moyens financiers et que ceux-ci soient soustraits à la mainmise de tiers.

Pour UBS, l'obligation de conserver les données en Suisse conformément au droit suisse est une condition obsolète. Elle demande que l'on octroie plus de flexibilité aux FI s'ils peuvent garantir que les conditions de sécurité correspondantes sont respectées. En outre, les services utilisateurs basés en dehors de la Suisse devraient être autorisés, ce qui rendra les échanges avec l'étranger inévitables dans une certaine mesure. C'est le seul moyen de garantir l'interopérabilité internationale des systèmes. La loi devrait donc uniquement établir que le niveau de sécurité et de protection des données prévu par le droit suisse doit être respecté. Les CFF et UBS proposent que les procédures de reconnaissance des fournisseurs d'autres prestations reconnues, comme par exemple les signatures électroniques et les plateformes de messagerie sécurisée, soient également valables pour d'autres domaines

si les procédures sont équivalentes dans une certaine mesure. La Poste affirme que les conditions de la reconnaissance des FI, des fournisseurs de services de certification reconnus (loi sur la signature électronique, SCSE, RS 943.03), des plateformes de messagerie sécurisée reconnues (ordonnance sur la reconnaissance des plateformes de messagerie, RS 272.11) et des communautés certifiées (LDEP) divergent. Or, les similitudes qui existent entre les prestations mentionnées justifieraient une harmonisation des conditions formelles et matérielles de la reconnaissance. La Poste et les CFF demandent des précisions en ce qui concerne les conséquences de l'obligation de renouveler la reconnaissance, en particulier en cas de non-reconduction de celle-ci.

Inclusion Handicap souhaiterait ajouter une condition : les FI reconnus doivent garantir que les personnes handicapées ne subiront pas d'inégalités lorsqu'elles demandent un e-ID. B. Oldani suggère de renoncer à exiger des FI qu'ils aient une assurance responsabilité civile suffisante. D. Muster propose que la liste établie à l'art. 4, al. 4, soit exhaustive et recommande de supprimer le terme « notamment ». B. Oldani suppose que l'avant-projet a été conçu par des juristes n'ayant aucune compréhension de l'informatique et propose de renoncer à la norme de délégation inscrite à l'al. 4 et ainsi à l'édiction de dispositions techniques. Pour lui, les problèmes éventuels doivent être résolus par des innovations techniques et non par des dispositions.

6.2.3 Art. 5 Niveau de garantie

FR et ZH approuvent la mise en place de trois niveaux de garantie différents. TG voudrait pouvoir établir un e-ID pour chaque niveau de garantie ; l'établissement d'un seul e-ID d'un niveau de garantie élevé, qui, selon l'art. 5, al. 3, AP, pourrait être utilisé pour des niveaux de garantie inférieurs, n'est pas souhaitable. NW émet des réserves sur les niveaux de garantie : les utilisateurs pourraient avoir des difficultés à déterminer le niveau de sécurité qui correspond aux niveaux de garantie faible, substantiel et élevé. GR remarque qu'il serait fort avantageux pour le vote électronique que les supports des systèmes e-ID reconnus remplissent les conditions nécessaires à la vérifiabilité et la dématérialisation du vote électronique. Il faudrait ainsi contrôler que le niveau de garantie élevé couvre également les exigences du vote électronique.

L'ASB et l'UBCS recommandent de fixer par voie d'ordonnance les dispositions d'exécution relatives aux exigences minimales pour chaque niveau de garantie (faible, substantiel et élevé) de manière rigoureuse, suivant des principes clairs, afin de tenir compte du dynamisme de ce domaine.

L'ISSS propose différentes formulations, fait des remarques et demande des précisions sur l'application de cette disposition. Elle signale en particulier que les exigences relatives à l'identification et à l'authentification du titulaire de l'e-ID devraient être identiques à celles prévues par la SCSE. La KARTAC et la SPA proposent que l'e-ID satisfasse aux exigences de la législation sur le blanchiment d'argent et des obligations en vigueur et qu'une identification déjà effectuée en vertu de la législation sur le blanchiment d'argent soit considérée comme équivalente. Elles recommandent d'autoriser l'attribution libre d'attributs supplémentaires à l'e-ID pour tous les niveaux de garantie ; l'art. 5 devrait être modifié en conséquence. Elles suggèrent également de compléter l'art. 5, al. 4 (« Le Conseil fédéral règle [...] en particulier les exigences minimales et indispensables [...] ») afin de garantir que la procédure d'établissement permette une identification et une authentification sûres, mais qu'elle soit également appropriée et conforme au principe de proportionnalité. Selon Digitalswitzerland, la large diffusion de cette solution en Suisse dépend principalement de la confiance de la population envers l'e-ID et de son utilisation simple, flexible et économique. En consé-

quence, l'attribution des données suivant les niveaux de garantie prend une importance cruciale.

La FMH remarque que la possibilité d'identifier le patient selon plusieurs niveaux de garantie répond au besoin de procéder à différents traitements médicaux dans le domaine de la santé ; l'utilisation de différents niveaux de garantie est également adaptée à l'authentification du patient dans le domaine de la cybersanté.

UBS propose de compléter l'art. 5, al. 4 (« Le Conseil fédéral règle [...] en particulier les exigences minimales adaptées [...] »), afin que l'identification et l'authentification s'effectuent de manière sûre mais également appropriée. La Poste estimerait judicieux de mentionner le règlement eIDAS à l'art. 5, al. 1. Elle considère que l'art. 5, al. 2, n'apporte rien de plus au projet et demande qu'il soit supprimé. Pour Swisscom, la loi devrait permettre aux FI de recourir à des procédures d'identification qui garantissent le même niveau de sécurité qu'un entretien personnel. De plus, il accorde une grande importance à ce qu'une personne qui a déjà été identifiée selon une procédure qui paraît équivalente ne doive pas répéter l'opération. Les CFF estiment que l'al. 2 ne présente pas grand intérêt et demandent sa suppression.

D. Muster estime que le soin apporté à l'identification et l'enregistrement correct des données personnelles pour un e-ID ne devraient pas dépendre des niveaux de garantie.

R. Hauser souligne l'importance des dispositions d'exécution ; il plaide en particulier pour que le niveau de garantie élevé puisse être mis en pratique selon une variante technique consistant en l'utilisation de clés privées (ou de leurs équivalents) à proximité physique de l'utilisateur. B. Oldani suggère de supprimer la totalité de l'article car il ne voit aucune raison valable de prévoir des niveaux de garantie différents. Selon lui, un document d'identité est soit valide, soit invalide ; il ne peut être partiellement valide.

6.2.4 Art. 6 Procédure d'établissement

FR souligne que l'utilisation de l'e-ID dans le cadre de l'activité étatique ne peut pas concerner plus de données personnelles que dans le monde réel et que ces données doivent jouir d'une sécurité adaptée. Il estime que l'absence de signature numérique qualifiée ou reconnue limite fortement l'expansion des prestations de cyberadministration. GE remarque que le processus d'établissement fédéral de l'e-ID, tel que proposé par l'avant-projet, omet une pratique reconnue à Genève dans le cadre de l'AeL, à savoir l'identification par courrier postal recommandé. SZ considère que dans le contexte technologique actuel, seul le contrôle des habitants est compétent pour réaliser un entretien personnel avec le requérant. ZG suggère de faire correspondre la liste des plateformes reconnues de messagerie sécurisée tenue par le DFJP avec la liste tenue par le service d'identité.

L'ACS requiert que l'entretien personnel soit mentionné dans la loi en tant que condition indispensable pour l'identification du requérant. L'association souhaiterait savoir si le futur titulaire d'un e-ID peut également limiter le nombre de données transmises par le service d'identité au FI ou le nombre de données obtenues par le FI lors de l'établissement de l'e-ID. Elle estime impératif que la loi garantisse la liberté de choix de chacun et que les conditions d'obtention d'un e-ID soient en accord avec l'intérêt de la population. Ainsi, aucun FI ne peut avoir une position de monopole et aucun accord ne peut avoir lieu entre les FI.

