Stellungnahme
zur Vorlage
E-ID-Gesetz (BGEID)

Version 1.4
2. Nov. 2018

Daniel Muster
it-rm IT-Riskmanagement GmbH
daniel.muster@it-rm.ch
www.it-rm.ch
8003 Zürich
044 433 03 78

Inhaltsverzeichnis

I Einleitung

I.1 Vorbemerkung

1.1. Der Autor dieses Dokuments hat sich an der Vernehmlassung dieser Gesetzesvorlage beteiligt und dabei bereits dort eine Reihe der hier aufgeführten Einwände eingebracht. An der Vernehmlassung haben sich viele beteiligt, Beanstandungen vorgebracht und mögliche Verbesserungen vorgeschlagen. Doch die Vorlage ans Parlament unterscheidet sich von der Version bei der Vernehmlassung nur marginal.

1.2. Fürs Verständnis der kommenden Abhandlungen könnte es hilfreich, vorgängig oder bei Unklarheiten das Dokument „Irrtum – Identifizieren versus Authentisieren“ bei folgender Webseite herunterzuladen und zu konsultieren:

http://www.it-rm.ch/files/Ident-Auth_daniel_s_Muster_09_09_2018_V_1_1.pdf

1.3. Dieses Dokument wird hier mit IDENT-AUTH referenziert.

I.2 Grundsätzliche, aber offen gebliebene Fragen

1.4. Beim Durchlesen der Gesetzesvorlage haben sich u.a. folgende Fragen gestellt:

- Was ist eine E-ID konkret? Stellt dies eine digitale Urkunde dar? Was eine E-ID ist, wird weder in der Gesetzesvorlage noch in der Botschaft dazu definiert.
- Wie fälschungssicher und wie leicht ist sie auf Dritte (missbräuchlich) übertragbar; dies abhängig von den verschiedenen Sicherheitsniveaus? Dies ist in Zusammenhang mit dem Diebstahl der Mittel für die Authentisierung von erheblicher Bedeutung. Mittel für die Authentisierung sind z.B. Chip Card zum Leisten einer elektronischen Signatur oder Login Name und Passwort.
- Wie steht die Gesetzesvorlage in Relation zu bestehenden Bundesbestimmungen wie zum Bundesgesetz über die elektronische Signatur (ZertES) oder zum elektronischen Patientendossier (EPDG)? Ist z.B. eine nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten auch (automatisch) ein Identity Provider (zu IdP, Art. 1 Abs. 1 Bst. c)?
- Weshalb wurden die Bestimmungen zum Thema E-ID anders als bei der EU-Verordnung (eIDAS-Verordnung) nicht mit den Bestimmungen zu den elektronischen Zertifikaten und Signaturen zusammengezogen und in einem Erlass festgehalten?
- Wie gestaltet sich die Anerkennung ausländischer E-ID-Aussteller?
- Welche Archivierungszeit bei welchen Geschäftsprozessen gilt es zu beachten?

- Wie nachvollzieh- und belegbar haben die einzelnen Prozesse zu sein? Ohne nachvollzieh- und belegbare Prozesse lässt sich z.B. eine Sorgfaltspflichtverletzung oder die Erfüllung der Sorgfaltspflicht nicht beweisen. Ohne dies wird die Durchsetzung oder die Abwehr einer Haftungsklage schwierig, insbesondere weil mehrere am Authentisierungsprozess beteiligt sind.
- Weswegen wurden andere Begriffe in dieser Gesetzesvorlage verwendet als bei der erwähnten Bestimmung der EU (eIDAS)?

I.3 Zur Botschaft der Vorlage

I.3.1 EU-Kompatibilität

1.5. In der Botschaft zur Gesetzesvorlage, S. 9 2. Abs. oben, wird von EU-Kompatibilitäten mit der eIDAS-Verordnung geschrieben. Doch die Vorlage weicht augenscheinlich u.a. in folgenden wesentlichen Punkten ab:

- Andere Begriffe werden eingeführt.
- Es kann in der Vorlage keine E-ID für juristische Personen oder für eine Behörde ausgestellt werden. Es ist nicht nur wichtig, wem man die Anmeldung am System einer Person zuordnen kann, sondern auch, wo man sich anmeldet. Z.B. beim Herunterladen oder beim Hinaufladen sensitiver und zwingend verlässlicher Informationen wie Wetterberichte für Rettungskräfte, Straf- und Betreibungsregisterauszüge, Gesundheitsdaten, Eingabe von Rechtsschriften an ein Gericht. *Im Übrigen dürfen seit 1.12017 geregelte Zertifikate für juristische Personen ausgestellt werden.*
- Die elektronischen Zertifikate werden bei eIDAS einbezogen und einer Sicherheitsstufe zugeordnet.
- Haftungsbestimmungen.

