Schweizerischer Gemeindeverband | Association des Communes Suisses | Associazione dei Comuni Svizzeri | Associaziun da las Vischnancas Svizras

Eidgenössischen Justiz- und
Polizeidepartements EJPD
Frau Bundesrätin
Simonetta Sommaruga
3003 Bern

Per E-Mail an:
copiur@bj.admin.ch

Bern, 29. Mai 2017

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)
Stellungnahme des SGV

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 23. Februar 2017 haben Sie dem Schweizerischen Gemeindeverband (SGV) das oben erwähnte Geschäft zur Stellungnahme unterbreitet. Für die Gelegenheit uns aus Sicht der rund 1'625 dem SGV angeschlossenen Gemeinden äussern zu können, danken wir Ihnen.

I. Grundsätzliches

Auf der einen Seite unterstützt der SGV Ablaufoptimierungen und medienbruchfreie Prozesse, welche durchaus dank einer E-ID ermöglicht würden. Auf der anderen Seite, zieht der SGV nach wie vor eine staatliche E-ID dem nun vorgesehenen Modell vor.

Den digitalen Identitätsausweis in die Hände der Privatwirtschaft zu delegieren, kann nicht zielfördernd sein und wird voraussichtlich auch weiterhin in der Bevölkerung auf wenig Akzeptanz stossen, **weshalb wir hier auf die Relevanz hinweisen, dass ein zukünftiger privater IdP über einen sehr umfassenden Datenbestand einer Person verfügen wird.** Es handelt sich dabei um mehr - respektive je nach Quellregister - um andere zusätzliche Daten, als sie heute in den einzelnen Registern zur Verfügung stehen.

Da das E-ID-Verfahren insbesondere für den Laien technisch komplex ist, muss die Bevölkerung transparent über ihre Rechte informiert werden und sich darauf verlassen können, dass der Staat, wie dies im Gesetzestext und dem erläuternden Bericht auch zum Ausdruck kommt, ausreichend um die Sicherheit besorgt ist und Daten nicht missbräuchlich verwendet werden. Ebenfalls muss der E-ID-Inhaber Klarheit darüber haben, was mit seinen Daten genau passiert bzw. welche Daten weitergegeben werden. Ein E-ID Inhaber muss unbedingt die Möglichkeit haben, Einfluss auf die Datenbekanntgabe respektive auf die Einschränkung der Datenbekanntgabe zu nehmen.

Da es sich nicht um eine staatliche E-ID handelt, muss zwingend gewährleistet sein, dass die Bevölkerung eine Wahlfreiheit hat und der Antrag für eine E-ID an keine Bedingungen geknüpft werden kann, die dem Interesse der Bevölkerung im Wesentlichen entgegensteht. Das heisst, dass weder ein E-ID-Anbieter eine Monopol-Stellung erhält, noch, dass Absprachen zwischen E-ID-Anbietern stattfinden.

Laupenstrasse 35
Postfach
3001 Bern
Tel. 031 380 70 00
www.chgemeinden.ch
verband@chgemeinden.ch

II. Zu den einzelnen Artikeln

Art. 6 Ausstellungsprozess

Abs. 1

Laut Erläuterungen wird eine E-ID in der Regel nach Vorsprache bei einem IdP ausgestellt. Die Registrierung beinhaltet je nach Sicherheitsniveau auch eine Identifizierung mittels elektronischer Medien. Aus Sicht des SGV ist in jedem Fall eine persönliche Vorsprache für die Beantragung einer E-ID zwingend. Mit den heutigen Mitteln erachten wir eine reine virtuelle Identifikation als relativ leicht manipulierbar für Personen mit dem nötigen technischen Wissen.

Ergänzung im Gesetz:

1 Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP. ***Eine persönliche Vorsprache zur Identitätsüberprüfung ist unabdingbar.***

Abs. 3

Für den SGV ist in diesem Punkt unklar, ob der zukünftige Inhaber einer E-ID auch die durch die Identitätsstelle übermittelnden Daten an den IdP oder durch den IdP abzurufende Daten einschränken kann. Gemäss Wortlaut von Art. 6 verstehen wir, dass die Personenidentifizierungsdaten nach Art. 7 Abs. 1 und 2 abschliessend übermittelt werden, wenn eine E-ID bei einem IdP beantragt wird.

Aus Sicht des SGV muss zwingend gewährleistet sein, dass diese Merkmale je nach Anforderungsniveau der gewünschten E-ID durch den Inhaber ebenfalls eingeschränkt werden können. Es ist durchaus denkbar, dass ein zukünftiger Inhaber ausschliessliche eine E-ID mit tiefem Sicherheitsniveau verwendet und deshalb nur die Grunddaten: Name, Vorname, Geburtsdatum auf seiner E-ID benötigt. **Aus diesem Grund stellt sich hier die Frage, wofür der IdP in einem solchen Fall den gesamten Datenumfang von Art. 7 Abs. 2 benötigt?**

Art. 7 Personenidentifizierungsdaten

Abs. 1 und 2

Der SGV unterstützt, wie im erläuternden Bericht beschrieben, die Einschränkung von Personenidentifizierungsdaten durch den Inhaber bei einer konkreten Anwendung einer E-ID, die vom IdP an eine Betreiberin von E-ID verwendeten Diensten übermittelt werden.

Abs.4

Inwiefern kann ein E-ID-Inhaber bezüglich diesen zusätzlichen vom IdP hinzuzufügenden Daten Einfluss nehmen? **Es muss auch hier unbedingt gewährleistet sein, dass ein E-ID-Inhaber diese einschränken kann bzw. seine Einwilligung erteilen muss.** Geht es hier doch immerhin um die durch den IdP – zwar nicht mit dem Staat verifizierten - zusätzlich zugewiesenen Daten, wie z.B. E-Mail-Adresse, Mobile-Telefon, Adresse etc.

Weiter ist darauf hinzuweisen, dass es Personen gibt, welche in den amtlichen Registern die Auskunft über Daten gegenüber Privaten haben sperren lassen. Äusserst heikel erachtet der SGV es deshalb, wenn Daten, wie die Adresse, Mobile-Nr. oder E-Mail-Adresse ohne Einwilligung der Person oder sogar in Unkenntnis des Inhabers hinzugefügt werden und diese Daten privaten Dritten bekannt gegeben würden. Oft sind Personen, die eine Adress- und Datensperre z.B. in den Einwohnerregistern beantragt haben an Leib und Leben bedroht.

Art. 8 Aktualisierung der Personenidentifizierungsdaten

Es muss auch hier sichergestellt sein, 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 (vgl. Einwand zu Art. 6 Abs. 3).

Art. 10 Datenbearbeitung und Datenweitergabe

Weshalb unterliegen die Daten nach Art. 7 Abs. 1 und 4 in diesem Zusammenhang nicht auch dem Handelsverbot? Nach Art. 7 Abs. 4 könnten hier eine Varietät an Daten hinzugefügt werden, die mit Name, Vorname und Geburtsdatum verknüpft werden.

Der Wortlaut im Bericht zu Art. 10 Absatz 3, Seite 27/28 ist in diesem Zusammenhang nicht präzis formuliert bzw. ist verwirrend. **Welche Daten dürfen nun gegen Entgelt weitergeben werden und welche nicht?**

Der E-ID Inhaber muss sich auf jeden Fall bewusst sein, welche Daten an Dritte weitergegeben werden und welche nicht.

Der SGV beantragt den Wortlaut des Gesetzes folgendermassen abzuändern:

Art. 10 Abs. 3

Weder (……) von E-ID-verwendenden Diensten dürfen die Personenidentifizierungsdaten gemäss Artikel 7 Abs. 2 oder die darauf basierenden Nutzungsprofile weitergeben. ***Für die Bekanntgabe der Daten nach Art. 7 Abs. 1 und 4 an Dritte ist das Einverständnis des E-ID Inhabers einzuholen.***

Gemäss Seite 10 und 12 (Grafik) des Konzeptes aus dem Jahre 2016 garantiert, wenn immer möglich, der Staat für sichere und verlässliche Attributsquellen.

In diesem Zusammenhang schliesslich möchte der SGV auf folgende Gegebenheiten aufmerksam machen: Es ist in der Praxis durchaus möglich, dass sich ein Datenfeld bzw. ein Attribut im Nachhinein als falsch erweist, wenn z.B. eine Person ihre Meldepflicht über eine Änderung eines Attributes gegenüber der Quelldatenbank nicht erfüllt hat oder sich das Datum infolge eines in der Vergangenheit liegenden Ereignisses rückwirkend verändert.

Wir danken Ihnen für die Kenntnisnahme und die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Gemeindeverband

Präsident	Direktor
	
Hannes Germann	Reto Lindegger
Ständerat	

Kopie an: Schweizerischer Städteverband, Bern

GEMEINDE **PFÄFFIKON ZH**

GEMEINDERATSKANZLEI

Hochstrasse 1, 8330 Pfäffikon ZH
Tel. 044 952 51 80 / Fax 044 952 52 00
gemeinderatskanzlei@pfaeffikon.ch
www.pfaeffikon.ch

23. Mai 2017

Gemeinderatskanzlei, Hochstrasse 1, Postfach 483, 8330 Pfäffikon

Eidgenössisches Justiz- und Polizeidepartement
Leiter Fachbereich Rechtsinformatik
Urs Paul Holenstein
Bundesrain 20
3003 Bern

Vernehmlassung E-ID-Gesetz

Sehr geehrte Damen und Herren
Sehr geehrter Herr Holenstein

Wir begrüssen die mit dem E-ID-Gesetz verbundene Stossrichtung, allgemein anerkannte elektronische Identifizierungseinheiten (E-ID) einzuführen. Mit dem Gesetz werden die Grundlagen geschaffen, um die Identifizierung und Authentifizierung von Personen bei der Anwendung von Online-Diensten über allgemein kompatible Schnittstellen zu ermöglichen. Insbesondere entspricht die E-ID einem grossen und immer wieder geäusserten Bedürfnis der Gemeinwesen, den elektronischen Behördenverkehr zu vereinfachen und zu erleichtern.

Gestützt auf die Vernehmlassungen des Regierungsrates und des VZGV (Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute) unterstützt der Gemeinderat die Bestrebungen, elektronische Prozesse effizient und sicher abwickeln zu können.

Die im Vorentwurf vorgesehene Aufgabenteilung zwischen Staat und Privaten setzt voraus, dass der Markt unkomplizierte und untereinander kompatible Identifikationslösungen entwickelt, die durch ständige Innovation vorangetrieben werden. Ob sich der Markt aufgrund der für den Aufbau von Kommunikations- und Informationsinfrastrukturen notwendigen Investitionskosten in diese vorgesehene Richtung bewegen wird, ist indessen ungewiss, zumal die privaten Akteure alle von Gesetz und Verordnung vorgegebenen Regeln zu berücksichtigen haben und da mit der Produktentwicklung eine kostenintensive Aufbauphase vorangehen dürfte. Insofern wird angeregt, unter der Leitung des Bundes eine Trägerschaft bestehend aus Bund, Kantonen und Gemeinden als Identitätsdienstleister einzusetzen, welche die zur Aufgabenerfüllung erforderliche Technologie durch Ausschreibung auf dem privaten Markt beschafft. Der Bund soll diese Trägerschaft anleiten und insbesondere mit finanziellen Mitteln zur Entwicklung einer ersten Identifikationslösung unterstützen. Der Betrieb dieser Trägerschaft soll auf einem selbsttragenden Geschäftsmodell beruhen und damit mittelfristig ohne staatliche Subventionen auskommen.

Die Erfahrungen, die der Kanton Zürich mit dem Elektronischen Patientendossier gemacht hat, zeigen klar, dass es den staatlichen Akteur im Lead braucht. Nur er verfügt über die nötige Autorität und Legitimation, alle weiteren Beteiligten in einen verbindlichen Prozess einzubinden. Gleichzeitig soll der Staat nicht selber als IT-Entwicklungsunternehmen auftreten. Deshalb ist die Technologie auszuschreiben.

Art. 9 Verwendung der Versichertennummer

Dass Art. 9 E-ID-Gesetz die Identitätsstelle berechtigt, die AHV-Nummer zu verwenden, ist zu begrüssen. Eine solche Verwendung der AHV-Nummer ist für ein effizientes und reibungsloses Funktionieren des Systems unumgänglich und bildet eines der Kernstücke des Gesetzes. Daher sollte dieser Grundsatz jedenfalls vollumfänglich beibehalten werden.

Vielen Dank für die Möglichkeit zur Vernehmlassung und die Berücksichtigung unserer Anregungen.

Freundliche Grüsse

Gemeinderat Pfäffikon

Marco Hirzel
Gemeindepräsident

Bennie Lehmann
Gemeindeschreiber-Stellvertreter

Schweizerischer Städteverband
Union des villes suisses
Unione delle città svizzere

Eidg. Justiz- und Polizeidepartement EJPD
Frau Bundesrätin Simonetta Sommaruga
Bundeshaus West
3003 Bern

Per Mail: copiur@bj.admin.ch

Bern, 30. Mai 2017

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

Sehr geehrte Frau Bundesrätin,
sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, zum Vernehmlassungsentwurf für das Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung nehmen zu können.

Allgemeine Einschätzung

Der Schweizerische Städteverband unterstützt den Grundsatz zur Schaffung von elektronischen Idenitifizierungseinheiten (E-ID). Im Rahmen von E-Government Schweiz ist die Schaffung einer nationalen digitalen Identität ein zentrales und prioritäres Vorhaben.

Gegenüber dem vorliegenden Konzept mit einer Aufgabenteilung zwischen Staat und Markt ist die Mehrheit unserer Mitglieder ablehnend eingestellt. Die Herausgabe einer digitalen Identität – gleich wie bei den analogen Identitätspapieren – gehört für die Mehrheit der Städte zu den Kernaufgaben der öffentlichen Hand. Hauptargument dafür ist das ungleich höhere Vertrauen in den Staat als Herausgeber von Identifizierungseinheiten.

Nur eine Minderheit unserer Mitglieder erachtet die vorgeschlagene Lösung mit einem Markt für mehrere staatlich anerkannte Identitätsdienstleister als praktikabel und mit tragbaren Risiken verbunden.

Aus städtischer Sicht besteht eine Reihe weiterer Unklarheiten betreffend Folgekosten. So ist offen, welches die Aufwände und Kosten für die Betreiber eines «E-ID-verwendenden Dienstes» (also besonders auch Verwaltungen) wären, die durch das komplexe System der Zertifizierungen ausgelöst würden. Wir verstehen das vorgestellte Konzept so, dass Verwaltungen, die Systeme zur elektronischen Identifikation anbieten, dann auch sämtliche vom Bund zertifizierte Identitäts-Provider (IDP) akzeptieren müssten. Heute haben die betroffenen Verwaltungen und Systembetreiber einen erheblichen Aufwand, die verschiedenen existierenden Systeme (z.B. SuisseID und mobileID der Swisscom)

Monbijoustrasse 8, Postfach, 3001 Bern
Telefon +41 31 356 32 32
info@staedteverband.ch, www.staedteverband.ch

technisch einzubinden. Auch wird aus den Konzepten und dem Gesetzesentwurf nicht klar, ob die Anbieter solcher Lösungen bei den Verwaltungen dafür Gebühren erheben dürfen. Heute ist es beispielsweise aufwändig und teuer, eine E-Payment-Lösung anzubieten und möglichst viele der oft verwendeten Zahlungsmittel einzubinden. So ähnlich könnte sich der geöffnete Markt der Identitätsprovider dereinst darstellen, wenn eine Gemeinde oder eine Stadt mit jedem der Anbieter bilaterale Verträge eingehen muss.

Bezüglich der Verwendung von Identitäten in der Praxis muss im Konzept und im Gesetzesentwurf auch Bezug auf das ebenfalls von E-Government Schweiz priorisierte Vorhaben IDV Schweiz genommen werden, welches zum Ziel hat, bestehende Identitäten föderieren zu können. Fraglich ist, ob gemäss dem vorliegenden Konzept die Kantone oder Gemeinden, welche ihre Daten zur Föderierung anbieten möchten, automatisch zu Identitätsprovidern würden und sich somit für den qualifizierten Austausch von Identitäten zertifizieren lassen müssten. Auch hier ist unklar, mit welchen Kosten und Aufwänden zu rechnen ist.

Konkrete Anliegen und Anträge

Der Städteverband beantragt daher, dass der Bund die Vorlage überarbeitet und mit einer Variante ergänzt, in der die Lösung mit einer einheitlichen staatlich abgegebenen E-ID konkretisiert wird. Eine Mehrheit der Städte favorisiert die letztgenannte Variante.

Falls das Konzept mit dezentraler Identifizierungsmittel-Ausgabe weiterverfolgt wird, so muss auf Bundesebene eine zentrale Anlaufstelle für Wissenstransfer und die Koordinationsaufgaben zwischen den IDP und Verwaltungen geschaffen werden. Um eine rasche flächendeckende Verbreitung der E-ID auf allen drei Staatsebenen sicherzustellen, sind vom Bund auch Mittel für Anschubfinanzierungen bereitzustellen. Ebenso unterstützen wir die Änderungsanträge des Verbands Schweizerischer Einwohnerdienste (VSED) zum vorgestellten Konzept.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Schweizerischer Städteverband

Präsident

Kurt Fluri, Nationalrat
Stadtpräsident Solothurn

Direktorin

Renate Amstutz

Kopie Schweizerischer Gemeindeverband
Verband Schweizerischer Einwohnerdienste

Centre Patronal

Office fédéral de la justice
3003 Berne

Par courriel :
copiur@bj.admin.ch

Paudex, le 19 mai 2017
PGB

Consultation: projet de loi fédérale sur les moyens d'identification électronique reconnus («loi e-ID»)

Madame, Monsieur,

Nous avons pris connaissance de la consultation relative au projet mentionné en titre. Comme nous en avons l'habitude lors des consultations fédérales, nous prenons la liberté de vous communiquer notre position – après avoir nous-mêmes requis l'avis d'un certain nombre de personnes.

L'identité électronique (désignée «e-ID»), telle qu'elle est conçue dans le projet du Conseil fédéral, doit permettre aux personnes physiques de s'identifier de manière fiable auprès des divers fournisseurs de services sur internet. Cette solution permettra de remplacer, à terme, les nombreux moyens d'identification spécifiques à chaque fournisseur ou à chaque administration.

Le Conseil fédéral fait le choix de renoncer à une e-ID délivrée et gérée par l'Etat, comme cela existe dans certains pays européens, et de confier l'établissement des e-ID à des fournisseurs privés reconnus par la Confédération. Cette solution présente l'avantage de s'appuyer – à moindres frais – sur une pratique déjà existante, puisque des acteurs privés importants (banques, CFF, La Poste) commercialisent déjà ou sont sur le point de commercialiser des identités électroniques utilisables auprès d'une grande variété de prestataires de services en ligne. Cela permettra aussi de rester relativement neutre et flexible face à l'évolution rapide de certaines techniques. La reconnaissance de ces solutions par la Confédération conférera à ces identifications une fiabilité officielle et un cadre juridique solide; elle ouvrira aussi la voie à une future reconnaissance internationale, tout au moins sur le plan européen.

Ce projet éveille manifestement des réactions contrastées. Certains de nos interlocuteurs expriment une crainte générale face au risque de piratage. D'autres sont favorables et jugent ce projet prioritaire pour le développement des transactions électroniques – par exemple pour l'établissement d'actes authentiques devant notaire. D'une manière générale, le respect de la protection des données revêt une grande importance.

Route du Lac 2
1094 Paudex
Case postale 1215
1001 Lausanne
T +41 58 796 33 00
F +41 58 796 33 11
info@centrepatronal.ch

Kapellenstrasse 14
Postfach 5236
3001 Bern
T +41 58 796 99 09
F +41 58 796 99 03
cpbern@centrepatronal.ch

www.centrepatronal.ch

Pour notre part, nous jugeons ce projet positivement. L'établissement d'une identité électronique reconnue pour les personnes physiques contribuera au développement des transactions en ligne. La solution proposée nous semble adéquate dans la mesure où elle accorde un rôle important à l'économie privée et préserve une certaine souplesse face à l'évolution de la technique et des habitudes sociales. Les moyens engagés par l'Etat paraissent raisonnables.

Nous vous remercions de l'attention que vous porterez à ce qui précède et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Centre Patronal

Pierre-Gabriel Bieri

Frau Bundesrätin
Simonetta Sommaruga
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundeshaus West
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

29. Mai 2017

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

Sehr geehrte Frau Bundesrätin

Im Februar 2017 haben Sie uns eingeladen, zum E-ID-Gesetz Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. economiesuisse nimmt gestützt auf den Input der betroffenen Mitglieder aus einer übergeordneten, gesamtwirtschaftlichen Sicht wie folgt Stellung:

Zusammenfassung

Im Zusammenhang mit der rasanten Entwicklung für Wirtschaft und Gesellschaft, welche der technologische Fortschritt mit sich bringt, ist der Staat gefordert, diesen Entwicklungen den nötigen Raum zu lassen und nicht durch vorauseilende Regulierung einzuschränken. Gleichsam gibt es Bereiche, in denen die gesetzlichen Voraussetzungen für Instrumente, welche in der digitalisierten Welt unverzichtbar sind, geschaffen werden müssen. In diesem Zusammenhang begrüsst economiesuisse die Vorschläge des Bundes zur Schaffung einer staatlich anerkannten E-ID. Im Zusammenhang mit erforderlichen Anpassungen für eine uneingeschränkte digitale Wirtschaft handelt es sich bei der E-ID um eines der prioritären Projekte in den kommenden Jahren.

Ohne breite Akzeptanz bei der Bevölkerung und der Wirtschaft wird sich die E-ID jedoch nicht durchsetzen. Es braucht daher einen gesetzlichen Rahmen, welcher eine vertrauenswürdige und glaubwürdige Herausgabe von E-ID ermöglicht. Diese muss sodann attraktive Anwendungsmöglichkeiten ermöglichen.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

Akzeptanz hängt stark vom Vertrauen ab. Dieses jedoch hängt nicht primär von der Frage ab, ob ein privater oder staatlicher Herausgeber die E-ID anbietet. Die Meinungen, ob die E-ID Lösung staatlich oder privat erfolgen soll, sind im Kreise unserer Mitglieder denn auch uneinheitlich. Der Blick ins Ausland zeigt, dass sowohl staatliche als auch private Lösungen das Potenzial haben, sich durchzusetzen oder zu scheitern. Vertrauen kann gerade auch durch private und breit akzeptierte Anbieter geschaffen werden. Auch aus ordnungspolitischer Sicht ist einer Marktlösung der klare Vorzug zu geben. Es sollte daher im Sinne einer maximalen Nutzung des möglichen Marktpotentials privaten Anbietern ermöglicht werden, ein attraktives E-ID Produkt anzubieten. Lediglich wenn sich herausstellen sollte, dass der Markt kein ausreichendes Interesse an entsprechenden Angeboten hat, sollte der Staat subsidiär im Sinne seines Grundversorgungsauftrages einspringen.