Economiesuisse fait observer que tous les habitants de la Suisse devraient pouvoir obtenir et utiliser un e-ID, sans discrimination. Ainsi, la fédération s'oppose à ce que l'obtention des e-ID soit limitée à certains citoyens, à ce que les coûts soient élevés pour l'utilisateur ou à ce que l'utilisation de l'e-ID soit trop complexe.

L'ISSS et la KARTAC proposent de mentionner dans la loi qu'une personne peut disposer de plusieurs e-ID (sous des pseudonymes différents) et que l'e-ID peut être rattaché aux téléphones portables habituellement utilisés en Suisse. La KARTAC et la SPA souhaiteraient que la procédure à suivre pour l'identification du requérant soit établie de façon explicite dans la loi. Elles aimeraient en particulier que l'entretien personnel y soit mentionné. L'ISSS et la KARTAC proposent que les FI reconnus puissent déléguer l'identification d'un requérant à un tiers (bureau d'enregistrement) ; les FI devraient alors répondre de l'exécution correcte de cette tâche par ce dernier. Digitalswitzerland affirme que la procédure d'identification auprès des FI devrait être établie dans la loi et souhaiterait que les FI puissent avoir recours à des procédés qui offrent un niveau de sécurité équivalent à l'entretien personnel, par exemple l'identification par vidéo. En outre, Digitalswitzerland estime important que le requérant ne doive pas procéder à une deuxième identification s'il a déjà fait l'objet d'une procédure considérée comme équivalente. L'ISSS propose de permettre aux personnes morales d'obtenir un e-ID et décrit une procédure correspondante. L'IG ICT ZH demande que la loi mentionne le but de la consignation de la transmission des données. La SPA plaide pour inscrire dans la loi qu'une personne peut obtenir plusieurs e-ID auprès d'un ou de plusieurs FI et que les moyens d'identification peuvent être gérés de manière centralisée.

Le VZGV demande que la loi indique le but de la consignation de la transmission des données. Pour la FMH, il est nécessaire de préciser le lien entre la LDEP et la vérification de l'identité du requérant lors du renouvellement des e-ID. L'IG eHealth serait favorable à ce que les bureaux des passeports et les offices de migration cantonaux encouragent l'établissement des e-ID. La FSA recommande de concevoir la procédure technique de manière à ce que le service d'identité ne doive pas requérir le consentement du requérant. Selon le VZGV, procéder à un entretien personnel devrait être obligatoire et systématique ; elle estime qu'avec les moyens actuels, les personnes disposant des connaissances techniques nécessaires peuvent relativement aisément falsifier une identification purement virtuelle. La loi devrait également impérativement permettre au titulaire de limiter le nombre de données attribuées à l'e-ID selon le niveau de garantie demandé.

UBS propose de mentionner dans la loi qu'une personne peut disposer de plusieurs e-ID. L'entreprise recommande de définir explicitement la procédure d'identification du requérant et en particulier de mentionner l'entretien personnel et l'identification par vidéo. D'après elle, il faudrait également établir dans la loi que les personnes qui ont déjà été identifiées selon une procédure suffisante pour l'obtention d'un e-ID ne doivent pas répéter le processus. La Poste et les CFF sont d'avis que la loi ne doit pas définir les étapes de la procédure d'établissement mais plutôt préciser quelles sont les conditions essentielles de cette procédure. La Poste souhaiterait qu'une autorité établisse des e-ID, en parallèle aux FI, et propose de modifier l'art. 6 à cet effet. Afin de faciliter l'accès aux e-ID, les CFF suggèrent de tirer parti des procédures officielles déjà appliquées par les autorités, l'identité du requérant étant en effet vérifiée lors de l'entretien visant à délivrer les documents d'identité traditionnels. Si le législateur décide de ne pas prendre cette proposition en compte, il devra prévoir un mécanisme de compensation financière entre les FI : ceux qui procèdent à une identification peu onéreuse devraient indemniser les FI qui ont assumé les coûts liés à l'identification.

La BFH propose d'établir l'e-ID selon la même procédure que celle prévue pour l'établissement et la remise des documents d'identité (carte d'identité et passeport). D. Muster suggère d'intégrer l'art. 6 (procédure d'établissement) à l'art. 3 (conditions personnelles). Pour B. Oldani, l'art. 6 devrait être modifié afin de permettre aux personnes morales de bénéficier d'un e-ID. F. Scotoni estime que la procédure prévue n'est adaptée pour aucune des parties concernées.

6.2.5 Art. 7 Données d'identification personnelle

AG et BE suggèrent de remplacer les termes « nom d'état civil » et « prénoms » par « nom selon le registre électronique de l'état civil (Infostar) » et « prénoms selon Infostar » dans l'art. 7, al. 1, let. b et c ; ils proposent également de modifier l'art. 7, al. 2, pour que le service d'identité ait l'*obligation* d'attribuer les données mentionnées suivant le niveau de garantie. BL estime que la possibilité d'attribuer d'autres données d'identification personnelle aux e-ID risque de favoriser leur fragmentation et de desservir l'interopérabilité des systèmes. BS préconise de réduire le nombre de données personnelles attribuées à un e-ID ou tout au moins de limiter l'utilisation et la communication de ces données. FR souligne l'importance de la protection des données. SO recommande d'inclure le domicile ou l'adresse de résidence dans la liste des éléments constitutifs de l'identité électronique et d'ajouter les registres des habitants cantonaux à la liste de l'art. 20, al. 2. GL suggère de clarifier quelles données personnelles sont attribuées à l'e-ID pour quel niveau de garantie. TG souhaiterait remplacer le lieu de naissance par le lieu d'origine et interdire explicitement l'attribution d'autres données à l'e-ID. SZ estime indispensable que la police puisse avoir accès à certains attributs de l'e-ID ; à ce titre, la police doit être incluse le plus rapidement possible dans les discussions à ce sujet.

Les Verts constatent que l'art. 7, al. 2 et 4, décrit un catalogue relativement important de données qui peuvent être utilisées (et de données sensibles, telles que les données biométriques) mais sans préciser toutefois à quelles fins et dans quel cadre ces données pourront être utilisées. C'est pourquoi ils soutiennent un système qui ne se base pas sur un « super-registre », mais sur un système d'accès différencié aux différents registres sous contrôle du citoyen.

Pour l'ACS, il est indispensable que le titulaire de l'e-ID ait la possibilité de limiter le nombre de données d'identification personnelle que les FI transmettent aux services utilisateurs. Elle estime donc extrêmement problématique que des données supplémentaires comme l'adresse, le numéro de téléphone ou le courriel puissent être attribuées à l'e-ID sans le consentement du titulaire ou sans qu'il en ait conscience, puis transmises à des tiers. Souvent, les personnes qui demandent au registre des habitants par exemple de bloquer la communication de leur adresse ou d'autres données à des particuliers craignent pour leur vie ou leur intégrité corporelle.

L'UBCS suggère d'ajouter la proposition suivante à l'art. 7, al. 4, AP : « [...], en particulier une adresse, un numéro de téléphone ou un numéro de client ». Pour le même alinéa, l'ASB propose d'obliger le FI à requérir le consentement du titulaire.

L'ISSS suggère de mentionner le lieu d'origine pour les ressortissants suisses et la nationalité pour les étrangers ; la KARTAC et la SPA souhaiteraient ajouter le lieu d'origine à la liste des données qui peuvent être attribuées à un e-ID. L'ISSS propose également de compléter la liste avec la mention d'« autres attributs biométriques » ou de « paramètres personnels additionnels » afin d'anticiper sur l'évolution de la numérisation. La KARTAC et la SPA proposent d'établir de manière contraignante dans la loi quelles données d'identification personnelle le service d'identité attribue à un e-ID pour chaque niveau de garantie. L'IG ICT ZH n'estime pas nécessaire de limiter le nombre de données d'identification personnelle. Pour SWITCH, les services utilisateurs devraient pouvoir utiliser gratuitement, et avec le moins de formalités possible, les attributs de base qui leur sont transmis avec le consentement du titulaire de l'e-ID.