1.6. In der Botschaft S. 13 1. Absatz, wird im Zusammenhang mit E-ID das „Vote électronique“ als Beispiel herbeigezogen. Beim elektronischen Abstimmen sollte jedoch zur Wahrung des Stimmgeheimnisses eine Zuordnung des abgegebenen elektronischen Abstimmungs- oder Wahlzettels zum Wähler oder Abstimmenden möglichst unterbunden werden. Also sollte dabei die Anonymität besonders geschützt werden. Mit der Anonymität werden jedoch zur Authentisierung entgegengesetzte Ziele zur E-ID verfolgt, siehe auch IDENT-AUTH, S. 6 folgende.

I.3.2 Begriffliches

1.7. Bei dieser Vorlage wie bereits auch beim ZertES (Art. 2 Bst. b Ziff. 2) wird der Begriff Identifizieren/Identifizierung (Art. 2 Abs. d) verwendet, welcher mit dem nicht überein-

stimmt, was die Allgemeinheit darunter versteht. Eine Signatur zusammen mit dem dazugehörigen Zertifikat vermag nicht, eine Person zu identifizieren; jedenfalls nicht, was sich die Allgemeinheit darunter vorstellt. Denn die Mittel zum Leisten einer elektronischen Signatur sind im Gegensatz zur eigenen Identität ohne nennenswerten Aufwand auf weitere Personen übertragbar.

1.8. Unter Identifizieren soll hier das verstanden werden, was die Polizei oder die Strafverfolgungsbehörde versteht, nämlich feststellen, wer jemand ist und wem man die Ereignisse (z.B. eine Straftat) zuordnen kann. Unter Authentisieren soll jedoch als das Zuordnen der Verantwortlichkeit definiert werden. Ausführlicher, warum es dieser Unterscheidung bedarf, siehe IDENT-AUTH, Kapitel II.

1.9. Folglich sollten die Begriffe „Authentisieren“ (in der EU Verordnung wohl als das elektronische Identifizieren bezeichnet) und „Identifizieren“ wegen ihrer rechtlichen Implikationen und Konsequenzen strikt auseinandergehalten werden; wie bei Eigentum und Besitz, oder Fahrer und Halter eines Fahrzeugs. Z.B. beim Strassenverkehr wird zwischen Fahrer und Fahrzeughalter unterschieden. Falls kein Unterschied, z.B. in Bezug auf die zivil- oder strafrechtliche Haftung gemacht werden sollte, so sollte das Parlament im vollen Bewusstsein der Sachlage darüber entscheiden, wie z.B. bei Art. 6 Abs. 1 OBG.

1.10. Ansonsten werden bei der Allgemeinheit mit den in der Gesetzesvorlage verwendeten Begriffen Assoziationen geweckt, welche mit dem Sachverhalt nicht kongruent sind. Arg wäre dies, wenn sich ein solches Missverständnis in einem strittigen Verfahren bei Gericht ereignen würde.

I.3.3 Biometrische Informationen

1.11. In der Botschaft, S.14:

> Der Einsatz der E-ID mit dem Sicherheitsniveau «hoch» verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss. Zusätzlich muss das Authentifizierungsmittel einen direkten Nachweis der Authentifizierung der Inhaberin oder des Inhabers liefern können, der vom E-ID verwendenden Dienst überprüft werden kann. Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung, integriert in einem abgesicherten Bereich mit persönlichem Zertifikat.

Biometrische Mittel sind dann geeignet, wenn das Erfassen der Prüfdaten (z.B. Einlesen eines Fingerabdrucks), das Vergleichen (mit den Fingerabdruckdaten in der Datenbank) und das Gewähren des Zutritts vollständig von „einer Hand“ vorgenommen werden. Z.B. beim Einlesen des Fingerabdrucks im Smartphone zwecks Gewährens des Zugangs zu den darauf abgespeicherten Daten ist dies erfüllt, oder bei Zutrittssystemen in einem Hochsicherheitstrakt wie einem Gefängnis. Beim Anmelden übers Internet erfolgt dies normalerweise nicht aus einer Hand, was zu erheblichen Sicherheitslücken führen kann. Z.B. weil die eingelesenen Fingerabdruckdaten kopiert, zu einem anderen Zeitpunkt, d.h. bei einem anderen Authentisierungsvorgang, eingespielt und an Dritte weitergeleitet werden können. Z.B. von demjenigen, welcher die Authentisierung prüft oder die biometrischen Daten einliest.