1. Grundsätzliche Überlegungen

Die Digitalisierung ist eine treibende Kraft für Innovationen in Wirtschaft und Gesellschaft. Noch ist bei vielen Entwicklungen nicht mit ausreichender Klarheit erkennbar, wohin sie gehen. Der Regulator ist in dieser Situation gefordert, die sich aus der technologischen Entwicklung ergebenden Chancen durch gute Rahmenbedingungen zu ermöglichen, ohne diese gleichzeitig durch vorauseilende Regulierungen abzuwürgen. Dies bedeutet, dass innovationshemmende Regulierungen abgebaut und gerade in den Bereichen, in welchen akuter Handlungsbedarf besteht, gezielt reduziert werden müssen. Dort, wo es neue gesetzliche Rahmenbedingungen braucht, muss der Staat aber aktiv werden und dabei auf die Bedürfnisse und Möglichkeiten der Wirtschaft eingehen.

economiesuisse unterstützt das Ziel des Bundes, die rechtlichen und organisatorischen Rahmenbedingungen zur Einführung einer E-ID für natürliche Personen zu schaffen. Die elektronische Identität E-ID ist eine Grundlage für viele digitale Anwendungen der digitalen Wirtschaft. Nur durch eine E-ID lassen sich kosten- und zeitintensive Medienbrüche bei der Nutzung von digitalisierten Dienstleistungen verhindern.

Jede Schweizerin und jeder Schweizer sollte sich im Internet mit der gleichen Qualität elektronisch ausweisen können wie mit dem Pass oder der Identitätskarte in der physischen Welt. **Um dieses übergeordnete Ziel zu erreichen, braucht es aus Sicht Wirtschaft folgende strategischen Eckwerte:**

- **Flächendeckende Einführung**: Alle Einwohnerinnen und Einwohner der Schweiz sollen die Möglichkeit erhalten, eine E-ID zu beziehen und zu verwenden. Hier darf es nicht zu störenden Ausschlusskriterien kommen wie z.B. die Beschränkung auf Bürgerinnen und Bürger, hohe Kosten für den Nutzer oder eine komplizierte Anwendung;
- **Rasche Einführung:** Die Einführung der E-ID ist überfällig. Nach der langjährigen politischen Debatte braucht es nun zeitnah einen klaren Rechtsrahmen;
- **Sinnvolle obligatorische Anwendungen der E-ID**: Der Staat soll mit gutem Beispiel vorausgehen: die E-ID soll im Behördenverkehr als vollwertige Alternative zu Identitätskarte (IDK) und Pass akzeptiert werden.

2. Voraussetzungen für eine breite Akzeptanz und Nutzung

Ohne breite Akzeptanz bei der Bevölkerung und der Wirtschaft wird sich die E-ID nicht durchsetzen. Aus Sicht von economiesuisse ist Vertrauen als Schlüsselfaktor entscheidend. Der Schweizer Pass und die IDK geniessen einen hervorragenden Ruf. Gleichzeitig ist die Schweizer Bevölkerung, wie aktuelle Befragungen zeigen, gegenüber digitalen Dienstleistungen und dem Umgang mit ihren Nutzerdaten eher kritisch eingestellt. Gerade deshalb ist entscheidend, dass der rechtliche Rahmen es ermög-

licht, dass vertrauenswürdige E-ID-Herausgeber möglich sind. Dies umfasst gerade auch ein Wahlrecht: Daten dürfen nicht zentralisiert oder zweckentfremdet werden und müssen vor Angriffen geschützt sein.

3. Grundsätzliche Überlegungen zum Konzept

Dass die E-ID in ihrer innersten Kernfunktion staatlich sein muss, ist weitgehend unbestritten. Unterschiedliche Auffassungen bestehen jedoch in der Frage, ob die Herausgabe an Private delegiert werden soll. Der Vorentwurf sieht vor, dass die E-ID von verschiedenen Unternehmen und Organisationen herausgegeben werden kann, die vom Bund dafür zertifiziert werden. Diese Lösung bevorzugt auch economiesuisse, nicht zuletzt, da sie es dem Markt ermöglich, innovative Lösungen zu entwickeln und dadurch das Nutzererlebnis für die Anwender zu steigern. Gleichsam wird der Staat auch gerade nicht in einem Bereich ausgebaut, in welchem Private dank ihrer Innovationskraft und Technologieführerschaft den trägen staatlichen Prozessen grundsätzlich überlegen sind.

Der Blick ins Ausland zeigt, dass sowohl staatliche als auch private Lösungen das Potenzial haben, sich durchzusetzen oder zu scheitern. In Estland und Deutschland wurden hoheitliche E-IDs eingeführt; dies mit völlig unterschiedlichen Erfolgsquoten bei der Durchsetzung in der Bevölkerung. In Schweden, Norwegen und Dänemark bestehen private Lösungen. Hier haben sich die Banken zu den wichtigsten Anbietern der E-ID durchgesetzt. Staatliche Minimalanforderungen sorgen für eine definierte Qualität und für die Interoperabilität. Die schwedische Lösung BankID gilt als erfolgreich und kommt bei verschiedensten Firmen, Banken und Behörden für die Identifikation und Authentifikation zur Anwendung.

Entsprechend muss auf jeden Fall einer privatwirtschaftlichen Lösung der Vorzug gegeben werden. Der Erfolg der E-ID in der Schweiz wird sich nicht an der Frage staatlich vs. privat entscheiden. Andere Kriterien wie Einfachheit in der Anwendung und eben Vertrauen werden eine viel wichtigere Rolle spielen. Die Diskussion, ob sich die Schweizerinnen und Schweizer nun wohler fühlen würden, wenn sie mit der staatlichen E-ID Bankgeschäfte tätigen oder private Güter erwerben müssten oder mit einer Bank oder Post E-ID die Steuern einreichen oder Gesundheitsdaten verwalten müssten, ist aus unserer Sicht nicht zielführend. Die Beispiele Estland und Schweden zeigen, dass sich E-IDs dort durchsetzen, wo die Bevölkerung Erfahrung mit E-Lösungen sammeln konnte, die Produkte direkt im Alltag angewendet werden konnten und dadurch auch Vertrauen gebildet werden konnte.

Für den Erfolg der E-ID ist daher entscheidend, dass die Beteiligten nun mit vereinten Kräften dafür sorgen, dass die E-ID in der Bevölkerung bekannt und anerkannt wird. Hierzu müssen das Potenzial und der Mehrwert aufgezeigt werden. Darüber hinaus müssen schnell attraktive E-Dienstleistungen entstehen, damit der Nutzen der E-ID erkannt und diese durch die breite Verwendung etabliert werden kann.

4. Zu einzelnen Punkten im Detail

4.1 Einbezug privater Anbieter

Die Bestimmung, wer Anspruch auf einen elektronischen Identitätsnachweis hat, ist eine hoheitliche Aufgabe; dies entspricht der Aufgabe des Staates bei der Herausgabe von Pass oder Identitätskarte. Hierbei ist es die Aufgabe des Staates, die Korrektheit der Personenidentifikationsdaten und die Authentizität der zu identifizierenden Person sicherzustellen. Weitere hoheitliche Aufgaben bestehen nicht. Insbesondere muss der Bund die E-ID-Systeme nicht auch technisch betreiben oder sogar die entsprechenden Anwendungen herausgeben.

Der Vorentwurf des Bundes sieht daher richtigerweise vor, dass die E-ID von verschiedenen Unternehmen und Organisationen herausgegeben werden können, die vom Bund dafür zertifiziert werden. Die Interoperabilität ist dabei aber stets sicherzustellen.

4.2 E-ID im Behördenverkehr akzeptiert

Um den Nutzen der E-ID zu fördern und die Digitalisierung der Schweiz voranzutreiben, sollte der Bund mit gutem Beispiel vorangehen. Die Vorlage ist dahingehend anzupassen, dass die Verwaltungen von Bund, Kantonen und Gemeinden dazu verpflichtet werden, die E-ID als gleichwertige Alternative zu Pass und IDK zu akzeptieren. Nur so ist es möglich, E-Government Angebote frei von Medienbrüchen und mit einem Mehrwert für die Nutzer auszustatten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Thomas Pletscher
Mitglied der Geschäftsleitung

Erich Herzog
Stv. Leiter Wettbewerb & Regulatorisches

Fédération des
Entreprises
Romandes

Secrétariat général

copiur@bj.admin.ch

Département fédéral de justice et police
Bundesrain 20
3003 Berne

Genève, le 29 mai 2017
FER No 16-2017

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID)

Madame, Monsieur,

Nous vous remercions de nous avoir consultés concernant l'objet susmentionné et nous nous permettons de vous transmettre ci-après nos considérations.

1. Présentation générale

Par décision du 19 décembre 2012, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'élaborer, en collaboration avec les autres départements compétents 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 a fait l'objet d'une consultation en 2014 et 2015 et, compte tenu des résultats, celui-ci a été remanié.

Les échanges passent effectivement de plus en plus par des voies dématérialisées. Afin de pouvoir faire des transactions importantes sur Internet, les partenaires ont besoin de se fier à l'identité de leur interlocuteur. Le Conseil fédéral souhaite ainsi créer le cadre juridique et organisationnel en vue de la reconnaissance par l'Etat de moyens d'identification électronique et de leurs fournisseurs. Plus concrètement, dans la sphère numérique, chaque système propose de nos jours son propre mécanisme d'identification, ce qui amène à des frais élevés. Selon le projet, des moyens d'identification électroniques (e-ID) acceptés et compatibles avec tous les systèmes permettraient de conclure des transactions et de faire des démarches administratives sur Internet de manière plus efficace.

Dans la nouvelle réglementation proposée, le Conseil fédéral propose un mécanisme de partage des tâches entre l'Etat et le secteur privé. Plus formellement, les fournisseurs d'identité (du secteur public ou privé) satisfaisant aux conditions requises seront habilités par la Confédération (organisme fédéral de reconnaissance) à délivrer des e-ID reconnus et à gérer des systèmes e-ID

reconnus. Des systèmes tels que ceux de la Poste et des CFF pourront par exemple être reconnus par la Confédération.
Etant donné que toutes les transactions ne demandent pas le même degré de sécurité, trois niveaux de garantie sont prévus pour l'e-ID : faible, substantiel et élevé. Le niveau de garantie requis pour les différents types d'applications est déterminé dans les réglementations spéciales ou par les exploitants d'un service utilisateur du secteur privé.

La réglementation prévoit également la mise en place d'un service fédéral chargé de transmettre aux fournisseurs reconnus d'e-ID les données d'identité nécessaires tirées des registres de la Confédération. La première fois, la personne concernée devra donner son accord exprès.

Les données d'identité seront transmises contre émolument dans l'objectif de financer les deux services de la Confédération. Le service d'identité serait créé au Département fédéral de justice et police, qui a la responsabilité des banques de données pertinentes. L'organisme de reconnaissance fera partie du Département fédéral des finances (qui assume déjà des tâches dans le domaine de la sécurité des TIC). Selon le rapport explicatif (p.12), l'introduction d'e-ID reconnus va requérir un investissement financier de 6,5 millions de francs de la part de la Confédération.

2. Considérations

A) Politico-économiques

Au cours de ces quinze dernières années, les expériences réalisées au sein des pays européens montrent des résultats plutôt mitigés. L'Allemagne, en particulier, a introduit une carte d'identité électronique et la moitié de la population allemande la possède à l'heure actuelle. Toutefois, il s'est avéré que cette carte a bénéficié d'un accueil peu favorable auprès du secteur privé et des citoyens en raison de la difficulté d'utilisation du système et du coût. Dans plusieurs pays, les systèmes déployés à grands frais n'ont pas encore fait leurs preuves. En Suisse, si de tels instruments (e-ID) sont utilisés ou développés, notre Fédération ne peut que recommander de tenir compte des expériences réalisées à l'étranger afin de ne pas commettre les mêmes erreurs.

Concernant la reconnaissance mutuelle des systèmes e-ID entre la Suisse et l'UE, le rapport explicatif fait mention (p.14) de la nécessité de conclure sur ce point de nouveaux accords bilatéraux. Si notre Fédération voit d'un œil positif la conclusion de tels accords, elle se demande si cette option est vraiment réaliste compte tenu de nos relations compliquées avec l'UE au cours de ces dernières années.

Par ailleurs, la loi e-ID crée de nouvelles tâches pour l'administration fédérale (création du service d'identité ainsi que de l'organisme de reconnaissance), ce qui implique des coûts. Le rapport explicatif mentionne un coût de 6,5 millions de francs, 1,5 million de francs de coûts d'exploitation informatique annuels et 0,7 million de francs pour les frais en personnel. Il est clairement indiqué que ces dépenses seront compensées à moyen terme par les recettes provenant des émoluments. Notre Fédération regrette qu'un plan de financement complet ne soit pas présenté avec cet avant-projet de loi ainsi qu'une appréciation globale des émoluments demandés. Faut-il rappeler ici que les expériences réalisées dans certains pays de l'UE ont échoué en raison notamment des coûts ?

De plus, il ne faudrait pas que le budget prévu par les nouvelles tâches ne soit amené à grossir année après année, sachant que les projets informatiques nécessitent beaucoup de ressources financières et que, in fine, des charges supplémentaires pèsent sur les personnes morales ou physiques pour financer un tel système. Cela ne serait pas très bien perçu, alors que la conjoncture reste difficile et que la Suisse est toujours confronté à la force de son franc.

B) Techniques

D'un point de vue technique, différents point méritent une attention particulière :

Notre Fédération est d'avis que les besoins d'interopérabilité et d'évolutivité doivent être pris en compte. En effet, le respect des standards informatiques actuels (SAMLv2, OAuth2, OpenIDConnect) est indispensable pour permettre une large diffusion auprès des fournisseurs de service, et maîtriser les coûts d'implémentation. Le développement des services en situation de mobilité doit également être intégré dans la réflexion (OAuth2 for Native Apps par exemple).

Par construction, un tel dispositif, peut présenter des failles de sécurité et ceci d'autant plus qu'il est utilisé par de nombreuses personnes. En d'autres termes, si le système se fait « hacker », il pourrait poser de graves difficultés.

Ainsi, la sécurité de l'ensemble du dispositif est la clef de voûte d'une utilisation à large échelle. Les mesures sécuritaires doivent être intégrées dans l'ensemble des étapes de construction et d'exploitation d'un tel projet. La compromission d'un tel système aurait des conséquences sociales et économiques beaucoup plus importante qu'un système très fortement décentralisé.

Notre Fédération souligne également que la mise en œuvre ou l'utilisation de registre apportent de la valeur à partir du moment où la qualité des données est satisfaisante. Il existe statistiquement un pourcentage résiduel d'erreur dont il faut tenir compte. La mise en place du registre UPI a nécessité des efforts importants pour corriger les cas d'attribution de NAVS13 erronés. Si l'incidence métier est restée relativement faible, qu'en serait-il de l'utilisation d'une identité électronique erronée ? Prévoir des processus d'exception permet d'éviter qu'un usager ne soit pris au piège dans un engrenage administratif inextricable qui, porté dans la presse nuirait passablement à la crédibilité du dispositif.

C) Juridiques

C. 1. Remarques juridiques générales

Notre Fédération prend acte que les dispositions du projet de loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID) sont compatibles avec la réglementation internationale, en particulier avec le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (**règlement eIDAS**)[1].

Nous nous plaisons à relever, tout comme les auteurs du projet, qu'il convient impérativement d'éviter « d'essuyer des plâtres » comme l'a fait l'Allemagne avec sa carte d'identité électronique, trop difficile à utiliser au quotidien et très onéreuse[2].

En ce qui concerne la fonction de l'e-ID et plus particulièrement la procédure de reconnaissance (et la certification) des systèmes e-ID, le renvoi aux procédures des plateformes de communication sécurisées dans les domaines des signatures électroniques et des procédures pénales, civiles et en matière de poursuites pour dettes et faillite (LP)[3] nous laisse perplexe.

---

[1] Cf. rapport explicatif relatif à l'avant-projet de Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID – ci-après « rapport explicatif »), pages 2 et 3

[2] Cf. rapport explicatif, page 15

En effet, en l'état, les **possibilités offertes par la loi sur la signature électronique (SCSE[4]) et ces plateformes sont peu ou mal utilisées,** notamment par les praticiens du droit. La **complexité** d'utilisation de celles-ci pour les utilisateurs et les problèmes de **sécurisation** des informations circulant via ces plateformes, nécessaire à la garantie de la **confidentialité** des contenus transmis, figurent parmi les principaux obstacles à une utilisation plus répandue.

Si la mise en place de l'e-ID se borne à renvoyer les utilisateurs à la SCSE et à ces procédures, sans amélioration notamment dans le sens d'une simplification, nous y voyons un **obstacle** majeur **à une large utilisation du système**, souhait exprimé par les auteurs du projet et partagé par notre Fédération.

C. 2. Commentaire article par article[5]

Ad. article 4 PL – Reconnaissance des fournisseurs d'identité (FI)

Notre Fédération décèle une difficulté en lien avec la **lettre a) de l'alinéa 2** de cette disposition.

En effet, cette disposition stipule que **seuls les FI qui ont leur siège social en Suisse** pourront être reconnu par l'organisme compétent.

Or, le rapport mentionne expressément[6] que *le Conseil fédéral s'est efforcé de ne pas exclure la possibilité de la notification au sens du règlement eIDAS. (...) les e-ID reconnus en Suisse pourront obtenir la reconnaissance européenne.* ***A cet effet, la conclusion d'un accord bilatéral avec l'UE ou chaque Etat membres sera nécessaire.***[7]

Ainsi, dans le contexte de la reconnaissance des e-ID, il est douteux que l'UE – ou l'Etat membre concerné – accepte celle-ci sans la reconnaissance en parallèle des FI européens en Suisse.

Ad. article 10 PL – Traitement et transmission des données

Notre Fédération salue la mention expresse figurant aux termes de cette disposition qui oblige l'obtention du **consentement du titulaire de l'e-ID pour la transmission des données** d'identification personnelles ainsi que le **traitement limité de ces données par l'Etat et les FI.**

Ad. article 11 PL – Expiration de la reconnaissance et 24 – Responsabilité

Nous nous interrogeons quant à la continuité de la responsabilité des FI en cas de cessation programmée de leurs activités, par exemple sous la forme **d'une responsabilité solidaire du FI qui cesse son activité et du FI qui la reprend.**

Par ailleurs, nous nous étonnons qu'outre la procédure de faillite, les procédures de sursis concordataire et de concordat par abandon d'actifs ne soient pas mentionnées.

---

[3] Cf. rapport explicatif, page 4
[4] RS 943.03
[5] Les dispositions non-mentionnées aux termes de la présente prise de position sont celles pour lesquelles la FER n'a pas de remarque à formuler
[6] Cf. rapport explicatif, page 40
[7] Ce sont les soussignés qui mettent en exergue

Nous proposons en conséquence que ces questions soit réglementées par analogie avec les articles 333 et suivants du Code des obligations (CO – transfert des rapports de travail) et 335k CO (absence de plan social obligatoire pendant une procédure de faillite ou de concordat).

Le renoncement, par les auteurs du projet, à instaurer une responsabilité causale à l'instar de celle prévue à l'art. 17 SCSE[8] nous apparaît en revanche positive, car incitative, notamment, pour le secteur privé pour proposer des services en qualité de FI.

Ad. article 12 PL – Mesures de surveillance et retrait de la reconnaissance

Notre Fédération estime que le libellé de l'alinéa 3 lettre d. de cette disposition n'est **pas assez dissuasif,** notamment en termes de protection de la population et de prévention contre la commission de nouvelles infractions.

Nous proposons en conséquence le libellé suivant : *Si une personne responsable, notamment des systèmes e-ID, a été condamnée par un jugement entré en force pour une infraction pénale.*

Ad. article 13 PL – Système e-ID subsidiaire de la Confédération

Cette disposition part du postulat qu'aucun acteur du secteur privé ne demande la reconnaissance de son système e-ID d'un niveau de garantie substantiel ou élevé.

Or, seule l'absence de **rentabilité** conduira, le cas échéant, un acteur privé à renoncer à demander la reconnaissance de son / ses système(s).

Par conséquent, il serait utile, en termes de prévisibilité budgétaire, de connaître **le coût** pour les contribuables suisses que générerait la reprise de ces activités par la Confédération elle-même.

Ad. article 17 PL – Devoirs (des fournisseurs d'identité)

Nous estimons, en ce qui concerne notamment l'alinéa 1 lettre c. de cette disposition, que les auteurs du PL n'ont pas suffisamment pris en compte les **contraintes de rentabilité** des potentiels acteurs privés intéressés à intervenir comme fournisseurs d'identité.

Le fait d'obliger les fournisseurs d'identité à démontrer en tout temps la validité des tous les e-ID qu'ils ont établis et permettre la vérification de ceux-ci de manière gratuite ne nous apparaît pas réaliste pour les entreprises concernées.

Notre Fédération souhaite donc la **suppression de la référence à la gratuité** aux termes de cette disposition.

Nous relevons en outre une erreur de dactylographie à l'alinéa 1 lettre d) : le renvoi à l'art. 4 al. 1 let. e doit être remplacé par un renvoi à l'art. 4 al. **2** let. e.

[8] loi sur la signature électronique, RS 943.03

En conclusion, notre Fédération émet un préavis favorable à cette loi e-ID **pour autant** qu'il soit tenu compte des remarques précitées, en particulier :

- Les expériences réalisées dans d'autres pays doivent servir de point de référence afin de ne pas commettre les mêmes erreurs ;
- Les coûts d'un tel dispositif ne doivent pas augmenter de manière disproportionnée ;
- Les besoins d'interopérabilité et d'évolutivité ainsi que le développement des services en situation de mobilité doivent faire partie de la réflexion dans son ensemble ;
- Les mesures sécuritaires doivent être intégrées dans l'ensemble des étapes de construction et d'exploitation d'un tel projet ;
- Il faudra veiller à une utilisation du système qui ne soit pas trop « lourd techniquement » pour les utilisateurs ;
- La reconnaissance parallèle des FI devra si possible être garantie entre la Suisse et les pays de l'UE, par exemple par la conclusion d'un accord bilatéral en la matière ;
- Des précisions devront être apportées sur la continuité de la responsabilité des FI en cas de cessation programmée de leurs activités ;
- La portée de l'article 12PL devrait être plus large afin que l'effet soit dissuasif ;
- Il sera nécessaire de tenir compte d'une manière plus approfondie des contraintes de rentabilité des potentiels acteurs privés intéressés à intervenir comme fournisseurs d'identité.

Nous vous remercions de l'attention que vous porterez à ce courrier et vous prions d'agréer, Madame, Monsieur, nos salutations les meilleures.