La CEC et l'Association suisse des officiers de l'état civil préconisent de remplacer les termes « nom d'état civil » et « prénoms » par « nom selon le registre électronique de l'état civil (Infostar) » et « prénoms selon Infostar » dans l'art. 7, al. 1, let. b et c. Pour Privatim, le fait que la liste ne soit pas exhaustive et que les FI puissent attribuer d'autres données personnelles à l'e-ID n'est pas compatible avec le principe de proportionnalité du droit de la protection des données, puisque des données pourraient être collectées, gardées en réserve et associées entre elles. Le VZGV estime qu'il n'est pas pertinent d'établir une liste définitive des données d'identification personnelle puisque bien d'autres données d'identification pourront être ajoutées aux systèmes d'information de la Confédération à l'avenir ; délimiter ou lister de manière exhaustive les données qui peuvent être utilisées n'est pas nécessaire. Pour la FSA, ni l'état civil, ni la nationalité ou le statut de séjour ne garantissent un meilleur niveau de sécurité ; il faudrait donc renoncer à utiliser ces données. Elle souhaiterait en outre compléter l'al. 3 avec une norme de délégation de compétence au Conseil fédéral, dans la mesure où la disposition actuelle n'impose aucune restriction. L'ASSH approuve le fait que le titulaire de l'e-ID puisse limiter les données que le FI transmet aux services utilisateur lors de l'utilisation de l'e-ID. Elle propose que le titulaire puisse également avoir une influence sur les données additionnelles, notamment pour limiter leur nombre.

UBS plaide pour que la liste à l'art. 7, al. 2, puisse être étendue à d'autres données d'identification personnelle en ajoutant la locution « en particulier » ; l'entreprise souhaiterait désigner les « autres données » au sens de l'al. 4 par le terme « attribut » et donner la possibilité aux FI d'attribuer ces données aux différents niveaux de garantie. La Poste et les CFF suggèrent d'inclure le lieu d'origine dans la liste.

Si la BFH s'oppose à l'établissement des e-ID par le secteur privé puisqu'elle considère que cette tâche relève de l'État, elle approuve nettement l'exploitation des fonctionnalités et des données de l'e-ID par le secteur privé. Afin que celui-ci puisse inclure des attributs supplémentaires dans les e-ID et ainsi améliorer et étendre leur utilisation, la loi doit autoriser les FI à attribuer d'autres données à l'e-ID. D'après B. Lehmann, les éléments biométriques, comme la photographie, que les FI attribuent aux e-ID de niveaux de garantie substantiel ou élevé permettent certainement de mieux protéger les titulaires contre la substitution, la falsification ou la copie de leur e-ID. Toutefois, la saisie de ces données biométriques constitue une violation du principe de protection de la sphère privée et porte atteinte au droit du titulaire de l'e-ID de disposer librement des informations qui le concerne. B. Oldani suggère de ne mettre à disposition que des e-ID d'un niveau de garantie élevé et recommande d'ajouter le « nom du registre du commerce », la « date de la fondation », le « numéro d'entreprise » et le « lieu de la fondation » comme attributs des personnes morales.

6.2.6 Art. 8 Mise à jour des données d'identification personnelle

BE suggère de modifier l'art. 8, al. 1, afin que le service d'identité informe immédiatement et le FI gratuitement (ou contre un faible émolument forfaitaire) de toute modification des données d'identification personnelle. BS demande de réglementer l'expiration, le renouvellement ou l'invalidité ainsi que le blocage et la révocation d'un e-ID. GL et ZH considèrent que la mise à jour trimestrielle d'un e-ID de niveau de garantie substantiel n'est pas suffisante ; ZH souhaiterait accorder au Conseil fédéral la compétence d'augmenter la fréquence des mises à jour. ZG exige de garantir dans la loi que les FI soient informés des décès le plus rapidement possible afin qu'ils puissent immédiatement bloquer les e-ID d'un niveau de garantie élevé concernés.

Pour l'ACS, cet article doit également garantir qu'un FI reconnu peut uniquement obtenir et actualiser les données nécessaires pour le niveau de garantie de l'e-ID concerné et pour lesquelles le titulaire a donné son consentement.

D'après l'UBCS, si le service d'identité bloque un numéro d'enregistrement de l'e-ID, il doit immédiatement en informer le FI concerné ; la loi doit explicitement établir la responsabilité du service d'identité à cet égard. L'ASB préconise de préciser que le blocage de l'e-ID ne constitue qu'une désactivation des données, lesquelles doivent à ce titre être conservées pendant dix ans. L'association recommande d'opter pour une procédure analogue à celle appliquée avec succès aux cartes bancaires.

L'ISSS propose des formulations relatives à l'établissement de l'e-ID pour des personnes morales.

La FMH relève que l'avant-projet n'évoque pas les « qualifications professionnelles » mentionnées à l'art. 7 SCSE pour les certificats réglementés. Pourtant, les documents d'identité électroniques selon la loi e-ID ne pourront être utilisés pour les applications de la cybersanté que si les procédures d'établissement et de révocation incluent l'organisme qui confirme les qualifications professionnelles. Privatim souhaiterait que la loi réglemente l'expiration, le renouvellement, l'invalidité, le blocage et la révocation des e-ID.

UBS souhaiterait établir dans la loi que les FI peuvent bloquer un e-ID sans que leur responsabilité ne soit engagée s'ils soupçonnent que les conditions de son utilisation ne sont plus remplies. La Poste, les CFF et SwissSign SA estiment que l'actualisation régulière de données qui varient rarement n'est pas nécessaire et plaident pour une mise à jour qui dépende de l'utilisation concrète de l'e-ID. Swisscom souhaiterait que la loi précise les obligations des FI quant au blocage et à la révocation des e-ID. Les CFF s'opposent à la mise à jour périodique des données d'identification personnelle prévue par l'avant-projet ; en effet, l'art. 8 implique que les FI peuvent utiliser des données datant d'un an selon les cas. La loi devrait plutôt prévoir que les FI ne contrôlent la validité des données auprès du service d'identité qu'au moment de l'utilisation de l'e-ID.

Selon B. Oldani, exiger des FI qu'ils endossent la responsabilité du blocage et de la révocation des e-ID n'est pas raisonnable. Il propose de centraliser les données de façon analogue au registre central des habitants.

6.2.7 Art. 9 Utilisation systématique du numéro AVS pour l'échange de données

BS demande que l'on examine la question de l'utilisation du n° AVS, qu'il serait éventuellement possible de remplacer par un identifiant spécifique au domaine. BS et SH recommandent de renoncer à créer un identifiant univoque supplémentaire tel que le numéro d'enregistrement de l'e-ID et d'utiliser le n° AVS. LU serait favorable à un numéro personnel unique, accessible à tous les services pour l'accomplissement de leurs tâches légales et permettant de traiter efficacement les données et les échanges de données. NE déplore que l'utilisation et la gestion du n° AVS ne soient pas clairement définies. UR demande que l'on libéralise autant que possible l'emploi du n° AVS des particuliers. VD soutient la proposition visant à utiliser le NAVS 13 comme identificateur de personnes, même si cette solution suscite les réticences des préposés à la protection des données personnelles. ZG – qui en use déjà ainsi dans le cadre de son logiciel d'identification cantonal – approuve l'idée que le nouveau numéro d'assurance sociale, qui ne permet pas de déduire des informations sur son titulaire, soit utilisé pour les demandes, puis comme attribut par le service d'identité. ZH approuve la possibilité d'utiliser le n° AVS.