1.12. Folglich sollten die beim IdP vorhandenen biometrischen Informationen nicht an einen E-ID-Dienst weitergeleitet werden dürfen, sonders besonders geschützt werden. Dies ist im Widerspruch zu Art. 5 Abs. 3 in Kombination mit Art 16 Abs. 1. Wenn jemand eine E-ID mit den entsprechenden Zugangsdaten stiehlt, dann erhält er bei einem Authentisierungsverfahren mit Sicherheitsniveau „hoch“ unter Umständen noch das Passfoto!

1.13. Das Transferieren von biometrischen Daten erhöht das Risiko für den Identitätsdiebstahl. Zum Identitätsdiebstahl, siehe dazu auch die allgemein verständliche Fernsehreportage der ARD mit dem Titel „Pässe für Kriminelle“: https://www.ardmediathek.de/tv/Reportage-Dokumentation/P%C3%A4sse-f%C3%BCr-Kriminelle/Das-Erste/Video?bcastId=799280&documentId=54850588

1.14. Eine entsprechende Bestimmung, keine biometrischen Daten für das Authentisieren zu verwenden und digital zu versenden, ist im Gesetz aufzunehmen. Fazit:

Biometrische Angaben für das Authentisieren tragen nicht zur Sicherheit bei, sondern fördern den Identitätsdiebstahl!

1.15. Der Bundesrat kann dies in der Verordnung nach Verabschiedung der Gesetzesvorlage noch festlegen, für welche Sicherheitsniveaus es welcher Sicherheitsdienste bedarf. Der Umfang seiner Kompetenzen aus diesem Gesetz ist folglich erheblich.

II Zu den einzelnen Artikeln in der Vorlage

II.1 Art. 1

II.1.1 Abs. 1

2.1 Hier fehlt, dass damit auch die Pflichten der Anerkennungs- und Aufsichtsstelle geregelt werden. Ohne dass die (Sorgfalts)pflichten zuvor festgelegt worden sind, kann keine Haftung begründet werden, siehe dazu auch Art. 28 Abs. 2. Rechte und Pflichten von Personen (Art. 164 Abs. 1 Bst. c BV) wie auch die Aufgaben des Bundes (164 Abs. 1 Bst. e BV) müssen in einem Gesetz definiert sein.

2.2 Im Gesetz wird nicht beschrieben, welche Pflichten und vor allem welche Kompetenzen die Aufsichtsbehörde besitzt. Z.B. Art. 19 enthält keine Aufsichtspflichten.

II.1.2 Abs. 2 Bst. a

2.3 Das Gesetz soll den sicheren Geschäftsverkehr fördern. Dies steht aber im Widerspruch zur Einführung von 3 Sicherheitsniveaus (Art. 4). Wenn das niedrigste Sicherheitsniveau bereits sicher ist, wozu werden dann noch die 2 höheren Niveaus benötigt?

II.1.3 Abs. 2 Bst. b

2.4 Grundsätzlich sollte jedes Gesetz die Persönlichkeit achten. Dies impliziert in der Schweiz auch, dass die Grundrechte (in ihrem Kerngehalt) nicht verletzt werden dürfen. Aus dem Wortlaut ist auch zu entnehmen, dass die Vorlage die Persönlichkeit beinahe aller Personen in der Schweiz schützt, weil über fast alle Personen Daten bearbeitet werden und nicht nur diejenigen, für welche eine E-ID ausgestellt wird.

II.2 Art.2

2.5 Hier sollten in Analogie zur eIDAS mehr Begriffe aufgeführt und definiert werden. In der Botschaft wird eine Reihe von Begriffen definiert.

II.3 Art. 3

II.3.1 Abs. 1 Bst. a und b

2.6 Frage: Warum können einzig natürliche Personen eine E-ID beziehen? Die entsprechende EU-Verordnung enthält auch Bestimmungen für Web Server. Z.B. stellen elektronische Zeitstempel elektronische, von einem Server ausgestellte Beglaubigungen dar. Zudem gibt es Anwendungen wie beim elektronischen Patientendossier, wo man Ge-

wissheit darüber haben will, bei welchem Betreiber eines Dienstes (z.B. eines Patientendossiers) man sich angemeldet hat, bevor man Daten hinauflädt oder Manipulationen vornimmt. Die Betreiber von E-ID-Diensten sollten sich beim Inhaber oder beim IdP auch elektronisch „ausweisen“ können/müssen.