Blaise Matthey
Secrétaire général

Olivia Guyot Unger
Directrice à la FER Genève

Hervé Nicolier
Directeur à la FER Genève

Yannic Forney
Délégué

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Bundesamt für Justiz
Frau Sandra Eberle
Herr Urs Paul Holenstein
Bundesrain 20
3003 Bern

copiur@bj.admin.ch

Bern, 29. Mai 2017 sgv-Kl/ds

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

Sehr geehrte Frau Eberle
Sehr geehrter Herr Holenstein

Der Schweizerische Gewerbeverband sgv, die Nummer 1 der Schweizer KMU-Wirtschaft, vertritt 250 Verbände und gegen 300‘000 Unternehmen. Im Interesse der Schweizer KMU setzt sich der grösste Dachverband der Schweizer Wirtschaft für optimale wirtschaftliche und politische Rahmenbedingungen sowie für ein unternehmensfreundliches Umfeld ein.

Mit Schreiben vom 23. Februar 2017 lädt uns das Eidgenössische Justiz- und Polizeidepartement ein, zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung zu nehmen. Der Schweizerische Gewerbeverband sgv dankt für die Möglichkeit zur Stellungnahme.

Die vom Bundesrat vorgeschlagene Lösung zur elektronischen Identifikation einer Person strebt eine Aufgabenteilung zwischen Staat und Markt an. Geeignete private oder öffentliche Identitätsdienstleister werden gemäss bestimmter Kriterien vom Bund zur Ausstellung von staatlich anerkannten E-ID ermächtigt. Mit dem Vorentwurf wird ein Rechts- und Standardisierungsrahmen für die Anerkennung von E-ID-Systemen und die Anerkennung der Identitätsdienstleister geschaffen. Dieser ist so ausgestaltet, dass eine spätere gegenseitige Anerkennung der anerkannten E-ID-Systeme zwischen der Schweiz und der EU oder einzelner Mitgliedstaaten möglich bleibt. Dazu wären entsprechende bilaterale Verträge nötig. Bei der vorgeschlagenen Lösung übernimmt der Bund fünf Aufgaben. Erstens erarbeitet er die Rechtsgrundlagen und bewirkt Transparenz und Sicherheit. Zweitens definiert er einzuhaltende Standards sowie Sicherheits- und Interoperabilitätsanforderungen für den Betrieb eines E-ID-Systems. Drittens betreibt er eine elektronische Schnittstelle, über welche anerkannte Identitätsdienstleister staatlich geführte Personenidentifizierungsdaten beziehen können. Viertens anerkennt er Identitätsdienstleister und ihre E-ID-Systeme und fünftens beaufsichtigt er diese.

Der Schweizerische Gewerbeverband sgv unterstützt die Vorlage. Ihr liegt ein marktwirtschaftlicher Ansatz zugrunde. Die am Markt beste Lösung soll sich durchsetzen. Sollte der Bund eine zentrale, staatliche Lösung anstreben, verursacht dies nicht nur hohe Kosten, sondern es besteht die Gefahr, dass nicht der neuste Stand der Technik angewendet wird. Würde zudem durch den Staat eine einzige digitale ID

eingeführt, ist das Potenzial einer umfassenden Überwachung gross. Bei der vorgeschlagenen Lösung gibt der Bund lediglich die Leitplanken vor, überlässt das Vertriebsmodell aber dem Markt.

Bereits haben die Post und die SBB mit der SwissID eine elektronische ID lanciert. Ab Herbst 2017 sollen die Postkundinnen und Postkunden und ab 2018 alle Besitzerinnen und Besitzer des «SwissPass» eine ID erhalten. Swisscom, UBS und CS möchten ebenfalls eine elektronische ID lancieren.

Wir danken für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Hans-Ulrich Bigler
Direktor, Nationalrat

Dieter Kläy
Ressortleiter

Eberle Sandra BJ

Von: Kohler Muster Isabel - RE SO <Isabel.Kohler@santesuisse.ch>
Gesendet: Dienstag, 23. Mai 2017 14:53
An: _BJ-Copiur
Cc: Holenstein Urs Paul BJ; Eberle Sandra BJ
Betreff: E-ID-Gesetz; Stellungnahme santésuisse im Rahmen der Vernehmlassung

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Besten Dank für die Möglichkeit zur Stellungnahme zum E-ID-Gesetz.

Wir haben die Unterlagen innerhalb der santésuisse-Gruppe geprüft und können Ihnen mitteilen, dass wir keine Bemerkungen zur Vernehmlassung haben.

Danke für die Kenntnisnahme und

freundliche Grüsse

Isabel Kohler Muster
_____

santésuisse
Die Schweizer Krankenversicherer
Isabel Kohler Muster
Rechtsdienst
Leiterin Rechtsdienst
lic. iur., Fürsprecherin
Römerstrasse 20
4502 Solothurn

Tel. +41 32 625 4131
Fax +41 32 625 41 51
Isabel.Kohler@santesuisse.ch
www.santesuisse.ch
Blog: www.monsieur-sante.ch

SwissBanking

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

Basel, 26. Mai 2017
J.001 / AER

Stellungnahme der SBVg: Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 22. Februar 2017 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) betreffend Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz).

Wir bedanken uns für die Konsultation in dieser für die Finanzbranche sehr wichtigen Angelegenheit. Gerne nehmen wir die Gelegenheit zur Stellungnahme wahr und unterbreiten Ihnen nachfolgend unsere Anliegen.

Allgemeine Bemerkungen:

- Das im Vorentwurf (VE) zum E-ID-Gesetz realisierte Konzept nimmt eine grundsätzlich vernünftige und angemessene Aufteilung von Aufgaben, Kompetenzen und Verantwortlichkeiten zwischen staatlichen Stellen und privaten Unternehmen vor und regelt in wirtschaftsfreundlicher Art und Weise den Umgang mit der E-ID zur Identifizierung bzw. Authentifizierung natürlicher Personen.
- Gemäss unserem Verständnis stellt die E-ID nicht das digitale Pendant zu physischen Ausweisen dar. Vielmehr baut die E-ID auf diesen Dokumenten auf. Entsprechend begrüssen wir es, dass Informationen, welche über die staatlich geführten Personenidentifizierungsdaten hinausgehen, Teil einer E-ID sein können.
- Die in Art. 5 VE-E-ID-Gesetz festgehaltene Kaskade von E-ID-Sicherheitsniveaus ermöglicht es, branchenspezifisch adäquate Lösungen in Bezug auf das Verhältnis zwischen Sicherheit und Benutzerfreundlichkeit zu finden. Die diesbezüglichen, in der Verordnung festzulegenden Mindestanforderungen sind aufgrund des raschen technologischen Wandels konsequent prinzipienbasiert zu formulieren.
- Unsere Anträge beinhalten sowohl Präzisierungen zur Erhöhung der Rechtssicherheit als auch Vorschläge, die darauf abzielen, die Verbreitung und Akzeptanz von E-IDs auf dem Markt zu erleichtern (z.B. Verankerung des E-ID-Brokers).

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Postfach 4182
CH-4002 Basel

T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org

I. Würdigung der Stossrichtung

Wir begrüssen ausdrücklich die Stossrichtung und das im Vorentwurf (VE) zum E-ID-Gesetz realisierte Konzept. Das vorgeschlagene E-ID-Konzept nimmt eine grundsätzlich vernünftige und angemessene Aufteilung von Aufgaben, Kompetenzen und Verantwortlichkeiten zwischen staatlichen Stellen und privaten Unternehmen vor und regelt in flexibler und damit wirtschaftsfreundlicher Art und Weise den Umgang mit der E-ID zur Identifizierung bzw. Authentifizierung von natürlichen Personen in ihrer Funktion als Kommunikations- und Geschäftspartner.

Die von Art. 5 VE-E-ID-Gesetz vorgeschlagene Kaskade von E-ID-Sicherheitsniveaus ermöglicht es, branchenspezifisch adäquate Lösungen in Bezug auf das Verhältnis zwischen Sicherheit und Benutzerfreundlichkeit zu finden.

Sinnvoll ist auch, dass gemäss E-ID-Konzept die Herrschaft über die vollständigen Datensätze beim EJPD als gesetzlich definierter Identitätsstelle liegt (Art. 19f. VE-E-ID-Gesetz). Diese kann die Daten nur mit dem Einverständnis der antragstellenden Person herausgeben. Die Identity Provider (IdP) können, solange sie die Bewilligungsvoraussetzungen erfüllen (Art. 4), auf die funktionsgemäss notwendigen Datensätze zugreifen und die Aktualisierung der Datensätze sicherstellen (Art. 8).

Die verschiedenen E-ID-Systeme müssen sodann kompatibel sein (Art. 18). Im Ergebnis wird ein sinnvolles E-ID-System geschaffen, welches mit Blick auf das Verhältnis von Sicherheit und Benutzerfreundlichkeit mit der physischen Identitätskarte vergleichbar ist. Dies ist sinnvoll, da auch in der elektronischen Welt keine absolute Sicherheit, die es ohnehin nicht gibt, gefordert werden soll.

Die Bestimmungen des VE-E-ID-Gesetzes sind allesamt geeignet, den mannigfaltigen branchenspezifischen Bedürfnissen gerecht zu werden und angemessene praxistaugliche technische Lösungen zu entwickeln, die das Vertrauen in das neue E-ID-Konzept fördern. Dieses muss durch den Bund aktiv verbreitet werden, eine internationale Anerkennung der E-ID ist dabei zu gewährleisten.

Während das E-ID-Gesetz die Identifizierung bzw. Authentifizierung der Identität von Kommunikationspartnern regelt, enthält das ZertES – dazu ergänzend – die für den verbindlichen Rechtsverkehr notwendigen Bestimmungen in Bezug auf die Anforderungen und die Verwendung von digitalen Zertifikaten. Aus dem Zusammenspiel dieser Regeln ergibt sich ein in sich stimmiges Gesamtkonzept.

II. Zu den einzelnen Bestimmungen

Art. 1 Abs. 1 lit. b: Verwendete Bezeichnung „Identitätsdienstleistung“

Die verwendete Bezeichnung *„Identitätsdienstleistung“* ist nicht klar und muss unseres Erachtens in *„Identifizierungsdienstleistung“* umformuliert werden. Die Dienstleistungserbringung muss auf einer Tätigkeit basieren. Im Zusammenhang mit dem VE-E-ID-Gesetz kann es sich nur um die Erbringung von Dienstleistungen im Bereich Identifizierung natürlicher Personen handeln (vgl. Definition des Begriffs *„Identifizierung“* in Art. 2 lit. d VE-E-ID-Gesetz). Art. 1 Abs. 1 lit. b muss daher wie folgt lauten:

> *„die Anerkennung der Anbieter von Identifizierungsdienstleistungen ~~Identitätsdienstleistungen~~ und ihrer E-ID-Systeme sowie die Aufsicht über diese Anbieter und Systeme;“*

Art. 1 Abs. 2 lit. b: Weite Verbreitung als Zweck

Mit Blick auf die bisherigen Erfahrungen mit ähnlichen Instrumenten (z.B. elektronische Signatur) sollte eine möglichst umfassende Verbreitung der anerkannten E-ID als definierter Zweck in das VE-E-ID-Gesetz aufgenommen werden. Eine rege Inanspruchnahme durch die Bevölkerung bedingt einerseits eine einfache, aber dennoch sichere Handhabung der E-ID, und andererseits ein möglichst weites Anwendungsfeld derselben. Letzteres umfasst sowohl den öffentlichen als auch den privaten Sektor. Dem erweiterten Zweck sollte insbesondere auch der Bundesrat bei der Ausarbeitung der entsprechenden Verordnung Rechnung tragen.

> *„eine weite Verbreitung, die Standardisierung und die Interoperabilität der E-ID sicherzustellen.“*

Art. 1 Abs. 3^{neu}: Orientierung an internationalen Standards

Eine Orientierung des E-ID-Gesetzes an internationalen Standards ist zwingend, um auch die Interoperabilität mit ausländischen Lösungen (insbesondere mit jenen der EU-Mitgliedstaaten) sicherzustellen. Wir regen daher an, solche Standards – wo möglich und sinnvoll – auch im schweizerischen Recht abzubilden.

> *„Es orientiert sich dabei an internationalen Standards.“*

Art. 2 lit. c: Erweiterung des Kreises der IdP um staatliche Stellen

Der Vorentwurf des E-ID-Gesetzes sieht als IdP nur private Anbieter vor, die – sofern sie bestimmte Kriterien erfüllen – eine Bewilligung erhalten (Art. 4). Dieses Bewilligungskonzept schliesst nicht aus, parallel dazu auch geeignete staatliche Stellen zur Sicherstellung der Systemkontinuität (vgl. dazu unsere Ausführungen zu Art. 13 Abs. 1 VE-E-ID-Gesetz) mit derselben Funktion zu betrauen. Demzufolge empfehlen wir, die Gesetzessystematik dahingehend anzupassen, dass neben bewilligten privaten Unternehmen auch geeignete staatliche Stellen die Funktion des IdP wahrnehmen können.

In Bezug auf die Bezeichnung „Identifizierungsdienstleistungen“ verweisen wir auf unsere Ausführungen zu Art. 1 Abs. 1 lit. b.

Der korrigierte Buchstabe lautet sodann:

> *„Identity Provider (IdP): nach diesem Gesetz anerkannter Anbieter von Identifizierungsdienstleistungen ~~Identitätsdienstleistungen~~; diese können privatrechtlich oder staatlich organisiert sein;“*

Art. 2 lit. l^{neu}: Aufnahme der Bezeichnung „E-ID-Broker“

Mit Blick auf eine möglichst umfassende Verbreitung der anerkannten E-ID regen wir an, die Funktion eines E-ID-Brokers analog dem etablierten Kreditkartensystem im Gesetzestext zu verankern. Ein E-ID-Broker fungiert als Vermittler zwischen IdP und E-ID-verwendenden Diensten. Eine solche Ausgestaltung der E-ID-Infrastruktur stellt insofern eine gewichtige Erleichterung für den E-ID-verwendenden Dienst dar, als lediglich eine vertragliche Vereinbarung und eine technische Verbindung, namentlich jene zum E-ID-Broker, zu unterhalten sind, womit das mehrfache Abschliessen von Vereinbarungen gemäss Art. 15 VE-E-ID-Gesetz entfallen kann. Die Sicherstellung der Verbindungen zu den IdP obliegt sodann dem E-ID-Broker.

Die Zwischenschaltung eines privaten E-ID-Brokers ist allerdings nicht zwingend, die Anbindung der E-ID-verwendenden Dienste an die IdP kann auch direkt erfolgen.

> *„E-ID-Broker: stellt die Verbindung zwischen den E-ID-verwendenden Diensten und den IdP her.“*

Art. 2 lit. k^{neu}: Aufnahme der Bezeichnung „Identitätsattribute“

Gesetzesentwurf und erläuternder Bericht gehen davon aus, dass neben den von der Identitätsstelle zum Abgleich der Daten zur Verfügung gestellten Identitätsmerkmalen auch noch weitere Identitätsattribute mit der E-ID verbunden werden können. Dies ist unseres Erachtens sinnvoll und könnte einen wichtigen Beitrag zur Verbreitung der E-ID leisten. Um dies noch klarer zum Ausdruck zu bringen, schlagen wir vor, den Begriff *„Identitätsattribute“* entsprechend zu definieren.

> *„Identitätsattribute: Weitere Identitätsmerkmale, die einer E-ID zugeordnet werden können und nicht bereits von der Identitätsstelle zur Verfügung gestellt werden.“*

Art. 3 Abs. 2: Alternative Verfahren zur elektronischen Identifizierung

Wir regen an, die in Art. 3 Abs. 2 VE-ID-Gesetz vorgesehenen alternativen Verfahren zur elektronischen Identifizierung und Authentifizierung bereits auf Gesetzesstufe zu definieren.

Art. 3 Abs. 3: Entsperrung einer E-ID

Neben der Sperrung wirf auch die Entsperrung einer E-ID Fragen auf, die vom Bundesrat adressiert werden sollten (z.B. Zeitpunkt und Voraussetzung der Entsperrung). Wir regen daher folgende Ergänzung von Absatz 3 an:

> *„Der Bundesrat regelt die Voraussetzung zum Bezug, den Ausstellungsprozess sowie die Sperrung, die Entsperrung und den Widerruf einer E-ID."*

Art. 4 Abs. 1 und 2: Anerkennung von IdP und E-ID-Broker

Wird im Gesetzestext der Begriff des E-ID-Brokers definiert, so sind die in Art. 4 normierten Anerkennungsvorschriften für IdP auch auf die E-ID-Broker auszudehnen. Die korrigierten Absätze 1 und 2 lauten sodann:

> *„IdP, die E-ID ausstellen wollen, und E-ID-Broker brauchen eine Anerkennung der Anerkennungsstelle (Art. 21)."* (Abs. 1)
>
> *„IdP und E-ID-Broker werden anerkannt, wenn sie: (…)"* (Abs. 2)

Art. 4 Abs. 2 lit. f: Haltung und Bearbeitung von E-ID-System-Daten

Gemäss Art. 4 Abs. 2 lit. f VE-E-ID-Gesetz müssen E-ID-System-Daten in der Schweiz sowie nach schweizerischem Recht gehalten und bearbeitet werden. Unseres Erachtens wird diese derart absolut formulierte Voraussetzung der Realität nicht gerecht (z.B. Cloud-Lösungen). Wir regen diesbezüglich eine grössere Flexibilität an.

Zudem sollten auch ausländische Betreiber von E-ID-verwendenden Diensten in der Schweiz zugelassen werden, was zwangsläufig einen gewissen transnationalen Datenverkehr voraussetzt. Mit Blick auf die grenzüberschreitende Interoperabilität sollte das Gesetz daher lediglich festhalten, dass das vom schweizerischen Recht vorgegebene Niveau an Datensicherheit und Datenschutz einzuhalten ist.

> *„die E-ID-System-Daten auf demjenigen ~~in der~~ für die Schweiz vorgeschriebenen Niveau an Datenschutz und Datensicherheit ~~nach schweizerischem Recht~~ halten und bearbeiten, welches die Durchsetzung der in der Schweiz geltenden Rechtsansprüche jederzeit gewährleistet;"*

Art. 4 Abs. 3^{neu}: Anpassung des Gesetzestextes im Hinblick auf die Integration von staatlichen Stellen als IdP

Wird im Gesetzestext definiert, dass auch staatliche Stellen als IdP anerkannt werden können (vgl. unsere Anmerkungen zu Art. 2 lit. c VE-E-ID-Gesetz), so entfällt für diese die Anerkennungsvoraussetzung des Art. 4 Abs. 2 lit. b VE-E-ID-Gesetz. Wir regen diesbezüglich die Einfügung eines neuen Abs. 3 an:

> *„Handelt es sich beim IdP um eine Verwaltungseinheit des Bundes oder eine staatliche Stelle, so entfällt die Anerkennungsvoraussetzung des Abs. 2 lit. b."*

Art. 5: Anforderungen an die verschiedenen Sicherheitsniveaus

Grundsätzlich begrüssen wir die branchenspezifisch flexibel anwendbare, in Art. 5 VE-E-ID-Gesetz vorgeschlagene Kaskade unterschiedlicher Sicherheitsniveaus. Die Mindestanforderungen für jede Sicherheitsstufe sind in einer Verordnung festzulegen (Art. 5 Abs. 4).

Dabei ist dem Umstand Rechnung zu tragen, dass Begriffe wie *„Sicherheit“* oder *„Stand der Technik“* sachlogisch dynamisch sind und sich entsprechend der fortschreitenden technischen Erkenntnisse laufend verändern. Demzufolge ist es unbedingt notwendig, dass die Mindestanforderungen auf Verordnungsstufe konsequent prinzipienbasiert formuliert werden. Dadurch wird einerseits der Dynamik des Themas Rechnung getragen. Andererseits wird jede Branche in die Lage versetzt, unter Anwendung von vernünftigen Ermessenserwägungen eine Lösung zu implementieren, welche der Grösse, der Komplexität, der Struktur und dem Risikoprofil des verwendeten Geschäftsmodells gerecht wird. Allzu starre regelbasierte Mindestanforderungen würden demgegenüber einen massiven unnötigen Aufwand für die in der Wirtschaftskette beteiligten privaten Marktteilnehmer generieren, ohne dass damit tatsächlich mehr Sicherheit gewonnen würde.

Wir würden es begrüssen, wenn auch im Hinblick auf die finale Fassung der Verordnung eine Konsultation der Wirtschaft erfolgt.

Art. 6 Abs. 2: Prüfung der persönlichen Voraussetzungen

In Bezug auf die persönlichen Voraussetzungen, die ein Antragsteller erfüllen muss, sollte in Art. 6 Abs. 2 VE-E-ID-Gesetz auf Art. 3 verwiesen werden. Der korrigierte Absatz lautet sodann:

> *„Der IdP überprüft die persönlichen Voraussetzungen gemäss Artikel 3.“*

Art. 7 Abs. 2: Technologieneutralität in Bezug auf Personenidentifizierungsdaten

Art. 7 Abs. 2 VE-E-ID-Gesetz nennt die Personenidentifizierungsdaten, welche für die Sicherheitsniveaus *„substantiell“* und *„hoch“* verwendet werden können. Diese Aufzählung ist abschliessend. Vor dem Hintergrund der ausdrücklich angestrebten Technologieneutralität sowie möglicher technologischer Entwicklungen (z.B. Verwendung von Stimmklangmustern oder biometrischen Daten) erscheint es sachgemäss, eine nicht abschliessende Aufzählung in Art. 7 Abs. 2 aufzunehmen oder die Aufzählung auf Verordnungsstufe zu regeln.

Art. 7 Abs. 4: Zuordnung von Daten durch den IdP

Gemäss Art. 7 Abs. 4 VE-E-ID-Gesetz kann der IdP einer E-ID neben den bereits in Abs. 1 bis 3 genannten Daten weitere Angaben zuordnen. In Übereinstimmung mit dem von uns vorgeschlagenen Art. 2 lit. k^{neu} sollte Art. 7 Abs. 4 wie folgt formuliert werden:

> *„Der IdP kann einer E-ID mit Einverständnis der Inhaberin oder des Inhabers der E-ID weitere Daten (Identitätsattribute) zuordnen.“*

Art. 8 Abs. 1: Aktualisierung der Personenidentifizierungsdaten

In Bezug auf den Begriff der *„Aktualisierung“* ist unklar, ob die Datensätze bei deren Abfrage überschrieben werden können oder ob es zu diesem Zweck eines Logs bedarf, welcher die Nachverfolgung der Historie gewährleistet. Wir bitten diesbezüglich um Klarstellung.