Pfäffikon ZH y est aussi expressément favorable et le juge indispensable au bon fonctionnement du système.

L'IG ICT ZH approuve l'extension du cercle des personnes habilitées à utiliser le n° AVS. La SDA relève que les numéros de structuration générés par le système ne doivent pas être communiqués : l'avant-projet va pour elle dans la mauvaise direction avec son « numéro d'enregistrement de l'e-ID ». Selon elle, s'il faut vraiment un nouveau registre, il devrait fonctionner sur la base d'un numéro attribué pour chaque nouvelle inscription faite avec un n° AVS. Pour la CSI, il est essentiel que le service d'identité puisse utiliser le n° AVS systématiquement dans le but prévu par l'avant-projet.

La FSA juge le n° AVS nécessaire à une attribution univoque de l'e-ID. Le VZGV approuve l'extension du cercle des personnes habilitées à utiliser le n° AVS. eGov-Schweiz propose de compléter l'e-ID par un identifiant cyberadministratif univoque pour toutes les personnes physiques et morales, l'emploi du n° AVS étant aussi possible. Selon cette association, il faut renoncer autant que possible à créer de nouveaux registres.

La Poste et les CFF suggèrent de veiller à éviter des incompatibilités qui empêcheraient d'utiliser l'e-ID pour les dossiers des patients.

Privatim, au contraire, s'oppose à l'idée de faire *de facto* du n° AVS, par quelques dispositions de loi, un numéro d'identité administratif d'usage général. Selon cet organisme, l'utilisation d'un identifiant unique pour tous les domaines accroît les risques de violation des droits de la personnalité, et il faut s'abstenir de laisser à de nombreuses autorités et à des particuliers l'usage du n° AVS dans le domaine de l'e-ID. B. Lehmann élève aussi de sérieuses objections relevant de la protection des données contre l'utilisation sans changements du n° AVS comme élément de l'identification des personnes ; il demande la création d'un numéro personnel permettant de désigner sans équivoque le titulaire de l'e-ID mais non de tirer des conclusions sur son identité.

6.2.8 Art. 10 Traitement et transmission des données

BL relève que la nécessité d'autoriser la communication des données ne doit pas empêcher les services de confiance de se rendre compte que les personnes sous curatelle ont l'exercice restreint des droits civils, parce qu'elles n'ont pas consenti à ce que cette information soit transmise. FR exige une interdiction stricte de l'utilisation des données à d'autres fins. JU et VS ne souhaitent pas non plus de communication des données du niveau de garantie faible sans consentement exprès du titulaire de l'e-ID. JU suggère de régler spécifiquement la transmission des données de mineurs.

Le PVL approuve le fait que le titulaire décide des données d'identification personnelle que le FI peut transmettre aux exploitants de services utilisateurs et que le FI doive obtenir son consentement exprès la première fois qu'il doit transmettre ses données d'identification. Il suggère que l'on précise que seules les données confirmées par les pouvoirs publics sont couvertes par l'interdiction de l'al. 3 mais non les données déjà en possession du FI qui n'ont pas de lien avec le système e-ID, et auxquelles ne doivent s'appliquer que les dispositions habituelles de la protection des données.

L'ACS estime que diverses questions méritent clarification, notamment concernant l'étendue de l'interdiction ou de l'autorisation de vendre les données d'identification visées à l'art. 7, al. 1 et 4. Selon elle, les titulaires doivent savoir dans tous les cas quelles données sont transmises à des tiers et lesquelles non. Elle propose de compléter l'art. 10, al. 3, dans les

termes suivants: « *Für die Bekanntgabe der Daten nach Art. 7 Abs. 1 und 4 an Dritte ist das Einverständnis des E-ID-Inhabers einzuholen.* »

La FER, favorable à l'exigence du consentement du titulaire, approuve la limitation du traitement des données par l'État et le FI. L'UBCS propose que l'on accorde le niveau de sécurité des services utilisateurs et les données personnelles transmises : les données d'un certain niveau de garantie ne pourraient être transmises à des services utilisateurs (par exemple des boutiques en ligne) que si ces dernières prouvent qu'elles présentent un niveau de sécurité suffisant. L'ASB et le VSBK suggèrent d'étendre le champ d'application de l'art. 10, al. 3, à tous les alinéas de l'art. 7 définissant les données d'identification au nom de la protection des données. L'UBCS trouve la limitation actuelle du traitement de données trop stricte et propose de baisser les exigences en vue de développements futurs possibles. L'ASB voit dans la règle proposée concernant la transmission de données une contradiction avec les exigences les plus élémentaires d'une protection des données raisonnable.

KARTAC et la SPA estiment que l'interdiction de transmettre les données, dans sa forme absolue de l'art. 10, al. 3, est excessive, incompatible avec la législation sur le blanchiment d'argent et impraticable. Elles suggèrent de la remplacer, ainsi que les profils d'utilisateur établis par le FI ou l'exploitant de service utilisateur, par un système qui n'aille pas à l'encontre des mécanismes juridiques (éprouvés) de la lutte contre le blanchiment d'argent et qui permette aux titulaires de l'e-ID d'avoir leur mot à dire quant à l'utilisation de leurs données. L'ASUT part du principe que les dispositions de la loi sur la protection des données (en cours de révision) seront pleinement applicables. La SPA considère que l'interdiction prévue n'est pas réaliste dans un groupe de sociétés et ne correspond pas à la réalité moderne. Pour la SFTI, la limitation du traitement de données à l'identification et à l'authentification pour le FI est trop restrictive, vu les défis et les besoins du quotidien ; elle réclame une formulation plus ouverte.

La FSA est d'avis que le commerce de données devrait être réduit au strict nécessaire et que la loi devrait déterminer quelles données peuvent être vendues, afin que tous soient traités de la même manière. Le VZGV demande que l'al. 3 soit complété par l'exigence d'une déclaration de consentement concernant la transmission à des tiers des données visées à l'art. 7, al. 1 et 4.

Swisscom et UBS proposent de clarifier dans le texte que la transmission de données est possible avec le consentement du titulaire. Swisscom est en outre d'avis qu'il faut renoncer à des dispositions de protection des données dans la loi e-ID là où celles de la loi sur la protection des données s'appliquent déjà. Pour La Poste et les CFF, il n'est pas clair si un FI peut transmettre les données d'identification de l'art. 7, al. 2, à des exploitants de services utilisateurs (al. 2) ou non (al. 3). Il faut mieux accorder entre eux et préciser les al. 1, 2 et 3. De plus, La Poste et les CFF recommandent de tenir compte du résultat de la révision de la LPD dans la version finale de l'art. 10.

Pour la BFH, les dispositions existantes de protection des données de l'UE et de la Suisse (lorsqu'elles sont plus strictes) suffisent pour régler efficacement l'attribution par l'État d'un e-ID national.

6.2.9 Art. 11 Expiration de la reconnaissance

Art. 12 Mesures de surveillance et retrait de la reconnaissance

AG demande que l'on règle la manière de procéder lors de la cessation planifiée des activités et l'expiration, le renouvellement ou l'invalidité, etc. d'un e-ID. BL voudrait que les systèmes e-ID qui ne sont pas repris sans interruption par un autre FI soient exploités subsidiai-

rement par la Confédération. BS demande que l'on complète le projet par une règle claire disant ce qu'il advient des données en cas de cessation des activités des services certifiés. BL suggère que l'on règle précisément à l'art. 12 le rapport de sécurité à livrer. FR relève que les droits des personnes concernées, les titulaires d'un e-ID, ne sont pas mentionnés. La personne concernée devrait pouvoir accéder à ses données et retirer à tout moment son consentement. Ainsi, elle doit être informée en cas de faillite ou de cessation d'activité du fournisseur ou de la reprise du système par un autre fournisseur.