2.7 Weitere Beispiele sind:

- Abfrage des Betreibungsregisterauszug eines Unternehmens
- Abfrage des Strafregisterauszugs
- Online Banking
- Eingabe von Rechtsschriften

2.8 Einige Geschäftsprozesse laufen automatisch ab, wie z.B. die Transaktionen unter Banken. Wenn nur an natürliche Personen eine E-ID ausgestellt wird, so fördert dies nicht den Geschäftsverkehr unter Privaten und den Behörden, was im Widerspruch zu Art. 1 Abs. 2 steht.

2.9 Seit 1.1.2017 ist es übrigens gestattet, elektronische Zertifikate auch für juristische Personen auszustellen (Art. 9 ZertES, Art. 6 VZertES). Warum hier davon abgewichen wird, lässt sich nicht aus der Botschaft entnehmen.

2.10 Folgende Frage stellt sich weiter:

- Muss eine natürliche Person handlungsfähig sein, bevor sie eine E-ID beziehen kann. Kann auch ein Minderjähriger oder ein beschränkt Urteilsfähiger eine E-ID beziehen?

2.11 In der Botschaft zum Gesetzesentwurf zu Art. 3 auf S. 34 wird der Kontrahierungszwang (hier die Verpflichtung, eine e-ID auf Antrag auszustellen) des IdP abgelehnt. Aus dem Wortlaut des Gesetzesentwurfs ist dies nicht zu entnehmen. Hierzu jedoch einige Beispiele für die Notwendigkeit eines Kontrahierungszwangs.

- Ein IdP A stellt seine Geschäftstätigkeit ein. Dessen Kunden haben Daten in einem Patientendossier. Haben die Kunden noch Zugang zum Patientendossier nach Einstellung der Geschäftstätigkeit des IdP A? Wenn nein, was geschieht, wenn IdP B sich nun weigert, E-ID-Einheiten an die ehemaligen Kunden von IdP A auszustellen, damit diese weiterhin auf ihre Patientendaten zugreifen können? Medizinische Fachkräfte stünden im Umgang mit dem Patientendossier vor ähnlichen Problemen.
- Wenn die E-ID in naher Zukunft die Bedeutung erlangt, welche aus der Botschaft zu entnehmen ist, ist nicht ersichtlich, warum einer Person die E-ID

grundlos verweigert werden kann. Dies käme unter Umständen einer Einschränkung der wirtschaftlichen Möglichkeiten gleich.

- Sollte die E-ID in irgendeiner Weise zwingend im Rahmen einer Registrierung beim e-Voting eingesetzt werden, dann käme die Weigerung, eine E-ID auszustellen, einer Einschränkung der Möglichkeiten gleich, sich politisch zu äussern.
- Subsidiär, d.h. wenn kein Privater eine IdP betreiben will, soll der Bund die Ausstellung vornehmen (Art. 10 Abs. 1). Eine amtliche Stelle hingegen darf keine Ungleichheit schaffen, indem sie jemandem eine E-ID verweigert, ohne dass sich dies auf Basis einer Vorschrift begründen lässt.

2.12 Vorschlag: Es sollten Voraussetzungen im Gesetz aufgeführt werden, unter welchen ein IdP sich weigern darf, eine E-ID auszustellen. Oder Voraussetzungen genannt werden, unter welchen der IdP E-IDs auszustellen hat. In Analogie dazu: Heute jemandem zu verweigern, eine E-Mail Adresse bei einem Telecom Dienstleister zu beziehen, würde ihn von der Geschäftswelt abschneiden und von seinem sozialen Umfeld isolieren.

2.13 Weiter sollte die Anerkennung ausländischer E-IDs geregelt werden, u.a. zwecks Interoperabilität, was einer der Zieles dieser Gesetzesvorlage ist (Art. 1 Abs. 2 Bst. c). Deswegen wird vorgeschlagen, dass ein zusätzlicher Absatz oder Artikel eingebaut wird, welcher die Anerkennung ausländischer E-IDs regelt. Dies ähnlich wie bei Art. 3 Abs. 2 ZertES.

II.4 Art. 4

2.14 Betreffend den verschiedenen Sicherheitsniveaus stellen sich folgende Fragen:

- Sind die Handhabung der E-ID und deren Rechtsfolgen für einen technisch nicht versierten Anwender einfacher verständlich, wenn anstatt 3 nur 1 Sicherheitsniveau verwendet wird?
- U.a. nebst der Rechtssicherheit, der liberalen Grundhaltung schafft Qualität, d.h. hier u.a. eine hohe Sicherheit, einen wirtschaftlichen Standortvorteil der Schweiz. Sollte deshalb nicht nur ein hohes Sicherheitsniveau verwendet werden, dies in Analogie *zur Österreichischen Bürgerkarte*? Wurde bei der Einführung der verschiedenen Sicherheitsniveaus berücksichtigt, dass ein hohes Mass an Verlässlichkeit als einen wirtschaftlichen Standortvorteil betrachtet werden kann? Z.B. die Einführung der Verbindlichkeit des Grundbucheintrags zu Beginn des letzten Jahrhunderts.
- Sollte das eGovernment Umfeld infolge der damit verbundenen Staatshaftung (z.B. das Verantwortlichkeitsgesetz des Bundes, VG) nicht ein hohes Sicher-