Art. 8 Abs. 2: Sperrung der E-ID

Es bestehen Unklarheiten hinsichtlich des Verfahrens zur Sperrung von E-ID sowie der diesbezüglichen Verantwortlichkeiten. Wir regen deshalb folgende Präzisierung des Absatzes an:

> *~~„Er ist verantwortlich, dass von ihm ausgestellt E-ID umgehend gesperrt oder widerrufen werden, wenn die E-ID-Registrierungsnummer nicht mehr verwendet werden darf.~~ Gesperrte oder nicht mehr aktive E-ID-Registriernummern werden seitens der Identitätsstelle umgehend den IdP gemeldet. Der IdP sperrt daraufhin von ihm ausgestellte E-ID.*

Ferner bitten wir, klarzustellen, dass es sich bei der Sperrung lediglich um die Deaktivierung der Datensätze unter Wahrung der gesetzlichen Aufbewahrungspflicht von 10 Jahren handeln kann. Unseres Erachtens ist analog den bewährten Prozessen bei Kredit- und Debitkarten zu verfahren. Demzufolge ist die fragliche E-ID, wenn sie nicht mehr benötigt wird, zu deaktivieren.

Art. 9 Abs. 1: Verwendung der Versichertennummer durch die Identitätsstelle

In Bezug auf die *„Versichertennummer“* sollte in Art. 9 Abs. 1 VE-E-ID-Gesetz auf Art. 7 Abs. 2 verwiesen werden. Der korrigierte Absatz lautet sodann:

> *„Die Identitätsstelle ist berechtigt, die Versichertennummer gemäss Art. 7 Abs. 2 systematisch zur Identifizierung von Personen beim elektronischen Datenaustausch mit den Personenregistern nach Artikel 20 Absatz 2 zu verwenden.“*

Art. 10 Abs. 2: Minimale Sicherheitsanforderungen an E-ID-verwendende Dienste

Wir sind der Meinung, dass ein E-ID-verwendender Dienst Personenidentifizierungsdaten der höheren Sicherheitsniveaus nur dann anfordern (und erhalten) darf, wenn er selber gewisse minimale Sicherheitsvorgaben erfüllt. Diese Vorgaben sind im Rahmen des Ausführungsrechts zu definieren.

Wir empfehlen die folgende Ergänzung von Artikel 10 Abs. 2 VE-E-ID-Gesetz:

> *„Sie dürfen Betreiberinnen von E-ID-verwendenden Diensten nur die Personenidentifizierungsdaten weitergeben, die dem geforderten und implementierten Sicherheitsniveau entsprechen und von der Inhaberin oder dem Inhaber der E-ID freigegeben sind“.*

Art. 10 Abs. 3: Sicherstellung von Vertraulichkeit für sämtliche Datensätze

Die von Art. 10 Abs. 3 VE-E-ID-Gesetz aufgestellte Regel ist nicht überzeugend. Das E-ID-System setzt sich nur durch, wenn seine Nutzer und alle weiteren direkt oder indirekt betroffenen Personen darauf vertrauen können, dass sämtliche verwendeten Daten vernünftigen Vertraulichkeitsregeln unterstehen. Das Verbot, lediglich die unter Art. 7 Abs. 2 VE-E-ID-Gesetz aufgeführten Daten (und die darauf basierenden Nutzungsprofile) Dritten bekannt zu geben, reicht nicht aus. Auch die Daten gemäss Art. 7 Abs. 1 benötigen gesetzlichen Vertraulichkeitsschutz. Bereits mit Bezug auf den amtlichen Namen und Vornamen bestehen i.d.R. legitime Geheimhaltungsinteressen. Die meisten Personen legen generell Wert auf Vertraulichkeit mit Bezug auf die Frage, mit welchen anderen Personen sie zu welchem Zweck welche Daten austauschen. Umso mehr gilt dies für die weiteren in Art. 7 Abs. 1 aufgeführten Daten *„E-ID-Registrierungsnummer“* und *„Geburtsdatum“*. Diese zusätzlichen Angaben identifizieren die betroffene Person eindeutig und beinhalten gerade deshalb ein erhebliches Fälschungs- und Missbrauchspotential. Gleiches gilt für allfällige zusätzliche Daten gemäss Art. 10 Abs. 3 und 4 VE-E-ID-Gesetz. Das Verbot der Bekanntgabe an Dritte muss sich demzufolge auf sämtliche in Art. 7 VE-E-ID-Gesetz geregelten Daten erstrecken. Dies ist auch deshalb richtig, weil andernfalls mit Bezug auf sämtliche in Art. 10 Abs. 2 nicht erwähnten Datensätze ein freier Datenhandel ermöglicht würde (argumentum e contrario), an welchem sich ein IdP oder eine Betreiberin von E-ID-verwendenden Diensten auf Kosten der betroffenen Personen sogar bereichern könnten. Dies widerspricht den grundsätzlichsten Anforderungen an einen vernünftigen Datenschutz.

Moderne Informatikanwendungen umfassen häufig IT-Systeme, die über mehrere Organisationen verteilt sind. Die Weitergabe von Personenidentifizierungsdaten über verteilte Applikationskomponenten (und somit Organisationen) hinweg (sog. „Identity Propagation“) ist ein wesentliches Element solcher Anwendungen und eine Kernfunktionalität von beispielsweise SAML. Die dafür notwendige Weitergabe von Personenidentifizierungsdaten ist aber nicht pauschal direkt im VE-E-ID-Gesetz zu regeln, sondern innerhalb der bestehenden Leitplanken gemäss Spezialgesetzen wie z.B. BankG und DSG mit geeigneter Information bzw. Vertragsgestaltung zu bewerkstelligen. Somit ist Art. 10 Abs. 3 VE-E-ID Gesetz wie folgt anzupassen:

> *„Weder anerkannte IdP noch Betreiberinnen von E-ID-verwendenden Diensten dürfen die Personenidentifizierungsdaten gemäss Artikel 7 ~~Absatz 1~~ Absätze 1 bis 4 oder die darauf basierenden Nutzungsprofile Dritten bekannt geben.“*

Art. 12 Abs. 3 lit. d: Aufhebung der Einschränkung auf Internetkriminalität

In Bezug auf die Sicherheitsanforderungen betreffend die für die E-ID-Systeme verantwortlichen Personen besteht unseres Erachtens eine Diskrepanz zwischen Art. 4 Abs. 2 lit. c und Art. 12 Abs. 3 lit. d VE-E-ID-Gesetz.

Für die Anerkennung eines IdP muss der Nachweis erbracht werden, dass die verantwortlichen Personen kein Risiko für die Sicherheit darstellen. Gemäss den Ausführungen im erläuternden Bericht (S. 28f.) kann dieser Nachweis durch die Einholung eines Strafregisterauszugs erfolgen. In diesem sind sämtliche Strafregistereinträge enthalten. Ein Entzug der Anerkennung des IdP kann hingegen ausgesprochen werden, wenn eine rechtskräftige Verurteilung einer verantwortlichen Person im Zusammenhang mit Internetkriminalität vorliegt. Rechtskräftige Verurteilungen z.B. im Bereich von Vermö-

gensdelikten können ebenso gut ein Risiko für die Sicherheit innerhalb eines IdP darstellen, dies umso mehr als es um die Bearbeitung von Personendaten geht. Daher sollte der Text nicht auf Fälle von Internetkriminalität beschränkt werden. Wir schlagen daher vor, Art. 12 Abs. 3 lit. d VE-E-ID-Gesetz wie folgt anzupassen:

> *„bei rechtskräftiger Verurteilung der für die E-ID-Systeme verantwortlichen Personen aufgrund von Straftaten, die ein Risiko für die Sicherheit bedeuten können ~~mit Internetkriminalität in Zusammenhang stehen~~."*

Art. 13 Abs. 1: Sicherstellung von Systemkontinuität durch subsidiäres E-ID-System des Bundes

Für den Fall, dass kein IdP für die Ausstellung der Sicherheitsniveaus *„substanziell"* oder *„hoch"* anerkannt ist, sieht Art. 13 Abs. 1 VE-E-ID-Gesetz lediglich vor, dass der Bundesrat den Betrieb durch eine Bundesbehörde vorsehen kann.

Die Sicherheitsniveaus *„substanziell"* und *„hoch"* sind für die breite Akzeptanz des E-ID-Konzeptes durch die Wirtschaft von entscheidender Bedeutung. Dies trifft in besonderem Masse auf die Finanzdienstleistungsbranche zu, deren Akteure gemäss zahlreichen aufsichtsrechtlichen Vorgaben alle Daten, anhand welcher Kunden direkt oder indirekt identifiziert werden können, streng vor unberechtigter Einsichtnahme Dritter zu schützen haben (vgl. insbesondere Bankkundengeheimnis gemäss Art. 47 BankG und die Anforderungen von FINMA-RS 2008/21 operationelle Risiken Banken, insbesondere Anhang 3). Damit sich das E-ID-Konzept im Markt durchsetzt, muss sichergestellt sein, dass diese qualifizierten Sicherheitsniveaus tatsächlich und dauernd zur Verfügung stehen, insbesondere auch dann, wenn sich ein anerkannter IdP aus dem Markt zurückziehen sollte. Dies lässt sich nur dadurch bewerkstelligen, dass die blosse Kann-Vorschrift durch eine Muss-Vorschrift ersetzt wird und jene den Bedürfnissen von Inhaberinnen und Inhabern einer E-ID als solchen Rechnung trägt. Demzufolge ist Art. 13 Abs. 1 VE E-ID Gesetz wie folgt anzupassen:

> *„Falls kein IdP für die Ausstellung von E-ID der Sicherheitsniveaus substantiell oder hoch anerkannt ist, ~~kann~~ bezeichnet der Bundesrat eine Verwaltungseinheit ~~bezeichnen~~, die für die Bedürfnisse ~~von Behörden~~ von Inhaberinnen und Inhabern einer E-ID ein E-ID-System betreibt und eine E-ID herausgibt."*

Art. 14 Abs. 2bis: Pflichten der Inhaberinnen und Inhaber von E-ID

Üblicherweise wird die Inhaberin oder der Inhaber einer E-ID zuerst feststellen, wenn ein Missbrauch der E-ID droht. Damit der IdP umgehend die notwendigen Massnahmen ergreifen kann, ist es der Inhaberin oder dem Inhaber einer E-ID zuzumuten, dem IdP eine solche Feststellung zu melden.

> *„Die Inhaberin oder der Inhaber einer E-ID meldet dem IdP, wenn Anhaltspunkte für einen Missbrauch oder die Benutzung der E-ID durch Unbefugte bestehen."*

Art. 15: Vereinbarung mit IdP

Wird im Gesetzestext der Begriff des E-ID-Brokers definiert, so ist Art. 15 VE-E-ID-Gesetz dahingehend anzupassen, als dass die Betreiberinnen von E-ID-verwendenden Diensten die entsprechende Vereinbarung entweder mit jedem IdP direkt oder mit dem E-ID-Broker schliessen.

> *„Wer einen E-ID-verwendenden Dienst betreiben will, braucht eine Vereinbarung mit einem IdP oder einem E-ID-Broker. Die Vereinbarung regelt insbesondere: (…)“*

Art. 17 Abs. 1 lit. g: Löschen der Daten nach sechs Monaten

Die in Art. 17 Abs. 1 lit. g VE-E-ID-Gesetz normierte Pflicht zur Löschung der Daten über die Anwendung einer E-ID nach sechs Monaten steht im Widerspruch zur gesetzlichen Datenaufbewahrungspflicht von 10 Jahren. Richtigerweise muss die Anforderung lauten, dass die Daten unter Wahrung der Aufbewahrungspflicht nach sechs Monaten nicht mehr zugänglich sein dürfen. Wir schlagen daher vor, Art. 17 Abs. 1 lit. g VE-E-ID-Gesetz wie folgt zu ändern:

> *~~„Er löscht die Daten über die Anwendung einer E-ID nach sechs Monaten.~~ Die Daten über die Anwendung einer E-ID müssen nach sechs Monaten unzugänglich gemacht worden sein. Der IdP hat alle Daten im Rahmen der Datenaufbewahrungspflichten aufzubewahren.“*

Art. 17 Abs. 1 lit. h^{neu}: Einverständnis bei der Übermittlung von Identitätsattributen

Da es sich bei Identitätsattributen um sensible Daten handeln kann, empfehlen wir, die Übermittlung derselben vom Einverständnis des E-ID-Inhabers abhängig zu machen.

> *„Bei jeder Übermittlung von Identitätsattributen an Betreiberinnen von E-ID-verwendenden Diensten ist das Einverständnis der Inhaberin oder des Inhabers der E-ID notwendig.“*

Art. 17 Abs. 2: Kundendienst

Meldungen über Störungen oder den Verlust einer E-ID müssen ordnungsgemäss entgegengenommen und bearbeitet werden können. Die Ausgestaltung eines entsprechenden Verfahrens sollte allerdings dem IdP vorbehalten bleiben. Er orientiert sich dabei am internationalen Standard.

> *„Er ~~sorgt für einen Kundendienst, der es erlaubt~~ organisiert sich so, dass Meldungen über Störungen oder Verlust einer E-ID entgegengenommen und bearbeitet werden können ~~entgegenzunehmen und zu bearbeiten~~. Er meldet Fehler in den Personenidentifizierungsdaten der Identitätsstelle.“*

Art. 18 Abs. 1: Interoperabilität durch E-ID-Broker

Neben den IdP sorgen insbesondere die E-ID-Broker für die zur Verbreitung der E-ID zwingend notwendige Interoperabilität von E-ID-Systemen. Entsprechend regen wir an, Art. 18 Abs. 1 VE-E-ID-Gesetz um den Begriff des E-ID-Brokers zu erweitern.

> *„IdP und E-ID-Broker ~~akzeptieren~~ sorgen dafür, dass ihre E-ID-Systeme gegenseitig akzeptiert werden und stellen sicher, dass die E-ID-Systeme interoperabel sind."*

Art. 18 Abs. 2: Interoperabilität durch Orientierung an internationalen Standards

Vgl. unsere Ausführungen zu Art. Art. 1 Abs. 3^{neu}.

> *„Der Bundesrat bestimmt die technischen Standards und definiert die Schnittstellen. Er orientiert sich dabei an internationalen Standards."*

Art. 20 Abs. 2: An das Informationssystem der Identitätsstelle gekoppelte Personenregister

Gemäss den Angaben im erläuternden Bericht (S. 32f.) hat aktuell nur der Bund Zugriff auf die in Art. 20 Abs. 2 VE-E-ID-Gesetz abschliessend aufgeführten Personenregister.

Wir würden es begrüssen, wenn das Informationssystem der Identitätsstelle zukünftig an weitere Register auf Ebene des Bundes (z.B. Register der Urkundspersonen, UPREG) und der Kantone und Gemeinden (z.B. Einwohnerregister, Handelsregister) angebunden wird. Die dadurch erreichte Ausweitung der von der Identitätsstelle zugeordneten Personenidentifizierungsdaten (z.B. auf die amtliche Wohnadresse) wäre wohl effizienter als die Zuordnung dieser Identitätsattribute separat durch jeden IdP. Beispielsweise würde diese Ausweitung der laufend aktualisierten Datenbasis einem IdP ermöglichen, zum Zweck der Bekämpfung der Geldwäscherei auf regelmässiger Basis die aktuellen Domiziladressinformationen zu verifizieren.

Art. 9 Abs. 1bis ZertES (im Anhang zum VE-E-ID-Gesetz)

Die im Zusammenhang mit dem neuen E-ID-Gesetz geplante Änderung des Bundesgesetzes über die elektronische Signatur (ZertES) sieht im vorgeschlagenen Art. 9 Abs. 1bis ZertES vor, dass bei Verwendung einer E-ID die persönliche Vorsprache generell entfällt. Dies geht sachlich zu weit. Aus dem Zusammenspiel von tiefem Sicherheitsniveau und Verzicht auf persönliche Vorsprache kann eine bestimmte Person nicht eindeutig identifiziert bzw. authentifiziert werden. Daraus entstehen massive Risiken, dass eine auf dieser Basis ausgestellte E-ID missbräuchlich oder zu rechtswidrigen Zwecken verwendet wird. Dementsprechend widerspräche eine auf solch schwacher Basis ausgestellte E-ID auch den einschlägigen Vorgaben des Bankenaufsichtsrecht und der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Korruption (vgl. z.B. Art. 4 ff. VSB 16).

Die von Art. 9 Abs. 1bis ZertES angeordnete Rechtsfolge darf sich demzufolge nur auf die Sicherheitsniveaus *„substanziell"* und *„hoch"*, nicht aber auf das tiefste Sicherheitsniveau *„niedrig"* erstrecken. Art. 9 Abs. 1bis ZertES ist somit wie folgt anzupassen:

„Wird der Identitätsnachweis durch eine E-ID gemäss E-ID Gesetz vom … erbracht, entfällt bei Verwendung des Sicherheitsniveaus hoch oder substanziell die persönliche Vorsprache.“

Mit dieser Regelung wird eine neue Ausnahme vom Grundsatz des persönlichen Erscheinens gemäss Art. 9 Abs. 1 lit. a ZertES geschaffen. Die übrigen diesbezüglichen Ausnahmen finden sich in Art. 7 Abs. 2 VZertES. Insofern wäre es systematisch überzeugender, genannte Ausnahme ebenfalls in Art. 7 VZertES statt in Art. 9 ZertES zu regeln.

III. Ergänzende Bemerkungen

Unternehmensinterne Anwendung von E-ID-Systemen

Im erläuternden Bericht (S. 34) zu Art. 23 VE-E-ID-Gesetz zum Thema *„Gebühren“* wird erwähnt, dass Unternehmen die Identifizierung ihrer Mitarbeitenden an einen anerkannten IdP auslagern und dessen E-ID-System für die Authentifizierung an ihrer IKT-Infrastruktur nutzen könnten.

Wir empfehlen die Ausweitung dieses Ansatzes wie folgt: Es geht für Unternehmen nicht nur um die „Authentifizierung an ihrer IKT-Infrastruktur“ sondern generell um die „Authentifizierung an der von ihnen genutzten IKT-Infrastruktur“. Dies schliesst insbesondere IKT-Anwendungen mit ein, die den Unternehmensmitarbeitenden im Internet (bzw. in einer „Cloud“) zur Verfügung gestellt werden.

Gleichzeitig weisen wir darauf hin, dass ein E-ID-System für die Nutzung im Unternehmen verschiedene Anforderungen erfüllen muss, die bei der privaten Nutzung so nicht gelten:

- Für eine unternehmensinterne Anwendung muss die E-ID eines Mitarbeitenden zwingend das Unternehmen als Attribut enthalten und dieses Attribut muss jedem E-ID-verwendenden Dienst übermittelt werden;
- Das Unternehmen muss die Möglichkeit haben, die Nutzung einer solchen E-ID auf definierte E-ID-verwendende Dienste einzuschränken (Grob-Autorisierung) und gegebenenfalls gänzlich zu sperren;
- Zudem muss es die Nutzung einer solchen E-ID pro E-ID-verwendenden Dienst auf einen Zugriffskontext einschränken können (Beispiel: Mitarbeitende dürfen die E-ID aus dem Unternehmensnetzwerk heraus nutzen, nicht aber über ein mit dem Internet verbundenes privates Gerät);
- Schliesslich muss das Unternehmen die Möglichkeit haben, die Ausstellungs- und Pflegeprozesse für die E-ID auf die unternehmensinternen Gegebenheiten anzupassen. Dies bezieht sich einerseits auf bestehende HR-Prozesse (für die Ausstellung und Sperrung einer E-ID), vor allem aber auf effiziente, sichere und benutzerfreundliche unternehmensinterne Prozesse für die Wiederbeschaffung von vergessenen, verlorenen oder defekten Authentifizierungsfaktoren.

Nutzung von Personendaten im sogenannten „Internet of Things“

Die Übertragung von Identitätsdaten an autonom agierende (persönliche) Geräte (bzw. Dinge im „Internet of Things“ [IoT]) ist ein langfristig gesehen wichtiges Thema, das im E-ID-Gesetz adressiert werden sollte. Der Standard eCH-0107 „Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM)“ wird diese Thematik in der Version 3 ebenfalls aufnehmen.

Zu überlegen ist, ob dieses Thema an geeigneter Stelle in diesem Gesetz oder in einer anderen Vorschrift sinnvoll zu regeln ist. Der Kern der Regelung könnte wie folgt lauten: Werden Personendaten einer E-ID einem Gerät zum Gebrauch überlassen, bleibt der Inhaber der E-ID für deren Nutzung verantwortlich.

SwissBanking

***

Wir bedanken uns für die wohlwollende Prüfung unserer Kommentare und Anliegen. Für allfällige Rückfragen oder eine vertiefte Erörterung unserer Stellungnahme stehen wir Ihnen selbstverständlich jederzeit gerne zur Verfügung.

Freundliche Grüsse
Schweizerische Bankiervereinigung

Andrew Ertl Martin Hess

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

31. Mai 2017

Frau Bundesrätin Simonetta Sommaruga
Vorsteherin EJPD
Bundeshaus West
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

Stellungnahme in der Vernehmlassung zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Im Januar 2017 haben Sie die interessierten Kreise eingeladen, zum Vorentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung zu nehmen. Diese Gelegenheit der Meinungsäusserung nehmen wir gerne wahr. Als Fachverband, der sich für gute Rahmenbedingungen für die international tätige Wirtschaft der Schweiz einsetzt, beachtet SwissHoldings übergeordnete, tendenziell gesamtwirtschaftliche Aspekte und zieht diese in ihre Überlegungen mit ein.

Haltung von SwissHoldings:

1. Die schweizerischen Unternehmen sind auf klare, liberale und zukunftsgerichtete Rahmenbedingungen für die digitale Wirtschaft angewiesen. In diesem Kontext nimmt das rechtssichere Management von elektronischen Identitäten und damit verbunden die Möglichkeit zur effizienten Authentifizierung eine zentrale Rolle ein.
2. Dem Rechtssetzungsvorhaben wird grundsätzlich zugestimmt. Eine kohärente regulatorische Basis für das Verwalten von E-Identitäten stellt auch einen gewichtigen Vorteil für den Wirtschaftsstandort Schweiz dar.
3. Es ist richtig, dem privaten Sektor bei der Verwaltung auch von e-Identitäten eine bedeutende Rolle zuzuordnen. Dabei muss aber ein möglichst freier Wettbewerb erhalten bleiben.
4. Der Einsatz von E-Identitäten muss dabei freiwillig bleiben. Zugleich soll die E-Identität gegenüber allen anderen Methoden der Identitätsfeststellung als gleichwertig gelten.
5. Die Begrifflichkeiten des neuen E-ID Gesetzes sind weitestmöglich mit denjenigen unter der europäischen eIDAS-Verordnung und der schon bestehenden schweize-

Nägeligasse 13, Postfach
CH-3001 Bern, Switzerland
www.swissholdings.ch
Phone +41 31 356 68 68
Fax +41 31 352 32 55
sh@swissholdings.ch

rischen Gesetzgebung über die elektronische Signatur (ZertES) abzustimmen beziehungsweise zu vereinheitlichen.