La FER se demande si la continuité de la responsabilité des FI est suffisamment assurée par la formulation de l'avant-projet et propose d'instituer une responsabilité solidaire du FI qui cesse son activité et du FI qui reprend l'e-ID. Elle approuve le fait qu'aucune responsabilité causale ne soit prévue et propose de citer d'autres motifs d'expiration que la faillite. L'UBCS demande que l'on précise à quel moment la cessation des activités doit être annoncée. La FER et l'ASB demandent un durcissement de l'art. 12, al. 3, let. d.

Privatim demande que l'on complète le projet par une règle claire disant ce qu'il advient des données en cas de cessation des activités d'un FI. Selon la FSA, il faut déterminer quel service peut décider du sort des données en cas de faillite ou, en d'autres termes, à qui elles échoient si elles ne peuvent pas être vendues lors de la liquidation ; de plus, elle considère que limiter les infractions à la seule cybercriminalité n'est pas nécessaire et de surcroît trop étroit.

La Poste et les CFF souhaitent une norme légale obligeant les FI à reprendre en bloc les titulaires d'e-ID d'un FI qui disparaît (contre une indemnisation par la Confédération).

B. Lehmann appelle à réfléchir sur la possibilité que la Confédération reprenne le système e-ID et les obligations légales qui lui sont liées, par analogie avec l'art. 13 de l'avant-projet, étant donné l'importance de l'identité électronique pour l'économie numérique et la société.

6.2.10 Art. 13 Système e-ID subsidiaire de la Confédération

AG approuve la désignation par le Conseil fédéral d'une unité administrative, laquelle pourra fournir autant que possible des prestations sans incidences financières, adaptées aux besoins des services publics. TG trouve bon que la Confédération puisse gérer un système e-ID adapté aux besoins des autorités. ZG propose de prévoir, à la place d'un système e-ID subsidiaire, l'octroi centralisé des e-ID d'un niveau de garantie substantiel ou élevé par la Confédération (sur le modèle des passeports et des cartes d'identité).

Le PVL veut que la Confédération soit tenue de par la loi d'offrir des e-ID des niveaux de sécurité substantiel et élevé lorsqu'aucun FI ne le fait sur le marché privé suisse.

La FER souhaite un répertoire des coûts qu'aurait un système e-ID subsidiaire de la Confédération au cas où aucun FI privé ne voudrait en gérer un faute de rentabilité. L'ASB et le VSBK proposent que ce système subsidiaire soit forcément mis en place dans le cas prévu par l'avant-projet afin d'assurer la continuité et qu'il soit en principe accessible à tous les acteurs du marché (et non pas aux seules autorités).

La FSA souhaite que la Confédération ait la compétence générale d'agir de son propre chef.

Selon Swisscom, le système e-ID subsidiaire de la Confédération ne doit pas être une possibilité, mais une obligation applicable à l'entrée en vigueur de la loi. Si le marché n'encourage pas dès le début l'utilisation des e-ID reconnues par l'État, la Confédération doit le faire et offrir un système au moins pour le domaine de la cyberadministration. Le développement de

l'e-ID dans ce domaine doit par conséquent être mentionné parmi les buts de la loi, à l'art. 1, al. 2.

Inclusion Handicap demande que la violation de l'art. 8, al. 2, Cst. ou de la Convention de l'ONU relative aux droits des personnes handicapées (RS 0.109) soit ajoutée aux motifs de retrait de la reconnaissance.

6.3 Section 3 Titulaires d'un e-ID (art. 14)

LU désire que l'on prévoie une norme pénale pour les cas dans lesquels le titulaire légal d'un e-ID transmettrait illicitement celui-ci à un tiers. ZG voudrait que la loi précise si une personne peut posséder plusieurs e-ID, tout en préconisant, pour des raisons de facilité, qu'elle ne puisse en posséder qu'un.

L'ISSS fait des propositions de formulation et des remarques et suggère des précisions quant à l'octroi d'un e-ID à des personnes morales. L'IG ICT ZH relève que les mesures nécessaires doivent dépendre du niveau de garantie.

Le VZGV fait la même remarque et propose une précision.

Swisscom et UBS souhaitent fixer à l'art. 14 le moment où le titulaire de l'e-ID doit signaler au FI que l'e-ID doit être bloqué ou révoqué, notamment en cas de soupçon d'abus.

F. Scotoni juge que la norme de délégation est en contradiction directe avec l'art. 164, al. 1, let. c, Cst. et demande une description plus précise des devoirs de diligence des titulaires.

6.4 Section 4 Exploitants d'un service utilisateur

6.4.1 Art. 15 Accord avec un FI

BL propose de prévoir une solution étatique efficace pour les services de l'État et les entreprises décentralisées du secteur public, ou du moins de créer la possibilité de régler dans un accord unique la collaboration de plusieurs collectivités publiques avec un FI. Il souhaite garantir les cantons contre un foisonnement d'émoluments, notamment parce qu'ils doivent accepter tous les e-ID. SZ recommande de créer une norme (eCH) assurant à l'échelle de la Suisse que des services en ligne identiques ou similaires requièrent le même niveau de garantie.

Le PVL propose que le texte statue plus clairement que l'exploitant d'un service utilisateur n'est pas tenu de conclure un accord avec tous les FI.

L'ASB propose d'instaurer une obligation de signaler les soupçons d'abus.

UBS souhaite qu'un intermédiaire soit institué et que la loi soit adaptée en conséquence. La Coop se félicite de la simplicité du texte et suggère que l'ordonnance soit aussi épurée, car la simplicité et la souplesse contribuent de manière décisive à ce que les consommateurs et les exploitants utilisent un système e-ID.

D. Muster pose des questions sur le contrôle du respect des accords et sur les devoirs de diligence et les compétences des auteurs de ces contrôles. B. Oldani demande la suppression de cet article qui lui semble inapplicable en pratique.

6.4.2 Art. 16 Autorités en tant qu'exploitants d'un service utilisateur

BE souhaite que l'obligation d'accepter tous les e-ID s'étende aux entreprises qui s'adressent à une grande partie de la population au titre d'un mandat ou d'une réglementation de droit fédéral. VS relève qu'une période de transition sera à prévoir pour que toutes les administrations concernées puissent adapter leur environnement d'identification à la loi proposée. UR préconise que le niveau de garantie des prestations des autorités soit fixé dans les lois sectorielles, que la photo et la signature ne soient requises que pour le niveau de garantie élevé et que les données biométriques ne soient pas collectées. ZH craint que l'obligation d'accepter tous les e-ID reconnus reviennent à une distorsion de la concurrence, car un e-ID coûteux et moins économique trouverait également un marché, son utilisation étant financée non par le titulaire mais compensée par des fonds étatiques. TG voudrait que l'on puisse disposer d'accords modèles.

Pour economiesuisse et SwissHoldings, l'e-ID devrait être accepté dans les échanges avec les autorités à l'égal des moyens d'identification et d'authentification matériels tels que la carte d'identité ou le passeport, mais sans obligation pour le titulaire.

La Poste et les CFF exigent une norme générale prévoyant que l'e-ID est reconnu dans tout le domaine législatif et pour tous les échanges avec les autorités et font une proposition de formulation. UBS propose que l'article soit formulé de manière plus globale et comprenne un mandat aux communes et aux cantons. Swisscom souhaite que l'e-ID reconnu par l'État soit le seul moyen accepté d'identification et d'authentification électronique auprès des services publics (que ce soit à l'interne pour les employés de l'administration fédérale ou bien pour les personnes physiques).