heitsniveau fordern und fördern? Die Verlässlichkeit oder das Vertrauen in die behördlichen Angaben stellt m.E. ebenfalls einen Standortvorteil dar.

- Der in Art. 9 BV garantierten Vertrauensschutz ist unabhängig von den Sicherheitsniveaus hoch, substanziell oder niedrig. Warum soll deshalb nicht einheitlich ein hohes Sicherheitsniveau (bei eGovernment Anwendungen) eingeführt und umgesetzt werden? Art. 9 BV stellt eine Garantie elementarer Gerechtigkeit dar, was ein Grundrecht darstellt (siehe J.-P.MÜLLER, S. 467 ff, RHINOW/SCHEFER, 1989 ff.). Daraus stellt sich die Frage, ob dies nicht im Widerspruch zu Art. 2 Abs. 2 Bst. b steht.
- Fragen oder Einwände zu der in der Gesetzesvorlage definierten Haftung, siehe Fragen und Anmerkungen in Kapitel II.13.
- Wurde eine Risikoanalyse im Vorfeld zum Gesetzesentwurf für die jeweiligen Sicherheitsniveaus und involvierten Parteien durchgeführt? Falls ja, wurde dabei berücksichtigt, dass das Stehlen von Identitätsangaben bereits heute beträchtlich ist und wohl In Zukunft noch zunehmen wird, insbesondere je einfacher und verbreiteter die E-ID sein wird? Siehe auch Swisscom Security Report 2017, zur Einführung einer Risikoanalyse bei der Rechtssetzung, siehe MUSTER, zum Identitätsdiebstahl ID-DIEBSTAHL.

II.5 Art. 5

2.15 In Absatz 3 soll eine e-ID ein Gesichtsbild enthalten. Es sollte hinzugefügt werden, dass diese Information für das Authentisieren nicht weitergereicht werden darf, siehe auch die Ausführungen zu den biometrischen Informationen in Kapitel I.3.3. Das Gesetz beabsichtigt, den Datenschutz zu achten. In diesem Sinne sollten nur so viele Informationen zu einer Person weitergereicht werden, wie notwendig und sicherheitserforderlich und -dienlich.

II.6 Art. 6

2.16 In der Botschaft zu Art. 6 Abs. 4 S. 38 unten: Auch auf die Gefahr hin, sich hier zu wiederholen: Die Zuordnung der EI-D zur SIM-Karte ermöglicht letztlich nicht eine (zweifelsfreie) Zuordnung zur natürlichen Person, d.h. nicht die Identifizierung einer natürlichen Person. Der Eigentümer des Handys, der Besitzer des Handys und derjenige, welcher mit dem Handy telefoniert, haben nicht identisch zu sein. Z.B. ein Kind telefoniert mit Handy des Vaters, welches der Arbeitgeber dem Vater des Kindes zur Verfügung gestellt hat. Dies gilt es auch im Hinblick auf (straf)rechtlich relevante Vorfälle zu beachten.

II.7 Art. 8

2.17 Zum Verwenden der Sozialversichertennummer oder AHV-Nr.

> Anmerkung: Das Wort Identifikator im Kontext zur AHV-Nr. assoziiert, dass eine Person damit identifiziert werden kann. Eine AHV-Nr identifiziert eine natürliche Person jedoch nicht. Ansonsten könnte man einzig durch Vorzeigen der AHV-Nr die Landesgrenze passieren.
> Die AHV-Nr. ist lediglich ein Schlüsselattribut oder eine Registernummer in einer Datenbank für Personendaten. Ein Schlüsselattribut ist in einer Datenbank mit Personendaten ein Attribut, welche nur Angaben zu einer Person enthält. Analog dazu ist die ISBN-Nr ein Schlüsselattribut in einer Datenbank mit darin enthaltenen Informationen zu Büchern.

2.18 Fragen:

- Was geschieht mit der Registriernummer beim Wechsel zu einem anderen IdP?
- Ist der Wechsel der Registriernummer zu einem anderen IdP-Provider gemäss dieser Vorlage möglich, analog der Handynummer und der SIM-Karte beim Wechsel des Telecom Providers?