A. Grundsätzliche Bemerkungen

SwissHoldings, der Verband der Industrie- und Dienstleistungskonzerne in der Schweiz, umfasst 62 der grössten Konzerne in der Schweiz, die zusammen rund 70 Prozent der gesamten Börsenkapitalisierung der SIX Swiss Exchange ausmachen. Unsere Mitgliedfirmen beschäftigen global rund 1,7 Millionen Personen, rund 200‘000 davon arbeiten in der Schweiz. Über die zahlreichen Dienstleistungs- und Lieferaufträge, die sie an KMU erteilen, beschäftigen die multinationalen Unternehmen der Schweiz – direkt und indirekt – über die Hälfte aller Angestellten in der Schweiz.

Digitale Technologien eröffnen Gesellschaft, Wirtschaft und Politik völlig neue Möglichkeiten. Die Digitalisierung ist Teil der Geschäftsmodelle und gewinnt weiter an Bedeutung. Dabei ist eine E-Identitätsinfrastruktur sowohl für die Bereitschaft der Unternehmen, in neue innovative Lösungen zu investieren, wie auch für das Vertrauen der Konsumenten sehr wichtig. Damit sich die digitale Wirtschaft entfalten kann, sind deshalb auch für den numerischen Raum die Grundlagen für eine vertrauenswürdige Identifizierung und Authentifizierung rasch weiterzuentwickeln.

B. Beurteilung des Vorentwurfs zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

1. Grosse Bedeutung als regulatorische Infrastruktur für die Digitalwirtschaft

Für viele digitale Anwendungen der digitalen Wirtschaft nimmt das rechtssichere Management von elektronischen Identitäten und damit verbunden die Möglichkeit zur effizienten Authentifizierung eine zentrale Rolle ein. SwissHoldings unterstützt daher die Absicht des Bundes, die rechtlichen und organisatorischen Rahmenbedingungen zur Einführung einer E-ID für natürliche Personen zu schaffen. Nur durch eine E-ID lassen sich kosten- und zeitintensive Medienbrüche bei der Nutzung von digitalisierten Dienstleistungen verhindern. Das langfristige Ziel muss jedoch bleiben, in der Schweiz für alle rechtlichen Personen, natürliche wie juristische, einen kohärenten Regulierungsrahmen zu bilden, der je nach Kontext auch dazu geeignet ist, ausländische wirtschaftliche Aktivitäten von in der Schweiz domizilierten Unternehmen und anderen schweizerischen Wertschöpfenden zu unterstützen.

Jede natürliche Person mit einem genügenden Bezug zur Schweiz sollte sich im digitalen Raum erschwinglich und mit der gleichen Qualität elektronisch ausweisen können wie mit dem Pass oder der Identitätskarte in der physischen Welt. Um dieses übergeordnete Ziel zu erreichen, braucht es aus Sicht Wirtschaft folgende strategischen Eckwerte:

- Flächendeckende Einführung:
  Alle Einwohnerinnen und Einwohner der Schweiz sollen die Möglichkeit erhalten, eine E-ID zu beziehen und zu verwenden. Hier darf es nicht zu behindernden Ausschlusskrite-

rien kommen wie z.B. die Beschränkung auf Bürgerinnen und Bürger, hohe Kosten für den Nutzer oder eine komplizierte Anwendung;

- Rasche Einführung:
  Die Einführung der E-ID ist überfällig. Nach der langjährigen politischen Debatte braucht es nun - wie bei der regulatorischen Ausformulierung der Datenpolitik - zeitnah einen klaren Rechtsrahmen;
- Breite Anwendung der E-ID:
  Die E-ID soll auch im Behördenverkehr als vollwertige - aber freiwillige - Alternative zu materiellen Identifikations- und Authentifikationsmitteln, wie Identitätskarte und Pass, akzeptiert werden.
- Effizienz und Wettbewerb bei der Umsetzung
  Die e-Identität will mit effizientem Einsatz technischer Mittel und intelligenter Dienstleistungen eine Grundlage für grosse wirtschaftliche Wertschöpfung bereiten. Dazu ist es nötig, dass zumindest dort, wo nicht direkt hoheitliche Aufgaben zur Disposition stehen, die besten - häufig auch bereits von unseren Mitgliedfirmen für ihr internes globales Identitätsmanagement eingesetzt - zur Verfügung stehenden Lösungen beziehungsweise die besten internationalen Standards in Betracht gezogen werden. Unter diesem Blickwinkel ist beispielsweise nicht einzusehen, weshalb eine IdP in jedem Fall gemäss Art. 4 VE-E-ID-Gesetz ihren Sitz in der Schweiz haben soll (es könnte sich ja - je nach Einsatzzweck - auch beispielsweise um eine aus betrieblichen Gründen im Ausland domizilierte Einheit eines Schweizer Unternehmens oder um eine ausländische Stelle handeln, die technisch die führende und damit effizienteste Lösung zur Verfügung stellen kann). Insbesondere soll nicht ohne Not mit einem sachlich unnötigen sogenannten Swiss Finish Strukturpolitik betrieben werden. Damit erst erhält das schweizerische e-Identifizierungsregime das Potential, zu einem wichtigen, positiven Faktor im internationalen Standortwettbewerb zu werden.

2. Angleichungsbedarf im internationalen Kontext

Wir erachten die möglichst weitgehende Konformität der schweizerischen Regelungen über elektronische Identifizierung und Authentifizierung mit dem harmonisierten europäischen Recht nach der eIDAS Verordnung als wichtige Voraussetzung für die sichere Abwicklung elektronischer Transaktionen durch in- und ausländische Personen, Unternehmen und Behörden mit Partnern in unserem Lande wie auch im digitalisierten europäischen Binnenmarkt. Es ist die die grösstmögliche Vereinheitlichung und Abstimmung der Begriffe des neuen E-ID Gesetzes mit der europäischen eIDAS Verordnung und der Gesetzgebung über die elektronische Signatur (ZertES) anzuzielen:

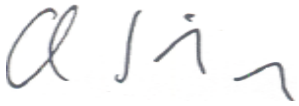
- Unterschiedliche Begriffe führen in der Umsetzung und praktischen Anwendung zu Verwirrung und damit zu Akzeptanzschwierigkeiten. Da wir die Akzeptanz einer E-ID als wesentlichen Erfolgsfaktor betrachten, ist dieses Risiko durch höchstmögliche Vereinheitlichung zu verringern. Wichtig erscheint uns vor allem, keine „eigenen“ Schweizer Begriffe zu definieren, sondern wenn immer möglich die eIDAS Terminologie zu verwenden. So wird etwa der Vorentwurf des E-ID Gesetzes wird als „Bundesgesetz über anerkannte elektronische Identifizierungseinheiten“ bezeichnet. Diese Formulierung sollte durch den Begriff „Elektronisches Identifizierungsmittel“ in Anlehnung an die eIDAS Verordnung ersetzt werden.

- Ebenfalls besteht mit dem ZertES eine Gesetzgebung bezüglich elektronischer Zertifizierungsdienste, welche einen thematisch zum E-ID Gesetz verwandten Bereich darstellen. Das E-ID-Gesetz sollte deshalb hinsichtlich seiner Anforderungen, sowie der für die Ausführung zuständigen Stellen möglichst übereinstimmend mit der Signaturgesetzgebung formuliert werden.
- Die E-ID soll für die Verwendung im Rahmen der EU-Verordnung Nr. 910/2014 (eIDAS) kompatibel sein. Der Bundesrat soll zu diesem Zweck internationale Abkommen abschliessen und die zu deren Ausführung erforderliche Bestimmungen erlassen können.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, für die wohlwollende Prüfung unserer Anliegen.

Freundliche Grüsse

SwissHoldings
Geschäftsstelle



Christian Stiefel
Vorsitzender der Geschäftsleitung

Jacques Beglinger
Mitglied der Geschäftsleitung

cc – SH-Vorstand

Geschäftsstelle

Wallstrasse 8
Postfach
CH-4002 Basel

Telefon 061 206 66 66
Telefax 061 206 66 67
E-Mail vskb@vskb.ch

Verband Schweizerischer Kantonalbanken
Union des Banques Cantonales Suisses
Unione delle Banche Cantonali Svizzere

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

copiur@bj.admin.ch

Datum 29. Mai 2017
Kontaktperson Marilena Corti
Direktwahl 061 206 66 21
E-Mail m.corti@vskb.ch

Stellungnahme des Verbands Schweizerischer Kantonalbanken: Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Damen und Herren

Am 22. Februar 2017 hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) die Vernehmlassung zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) eröffnet. Wir bedanken uns für die Gelegenheit, unsere Positionen und Überlegungen im Rahmen des Vernehmlassungsprozesses einbringen zu können.

Experten aus unserer Bankengruppe haben den Vorentwurf des E-ID-Gesetzes (VE E-ID-Gesetz) eingehend geprüft. Gerne nutzen wir die Möglichkeit, Ihnen unsere wichtigsten Anliegen darzulegen.

Zusammenfassung

- Die Kantonalbanken **unterstützen** das vorgeschlagene Konzept des Bundesrats, weil es die **Innovations- und Wettbewerbsfähigkeit des Wirtschaftsstandorts Schweiz stärkt**.

- Wichtig für eine **hohe Marktdurchdringung der E-ID** sind ein **klares und eindeutiges Sicherheitskonzept**. Wichtige Erfolgsvoraussetzungen sind aus Sicht der Kantonalbanken prinzipienbasierte Mindestanforderungen an Sicherheitsniveaus sowie die Kongruenz von Sicherheitsniveaus zwischen den verschiedenen Stellen.

- Zentral sind zudem vertrauens- und akzeptanzfördernde Vorgaben wie ein **starker und umfassender Datenschutz.** Ebenso bleibt die **Sicherstellung einer schweizweiten – nicht auf die Behörden beschränkten – Systemkontinuität** vordringlich.

- Verbesserungsbedarf gibt es schliesslich in den Bereichen Rechtssicherheit, Interoperabilität und Zukunftsoffenheit. Nötig sind insbesondere **klare Prozessdefinitionen zu Gunsten von mehr Rechtssicherheit und mehr Flexibilität**.

Die Kantonalbanken begrüssen die Bestrebungen des Bundesrats, die Digitalisierung der Wirtschaft und zentraler Geschäftsprozesse weiter voranzutreiben. Mit der Schaffung eines E-ID-Gesetzes liefert er einen wichtigen Baustein. Das vorgeschlagene Konzept – insbesondere die vorgesehene Aufgabenteilung zwischen Staat und Markt aufgrund der Erfahrungen in anderen Ländern – ist sinnvoll und zielführend. Zudem eröffnet es für Banken neue Geschäftsfelder, so können sie beispielsweise, unter Erfüllung gewisser Bedingungen, als Anbieter von Identitätsdienstleistungen (IdP) auftreten. Darin sehen wir insgesamt eine Stärkung der Wettbewerbs- und Innovationsfähigkeit des Schweizer Wirtschafts- und Finanzstandorts, die wir ausdrücklich befürworten. Dieser marktnahe, liberale Ansatz ist – zumal mit Blick auf andere innovationshemmende Regulierungsvorhaben – positiv zu werten.

Damit sich die E-ID nachhaltig entwickeln und erfolgreich im Markt durchsetzen kann, sind aus Sicht der Kantonalbanken die nachfolgend beschriebenen Handlungsfelder und damit einhergehende Anliegen wichtig. Unsere Anregungen zielen darauf ab, die Chancen für praxistaugliche, durch den Markt getragene E-ID-Lösungen zu verbessern.

1. Konsistente und prinzipienbasierte Formulierung der Sicherheitsanforderungen

Die in Art. 5 VE E-ID-Gesetz vorgeschlagene Kaskade von E-ID-Sicherheitsniveaus ist sinnvoll, da sie branchenspezifisch adäquate Lösungen mit Blick auf das Verhältnis von angemessener Sicherheit und Benutzerfreundlichkeit ermöglicht. Die Sicherheitsanforderungen im E-ID-Gesetz und die entsprechenden Ausführungsbestimmungen müssen dabei konsistent und prinzipienbasiert ausgestaltet sein. Dadurch werden insbesondere Reputationsrisiken, welche durch die zahlreichen beteiligten Akteure entstehen können, minimiert. Weiter wird so eine effiziente, kostenschonende Umsetzung gewährleistet. Wir sehen in diesem Zusammenhang noch folgende Schwachstellen, die beseitigt werden sollten:

- **Prinzipienbasierte Festlegung der Mindestanforderungen an die verschiedenen Sicherheitsniveaus (Art. 5 VE E-ID-Gesetz)**: Die Ausführungsbestimmungen der Mindestanforderungen für jede der drei Sicherheitsstufen (niedrig, substanziell, hoch) erfolgen auf Verordnungsebene und müssen konsequent prinzipienbasiert erfolgen, damit sie den dynamischen Entwicklungen in diesem Bereich Rechnung tragen. Ebenso soll es dadurch jeder Branche möglich sein, Lösungen zu entwickeln, die der Grösse, der Komplexität, der Struktur und dem Risikoprofil der jeweiligen Geschäftsmodelle angemessen sind. Wir würden es daher begrüssen, wenn die Wirtschaft in dieser Angelegenheit konsultiert werden würde.

- **Kongruenz der Sicherheitsniveaus von E-ID-verwendenden Diensten und übermittelten Personendaten (Art. 10 Abs. 2 und Art. 15 VE E-ID-Gesetz)**: 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. Wir empfehlen daher die folgende Ergänzung von Artikel 10 Abs. 2 VE E-ID-Gesetz:

  > *[2]… weitergeben, die dem geforderten und implementierten Sicherheitsniveau entsprechen und… [Rest gemäss VE E-ID Gesetz].*

- **Angemessene Sicherheitsniveaus sicherstellen (Art. 5 Abs. 1 und 2 VE E-ID-Gesetz und Änderung von Art. 9 Abs. 1bis ZertES im Anhang zum VE E-ID Gesetz)**: An geeigneter Stelle sollte eine Anforderung verankert werden, die darauf abzielt, dass das bei den E-ID-verwendenden Diensten implementierte Sicherheitsniveau – insbesondere für die beiden hohen Sicherheitsniveaus nach Art. 5 Abs. 1 – angemessen ist.

  Die im Kontext des E-ID-Gesetzes geplante Änderung des Bundesgesetzes über die elektronische Signatur (ZertES) sieht im vorgeschlagenen Art. 9 Abs. 1bis ZertES vor, dass bei Verwendung einer E-ID die persönliche Vorsprache generell entfällt. Dies geht zu weit. Aus dem Zusammenspiel von tiefem Sicherheitsniveau und dem Verzicht auf persönliche Vorsprache kann eine bestimmte Person nicht eindeutig identifiziert bzw. authentifiziert werden. Daraus entstehen massive Risiken, dass eine auf dieser Basis ausgestellte E-ID missbräuchlich oder zu rechtswidrigen Zwecken verwendet wird. Dementsprechend widerspräche eine auf solch schwacher Basis ausgestellte E-ID auch den einschlägigen Vorgaben des Bankenaufsichtsrechts und der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Korruption (vgl. z.B. Art. 4 ff. VSB 16). Die von Art. 9 Abs. 1bis ZertES angeordnete Rechtsfolge darf sich demzufolge nur auf die Sicherheitsniveaus «substanziell» und «hoch», nicht aber auf das tiefste Sicherheitsniveau «niedrig» erstrecken. Art. 9 Abs. 1bis ZertES ist somit wie folgt anzupassen:

  > *Wird der Identitätsnachweis durch eine E-ID gemäss E-ID Gesetz vom … erbracht, entfällt bei Verwendung des Sicherheitsniveaus hoch oder substanziell die persönliche Vorsprache.*

  Dieser angepasste Gesetzestext erfüllt die Anforderungen von Art. 7 Abs. 1 der Verordnung über die elektronische Signatur (VZertES). Auch sonst sind die Formulierungen widerspruchsfrei. Art. 9 Abs. 1bis ZertES stellt eine Ergänzung zu Art. 7 VZertES dar. Dieser darf deshalb im Zuge der Einführung von Art. 9 Abs. 1bis ZertES keinesfalls gelöscht werden. Aus systematischen Gründen empfehlen wir indessen, die Regelung von Art. 7 VZertES neu ebenfalls in der ZertES und damit auf Gesetzesstufe zu regeln.

2. Vertrauens- und akzeptanzfördernde Massnahmen

Eine E-ID wird erst dann akzeptiert und breit genutzt werden, wenn sie einfach, transparent und kostengünstig zu handhaben ist, und die Nutzer selbst bestimmen können, wie mit ihren Daten umgegangen wird («Digitale Selbstbestimmung»). Wir weisen in diesem Zusammenhang auf die folgenden Punkte hin:

- **Stärkung der Vertraulichkeit für sämtliche Datensätze (Art. 10 Abs. 3 VE E-ID-Gesetz)**: Der Erläuterungsbericht zum VE E-ID-Gesetz weist im Zusammenhang mit der Datenbearbeitung und Datenweitergabe zu Recht auf die hohe Bedeutung der Regelung des Datenschutzes hin (S. 27). Den Kantonalbanken ist der sorgfältige Umgang mit personenbezogene Daten ein wichtiges Anliegen. Deswegen regen wir an, zur Stärkung des Datenschutzes den Geltungsbereich von Art. 10 Abs. 3 auf sämtliche Absätze von Artikel 7 zu Personenidentifizierungsdaten auszuweiten.

  [3] Weder anerkannte IdP noch Betreiberinnen von E-ID-verwendenden Diensten dürfen die Personenidentifizierungen gemäss Art 7 ~~Absatz 2~~ oder die darauf basierenden Nutzungsprofile Dritten bekannt geben.

- **Förderung der Verbreitung der E-ID (Art. 1 Abs. 2 Bst. b und Art. 20 VE-ID-Gesetz)**: Eine flächendeckende Verbreitung sollte im Zweckartikel des E-ID-Gesetzes verankert werden. Deswegen regen wir an, den bestehenden Gesetzestext wie folgt zu erweitern:

  b. <u>eine weite Verbreitung</u>, die Standardisierung und die Interoperabilität der E-ID sicherzustellen.

  Wir erachten es in diesem Zusammenhang weiter als sinnvoll, wenn eine flächendeckende Vergabe der E-ID-Registrierungsnummer angestrebt wird (Art. 20 VE E-ID-Gesetz). Dies würde dem nach unserem Verständnis intendierten Ziel des Gesetzesvorschlags, den Zugang zu einer E-ID für alle zu stärken, dienlich sein. Daher würden wir es begrüssen, wenn bei der Ausstellung eines Ausweises (gemäss Art. 3 Abs. 1 Bst. a und b VE E-ID-Gesetz) automatisch eine E-ID-Registrierungsnummer generiert und den Personendaten zugeordnet wird, sofern eine solche noch nicht zugeordnet worden ist und dies vom Inhaber des Ausweises gewünscht wird. Damit würden Personen, welche die persönlichen Voraussetzungen für eine E-ID erfüllen, auf die E-ID aufmerksam gemacht. Dies könnte als Pflicht der Identitätsstelle in Artikel 20 des E-ID-Gesetzes verankert werden. Wir begrüssen explizit, dass durch die E-ID-Registrierungsnummer, welche durch die Identitätsstelle vergeben wird, die jeweilige widerspruchsfreie Zuordnung der Personenidentifizierungsdaten zu ein und derselben Person erreicht wird (Erläuterungsbericht, S. 19).

- **Keine unverhältnismässigen Gebühren (Art. 23 VE E-ID-Gesetz)**: Zur Förderung der Marktdurchdringung sollten die durch den Bundesrat festgelegten Gebühren möglichst niedrig ausfallen. Die im Erläuterungsbericht (S. 34) aufgeführte Option auf einen Verzicht der vollständigen Kostendeckung des Verwaltungsaufwands ist daher ausdrücklich zu begrüssen. Wir erwarten, dass dies, wie vorgesehen, konsequent umgesetzt wird.

- **Systemkontinuität auch bei E-ID-Systemen des Bundes (Art. 4 Abs. 2 Bst. a und b sowie Art. 13 VE E-ID-Gesetz)**: Der Erfolg der E-ID hängt entscheidend von der Glaubwürdigkeit und Verfügbarkeit bzw. Zugänglichkeit des Systems, also dessen Kontinuität, ab. Sollte aller Erwartungen nach zum Trotz der Markt nicht angemessen funktionieren und keine E-IDs für sämtliche drei Sicherheitsniveaus hervorbringen, wird dem Bundesrat richtigerweise die Kompetenz eingeräumt, öffentliche Stellen zu bezeichnen, die für die Bedürfnisse der Behörden E-ID-Systeme betreiben (Erläuterungsbericht, S. 22). Dies impliziert, dass auch staatliche Stellen die Funktion des IdP wahrnehmen können. Ein subsidiäres E-ID-System sollte für den oben aufgeführten Fall im Sinne der Systemkontinuität aber zwingend betrieben werden *müssen*, und dieses sollte grundsätzlich allen Marktteilnehmern (nicht nur Behörden) dauerhaft zugänglich sein. Deswegen fordern wir die folgende Anpassung von Art. 13 Abs. 1 VE E-ID-Gesetz:

  [1] Falls kein IdP für die Ausstellung von E-ID der Sicherheitsniveaus substanziell oder hoch anerkannt ist, ~~kann~~ bezeichnet der Bundesrat eine Verwaltungseinheit ~~bezeichnen~~, die für die Bedürfnisse von Inhaberinnen und Inhabern einer E-ID ~~Behörden~~ ein E-ID-System betreibt und eine E-ID herausgibt.

3. Rechtssicherheit durch klare und konsistente Begriffsdefinition

Hinsichtlich der relevanten Prozesse und Begriffe sollte ausreichende Rechtssicherheit bestehen. Wie in der Stellungnahme der Schweizerischen Bankiervereinigung (SBVg) zu Recht angemerkt, bestehen bspw. noch Unklarheiten bezüglich des Prozesses zur Sperrung der E-ID-Registrierungsnummer (Art. 8 Abs. 2 VE E-ID-Gesetz). Aus der Gesetzesnorm sollte klar hervorgehen, dass es in der Verantwortung der Identitätsstelle liegt, umgehend eine Meldung an die IdP machen, sobald sie eine E-ID-Registrierungsnummer sperrt (vgl. den entsprechenden Formulierungsvorschlag der SBVg). Zur Stärkung der Rechtssicherheit erachten wir es als angebracht auf den relevanten Artikel zu verweisen (u.E. auf Art. 3 VE E-ID-Gesetz «Persönliche Voraussetzungen»).