6.5 Section 5

6.5.1 Art. 17 Devoirs

Pour BL, il est de l'intérêt de la protection des enfants et adolescents et des personnes dont l'exercice des droits civils est restreint de toujours transmettre l'âge des mineurs et lesdites restrictions. BL se demande qui est chargé de la vérification visée à l'al. 1, let. c. TG souhaite que l'on utilise le terme de « personne concernée » et que l'on intègre dans la loi des règles sur le déblocage de l'e-ID. ZH suggère que le titulaire de l'e-ID ait la possibilité d'exiger une prolongation de la durée de conservation des données relatives à l'utilisation de l'e-ID et par ailleurs de consulter ses données puis, le cas échéant, de les effacer (par ex. après le délai de six mois). ZH veut que l'on oblige les FI à transmettre la liste de blocage au service d'identité visé à l'art. 19 et que l'on examine si les autorités de poursuite pénale devraient aussi avoir accès à cette liste.

Le fait d'obliger les fournisseurs d'identité à démontrer en tout temps la validité de tous les e-ID qu'ils ont établis et permettre la vérification de ceux-ci de manière gratuite n'apparaît à la FER pas réaliste pour les entreprises concernées. La FER souhaite donc la suppression de la référence à la gratuité aux termes de cette disposition. L'UBCS souhaite une clarification de l'al. 1, let. g, et une plus grande conformité avec d'autres obligations légales de conservation.

La FMH constate que la question de la publication de la révocation ou du blocage ou de son accessibilité aux utilisateurs de l'e-ID, par ex. au service gérant le dossier du patient, n'est pas réglée.

La Poste et les CFF proposent de supprimer le terme « périodique » (let. e) ou de le remplacer par « régulière ». UBS veut que seul le service d'identité puisse vérifier en tout temps la

validité de l'e-ID, car cette obligation ne peut pas être imposée sans limite aux FI, notamment vis-à-vis des services utilisateurs. UBS et Swisscom proposent de biffer la let. g, car d'une part les principes du droit de la protection des données s'appliquent et d'autre part, il pourrait y avoir des prescriptions requérant une plus longue durée de conservation. UBS souhaite que l'on exige le consentement exprès du titulaire de l'e-ID chaque fois que sont transmis des attributs autres que les données d'identification personnelle. Elle trouve important que les notifications de problèmes techniques ou de perte puissent être transmises et traitées, à charge du FI d'en organiser les modalités.

Inclusion Handicap demande que les moyens techniques nécessaires pour obtenir le consentement du titulaire soient utilisables facilement et rapidement par les personnes handicapées, de sorte que ces dernières puissent utiliser les services client de la même manière que les personnes sans handicap. L'organisme souhaite disposer de plusieurs moyens de communication sans barrière.

6.5.2 Art. 18 Interopérabilité

L'UBCS trouve important que le nouveau service d'identité qui doit fixer les normes pour l'interopérabilité des systèmes e-ID s'attelle à cette tâche en priorité, et que le Conseil fédéral examine et assure en second lieu l'interopérabilité avec l'étranger.

KARTAC et la SPA suggèrent d'inscrire dans la loi que l'on se fondera sur les normes internationales dans les ordonnances (techniques). Pour Digitalswitzerland, l'interopérabilité est un élément central pour le succès de l'e-ID. Cette association approuve l'idée d'une plateforme servant d'intermédiaire ; le Conseil fédéral devrait encourager cette solution et clarifier la question. SWITCH voudrait que la question du roaming entre les prestataires, qui n'est pas testée par le marché, soit clarifiée, de sorte que les critères en soient fixés avant l'accréditation et bien avant la mise sur le marché.

Privatim juge disproportionnée la communication de données, même avec le consentement des personnes concernées.

La Poste, les CFF et SwissSign SA estiment nécessaire de régler la compensation financière entre les participants, dans le sens d'un émolument de roaming, pour éviter la discrimination de FI qui ont un grand volume d'e-ID. En outre, La Poste et les CFF jugeraient bon que l'on tienne aussi compte de l'interopérabilité internationale et que l'on prescrive par exemple la mise en place et l'exploitation de serveurs STORK par la Confédération. Swisscom et UBS proposent que l'on prévoie un intermédiaire dans la loi.

La BFH propose que l'on confie à la Fédération suisse d'identités (FSI) un rôle actif dans le domaine des e-ID en Suisse et dans les relations avec l'étranger.

6.6 Section 6 Service d'identité électronique suisse

6.6.1 Art. 19 Organisation

BL, craignant une perte de know-how et de synergies si la mise en œuvre de la loi est partagée entre deux départements, propose qu'elle soit rassemblée entre les mains d'un seul. LU estime nécessaire que les autorités de poursuite pénale puissent s'informer des e-ID délivrés et signaler les abus auprès d'un service unique. UR approuve l'implantation du service d'identité au DFJP.

La Poste et les CFF demandent l'instauration de règles de coordination entre le service d'identité et l'organisme de reconnaissance, distribués entre le DFJP et le DFF (art. 19 et 21).

6.6.2 Art. 20 Tâches et devoirs

SO demande que l'on examine la possibilité de faire du domicile et de la résidence des éléments de l'identification électronique, en complétant le cas échéant la liste de l'art. 20, al. 2, par les plateformes cantonales des registres des habitants.

Le SFTI souhaite un nouvel alinéa consacrant l'univocité du numéro d'enregistrement de l'e-ID.

6.7 Section 7 Organisme de reconnaissance des FI

6.7.1 Art. 21 Compétence

L'ISSS propose de fondre l'organisme de reconnaissance des FI et l'organisme d'accréditation des organismes de reconnaissance institué par la SCSE.

La Poste et les CFF demandent que l'on fasse de l'al. 1 une norme de délégation habilitant le Conseil fédéral à déterminer les compétences de l'organisme de reconnaissance, dans le but d'harmoniser les compétences et devoirs de surveillance des différents fournisseurs de certifications.

D. Muster souhaite l'institution d'une autorité de surveillance et une harmonisation avec la SCSE concernant l'organisme de reconnaissance.

6.7.2 Art. 22 Liste des FI

Aucune remarque.

6.8 Section 8 Émoluments (art. 23)

En ce qui concerne l'accessibilité et les coûts, le canton de FR est d'avis que le recours large à l'identification électronique nécessite que le coût soit aussi bas que possible pour les utilisateurs et que le principe d'utilisation soit aussi simple que possible. Au sujet du financement, il souligne la nécessité d'introduire un plafond de coûts annuel, afin de garantir une maîtrise des budgets. ZG voit une contradiction – à éliminer – entre l'art. 20, al. 4, et l'art. 23, al. 1, pour ce qui est des émoluments dus pour les prestations des FI.

Il ne faut pas, selon le PVL, que le succès des e-ID sur le marché soit entravé par des émoluments trop élevés pour les FI.

DigitalSwitzerland approuve la première transmission gratuite des données d'identification personnelle lors de l'établissement de l'e-ID. La SPA suggère, lorsque l'on fixe les émoluments, de mettre en balance l'intérêt qu'a la Confédération à financer ses unités administratives et l'intérêt économique prépondérant que présente la diffusion de l'e-ID auprès de la population.

L'UBCS est favorable à l'option, envisagée dans le rapport explicatif (p. 33), de ne pas couvrir entièrement les coûts administratifs. IG eHealth propose de mettre à jour les données

d'identification personnelle selon les besoins, le modèle de perception des émoluments prévus étant contreproductif à cet égard.

La Poste, CFF et SwissSign SA estiment que la mise en place et l'exploitation du service d'identité de l'État doivent être financées par la Confédération, sans que celle-ci perçoive d'émoluments pour les prestations du service d'identité, et les FI pouvant obtenir les données gratuitement. Faute de quoi, il faudrait selon eux au minimum une égalité de traitement entre les FI du secteur privé et ceux des pouvoirs publics.