II.8 Art. 9

Wie sieht es um die Sicherheit der Haltung der Daten für die Personenidentifizierung aus?

II.9 Art. 10

2.19 Angesichts der folgenden Argumente stellt sich die Frage, ob der Betrieb eines IdP nicht eine öffentliche Aufgabe des Bundes darstellt, welche auch von einem Privaten erfüllt werden kann, wie z.B. eine Krankenkasse, die Grundversorgung in der Telekommunikation. Siehe dazu auch [RÜTSCHE] mit weiteren Beispielen und einer knappen Anleitung, wie zwischen öffentlichen und privaten Aufgaben unterschieden werden kann.

- Subsidiär hat der Bund einen IdP zu betreiben, falls kein Privater dies vornimmt (Abs. 1).
- Die E-ID wird wohl in Zukunft in etwa gleich bedeutsam sein wie eine Grundversorgungsdienstleistung in der Telekommunikation.
- Die Gebühren für die E-ID Dienstleistungen werden durch den Bund festgelegt, siehe Art. 27 Abs. 3.

- Art. 17, wonach der Bund (ISB) einen oder 2 IdP dazu verpflichten kann, gleiche Bedingungen zu schaffen.
- Die zwingende Akzeptanz einer E-ID (Art. 22)
- Erarbeitung von Dienstleistungsverträgen mit den E-ID-Dienstleister (Art. 15 Abs. 1 Bst. k).
- Der Kontrahierungszwang, eine E-ID auszustellen, wenn dieser eingeführt werden sollte.
- Das Sicherstellen der Interoperabilität der E-ID-Dienstleister untereinander (Art. 18 Abs. 1)

2.20 Das Erfüllen öffentlicher Aufgaben impliziert eine Staatshaftung und somit eine andere als die in dieser Gesetzesvorlage aufgeführte Haftungsbestimmung, siehe dazu auch RÜTSCHE.

II.10 Art. 12

II.10.1 Abs. 3

2.21 Die E-ID-Daten wie ein elektronisches Zertifikat können kopiert werden. (Beim Zertifikat ist dies in Bezug auf die IT-Sicherheit irrelevant.) Von wem (Inhaber der E-ID, Betreiber von E-ID verwendeten Diensten oder Hacker) lässt sich vielfach nicht zurückverfolgen und somit nicht feststellen, weil diese Informationen gemäss meinem aktuellen Verständnis meist und wie angedacht mehreren Parteien zugänglich sein werden. Somit ist vermutlich die darauf beruhende Sicherheit nicht umfassend, einfach und bequem, wie dies erwähnt wurde (Art. 1 Abs. 2 Bst. a).

II.11 Art. 13

2.22 Fragen:

- Ist eine Trennung zwischen Vollzugs- (Anerkennungsstelle) und Aufsichtsbehörde nicht sinnvoll, siehe z.B. den Konsumgütermarkt, HOLLIGER, Produktsicherheitsgesetz, S. 23 ff und das ZertES? Eine Beschreibung der Aufgaben, Rechte und Pflichten der Aufsichtsbehörde sollte folglich separat aufgeführt werden.
- Wenn ein Zertifikatsausteller zugleich auch IdP sein sollte, wie erfolgt dann die Anerkennung? Nach ZertES, E-ID oder beides miteinander?
- Warum wurde ein anderes Modell als beim ZertES kreiert?
- Es macht wenig Sinn die Aufsicht der Anerkennungsstelle unterzuordnen, siehe Bild in der Botschaft, S.16.

- Hat der dafür angedachte verantwortliche Bereich ISB im EFD ausreichend im Verwaltungsrecht des Bundes fachkundiges Personal, damit Verfügungen erlassen und die beim ISB eingereichten Beschwerden abhandelt werden können? Müsste dazu nicht das Personal beim ISB aufgestockt werden, was mit Mehrkosten verbunden ist? Dass beim ISB viel in IT fachkundiges Personal vorhanden ist, steht ausser Frage.
- Wäre es folglich nicht angebracht, die Anerkennung (Konzessionserteilung) oder zumindest die Aufsicht beim Bakom anzusiedeln, einem Bundesamt, welches darin bereits langjährige Erfahrung besitzt und somit bestens dazu geeignet und qualifiziert ist? Damit werden auch Überschneidungen und mögliche Inkompatibilitäten vermieden, wenn z.B. E-IDs bei der Grundversorgung in der Telekommunikation verwendet werden.
- Welche Rechtsmittel bei einer Verfügung über den Entzug oder einer Anerkennung bestehen, wie läuft ein solches Verfahren ab und wie sind die damit verbundenen Fristen ausgestaltet? Besteht z.B. ein Rechtsmittel mit aufschiebender Wirkung gegen eine solche Verfügung? Hierzu auch Kommentar zu Art. 19 Abs. 3.