Zu Gunsten der Klarheit regen wir an, Art. 7 Abs. 4 VE E-ID-Gesetz wie im Erläuterungsbericht skizziert zu ergänzen:

> *[4] Der IdP kann einer E-ID weitere Daten zuordnen, insbesondere eine Adresse, Telefon- oder Kundennummer.*

Artikel 11 Abs. 2 VE E-ID-Gesetz regelt, dass der IdP der Anerkennungsstelle die geplante Geschäftsaufgabe unter Angabe des geplanten Vorgehens bezüglich der ausgestellten E-ID meldet. Jedoch wird nicht geregelt zu welchem Zeitpunkt diese Meldung erfolgen muss. Wir regen an, dies zu präzisieren.

In Art. 12 Abs. 2 VE E-ID-Gesetz wird festgehalten, dass die Anerkennungsstelle eine «angemessene» Frist zur Mängelbehebung setzt. Wir erwarten, dass dies in den Ausführungsbestimmungen näher bestimmt wird.

Zudem scheint uns die vorgeschlagene Dauer der Aufbewahrung von sechs Monaten in Zusammenhang mit der Löschung von Daten über die Anwendung der E-ID nicht konform mit der gesetzlichen Aufbewahrungspflicht von 10 Jahren. Wir regen entsprechend eine Klärung bzw. Anpassung von Art. 17 Abs. 1 Bst. g VE E-ID-Gesetz an.

4. Sicherstellung der Interoperabilität

Es ist von grosser Bedeutung, dass die verschiedenen E-ID-Systeme von Anfang an interoperabel sind. Nur so können hohe Anpassungskosten vermieden werden. Daher regen wir an, dass der Bundesrat insbesondere die technischen Standards für die Schweiz zeitnah auf dem Verordnungs- und Weisungsweg erlässt (Art. 18 VE E-ID-Gesetz). Es ist 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.

5. Zukunftsoffenheit Rechnung tragen

- **Flexibilität bei der Datenbearbeitung gewährleisten (Art. 10 Abs. 1 VE E-ID-Gesetz)**: Ein E-ID-Gesetz muss so ausgearbeitet sein, dass es für künftige technologische und rechtliche Entwicklungen in einem hinreichenden Mass offen ist. Wir sehen etwa einen höheren Flexibilitätsbedarf bei der Datenbearbeitung (Art. 10 Abs. 1 VE E-ID-Gesetz) für geboten. Die aktuelle Eingrenzung der Datenbearbeitung (Beschränkung auf Identifizierung und Authentifizierung; Art. 10 Abs. 1 VE E-ID-Gesetz) ist unseres Erachtens zu restriktiv. Diese Vorgabe sollte hinsichtlich möglicher künftiger Entwicklungen abgeschwächt werden.

- **Schaffung einer E-ID für juristische Personen**: Der Vorentwurf regelt nur die E-ID natürlicher Personen. Unseres Erachtens wäre es notwendig, dass sich auch juristische Personen elektronisch identifizieren können. Wir regen daher an, diese Option zu prüfen oder darzulegen, weshalb (vorerst) darauf verzichtet wurde.

- **Handhabung von Personendaten im Zusammenhang mit dem Internet of Things**: Langfristig sehen wir Regelungsbedarf im Zusammenhang mit der Übertragung von Identitätsdaten an autonom agierende Geräte (bzw. Dinge im Internet of Things, IoT). Wir regen an zu prüfen, ob dieses Thema bereits im Rahmen des E-ID-Gesetzes angegangen werden kann.

Wir bedanken uns für die wohlwollende Prüfung unserer Bemerkungen und Anliegen. Für allfällige Rückfragen stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Verband Schweizerischer Kantonalbanken

Hanspeter Hess
Direktor

Dr. Adrian Steiner
Leiter Public Affairs

Eidgenössisches Justiz- und
Polizeidepartement
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

per E-Mail: copiur@bj.admin.ch

Bern, 29. Mai 2017

Stellungnahme zum Vorentwurf Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin

Der Schweizerische Verband der Telekommunikation (asut) wurde am 22. März 2017 zur Vernehmlassung zum Entwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) eingeladen. Wir bedanken uns für die Möglichkeit zur Stellungnahme und nehmen diese hiermit fristgerecht war.

Für die Telekommunikations-Branche ist eine funktionierende und allgemein akzeptierte E-ID ein wichtiges Anliegen, das hohe Priorität hat. In diesem Sinne möchte asut folgende Punkte im Rahmen der Vernehmlassung hervorheben.

1. Dringender Bedarf für eine E-ID für Behörden und Wirtschaft

Onlineprozesse vereinfachen den Austausch von Informationen, ermöglichen Effizienzgewinne und entsprechen einem Bedürfnis von Kundinnen und Kunden bzw. Bürgerinnen und Bürgern. Im Gegensatz zu einer physischen Transaktion in einem Geschäft oder bei einer Behörde, lässt sich die Authentizität der beteiligten Parteien im Onlinebereich aber nur schwierig oder gar nicht feststellen. Entsprechende IDs haben sich bisher am Markt nicht durchgesetzt und im Onlinehandel hat sich die Kreditkarte als «Ausweis» etabliert.

Mit der fortschreitenden Digitalisierung von Wirtschaft, Behörden und Gesellschaft ist diese Situation nicht mehr haltbar. Es besteht dringender Bedarf nach einem digitalen Pendant zum Reisepass für die Online-Welt. Gleichzeitig ermöglicht die Digitalisierung, dass eine elektronische Identitätskarte nicht mehr zwingend vom Staat angeboten werden muss, sondern auch von privaten Anbietern, wobei die staatlichen Register und Daten die Grundlage für eine staatlich anerkannte Authentisierung darstellen.

Unabhängig vom Anbieter einer staatlich anerkannten E-ID sind folgende Punkte entscheidend für den Erfolg der E-ID:

- Es muss sichergestellt sein, dass Anwenderinnen und Anwender Vertrauen in die E-ID haben und damit die E-ID und die mit ihr verbundenen Dienste auch auf grosse Akzeptanz stossen.
- Um dies zu erreichen ist es wichtig, dass rasch staatliche und private Anwendungen angeboten werden, die auf der E-ID aufbauen. Nur wenn die E-ID im Alltag nützlich ist und regelmässig verwendet

asut
Schweizerischer Verband der Telekommunikation
Klösterlistutz 8
3013 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

wird, wird sie sich durchsetzen. Dazu müssen neben Vertrauen auch Einfachheit, Sicherheit, Datenschutz und ein finanziell interessantes Angebot garantiert sein.
- Dem Markt kommt eine wichtige Rolle bei der Umsetzung und Anwendung der E-ID zu. Deshalb muss den Anbietern aus der Wirtschaft (Identity Providern) ermöglicht werden, im Zusammenhang mit einer E-ID interessante Geschäftsmodelle anzubieten, die über die Basis-Attribute einer staatlichen E-ID hinausgehen.

2. Grundsätze einer E-ID in der Schweiz

asut begrüsst den Vorschlag des Bundesrates, dass private, aber zertifizierte Identity Provider eine E-ID anbieten können, die auch im Behördenverkehr verwendet werden soll. Die Einführung einer E-ID in der Schweiz kommt jedoch – im Vergleich mit anderen europäischen Ländern – sehr spät. Ein E-ID-Gesetz muss daher die rasche Einführung und breite Anwendung der E-ID ermöglichen und unterstützen. Mit den folgenden Grundsätzen einer E-ID in der Schweiz wird dies aus Sicht der asut erreicht.

Die parallelen Aktivitäten staatlicher und privater Akteure sind keine Doppelspurigkeiten, sondern notwendige Bedingung für eine rasche Einführung der E-ID in der Schweiz. Ohne dieses Vorgehen droht eine Schweizer E-ID zu scheitern, bzw. wird sich auf einige wenige Prozesse beschränken und die erwarteten Vorteile und Effizienzgewinne werden sich nicht realisieren lassen.

a) Staatliche Register als Basis
   Um Identität und Authentisierung einer natürlichen Person zu prüfen, muss auf staatliche Informationsquellen zugegriffen werden (Register etc.). Der Gesetzesentwurf sieht dies bereits so vor; daran ist auch festzuhalten. Ohne eine staatliche Quelle fehlt einer E-ID die Vertrauensgrundlage in der Bevölkerung und insbesondere für qualifizierte Anwendungen wird kein Durchbruch möglich sein.
b) Automatisierte Schnittstellen
   Der Bund hat für die automatisierte Verifizierung von Basis-Attributen die entsprechenden Schnittstellen zur Verfügung zu stellen. Diese Funktion ist die Basis der E-ID und hat damit allen Identity Providern über standardisierte Schnittstellen zugänglich zu sein. Ob er die notwendigen IT-Systeme selbst erstellt und betreibt ist dem Bund überlassen.
c) Interoperabilität
   Basis-Attribute, die für die Identifikation und Authentisierung notwendig sind, sind zertifizierten Identity Providern automatisiert zugänglich zu machen. Gleichzeitig ist Interoperabilität diesbezüglich auch zwischen den Identity Providern zu implementieren.
d) E-ID durch private Identity Provider
   E-ID-Angebote von privaten Identity Providern fördern die Innovation und tragen zu einer raschen Verbreitung und Anwendung von E-ID basierten Diensten bei. Zertifizierte Identity Provider greifen dabei auf die staatlichen Schnittstellen zur automatisierten Verifizierung der Basis-Attribute zu. Damit ist sichergestellt, dass die Verifizierung und Authentisierung durch Identity Provider dieselbe Qualität und Vertrauenswürdigkeit aufweist, wie eine staatliche E-ID. Damit ermöglichen private E-ID auch die Authentisierung im Verkehr mit Behörden (e-Government, Auweisplicht etc.).
e) Basis-E-ID-Angebot durch den Staat
   Die E-ID soll allen Bürgerinnen und Bürgern zur Verfügung stehen und zwar auch solchen, die keine E-ID eines privaten Anbieters wollen. Nur wenn der Staat eine Basis-E-ID zur Verfügung stellt und zwar so rasch als möglich (mit dem Inkrafttreten des Gesetzes), ist zudem gewährleistet, dass es effektiv eine E-ID gibt – unabhängig von den privaten Angeboten. Für ein staatliches E-ID-Angebot müssen dabei dieselben Rahmenbedingungen gelten, wie für eine private E-ID eines zertifizierten Identity Providers. Ansonsten besteht die Gefahr einer Wettbewerbsverzerrung. Weiter ist sicherzustellen, dass die Kompatibilität mit internationalen Standards (insbesondere mit der eIDAS-Verordnung) gewährleistet ist.
f) Zwingende Verwendung der E-ID im Verkehr mit Behörden
   Überall dort, wo im Verkehr mit Behörden eine Ausweispflicht oder Ähnliches besteht, soll die Verwendung der E-ID zwingend vorgeschrieben werden. Damit wird die Anwendung der E-ID bevorzugt und e-Government-Prozesse werden unterstützt. Dies trägt zu einer raschen Verbreitung der E-ID bei und führt zu Effizienzgewinnen bei der öffentlichen Hand und in der Privatwirtschaft. Ausnahmen für die E-ID-Pflicht sind im Einzelfall möglich, aber bewilligungspflichtig.

Die bisherige Debatte hat gezeigt, dass die verschiedenen Rollen im E-ID-Prozess noch nicht genügend geklärt sind und oftmals zu Missverständnissen führen. Zudem bestehen offene Fragen zum Modell (z.B.

Interoperabilität) und zur technischen Umsetzung. asut schlägt daher vor, umgehend eine Expertengruppe einzusetzen, um möglichst rasch Lösungen für die offenen Punkte zu erarbeiten. Dies soll parallel zum weiteren Gesetzgebungsprozess geschehen, damit nicht unnötig Zeit verloren geht.

3. Rasche Verbreitung und Anwendung der E-ID sicherstellen

Die duale Vorgehensweise einer staatlichen E-ID durch den Bund und staatlich anerkannter E-IDs von zertifizierten privaten Identity Providern unterstützt eine rasche Verbreitung der E-ID in der Schweizer Bevölkerung und führt zudem zu einem breiten Angebot von zusätzlichen Dienstleistungen, die auf E-ID basieren. Folgende Vorschläge tragen dazu bei, dass sich die E-ID rasch als «DAS» Online-Authentifizierungsinstrument in der Schweiz durchsetzt.

a) Förderung der E-ID im Rahmen der Ausweissausstellung (Passbüro)
   Die zwingende Verwendung der E-ID im Verkehr mit Behörden – dort wo eine Ausweispflicht besteht – führt rasch zu einer Nachfrage nach einer E-ID. Gleichzeitig ist die persönliche Vorsprache bei den Behörden gemäss Art. 3 VE ein Hindernis. Daher sollen bereits bestehende E-ID privater und zertifizierter Identity Provider nachträglich anerkannt werden, wenn die zugrundeliegende Authentisierung bei der Ausstellung gewissen Vorgaben entspricht. Damit wird verhindert, dass Anwenderinnen und Anwender mehrmals vorstellig werden müssen.
   Unabhängig davon, ob die E-ID von staatlichen oder privaten Stellen angeboten wird, soll der Staat eine aktive Rolle bei der Förderung der E-ID einnehmen. Dies umfasst Informationen über den Anwendungsbereich der E-ID, die Vorteile deren Nutzung im staatlichen und privaten Bereich sowie zur konkreten Handhabung. Zudem soll im Rahmen des Bezuges herkömmlicher Ausweise im «Passbüro» automatisch auch eine E-ID abgegeben werden, wobei nicht nur die staatliche E-ID angeboten wird, sondern auch die Möglichkeit einer E-ID eines privaten zertifizierten Identity Providers.
b) Zwingende Nutzung der E-ID im Behördenverkehr
   Wie oben ausgeführt trägt die zwingende Nutzung einer staatlichen oder staatlich anerkannten E-ID eines Identity Providers im Behördenverkehr massgeblich zur raschen Verbreitung der E-ID bei und ermöglicht Effizienzen bei den staatlichen Stellen. Die Vorzüge einer E-ID werden sich nicht einstellen, wenn die E-ID nur eine Option zu den heutigen analogen Prozessen bleibt. Bund und soweit möglich auch Kantone und Gemeinden sollen daher überall, wo man sich staatlichen Stellen gegenüber identifizieren und authentisieren muss, die E-ID des Bundes oder der Identity Provider als einzige Möglichkeit zwingend vorschreiben. Begründete Ausnahmen sind möglich, müssen jedoch bewilligt werden.
c) Entscheidende Punkte rasch klären
   Wichtige Aspekte wie beispielsweise die Ausgestaltung der Interoperabilität oder der Gebühren sind im Gesetz nicht geregelt und sollen auf Verordnungsstufe geklärt werden. Dies schafft jedoch Risiken bei der Ausarbeitung neuer Geschäftsmodelle durch private Identity Provider und führt damit zu Verzögerungen bei der Einführung der E-ID am Markt. Zu den relevanten Punkten müssen daher in den nächsten Monaten die Anforderungen formuliert und im Sinne von technischen Richtlinien publiziert werden. Damit besteht Rechtssicherheit bei der Konzeption und Einführung der für die E-ID notwendigen Systeme und Prozesse.
d) E-ID-Ökosystem ermöglichen
   Identity Provider haben gemäss Art. 7 Abs. 4 VE die Möglichkeit, der E-ID weitere Daten zuzuordnen. Dabei können «Identitäts-Broker» ein wichtiges Bindeglied zwischen den Identity Providern und Diensten, welche die E-ID verwenden, darstellen. Sie tragen damit nicht nur zur rascheren Verbreitung der E-ID bei, sondern auch zur Entwicklung eines dynamischen «E-ID-Ökosystems». Dazu ist insbesondere die Frage der Interoperabilität entscheidend für die vielfältige und einfache Anwendung der E-ID. Auch dieser Punkt ist frühzeitig anzugehen. Dabei muss geklärt werden, inwiefern Dienstanbieter zur Herausgabe bzw. Weiterleitung von Attributen verpflichtet sind. Wichtig ist zudem die Weitergabe der Basis-Attribute, damit ein initialer Identifikationsprozess nicht mehrfach wiederholt werden muss, wenn eine weitere E-ID beschafft oder eine Dienstleistung von anderen E-ID verwendenden Diensten bezogen werden soll.
e) Vereinfachungen bei der erstmaligen Identifikation
   Bereits im Bereich der elektronischen Signaturen zeigt sich, dass eine einfache erstmalige Identifikation ein Erfolgsfaktor darstellt. Eine persönliche Vorsprache ist hingegen eine Hürde, die die Verbreitung der E-ID bremst. Moderne Technologien erlauben bereits heute eine «Remote-Identifikation», welche eine gleichwertige Sicherheit bietet, wie das persönliche Erscheinen. Denkbar ist der Einsatz von audiovisuellen Mitteln (z.B. Videoidentifikation). Dazu sollen die Regelungen des Art. 7 Abs. 1 und 2 der Verordnung über die elektronische Signatur (VZertES; SR 943.032) übernommen werden.

Damit bereits bezwungene Hürden nicht ein zweites Mal unnötig genommen werden müssen, erscheint es asut wichtig, dass eine bereits erfolge Identifikation, die als gleichwertig anzusehen ist, nicht ein zweites Mal durchgeführt werden muss. Im Vorentwurf wird dies im Bereich der elektronischen Signatur auch konkretisiert mit einer Änderung des ZertES (Anhang Änderung anderer Erlasse; Ziff. 4 ZertES). Analog sollten bereits erfolgte, gleichwertige Identifikationen, z.B. diejenige nach den Regeln des ZertES, auch im Bereich des E-ID-Gesetzes verwendet werden können. Für die potentielle Inhaberin einer E-ID bzw. den potentiellen Inhaber einer E-ID stellt dies eine entscheidende Erleichterung des Prozesses dar. Dabei ebenfalls zu regeln sind die finanziellen Aspekte (doppelte Identifizierungen resp. Authentisierungen, Zugänglichmachen von weiteren Attributen etc.).

4. Einzelpunkte aus dem Vorentwurf

a) Zu Art. 10 (Datenschutz)
asut geht davon aus, dass die Vorschriften des Datenschutzgesetzes (in Revision) vollumfänglich Anwendung finden werden. Es ist fraglich, ob anderslautende Regelungen sich hier aufdrängen, sind doch insbesondere auch in Zukunft die Regelungen rund um die Nutzung von Daten detailliert im Datenschutzgesetz enthalten. Anderslautende Regelungen scheinen hier nicht nötig.

b) Zum Anhang Änderung anderer Erlasse; Ziff. 4 ZertES
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.

c) Allgemein zum Anhang Änderung anderer Erlasse
Die Gesetzgebung des Bundes sieht an verschiedenen Stellen Prozesse vor, in denen die Identität einer natürlichen Person durch persönliches Erscheinen mit Vorweisen eines Ausweisdokuments oder einer sonstigen qualifizierten Prüfung (Identifikation von Bankkunden) geprüft werden muss. Wo immer möglich, sollen diese Prozesse mit einer digitalisierten Variante mit Einsatz der E-ID zwingend vorgeschrieben werden. asut denkt hier beispielsweise an den Prozess zur Erfassung von Personendaten beim Verkauf von SIM-Karten (Art. 19a VÜPF; SR 780.11). Für Inhaberinnen und Inhaber einer E-ID wären solche Erleichterungen der Prozesse bei Beibehaltung der Sicherheit ein wirklicher Gewinn, der die E-ID attraktiv machen würde.

Der Vorentwurf zum E-ID-Gesetz legt die Grundlage für die Einführung der E-ID in der Schweiz. asut begrüsst die vorgeschlagenen Punkte. Gleichzeitig besteht ein deutlicher Verbesserungsbedarf, um die erfolgreiche und rasche Einführung der E-ID in der Schweiz sicherzustellen. Angesichts der Komplexität (technische Systeme, Prozesse, Abhängigkeiten zwischen den Playern etc.) schlägt asut deshalb vor, dass eine Expertengruppe zur Verbesserung des Vorentwurfs eingesetzt werden soll.

Gerne stehen wir Ihnen im Rahmen dieser Expertengruppe oder zur Erläuterung unserer Überlegungen zur Verfügung. Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

asut – Schweizerischer Verband
der Telekommunikation

Peter Grütter
Präsident

digitalswitzerland

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

29. Mai 2017

E-ID-Gesetz
Stellungnahme zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten

Sehr geehrte Frau Bundesrätin

Hiermit nehmen wir Stellung zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Dürfen wir Sie bitten, digitalswitzerland (info@digitalswitzerland.com) für zukünftige Vernehmlassungseröffnungen auf Ihre Adressliste zu setzen?

digitalswitzerland unterstützt die vorgegebene Stossrichtung der Aufgabenteilung zwischen Staat und Markt. Der Staat gibt den rechtlichen Rahmen und Standards vor, betreibt die Identitäts- sowie die Anerkennungsstelle und gibt die Personenidentifizierungsdaten an staatlich anerkannte Identity Provider heraus, welche die E-ID für die breite Öffentlichkeit nutzbar machen.

Auch digitalswitzerland erachtet den Staat nicht als besten direkten Herausgeber von E-ID-Lösungen, da für ein solches Produkt maximale Flexibilität und ein Verständnis für den Endnutzer gefragt ist, welches von Privaten über Jahre angeeignet wurde.

Nachfolgend möchten wir auf einzelne Punkte im Vorentwurf eingehen:

Funktionierende Sicherheitsniveaus (Art. 5)
Die vorgeschlagenen und an internationalen Standards ausgerichteten Sicherheitsniveaus werden unterstützt.
digitalswitzerland sieht das Vertrauen der Bevölkerung in die E-ID-Lösungen sowie die einfache, flexible und kostengünstige Handhabe als wichtigste Merkmale für eine breite Anwendung in der Schweiz. Die Bewertung der Daten nach Sicherheitsniveaus ist entsprechend von zentraler Bedeutung.

Ausstellungsprozess (Art. 6)

Das Erlangen der E-ID muss so einfach wie möglich sein.

Deshalb sollte für den Identifikationsprozess bei den IdP bereits im Gesetz festgehalten werden, dass Verfahren, die eine gleichwertige Sicherheit zum persönlichen Erscheinen bieten, von IdP verwendet werden können. Als konkretes Beispiel sollte auch das Verfahren mittels Videoidentifikation als Ersatz für das persönliche Erscheinen im Gesetz aufgenommen werden. Damit bereits bezwungene Hürden nicht mehrmals überwunden werden müssen, ist es wichtig, dass eine bereits erfolgte Identifikation, die als gleichwertig anzusehen ist, nicht ein zweites Mal durchgeführt werden muss.

Interoperabilität (Art. 18)

Die Interoperabilität ist zentraler Bestandteil für die erfolgreiche Einführung der E-ID-Lösung.