NüGlarus estime que les fournisseurs de service ne devraient en principe pas avoir à payer pour utiliser l'e-ID d'un FI, de sorte que l'utilisation des nouvelles technologies ne soit pas ralentie. B. Oldani est aussi opposé à la perception d'émoluments par le service d'identité et l'organisme de reconnaissance. Selon lui, les émoluments doivent couvrir les coûts, et une baisse des coûts due aux progrès technologiques entraînerait une baisse des émoluments. Il voit aussi des économies de plusieurs millions pour les autorités (Confédération cantons, communes) en papier à lettres, enveloppes et frais de port grâce aux e-ID qui leur permettront de recourir davantage au courrier électronique, économies qui permettront de financer les dépenses dues à l'e-ID.

6.9 Section 9 Responsabilité (art. 24)

BE, SO et GL indiquent que les services utilisateurs d'e-ID ou les FI peuvent aussi être des services étatiques, soumis à un autre droit de la responsabilité que la loi sur la responsabilité (RS 170.32). ZG souhaite qu'au moins les e-ID d'un niveau de garantie élevé soient conçus de telle manière qu'on puisse les utiliser pour conclure des actes juridiques.

La FMH suggère de prévoir, comme dans la SCSE, une règle qui interdit aux FI d'exclure leur responsabilité pour les dommages causés par eux-mêmes ou leurs auxiliaires.

Selon La Poste, il faut veiller à ce que les règles de responsabilité ne constituent pas un désavantage concurrentiel pour les entreprises suisses.

Inclusion Handicap insiste sur l'importance d'une utilisation sans barrière de l'e-ID, étant donné que les utilisateurs de celui-ci doivent répondre des dommages causés par une erreur d'utilisation. Comme c'est généralement le cas dans le cyberspace, la preuve libératoire ne sera pas facile à fournir. D. Muster demande que l'on règle plus clairement la responsabilité de chaque partie, comme dans le règlement européen. F. Scotoni trouve la règle de responsabilité proposée plus désavantageuse qu'une responsabilité de l'État dans une solution étatique. B. Oldani exige la suppression de cet article qu'il trouve inapplicable en pratique, aucun fabricant de logiciel au monde ne répondant de son logiciel.

6.10 Section 10 Dispositions finales

Digitalswitzerland demande au Conseil fédéral de forcer l'avancement de la date de l'entrée en vigueur de la loi et donc le lancement d'une solution informatique pour un e-ID généralement reconnu.

6.11 Modification d'autres actes

BL propose une modification de l'art. 41, al. 6, de la loi sur les étrangers (RS 142.20) : « *Das SEM legt die Form und den Inhalt der Ausweise fest. Für Ausweise, welche nicht zum Bezug einer anerkannten elektronischen Identifizierungseinheit (E-ID) nach dem Bundesgesetz*

über anerkannte elektronische Identifizierungseinheiten berechtigen, legt das SEM Inhalt, Ausstellung, Verwendung, Sperrung und Widerruf zur elektronischen Identifizierung fest. Es kann die Ausfertigung der Ausweise und die Ausstellung der elektronischen Identifizierung teilweise oder ganz Dritten übertragen. » TG s'oppose à la suppression, dans la SCSE, de l'obligation de se présenter en personne.

L'UBCS souhaite que les exigences auxquelles les services utilisateurs doivent répondre en termes de niveau de garantie soient fixées dans la loi aux endroits appropriés et notamment que la SCSE précise que seuls sont dispensés de se présenter en personne les titulaires d'un e-ID de niveau élevé ou substantiel.

L'ASUT fait la même demande, par analogie à l'art. 24, ch. 1, let. b, du règlement eIDAS, tout en approuvant la modification de la SCSE ; elle propose que, dans tous les cas où la législation prévoit que l'identité d'une personne physique est contrôlée sur la base d'un document d'identité ou autre contrôle qualifié (par ex. identification d'un client par la banque), l'entité qui fait le contrôle soit aussi tenue d'accepter une identification numérique par l'e-ID, partout où c'est possible. L'ISSS voudrait que le niveau de garantie de l'e-ID soit inscrit dans la SCSE et que l'on modifie la loi sur les documents d'identité concernant la remise de titres à des étrangers et la gestion du n° AVS.

Selon le SFTI, il faudrait que l'art. 9, al. 1^{bis}, SCSE ne s'applique qu'aux e-ID du niveau de garantie substantiel ou élevé et, d'autre part, qu'il soit coordonné avec l'art. 7 de l'ordonnance sur la signature électronique (RS 943.032).

La FMH juge la modification de la SCSE incompatible avec le système de niveaux de garantie de l'art. 5, al. 1, de la nouvelle loi. La FCS désire que l'on modifie la loi fédérale sur le crédit à la consommation, notamment les art. 9, 11 et 12, pour remplacer la forme écrite par une forme plus souple qui permettrait de conclure des contrats en ligne.

La Poste et les CFF souhaitent que l'on mentionne les e-ID, comme référence de l'identité électronique, ainsi que les niveaux de garantie au minimum dans la LDEP, la SCSE, l'ordonnance de la CHF sur le vote électronique (RS 161.116), divers actes de régulation des marchés financiers, les ordonnances sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (OCEI-PCPP ; RS 272.1) et dans le cadre de procédures administratives (OCEI-PA ; RS 172.021.2), etc. Les CFF suggèrent de préciser le niveau de garantie des e-ID à utiliser dans la SCSE. La Poste demande que l'on y écarte les e-ID de niveau de garantie faible (nom d'utilisateur/mot de passe) pour l'établissement des certificats qualifiés. Swisscom approuve la modification de la SCSE en demandant que – comme à l'art. 24, ch. 1, let. b, du règlement eIDAS – on exige le niveau de garantie substantiel ou élevé. La Coop préconise une révision du code des obligations assimilant les transmissions électroniques qui permettent d'enregistrer durablement une convention à la forme écrite, afin de soutenir le commerce électronique.

6.12 Rapport explicatif

AG, BE, BL, GL, SH, SZ, ZH souhaiteraient un exposé plus détaillé des conséquences financières du projet pour les cantons et les communes.

Selon l'UVS, il subsiste une incertitude concernant les coûts du projet, notamment pour ce qui est des dépenses que le système complexe de certification entraînerait pour l'exploitant d'un service utilisateur.

La CSI souligne que la date prévue pour la mise en œuvre des e-ID, fin 2019 ou courant 2020, est très tardive en considération du besoin urgent en solutions informatiques d'IAM. Elle juge important pour les projets de cyberadministration en cours que l'on vise une mise en œuvre commune. Il faut étroitement coordonner, selon elle, les projets de la Confédération tels que le TID et la législation sur l'e-ID. Ces interdépendances devraient être expliquées dans le message.

7 Consultation

Selon l'art. 9 de la loi du 18 mars 2005 sur la consultation (RS 172.061), sont accessibles au public les documents soumis à consultation, les avis exprimés, après expiration du délai de consultation, et le rapport rendant compte des résultats, une fois que le Conseil fédéral en a pris connaissance. Les avis exprimés sont intégralement publiés sur le site de l'Office fédéral de la justice (page d'accueil de l'OFJ > État et Citoyen > Projets législatifs en cours > Loi e-ID).