II.12 Art. 15

2.23 Fragen:

- Wer kontrolliert, dass die Vereinbarungen (Abs. 1 Bst. k) eingehalten werden und welches sind die Kriterien der Vereinbarung?
- Wird nicht eine Vereinbarung mit allen IdP benötigt, oder werden die Daten unter den IdP abgeglichen? Werden die Daten unter den IdPs abgeglichen und bei verschiedenen Dienstleitern gespeichert, so stellt dies nicht ein erhöhtes Risiko dar? Diese Anmerkung gilt auch für Art. 18.
- Hat der E-ID-Dienstleister die Verträge widerspruchslos zu akzeptieren? Falls er damit nicht einverstanden ist, welche Rechtsmittel besitzt er, sich dagegen zu wehren? Ist dies ein Bundesverwaltungs- oder ein privatrechtliches Verfahren?
- Ist der IdP Kontroll- und Vollzugsbehörde für die Sicherheit des Betreibers von E-ID-Dienstleistungen? Wenn ja, dann stellt sich die Frage nach den Sorgfaltspflichten und den Befugnissen bei der Kontrolle.

2.24 **Bemerkung zu Abs. 1 Bst. l:** Der Wandel der Technik, insbesondere in der IT, ist enorm. Um diesem Wandel Rechnung zu tragen, werden in Gesetzen und Verordnungen beim Festlegen der gebotenen Sorgfalt gerne Formulierung wie "Stand der Technik und des Wissens" oder „Alle“ verwendet, so auch z.B. bei Art. 8 Abs. 2 VDSG und Art. 3 Abs. 2 PrSG. *"Der Stand des Wissens krankt jedoch an einer beträchtlichen Unbe-*

stimmtheit, weil er uferlos ist.", siehe HOLLIGER, S. 125, Kommentar zu Art. 3 Abs. 2 PrSG. Aus der Formulierung in Abs. 1 Bst. l stellt sich die Frage, ob der Austausch eines Netzwerkkabels gemeldet werden muss.

II.13 Art. 18

2.25 Wie werden die Aufgaben nach Abs. 1 vergütet?

II.14 Art. 19

II.14.1 Abs. 3

2.26 M.E. sollten die wichtigsten Grundsätze des strittigen (Verwaltungs)verfahrens und die dazu gehörigen Rechtsmittel und Fristen in einem Gesetz festgehalten werden. Die Vollzugsbehörde kann nicht unbefangen ein Verfahren in Grundsätzen regeln, wenn sie davon direkt betroffen ist. Anmerkung: Die Aufzählung in Art. 164 BV ist nicht abschliessend, RHINOW/SCHEFER, Rz. 2726.

2.27 Verfahrensgarantien gehören zu den elementaren und folglich zu den wichtigen Bestandteilen eines Rechtsstaates, wie auch zu Rechten einer Partei (Art. 164 Abs. 1 Bst. c BV). Bestanteile von grosser Wichtigkeit sind in einem Gesetz und nicht in einer Verordnung festzuhalten, siehe MÜLLER/UHLMANN, Rz 227 ff.

II.15 Art. 25

2.28 Warum wird die Anerkennungs- und Aufsichtsstelle namentlich mit ISB genannt? Bei einer Namensänderung der Bundestelle müsste das Gesetz geändert werden.

II.16 Art. 28

II.16.1 Abs. 1

2.29 Im Sinne der Rechtssicherheit sollte die Haftung der jeweiligen Partei klarer geregelt werden, wie in der EU-Verordnung. Folgende Fragen ergeben sich aus den Haftungsbestimmungen in der Vorlage.

- Wird folgender Fall durch den allgemeinen Teil des OR abgedeckt? Hat Anton den von Bernhard an Christoph *absichtlich* verursachten Schaden zu begleichen? Der Schaden entstand dadurch, dass Bernhard aufgrund einer von Anton begangenen Sorgfaltspflichtverletzung Christoph absichtlich täuschen konnte. Die Frage basiert auf folgenden Überlegungen:

  Nach Art. 17 ZertES haftet die Anbieterin von Zertifizierungsdienste, hier Anton, für Schäden an einem Dritten, hier Christoph infolgedessen, dass dieser

sich auf ein gültiges geregeltes Zertifikat verlassen hat, siehe dazu auch IDENT-AUTH, Kapitel VII.
Richtet sich die Haftung jedoch nach dem allgemeinen Teil des OR, dann stellt sich die Frage, ob das absichtliche Zufügen eines Schadens von Bernard an Christoph ein Grobverschulden darstellt und somit einen Unterbruch des adäquaten Kausalzusammenhangs und einen Haftungsausschluss betreffend die von Anton begangene Sorgfaltspflichtverletzung. Zum groben Drittverschulden, s. [KELLER I], S. 81 ff., S. 97 ff, 109 ff.