Für digitalswitzerland ist die gegenseitige Akzeptanz der E-ID-Systeme zwischen den IdP von elementarer Bedeutung. Um die Interoperabilität zu garantieren, befürwortet digitalswitzerland eine Vermittlerplattform, durch welche Identitäts-Attribute zwischen den IdP transferiert werden können. Eine solche Lösung wird im Bericht zum E-ID-Gesetz auf Seite 32 angedeutet. Die Thematik wie eine solche Vermittlerplattform zu gestalten ist, sollte durch den Bund gefördert und abschliessend geklärt werden.
Durch eine maximale Interoperabilität sollte die E-ID-Lösung auf breiten Zuspruch in der Bevölkerung treffen.

Des Weiteren ist es erforderlich, dass die vom Bundesrat definierten technischen Standards und Schnittstellen mit ausländischen Standards und Schnittstellen kompatibel sind.

Moderate Gebühren (Art. 23)

Die geplante kostenlose Erstübermittlung von Personenidentifizierungsdaten im Herausgabeprozess wird begrüsst.

Es wird als wichtig erachtet, dass der Bund als Anreizgeber für eine breite Akzeptanz der E-ID-Lösung auftritt und nicht mittels hohen Gebührenabgaben diese verhindert. Es müssen nichtdiskriminierende Gebührenmodelle erarbeitet werden, die den Endnutzer von einer Benutzung einer E-ID-Lösung nicht abschrecken.

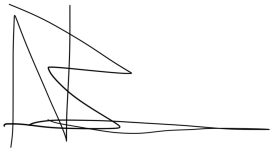
Schnellstmögliche Umsetzung (Art. 26)

Das Inkrafttreten des E-ID-Gesetzes und der damit fallende Startschuss für eine breite anerkannte E-ID-Lösungen muss vom Bundesrat forciert werden. Die Umsetzung des E-ID-Gesetzes muss nach den obliegenden Fristen umgehend ausgeführt werden.

Das E-ID-Gesetz ist die Grundlage und Voraussetzung diverser im Aktionsplan zur Strategie «Digitale Schweiz» des Bundesrats definierten Massnahmen für die Bundesverwaltungen.

Wir bedanken uns für die Berücksichtigung unserer Eingabe und stehen für Fragen jederzeit gerne zur Verfügung.

Freundliche Grüsse
digitalswitzerland



Nicolas Bürer
Managing Director

Daniel Scherrer
Head of Communications

IG ICT
INTERESSENGEMEINSCHAFT DER ZÜRCHER GEMEINDEN
FÜR INFORMATION AND COMMUNICATIONS TECHNOLOGY

Rapperswil, 18. April 2017

Eidgenössisches Justiz- und Polizeidepartement

Bundesamt für Justiz

Bundeshaus West

CH-3003 Bern

Per E-Mail

Vernehmlassung E-ID-Gesetz

Gerne nimmt die IG ICT Zürcher Gemeinden als Verband der IT-Verantwortlichen im Kanton Zürich Stellung zum E-ID-Gesetz. Die IG ICT fokussiert sich ausschliesslich auf die organisatorischen oder technischen Rahmenbedingungen.

Die IG ICT begrüsst den vorliegenden Vorentwurf. Die aufgezählten Vorteile gemäss Kapitel 2.2, *Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete* des *Erläuternden Bericht zum Vorentwurf* sind aus Sicht der IG ICT stimmig.

a) Die IG ICT hat folgende Anmerkungen zum Vorentwurf:

Art. 6 Abs. 5 Protokollierung

Der Zweck der Protokollierung muss aufgeführt werden.

Art. 7 Abs. 2 Abschliessende Nennung

Das Argument der abschliessenden Nennung der Personenidentifizierungsdaten ist nicht einleuchtend, es können durchaus weitere Identifizierungsdaten in den Bundessystemen zukünftig aufgenommen werden, eine Beschränkung ist daher nicht notwendig.

Art. 12 Abs. 2 und 3 Fristen

Es sind kurze Fristen vorzusehen. Ein allfälliger Entzug muss bei Abs. 2 lit. d in den Verordnungen mit sehr kurzen Fristen erfolgen, wobei ein Warten auf ein abgeschlossenes Verfahren je nach Sicherheitsstufe möglicherweise zu lange dauert

Johannisbergstrasse 25
8645 Rapperswil-Jona
Tel 078 808 21 30
Web www.igict.ch
E-Mail igict@igict.ch

Art. 14 Abs. 2 Pflichten der Inhaberinnen und Inhaber

Die notwendigen Massnahmen sind abhängig von der Sicherheitsstufe nach Art. 5 Abs. 1..

b) Anmerkungen zu den später zu erarbeitenden Verordnungen

Die Verlagerung der Anforderungen Standards, Schnittstellen, technische Anforderungen auf die Verordnungen hat zur Folge, dass neben dem Bund auch die Kantone und insbesondere die Gemeinde betroffen werden. Die Erarbeitung der Verordnungen und deren späteren Inhalte müssen auf die Bedürfnisse und den Wissenstand bei komplexen Vorhaben wie der E-ID Rücksicht nehmen.

Die IG ICT begrüsst die angedachte Erweiterung des Kreises der Berechtigten zur Verwendung der Versichertennummer.

Freundlich grüsst

IG ICT Zürcher Gemeinden
Präsident

Andrea Carlo Mazzocco

Johannisbergstrasse 25
8645 Rapperswil-Jona
Tel 078 808 21 30
Web www.igict.ch
E-Mail igict@igict.ch

ISSS – Information Security Society Switzerland

Bollwerk 21

3011 Bern

Per E-Mail zu Handen: copiur@bj.admin.ch

Frau Bundesrätin Simonetta Sommaruga

Eidg. Justiz- und Polizeidepartement

3003 Bern

29. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Im Namen des Vereins ISSS bedanken wir uns für die Möglichkeit, unsere Stellungnahme zum Entwurf eines E-ID-Gesetzes einzubringen.

Die Information Security Society Switzerland (ISSS; http://www.isss.ch) ist die führende Fachorganisation in der Schweiz auf dem Gebiet der ICT-Sicherheit. Ihr gehören heute mehr als 1100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft an. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftlichen Aspekten von ICT-Sicherheit und Informationsschutz auseinander. ISSS ist offizieller ICT Security Fachpartner von SwissICT.

Die elektronische Identität ist ein wesentlicher Bestimmungsfaktor für die Gewährleistung der Informationssicherheit stellt aber auch heikle Fragen zum Datenschutz.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der elektronischen Identität in der Schweiz leisten können und danken Ihnen für die Berücksichtigung unserer Anträge, welche wir Ihnen, wenn immer möglich, zu Ihrer Unterstützung gleich als ausformulierte Textvorlage mit dazugehöriger Begründung einreichen.

An der ISSS Stellungnahme haben folgende ISSS Mitglieder mitgearbeitet (in alphabetischer Reihenfolge):

Umberto Annino, Präsident ISSS, InfoGuard AG

Dr. Thomas Dübendorfer, Präsident Swiss ICT Investor Club (SICTIC) und Past-President ISSS

Beat Lehmann, Acting Counsel, Alcan Holdings Switzerland

Daniel Linder, Ergonomics AG

Doron Moritz, Tessaris Integrated Security AG

Adrian Müller, ID Cyber-Identity AG

Lorenz Neher, PwC

Fridel Rickenbacher, Partner, MIT-GROUP

Reto Scagnetti, Head of Sales, QuoVadis Trustlink Schweiz AG

Freundliche Grüsse

Umberto Annino, Präsident ISSS, Leitung ISSS “Taskforce E-ID-Gesetz”

Allgemeine Anmerkungen zum Vorentwurf „Bundesgesetz über anerkannte elektronische Identifizierungseinheiten – E-ID-Gesetz“

Elektronische Identität – Aufgaben von Staat und Wirtschaft

Wir sind der Meinung, dass die Ausstellung einer (elektronischen) Identität – analog den amtlichen Ausweispapieren in der nicht-digitalen Welt – **grundsätzlich eine hoheitliche Aufgabe des Staates** ist.

In diesem Sinne unterstützen wir die Position der ”Swiss Data Alliance”, die in ihrer entsprechenden Stellungnahme fundiert erläutert wird.

Daher ist der Gesetzesentwurf dahingehend anzupassen, dass nicht nur private Anbieter (IdP) eine elektronische E-ID ausstellen dürfen, sondern auch der Staat diese Aufgabe wahrnehmen kann.

Insbesondere sollte der Bund im Sinne eines erweiterten Art. 13 E-ID-Gesetz dafür sorgen, dass dort wo private Anbietern eine elektronische E-ID der Sicherheitsniveaus ”substantiell“ oder ”hoch” nicht, nur mit Verzug oder nur mit Einschränkungen anbieten, den interessierten Anwendern eine entsprechende E-ID zur Verfügung stellt.

Im Weitern ist uns bewusst, dass die von uns als Vertreterin vieler potentieller Anwender geforderte Konformität der E-ID nach dem Entwurf des E-ID Gesetzes Anpassungsprobleme hervorrufen kann, vor allem weil in der Schweiz die Bereiche ”elektronische Identifizierung“ einerseits im E-ID Gesetz, die elektronische Unterschrift und das elektronische Siegel andererseits im ZertES, somit in verschiedenen Erlassen geregelt sein wird.

Wir weisen daher den vorliegenden Gesetzesentwurf nicht zurück, betrachten ihn jedoch nur als ersten Schritt zur Schaffung von Grundlagen für die rasch fortschreitende Digitalisierung von Wirtschaft und Gesellschaft unsere Landes und würden längerfristig, analog zur EU Verordnung Nr. 910/2014 (eIDAS Verordnung, einer Lösung aller mit elektronischer Identifizierung und Vertrauensbildung zusammenhängenden Fragen in einem einzigen integrierten Erlass den Vorzug geben.

Konformität des E-ID Gesetzes mit der eIDAS Verordnung und dem ZertES

Wie vorstehend erwähnt betrachten wir die möglichst weitgehende Konformität der schweizerischen Regelungen über elektronische Identifizierung und Authentifizierung mit dem harmonisierten europäischen Recht nach der eIDAS Verordnung als wichtige Voraussetzung für die sichere Abwicklung elektronischer Transaktionen durch in- und ausländische Personen, Unternehmen und Behörden mit Partnern in unserem Lande wie auch im digitalisierten europäischen Binnenmarkt.

Wir empfehlen daher die grösstmögliche Vereinheitlichung und Abstimmung der Begriffe des neuen E-ID Gesetzes mit der europäischen eIDAS Verordnung und der Gesetzgebung über die elektronische Signatur (ZertES). Unterschiedliche Begriffe führen in der Umsetzung und praktischen Anwendung zu Verwirrung und damit zu Akzeptanzschwierigkeiten. Da wir die Akzeptanz einer E-ID als wesentlichen Erfolgsfaktor betrachten, ist dieses Risiko durch höchstmögliche Vereinheitlichung zu verringern.

Der Vorentwurf des E-ID Gesetzes wird als „Bundesgesetz über anerkannte elektronische Identifizierungseinheiten“ bezeichnet. Diese Formulierung sollte durch den Begriff „Elektronisches Identifizierungs**mittel**“ in Anlehnung an die eIDAS Verordnung ersetzt werden.

Auch die weiteren Begriffe in der Spalte „eIDAS Deutsch“ von Ziff. 5.2 ”Begriffskonkordanztabelle“ des erläuternden Berichts sollten, soweit sinnvoll und anwendbar in Absatz 2 des E-ID Gesetzes gleichlautend angewendet werden. Wichtig erscheint uns vor allem, keine „eigenen“ Schweizer Begriffe zu definieren, sondern wenn immer möglich die eIDAS Terminologie zu verwenden

Mit dem ZertES besteht eine Gesetzgebung bezüglich elektronischer Zertifizierungsdienste, welche einen thematisch zum E-ID Gesetz verwandten Bereich darstellen. Das E-ID-Gesetz sollte deshalb hinsichtlich seiner Anforderungen, sowie der für die Ausführung zuständigen Stellen gleich, jedenfalls aber möglichst übereinstimmend mit der Signaturgesetzgebung formuliert werden.

E-ID für juristische Personen

Im "Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES)" werden Vorgaben für "geregelte Zertifikate" aufgestellt (für natürliche Personen oder UID-Einheiten).

Die eIDAS Verordnung ist durchgehend in gleicher Art und Weise sowohl für natürliche wie auch für juristische Personen anwendbar. Nach unserer Meinung ist die Verfügbarkeit einer elektronischen Identität vor allem für die im integrierten europäischen elektronischen Binnenmarkt tätigen Unternehmen besonders wichtig. Es ist für uns daher schwer verständlich, weshalb das kommende E-ID Gesetz, in Abweichung zur Signaturgesetzgebung und im Gegensatz zum harmonisierten europäischen Recht , auf die elektronische Identität der juristischen Personen, insbesondere der gemäss Art. 3 UID Gesetz im UID-Register eingetragenen UID-Einheiten verzichten will.

Der Umstand, dass der Vorentwurf zum E-ID-Gesetz die Verfügbarkeit der E-ID für UID-Einheiten bisher nicht in Betracht zieht und deshalb an verschiedenen Stellen angepasst werden müsste, liegt in der Natur der Sache, ist aber unseres Erachtens kein Grund, auf die Berücksichtigung von juristischen Personen bzw. von UID-Einheiten im E-ID-Gesetz zu verzichten.

Das E-ID-Gesetz sollte unseres Erachtens analog zur eIDAS Verordnung ein breites Anwendungs- bzw. Angebotsspektrum bieten. Deshalb erachten wir die Einschränkung auf natürliche Personen als nicht zielführend. Die Entscheidung über die Marktchancen und die Verfügbarkeit eines Angebots von E-IDs für UID-Einheiten kann den IdP überlassen werden und sollte nicht vom Gesetzgeber getroffen werden.

Nach unserer Auffassung würde es übrigens nur einen kleinen Schritt bedeuten, die Verfügbarkeit der E-ID für UID-Einheiten gesetzlich zu regeln, also diese im E-ID-Gesetz zu berücksichtigen:

In Artikel 4 „Geregelte Zertifikate“ der VZertES steht in Abschnitt 1, Buchstabe b „Das BAKOM regelt das Format der geregelten Zertifikate für die folgenden Anwendungen:
b. die elektronische Identifikation einer solchen Person oder Einheit“
Wir empfehlen, eine entsprechende Bestimmung – da im VZertES für natürliche und juristische Personen geltend – auch in das E-ID-Gesetz aufzunehmen.

Datenschutz

Dem Datenschutz ist besondere Beachtung zu schenken. Insbesondere beim Sicherheitsniveau „substanziell“ und „hoch“ besteht bei den zusätzlichen Personenidentifizierungsdaten, umfassend insbesondere Versichertennummer, Gesichtsbild und Unterschriftsbild, ein hohes Missbrauchspotenzial. Die Bestimmungen in Artikel 10 „Datenbearbeitung und Datenweitergabe“ des E-ID-Gesetz sind ggf. in

einer Verordnung weiter zu präzisieren, um eine missbräuchliche Verwendung – durch die IDP selber oder durch Dritte – möglichst auszuschliessen.

Die immer mehr um sich greifende Verwendung der Versichertennummer nach Art. 50c AHVG in Bereichen ausserhalb des Sozialversicherungsrechts befördert die Möglichkeit der Herstellung von Persönlichkeitsprofilen im Sinne von Art. 3 Bst. d DSG und sollte nach Art. 36 Abs. 4 Bst. c DSG nur zurückhaltend zugelassen werden. Es sollte technisch möglich sein, für die Zwecke der E-ID auf der Grundlage der AHV-Versichertennummer durch geeignete Algorithmen eine eindeutig identifizierende jedoch auf die AHV-Versichertennummer nicht rückführbare numerische Kennzeichnung zu schaffen.

Konkrete Anpassungsvorschläge zum Vorentwurf „Bundesgesetz über anerkannte elektronische Identifizierungseinheiten – E-ID-Gesetz“

Formatverwendung:
~~Durchgestrichen~~: ersatzlos streichen oder ersetzen
Fettschrift: neu einzufügen
Anmerkung (fett, kursiv): Anmerkungen, Erläuterungen, Erklärungen der Taskforce Mitglieder

Art.	Abs.	Bst.	Bemerkung/Anregung
1	1	a	**Gegenstand und Zweck** Inhalt, Ausstellung, Verwendung, ~~Sperrung ,~~ **Aussetzung, Reaktivierung (nach einer Aussetzung),** Widerruf **und Erneuerung (nach einem Widerruf)** […] Anmerkung: Der Begriff „Sperrung“ wird oft als Überbegriff für Aussetzung / Suspendierung und Widerruf verwendet. Auch wird er in der eIDAS Verordnung nicht verwendet; dort wird aber von „Aussetzung“ gesprochen. Eine Aussetzung oder Suspendierung sollte zudem nur zeitlich beschränkt möglich sein – keinesfalls sollte eine „unbeschränkte“ Suspendierung ermöglicht werden. Die zeitliche Dauer soll dabei im Bereich von maximal einigen Wochen angesetzt werden. Auch in den folgenden Artikeln sollte „Sperrung“ durch „Aussetzung“ bzw. durch „Aussetzung oder Widerruf“ ersetzt werden.
1	2	c	(neuer Buchstabe) **„und die internationale Anerkennung der Aussteller von Identifizierungsmitteln und ihrer elektronischen Identifizierungssysteme zu ermöglichen“** ***Anmerkung***: Diese Ergänzung wäre eine Formulierung analog zu ZertES und würde eine Grundlage die Herstellung von Konformität mit der eIDAS Verordnung bilden. Die (technische) Umsetzung ist möglicherweise aufwändig. Zudem ist zu klären, was dies für einen IdP bedeutet, der diese Funktionalität nicht umsetzen kann oder will.
2		a	~~elektronische Identifizierungseinheit: eine elektronische Einheit, die zur Identifizierung und Authentifizierung einer natürlichen Person verwendet wird;~~ **elektronisches Identifizierungsmittel: eine materielle oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung von natürlichen oder juristischen Personen verwendet wird.** ***Anmerkung***: Definition angelehnt an Art. 3 Ziff. 2 eIDAS Verordnung. Auch die weiteren E-ID-spezifischen Definitionen sollten weitestgehend aus Artikel 3 (Ziffern 1.-6) der eIDAS Verordnung übernommen bzw. damit abgeglichen werden.
2		b	Anerkanntes elektronische ~~Identifizierungseinheit~~ **Identifizierungsmittel** (E-ID) die von einem IdP nach den Vorgaben dieses Gesetzes ausgestellt wird.

2		i	In eIDAS ist „vertrauender Beteiligter“ definiert. Diese Definition aus eIDAS auch für Artikel 2 im E-ID-Gesetz berücksichtigen und ggf. übernehmen. (In der Begriffskonkordanztabelle im erläuternden Bericht wird dieser Begriff auf „Betreiberin von E-ID-verwendenden Diensten“ abgebildet.)
3		c	(neuer Buchstabe) **„Natürliche Personen, welche eine Versichertennummer nach Art. 50c AHVG zugeteilt wurden“**
3		d	(neuer Buchstabe) **„Natürliche Personen, welche ein von der Schweiz anerkanntes ausländisches Identifikationsmittel besitzen.“** Vgl. dazu den Passus aus VZertES, Art. 5.1, „Natürliche Personen, welche über einen von der Schweiz anerkannten Pass, eine Schweizer Identitätskarte oder eine für die Einreise in die Schweiz anerkannte Identitätskarte verfügen.“
3		e	(neuer Buchstabe) **„Die im Unternehmens-Identifikationsregister (UID-Register) eingetragenen UID-Einheiten gemäss Art. 3 Bst. c des Bundesgesetzes über die Unternehmens-Identifikationsnummer (UIDG) vom 18. Juni 2010 – SR 431.03**
3		f	(neuer Buchstabe) **„Juristischen Personen mit Domizil im Ausland, welche im Ausland in einem von der Schweiz anerkannten Unternehmensregister geführt werden oder in einem von der Schweiz anerkannten Handelsregister eingetragen sind.“**
3	3		***Anmerkung***: Die (weitere) Bearbeitung, Weiterverwendung, Veräusserung etc. der (personenbezogenen) Daten von suspendierten oder widerrufenen E-ID ist ebenfalls zu regeln.
4	2	c	Bezeichnung: „… verantwortlichen Personen kein Risiko für die Sicherheit darstellen…“ ***Anmerkung***: Wie ist „kein Risiko“ genau definiert? Ein risiko-freier Zustand existiert in der Praxis so nicht. Wie wird dieser Aspekt kontrolliert und wer ist dafür verantwortlich? Soll eine Personensicherheitsprüfung gemäss oder analog zu Art. 32 ff des Entwurfs für ein Informationssicherheitsgesetz (ISG) durchgeführt werden? Wird es einen Sicherheitsbeauftragten entsprechend dem ”Datenschutzverantwortlichen gemäss Art. 11 Ab. 5 Bst. e DSG iVm Art. 12a und 12b VDSG geben?
4		d	Bezeichnung: „… erforderlichen Fachkenntnisse…“ ***Anmerkung***: was bedeutet dies konkret? An welche Ausbildungen und Zertifizierungen wird dabei gedacht?
4		f	Bezeichnung: „… in der Schweiz…“ ***Anmerkung***: bedeutet dies, dass keine grenzüberschreitende Verarbeitung von E-ID-System-Daten (via Internet, Cloud Services) möglich sein soll?

5	1	c	Bezeichnung: „… Verhinderung des Identitätsmissbrauchs…“ ***Anmerkung***: absolute Formulierung ist nicht praktikabel, besser wäre u.E. z.B. „**Möglichst hohe Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung nach dem jeweiligen Stand der Technik “**
5	5		(neuer Abschnitt) **Der Bundesrat stellt sicher, dass die Anforderungen an die Identifizierung und die Authentifizierung des Sicherheitsniveaus hoch gemäss E-ID-Gesetz vom ….17 sowie diejenigen für geregelte Zertifikate gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur identisch sind.**
5	6		(neuer Abschnitt) **Für Personen welche für sich auf elektronischem Weg einen mit einer gültigen qualifizierten elektronischen Signatur gemäss dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur signierten Antrag einreichen kann ohne nochmalige Identifizierung direkt eine E-ID mit Schutzniveau ”hoch” ausgestellt werden.**
6	6		**Ausstellungsprozess** Wer eine E-ID **erwerben** will, beantragt deren Ausstellung bei einem IdP. **Eine Person kann mehr als eine E-ID haben. Eine E-ID kann auf das Pseudonym der antragstellenden Person ausgestellt werden** (neuer Abschnitt) **Die E-ID soll auch auf den in der Schweiz üblicherweise verwendeten Mobilgeräten verwendet werden können.**(neuer Abschnitt) neuer Abschnitt) **Anerkannte IdP können die Prüfung der Identität der antragstellenden Person an Dritte delegieren (Registrierungsstellen). Sie haften für die korrekte Ausführung der Aufgabe durch die Registrierungsstelle.** **Anmerkung**: Statt „Registrierungsstelle“ (auch als „Registration Authority“ bezeichnet) kann ggf. der Begriff „Identifizierungsstelle“ (auch als „Identification Authority) – nicht zu verwechseln mit der im E-ID-Gesetzesentwurf referenzierten Identitätsstelle – verwendet werden.