Verzeichnis der Eingaben
Liste des organismes ayant répondu
Elenco dei partecipanti

Kantone / Cantons / Cantoni

AG	Aargau / Argovie / Argovia
AI	Appenzell Innerrhoden / Appenzell Rh.-Int. / Appenzello Interno
AR	Appenzell Ausserrhoden / Appenzell Rh.-Ext. / Appenzello Esterno
BE	Bern / Berne / Berna
BL	Basel-Landschaft / Bâle-Campagne / Basilea-Campagna
BS	Basel-Stadt / Bâle-Ville / Basilea-Città
FR	Freiburg / Fribourg / Friburgo
GE	Genf / Genève / Ginevra
GL	Glarus / Glaris / Glarona
GR	Graubünden / Grisons / Grigioni
JU	Jura / Giura
LU	Luzern / Lucerne / Lucerna
NE	Neuenburg / Neuchâtel
NW	Nidwalden / Nidwald / Nidvaldo
OW	Obwalden / Obwald / Obvaldo
SG	St. Gallen / Saint-Gall / San Gallo
SH	Schaffhausen / Schaffhouse / Sciaffusa
SO	Solothurn / Soleure / Soletta
SZ	Schwyz / Svitto
TG	Thurgau / Thurgovie / Turgovia
TI	Tessin / Ticino
UR	Uri
VD	Waadt / Vaud
VS	Wallis / Valais / Vallese
ZG	Zug / Zoug / Zugo
ZH	Zürich / Zurich / Zurigo

Parteien / Partis politiques / Partiti politici

PBD	Bürgerlich-Demokratische Partei BDP Parti bourgeois-démocratique PBD Partito borghese democratico PBD
PDC	Christlichdemokratische Volkspartei CVP Parti démocrate-chrétien PDC Partito Popolare Democratico PPD
PLR	FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLR. I Liberali Radicali PLD. Ils Liberals
PES	Grüne Partei der Schweiz GPS Parti écologiste suisse PES Partito ecologista svizzero PES
PVL	Grünliberale Partei glp Parti vert'libéral pvl
Parti pirate	Piratenpartei Parti pirate Partito Pirata
PS	Sozialdemokratische Partei der Schweiz SP Parti socialiste suisse PS Partito Socialista Svizzero PS
UDC	Schweizerische Volkspartei SVP Union démocratique du centre UDC Unione Democratica di Centro UDC

Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete sowie Gebietskörperschaften / Associations faîtières des communes, des villes et des régions de montagne qui œuvrent au niveau national et collectivités locales / Associazioni mantello nazionali dei Comuni delle città e delle regioni di montagna e autorità territoriali

ACS	Schweizerischer Gemeindeverband Association des communes suisses Associazione dei Comuni Svizzeri Associaziun da las Vischnancas Svizras
UVS	Schweizerischer Städteverband Union des villes suisses Unione delle città svizzere
Pfäffikon ZH	Gemeinde Pfäffikon ZH

Gesamtschweizerische Dachverbände der Wirtschaft / Associations faîtières de l'économie qui œuvrent au niveau national / Associazioni mantello nazionali dell'economia

CP	Centre patronal
Economiesuisse	Verband der Schweizer Unternehmen Fédération des entreprises suisses Federazione delle imprese svizzere Swiss business federation
FER	Fédération des entreprises romandes
ASB	Schweizerische Bankiervereinigung (SBV) Association suisse des banquiers (ASB) Associazione svizzera dei banchieri (ASB) Swiss Bankers Association
USAM	Schweizerischer Gewerbeverband (SGV) Union suisse des arts et métiers (USAM) Unione svizzera delle arti e mestieri (USAM)
SwissHoldings	Verband der Industrie- und Dienstleistungskonzerne in der Schweiz Fédération des groupes industriels et de services en Suisse Federation of Industrial and Service Groups in Switzerland
UBCS	Verband Schweizerischer Kantonalbanken Union des banques cantonales suisses Unione delle Banche Cantionali Svizzere

Vereinigungen im IKT-Bereich / Associations du domaine informatique et télécommunications

ASUT	Verband der Telekommunikationsbranche in der Schweiz Association du secteur des télécommunications en Suisse
Digitalswitzerland	Schweizer Verein für die Digitale Innovation Association suisse pour l'innovation digitale Associazione svizzera per lo sviluppo digitale
IG ICT ZH	Interessengemeinschaft der Zürcher Gemeinden für Information and Communications Technology
ISSS	Information Security Society Switzerland Fachverband in der Schweiz für ICT-Sicherheit
KARTAC	Interessengemeinschaft der Zahlkartenindustrie
SDA	Swiss Data Alliance
SFTI	Swiss Fintech Innovations Verband schweizerischer Finanzinstitute zur Förderung von digitalen Innovationen
CSI	Schweizerische Informatikkonferenz Conférence suisse sur l'informatique Conferenza svizzera sull'informatica Conferenza svizra d'informatica

SPA	Swiss Payment Association Branchenorganisation der Schweizer Herausgeber (Issuer) von Kreditkarten der internationalen Kartenorganisationen
Swico	Wirtschaftsverband für die digitale Schweiz Association suisse de l'information de la télématique et de l'organisation SWICO
swissICT	Schweizerischer Verband der Informations- und Kommunikationstechnologie
SWITCH	Stiftung neutrale Technologie- und Dienstleistungsplattform der Schweizer Hochschulen

Andere Vereinigungen / Autres associations

JDS	Demokratische Juristinnen und Juristen der Schweiz DJS Juristes démocrates de Suisse JDS Giuristi e Giuriste Democratici Svizzeri GDS Giuristas e Giurists Democratics Svizzers GDS
eGov-Schweiz	Verein zur Förderung der Innovation im eGovernment Association favorisant la promotion de l'innovation dans la cyberadministration (eGovernment)
FMH	Verbindung der Schweizer Ärztinnen und Ärzte FMH Fédération des médecins suisses FMH Federazione dei medici svizzeri FMH
IG eHealth	Interessengemeinschaft eHealth
Inclusion Handicap	Dachverband der Behindertenorganisationen Association faîtière des organisations suisses de personnes handicapées
CEC	Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst Conférence des autorités cantonales de surveillance de l'état civil Conferenza delle autorità di vigilanza sullo stato civile
FCS	Verband Konsumfinanzierung Schweiz (KFS) L'association Financement à la consommation Suisse (FCS)
ParlDigi	Parlamentarische Gruppe Digitale Nachhaltigkeit Intergroupe parlementaire Informatique durable
Privatim	Die schweizerischen Datenschutzbeauftragten Les préposé(e)s suisses à la protection des données Gli incaricati svizzeri della protezione die dati
FSA	Schweizerischer Anwaltsverband SAV Fédération suisse des avocats Federazione Svizzera degli Avvocati Swiss Bar Association
Association suisse des officiers de l'état civil	Schweizerischer Verband für Zivilstandswesen Association suisse des officiers de l'état civil Associazione svizzera degli ufficiali dello stato civile

SKS	Stiftung für Konsumentenschutz
ASSH	Verband Schweizerischer Einwohnerdienste (VSED) Association suisse des services des habitants (ASSH) Associazione svizzera dei servizi agli abitanti (ASSA) Associaziun svizra dals servetschs ais abitants (ASSA)
VZGV	Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute

Unternehmen / Entreprises /

Coop	Groupe Coop
La Poste	Die Post La Poste La posta Swiss Post
CFF	Schweizerische Bundesbahnen SBB Chemins de fer fédéraux suisses CFF Ferrovie federali svizzere FFS
Swisscom	Swisscom (Schweiz) AG Swisscom (Suisse) SA
SwissSign SA	Gemeinschaftsunternehmen der Post und der SBB Co-entreprise de la Poste et des CFF
UBS	UBS Schweiz UBS Suisse

Weitere Interessierte und Privatpersonen / Autres milieux intéressés et particuliers / e privati

BFH	Berner Fachhochschule Haute école spécialisée bernoise
Société numérique	Digitale Gesellschaft Société numérique Società Digitale Societad Digitala Digital Society
droitsfondementaux.ch	grundrechte.ch droitsfondementaux.ch dirittifondamentali.ch
NüGlarus	Standortinitiative Kanton Glarus
Open Geneva Hackathon	Bruno Chanel Jörn Erbguth Jean-Henry Morin Vincent Pignon Alexis Roussel Guillaume Saouli

Particuliers

Ralf Hauser
Stefan Häusler
Beat Lehmann
Daniel Muster
Beat Oldani
Fabio E. R. Scotoni

Ont renoncé à prendre position :

- Santésuisse
Branchenorganisation der Schweizer Krankenversicherer
Organisation de la branche de l'assurance-maladie sociale
- Schweizerischer Arbeitgeberverband
Union patronale suisse
Unione svizzera degli imprenditori