- Richtet sich die Haftung des IdP nach unerlaubter Handlung (OR 41), aus Vertrag (Art. 97 Abs. 1 ff.) oder nach den Vorgaben eines konzessionierten Gewerbes (Art. 100 Abs. 2 und Art. 101 Abs. 3 OR)? Welche Haftung darf der IdP folglich aus Vertrag wegbedingen?
- Ist es sinnvoll, die Haftungsbestimmungen (Umfang der Gefahrtragung und unbegrenzte Höhe des Schadenersatzes) für die verschiedenen Sicherheitsniveaus gleich auszugestalten?
- Wie haftet der IdP, wenn er zugleich ein nach ZertES anerkannter Aussteller von Zertifikaten ist?
- Wie haftet der IdP, wenn eine Bundesbehörde einen IdP betreibt, siehe dazu Abs. 2? Der Bund haftet grundsätzlich nach dem Verantwortlichkeitsgesetz (VG), ein Kanton nach dessen Staatshaftung

2.30 In IDENT-AUTH, Kapitel VII, wird dargelegt, warum eine Haftung nach OR beim Authentisieren im eGovernment Umfeld wenig sinnvoll ist.

2.31 Welche Prozesse nachvollzieh- und belegbar sein müssen/sollten, wurde in der Vorlage nicht aufgeführt. Die Nachvollzieh- und Belegbarkeit von Transaktionen sind jedoch Voraussetzung für ein strittiges Verfahren bei der Haftung.

III Angaben

III.1 Quellen

HOLLIGER	Eugénie Holliger-Hagmann, Produktesicherheitsgesetz PrSG, Schulthess Verlag 2010
ID-DIEBSTAHL	Pässe für Kriminelle: Fernsehreportage der ARD, https://www.ardmediathek.de/tv/Reportage-Dokumentation/P%C3%A4sse-f%C3%BCr-Kriminelle/Das-Erste/Video?bcastId=799280&documentId=54850588
IDENT-AUTH	Daniel Muster, Irrtum – Identifizieren versus Authentisieren, Sept. 2018, http://www.it-rm.ch/files/Ident-Auth_daniel_s_Muster_09_09_2018_V_1_1.pdf
J.-P.MÜLLER	Jörg-Paul Müller, Grundrechte in der Schweiz, Stämpfli Verlag, 3. Auflage, 1999
KELLER I	Alfred Keller, Haftpflicht im Privatrecht, Stämpfli Verlag AG, Bern 1993
MÜLLER/ UHLMANN	Georg Müller, Felix Uhlmann, Elemente einer Rechtsetzungslehre, 3. Auflage, Schulthess Verlag, 2013
MUSTER	CAS Arbeit an der ZHAW, Bedarf an Regulierung und Interdisziplinarität betreffend Haftung bei Internet der Dinge (IoT), September 2017
RHINOW/ SCHEFER	René Rhinow, Markus Schefer, Verfassungsrecht, Helbling Lichtenhahn Verlag, 2. Auflage, 2009
RÜTSCHE	Bernhard Rütsche, Was sind öffentliche Aufgaben?, Recht 2013 Heft 4, Stämpfli Verlag
SWISSCOM	Swisscom, Security Report 2017

III.2 Abkürzungsliste und Gesetzestexte

Abs.	Absatz
Bst.	Buchstabe
BV	Bundesverfassung
EFD	Eidgenössisches Finanzdepartement
eIDAS	Verordnung der 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
EPDG	Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015, SR 816.1

EPDV	Verordnung über das elektronische Patientendossier vom 22. März 2017, SR 816.11
ff.	folgende
ISB	Informatik-Steuerungsorgan des Bundes
OBG	Ordnungsbussengesetz vom 24. Juni 1970, SR 741.03
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches vom 30. März 1911, SR 220
PrSG	Bundesgesetz über die Produktesicherheit vom 12. Juni 2009, SR 819.1
Rz	Randziffer
S.	Seite
u.a.	unter anderem
usw.	und so weiter
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten vom 14. März 1958, SR 170.32
VZertES	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032
z.B.	zum Beispiel
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18. März 2016, SR 943.03