6	7		(neuer Abschnitt) **Jede im UID-Register des Bundesamtes für Statistik eingetragene UID-Einheit kann ohne weiteren Nachweis bei einem IdP die Ausstellung einer E-ID mit Schutzniveau „substanziell“ verlangen, sofern sie noch keine hatte.** **Jeder Schweizer und jede Schweizerin kann bei Ausstellung oder Erneuerung eines gültigen Ausweises gemäss Bundesgesetz vpm 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige ohne weiteren Nachweis bei der ausstellenden Stelle die Ausstellung einer E-ID mit Schutzniveau „substanziell“, verlangen sofern sie noch keine hatte.** **Jede Ausländerin und jeder Ausländer kann bei Ausstellung oder Erneuerung eines gültigen Ausländerausweises gemäss Bundesgesetz vom 10. Dezember 2003 ohne weiteren Nachweis bei der ausstellenden Stelle die Ausstellung einer E-ID mit Schutzniveau „substanziell“ verlangen, sofern sie noch keine hatte.** **Wer die Ausstellung einer E-ID mit höherem oder tieferem Schutzniveau als „substanziell“ beantragen will, beantragt deren Ausstellung direkt beim betreffenden IdP bzw. bei der ausstellenden Stelle.**
6	5		***Anmerkung***: Welche Attribute der Datenübermittlung werden wie, durch wen und unter Berücksichtigung welcher Sicherheitsanforderungen protokolliert? Der Zugriff und die Weitergabe auf diese ggf. personenbezogenen Protokolldaten sind zwingend zu regeln. Anforderungen des Datenschutzgesetzes sind zwingend einzuhalten und möglichst restriktiv auszulegen. Wir empfehlen, diese Aspekte in einer Verordnung zu regeln.
7	2	i	(neuer Buchstabe) **Bürgerort (bei Schweizer Staatsangehörigen)** **Nationalität (bei ausländischen Staatsangehörigen)**
7	2	j	(neuer Buchstabe) **Weitere „biometrische Attribute“ oder „persönliche Zusatzparameter“** ***Anmerkung***: als sinnvolle Offenheit für die Zukunft der Digitalisierung. Ggf. sind die möglichen biometrischen Attribute und persönlichen Zusatzparameter in einer Verordnung zu präzisieren.
8	2		Er ist verantwortlich, dass von ihm ausgestellte E-ID umgehend gesperrt oder widerrufen werden, wenn die E-ID-Registrierungsnummer nicht mehr verwendet werden darf. ~~(Anm. Übersetzung: Er sperrt oder widerruft ...)~~
8	1		***Anmerkung***: wie erfolgt die Authentisierung des IDP gegenüber der Identitätsstelle? Ist eine stärkere Authentisierung vorgesehen bei Buchstabe b. oder c.?
10	2		Sie dürfen Betreiberinnen von E-ID-verwendenden Diensten nur die Personenidentifizierungsdaten weitergeben, die dem geforderten Sicherheitsniveau entsprechen ~~und~~ **sowie weitere Daten, welche** von der Inhaberin oder dem Inhaber der E-ID freigegeben sind
14	1		Eine E-ID ist persönlich und darf Dritten nicht zum Gebrauch überlassen werden. **Bei E-IDs von juristischen Personen darf diese nur von den dafür ausdrücklich ermächtigten Vertretern verwendet werden.**

17	1	b	Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der **natürlichen bzw. juristischen** Person.
18	2		2 Der Bundesrat bestimmt die technischen Standards und definiert die Schnittstellen.
18	3		(neuer Abschnitt) **Die E-ID soll für die Verwendung im Rahmen der Verordnung Nr. 910/2014 (eIDAS) kompatibel sein. Der Bundesrat kann zu diesem Zweck internationale Abkommen abschliessen und erlässt die zu deren Ausführung erforderliche Bestimmungen**
21	1		(komplett ersetzen) **Die Aufsicht (Akkreditierungsstelle) für anerkannte Identitätsdienstleister gemäss diesem Gesetz und für anerkannte Anbieterinnen von Zertifizierungsdienstleistungen gemäss Bundesgesetz vom 18. März 2016 über die elektronische Signatur ist identisch.**
21	2		(komplett ersetzen) **Der Bundesrat bestimmt die Akkreditierungsstelle.**
21	3		(neuer Abschnitt) **Die Akkreditierungsstelle bestimmt eine Anerkennungsstelle und regelt die Anerkennung der Identitätsdienstleister (IdP) und deren E-ID-Systeme.**
22			Die ~~Anerkennungsstelle~~ **Akkreditierungsstelle** veröffentlicht die Liste der anerkannten IDP und deren E-ID-Systeme.
Anhang			(Änderung anderer Erlasse) Bundesgesetz vom 18. März 2016 über die elektronische Signatur Art. 9 Abs. 1bis Wird der Identitätsnachweis durch eine ~~E-ID~~ **Elektronisches Identifizierungsmittel der Stufe hoch** gemäss E-ID-Gesetz vom ⋯.17 erbracht, entfällt die persönliche Vorsprache.
Anhang			(Änderung anderer Erlasse) Die nachstehenden Bundesgesetze werden wie folgt geändert: 1. Ausweisgesetz vom 22. Juni 2001 Art. 1 Abs. 3 zweiter Satz 3 ⋯ Diese können auch ausländische Staatsangehörige sein. Art. 11 Abs. 1 Bst. k 1 Das Bundesamt für Polizei führt ein Informationssystem. Es enthält die im Ausweis aufgeführten und gespeicherten Daten einer Person und zusätzlich folgende Daten: k. die Versichertennummer gemäss Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung. 3 Die Datenbearbeitung dient weiter der Ausstellung und Aktualisierung von elektronischen Identifizierungsmitteln gemäss dem Bundesgesetz vom ⋯.17 über anerkannte elektronische Identifizierungseinheiten.

KARTAC
Interessengemeinschaft der Zahlkartenindustrie

KARTAC | Postfach 59 | 8152 Glattbrugg

Bundesamt für Justiz
Frau Sandra Eberle
Herr Urs Paul Holenstein
Bundesrain 20
3003 Bern

Per Mail: copiur@bj.admin.ch

Glattbrugg, 23. Mai 2017

Vernehmlassung zum Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz): Stellungnahme der Interessengemeinschaft der Zahlkartenindustrie KARTAC

Sehr geehrte Frau Eberle
Sehr geehrter Herr Holenstein
Sehr geehrte Damen und Herren

Mit diesem Schreiben nehmen wir Bezug auf die am 22. Februar 2017 eröffnete Vernehmlassung zum Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Wir bedanken uns in diesem Zusammenhang für die Möglichkeit zur Stellungnahme, von der wir gerne Gebrauch machen.

Die Interessengemeinschaft der Zahlkartenindustrie KARTAC bezweckt die Interessenvertretung und Meinungsbildung ihrer Mitglieder[1] gegenüber anderen Vereinigungen, Firmen, Institutionen, Gesetzgeber und der Öffentlichkeit zur Wahrung der Interessen der Zahlkartenindustrie. Die Mitglieder sind Herausgeber von physischen und digitalen Charge-, Debit-, Kredit- und Prepaidkarten sowie von Kundenkarten mit Zahlfunktion. Darüber hinaus gehören der KARTAC Organisationen an, die im Namen und Auftrag von Kartenherausgebern die Issuing-Funktion wahrnehmen.

Die KARTAC hat den Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) in enger Abstimmung mit der Swiss Payment Association (SPA) geprüft und vertritt weitestgehend die identischen Ansichten, wie sie in der SPA Stellungnahme vorzufinden sind.

[1] Mitglieder der KARTAC sind per Mai 2017 folgende Unternehmen: Accarda AG, BonusCard.ch AG, CCC Credit Card Center AG, Cembra Money Bank AG, Cornèr Bank AG, Magazine zum Globus AG, MF Group AG, Möbel Pfister AG, PayRed Card Services AG, paysafecard.com Schweiz GmbH, PostFinance AG, Swiss Bankers Prepaid Services AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Card Services SA.

Management Summary

Oberste Zielsetzung der unterbreiteten Gesetzes-Vorlage muss es sein, optimale Rahmenbedingungen für eine **weite Verbreitung und eine hohe Nutzung von elektronischen Identifizierungseinheiten** (E-ID) zu schaffen. Ein möglichst einfacher Zugang zu den E-ID, verhältnismässige Gebühren, ein breites E-ID-Einsatzspektrum und durch das übergeordnete Recht abgesteckte massvolle Verordnungsbestimmungen sind wichtige Voraussetzungen dafür. Das Einsatzspektrum der E-ID soll sich nicht auf die Verwendung im Online-Umfeld beschränken, sondern die E-ID auch in anderen Lebens- und Wirtschaftsbereichen zum Einsatz kommen (z.B. Einsatz im stationären Handel), so dass redundante Verfahren zu Gunsten aller Betroffenen und damit verbundene Umstände und Zusatzkosten vermieden werden.

Die Grundversorgung der Bevölkerung mit E-ID muss sichergestellt sein. Der uneingeschränkte Zugang zu und die dauernde Verfügbarkeit der E-ID stellen eine absolute Notwendigkeit dar. Instrumente dafür sind ein Kontrahierungszwang für den Identity Provider (IdP) und die Sicherstellung der Kontinuität der E-ID-Services für den Fall, dass ein IdP seine Dienstleistungen nicht mehr erbringen darf, kann oder will.

Die internationale Interoperabilität bzw. die internationale Anwendbarkeit der schweizerischen E-ID ist zeitnah sicherzustellen. Damit die E-ID – als Online-Ausweise im grenzenlosen Internet – für die Bevölkerung einen hohen Nutzen schaffen, müssen sie möglichst auch international zum Einsatz gebracht werden können. Dafür erforderliche bilaterale Abkommen – insbesondere mit der EU/einzelnen europäischen Staaten – sind möglichst rasch abzuschliessen.

1. Grundsätzliche Ausführungen

1.1 Oberstes Ziel: Weite Verbreitung und hohe Nutzung der E-ID

Aus Sicht der KARTAC muss es die oberste Zielsetzung der unterbreiteten Gesetzes-Vorlage sein, optimale Rahmenbedingungen für eine weite Verbreitung und eine hohe Nutzung von elektronischen Identifizierungseinheiten zu schaffen. Nachdem dies bei früheren ähnlichen Vorhaben (z.B. SuisseID) nicht gelungen ist, darf die vorliegende Chance nicht erneut vertan werden, andernfalls das volkswirtschaftliche Schadenspotenzial erheblich sein dürfte. Damit die Schweiz die Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen und volkswirtschaftliche Gewinne erzielen kann, ist eine möglichst weite Ausbreitung und hohe Verwendung der E-ID unerlässlich, sowohl im Online-Umfeld, als auch in anderen Bereichen des öffentlichen Lebens und der Wirtschaft. Insbesondere sollte darauf geachtet werden, Redundanzen zu vermeiden, die die Verwendung verkomplizieren und unnötige Zusatzkosten produzieren könnten. Die KARTAC hat in Kooperation und enger Abstimmung mit der SPA daher die unterbreitete Gesetzesvorlage ganz besonders unter dem Aspekt der hohen Verbreitung/Nutzung geprüft und wird in der vorliegenden Stellungnahme verschiedentlich darauf zu sprechen kommen.

1.2 Unterstützung für die Initiative des Bundesrats

Die KARTAC begrüsst die Anstrengungen des Bundesrats, die erforderlichen rechtlichen und organisatorischen Rahmenbedingungen für die Anerkennung von E-ID und deren Anbieter zu schaffen. Damit wird eine zentrale Voraussetzung dafür realisiert, dass künftig auch anspruchsvolle Geschäfte mit vernünftigem Aufwand sicher online abgewickelt werden können. Ziel muss es sein, mit umfassend verfügbaren, breit akzeptierten bzw. genutzten und vielfältig einsetzbaren E-ID die digitale Abwicklung auch anspruchsvoller Geschäfts- und Verwaltungsprozesse zu ermöglichen bzw. effizient und effektiv auszugestalten.

1.3 Zweckmässige Aufgabenteilung zwischen Staat und Privaten

Die KARTAC begrüsst das Konzept, wonach eine Aufgabenteilung zwischen Staat und privaten Anbietern vorgenommen werden soll und private Identifizierungsdienstleister von einer staatlichen Anerkennungsstelle eine Zulassung zur Herausgabe von staatlich anerkannten elektronischen Identifizierungsmitteln erlangen können. Diese Konzeption verspricht einen zügigen und effizienten Aufbau bzw. Betrieb des Systems, eine zeitgerechte Weiterentwicklung desselben entlang rasch voranschreitender digitaler Entwicklungen und den Schutz bereits getätigter privater Investitionen in existierende oder sich im Aufbau befindliche elektronische Identifizierungsinstrumente.

1.4 Sicherstellung der Grundversorgung der Bevölkerung mit E-ID

Mit der vorgesehenen (von der KARTAC unterstützten) teilweisen Auslagerung einer bisher rein staatlichen Aufgabe (Herausgabe von Pässen und Identitätskarten) an Private ist u.a. das Risiko verbunden, dass nicht für jede/n Berechtigte/n Zugang zu einer E-ID besteht bzw. dass eine solche nicht ständig verfügbar ist. Der uneingeschränkte Zugang zu und die dauernde Verfügbarkeit der E-ID stellen jedoch eine absolute Notwendigkeit dar; dies ganz besonders unter dem Aspekt, dass die E-ID in Kombination mit z.B. der elektronischen Signatur das Potential besitzen, sich zum zentralen Identifizierungsmittel der näheren Zukunft zu entwickeln. Ohne eine jederzeit verfügbare E-ID kann eine Person zukünftig dauernd oder vorübergehend von wesentlichen Teilen des wirtschaftlichen Lebens ausgeschlossen bleiben. Für die KARTAC ist es deshalb von zentraler Bedeutung, das E-ID-Gesetz so auszugestalten, dass die Grundversorgung der Bevölkerung mit E-ID bestmöglich und nachhaltig sichergestellt wird. Dazu gehören die gesetzliche Verankerung eines Kontrahierungszwangs für den Identity Provider (IdP) und die Sicherstellung der Kontinuität der E-ID-Services für den Fall, dass ein IdP seine Dienstleistungen nicht mehr erbringen darf, kann oder will. Beide Themen-Bereiche regelt der Vorentwurf nicht oder nicht ausreichend.

1.5 Keine prohibitiven Gebühren

Es ist vorgesehen, die beiden neuen Bundesstellen (Identitätsstelle und Anerkennungsstelle) über Gebühren zu finanzieren. Wie vorstehend angesprochen, ist es – ganz besonders auch aus einem volkswirtschaftlichen Blickwinkel heraus – von entscheidender Bedeutung, dass die E-ID in der Bevölkerung eine grosse Ausbreitung erfährt bzw. dass jedermann nicht nur theoretisch sondern auch faktisch Zugang zu einer E-ID hat. Ein zu hoher Endkunden-Preis für den Erwerb bzw. Betrieb einer E-ID stünde dieser zentralen Zielsetzung diametral entgegen. Bei der Gebühren-Festsetzung ist daher 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.

1.6 Zeitnahe Sicherstellung von internationaler Interoperabilität bzw. Anwendbarkeit der schweizerischen E-ID

Damit die E-ID – als Online-Ausweise im grenzenlosen Internet – für die Bevölkerung einen möglichst hohen Nutzen schaffen (und damit auch nachgefragt werden bzw. eine weite Verbreitung erfahren), müssen sie möglichst auch international – ganz besonders europäisch – zum Einsatz gebracht werden können. Gemäss Erläuterndem Bericht zum Vorentwurf für ein E-ID-Gesetz berücksichtigt der Vorentwurf insbesondere die Vorgaben für die EU-Kompatibilität gemäss eIDAS-Verordnung[2]. So wird u.a. auf Seite 13 festgehalten: „In der eIDAS-Verordnung und den entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das Konzept für schweizerisch anerkannte E-ID-Systeme richtet sich an diesen internationalen Vorgaben aus, sodass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten." Zu beachten ist diesbezüglich allerdings, dass schweizerische E-ID nur dann europaweite Anerkennung erlangen, wenn die Schweiz dazu ein bilaterales Abkommen mit der EU oder bilaterale Abkommen mit einzelnen Mitgliedstaaten schliesst. Auch wenn der bilaterale Weg zwischen der EU und der Schweiz faktisch nach wie vor blockiert erscheint, ist es aus Sicht der KARTAC für den Erfolg – und damit für die Etablierung – der schweizerischen E-ID unerlässlich, dass der Bundesrat nach Erlass des E-ID-Gesetzes rasch und mit Nachdruck auf ein Anerkennungs-Abkommen mit der EU drängt.

1.7 Regelung von Eckwerten und Leitplanken anstelle von Prozessen

Der unterbreitete Vorentwurf fokussiert stark auf die Regelung von Prozessen. In der digitalen Welt, welche einem permanenten und raschen Wandel unterzogen ist, kann sich dies als Hemmschuh erweisen, wenn es darum geht, mit neuen Entwicklungen angemessen Schritt zu halten. Die KARTAC schlägt daher vor, im Gesetz verstärkt Eckwerte und Leitplanken in generischer Weise festzulegen und auf die Umschreibung von Prozessen zu verzichten bzw. diese – bei Bedarf – auf Verordnungsstufe zu umreissen. Das Gesetz soll möglichst viele Prinzipien und möglichst keine Regeln enthalten. Damit kann sichergestellt werden, dass das Gesetz auf lange Sicht eine verlässliche, aber dennoch genügend flexible Grundlage für den innovativen Einsatz von E-ID schafft.

1.8 Regelungen auf Verordnungsstufe zugunsten einer weiten Verbreitung und hohen Nutzung der E-ID

In der digitalen Welt, die einem ständigen Wandel unterworfen ist, ist es zweckmässig, gute Voraussetzungen für die zeitgerechte Weiterentwicklung der regulatorischen Rahmenbedingungen bzw. die Berücksichtigung neuer Realitäten zu schaffen. Der Vorentwurf wird diesem Anspruch insofern gerecht, als er dem Bundesrat eine breite Palette an Themen zuweist, welche auf Verordnungsstufe – und damit in einem vergleichsweise raschen Rechtsetzungsverfahren – geregelt bzw. detailliert werden können. Dabei sind aus Sicht der KARTAC allerdings folgende zwei zentralen Punkte zu beachten: Zum einen sind in den einzelnen Themen auf Gesetzesstufe klare Leitplanken bzw. Schranken für den Verordnungsgeber zu setzen, zum anderen hat der Verordnungsgeber seine Rechtsetzungskompetenz dem Zweck und den Zielen des übergeordneten Gesetzes entsprechend auszuüben.

[2] 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/EG1

Vorliegend bedeutet dies nach Auffassung der KARTAC insbesondere, dass auch der Bundesrat so regulieren soll, dass optimale Rahmenbedingungen für eine weite Verbreitung und eine hohe Nutzung von E-ID geschaffen werden.

1.9 Änderung anderer Erlasse: Umfassende Beseitigung von rechtlichen Hindernissen für den E-ID-Einsatz

Die KARTAC ist der Auffassung, dass die im Anhang zur E-ID-Gesetzes-Vorlage enthaltene Auflistung anderer Erlasse, welche geändert werden sollen, zu eng gehalten ist. Für den Erfolg bzw. die erforderliche hohe Verbreitung von E-ID ist es zwingend, dass diese in den verschiedensten Lebenssituationen bzw. in den unterschiedlichsten Geschäfts- und Verwaltungsprozessen zur Anwendung kommen können. Es ist deshalb darauf zu achten, dass in der gesamten Schweizer Rechtsordnung die nötigen Voraussetzungen für die Einsetzbarkeit von E-ID geschaffen werden bzw. dass rechtliche Hürden, welche dem entgegenstehen, umfassend beseitigt werden.

2. Ausführungen zu einzelnen Gesetzesartikeln und Anträge der KARTAC

Nachstehend finden sich zu ausgewählten Artikeln des Vorentwurfs zu einem E-ID-Gesetz die Einschätzungen und Anträge der KARTAC:

2.1 Allgemeine Bestimmungen (Art. 1 f. VE E-ID-Gesetz)

- **Antrag: „Weite Verbreitung und Nutzung" in die Zweckbestimmung aufnehmen (Art. 1 Abs. 2 lit. b VE E-ID-Gesetz)**

  Das Ziel einer möglichst umfassenden Verbreitung der E-ID soll in den Zweckartikel des E-ID-Gesetzes aufgenommen werden. Wie bereits in den grundsätzlichen Ausführungen dargelegt, muss es das oberste Ziel des Gesetzgebers sein, ein Instrument zur Verfügung zu stellen, dass von der Bevölkerung breit angenommen und rege genutzt wird. Dies bedingt einerseits eine einfache aber dennoch sichere Handhabung der E-ID und anderseits ein möglichst weites Anwendungsfeld derselben sowohl im öffentlichen als auch im privaten Sektor. Die Aufnahme des zusätzlichen Ziels der „weiten Verbreitung und Nutzung der E-ID" in den Zweckartikel soll insbesondere auch den Bundesrat bei der Ausarbeitung der E-ID-Verordnung leiten.

  Die KARTAC beantragt, den Zweckartikel (Art. 1 Abs. 2 lit b VE E-ID-Gesetz) wie folgt zu ergänzen (Ergänzung = unterstrichen):

  > „Es hat zum Zweck:
  >
  > a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
  >
  > b. eine weite Verbreitung und Nutzung, die Standardisierung und die Interoperabilität der E-ID sicherzustellen."

- **Antrag: „Nationale und internationale Interoperabilität" in die Zweckbestimmung aufnehmen (Art. 1 Abs. 2 lit. b VE E-ID-Gesetz)**

  Inhaberinnen und Inhaber einer E-ID sollen diese bei allen E-ID-verwendenden Diensten einsetzen können, und zwar unabhängig davon, ob der Betreiber eines E-ID-verwendenden Dienstes mit demjenigen IdP eine Vereinbarung hat, der die E-ID ausgestellt hat. Dieser zentrale Aspekt der Interoperabilität fokussiert primär auf den nationalen Bereich.

Daneben ist es für die breite Einsatzbarkeit (und damit die weite Verbreitung) der E-ID genauso wichtig, dass die Interoperabilität auch zwischen den einzelnen länderspezifischen Systemen sichergestellt wird. Zu diesem Zweck sind von der Schweizer E-ID-Lösung die massgeblichen internationalen Standards zu beachten bzw. es sind adäquate Lösungen dazu zu treffen, insbesondere was die EU anbelangt. Damit werden die Voraussetzungen dafür geschaffen, dass die schweizerische E-ID zumindest europaweite Anerkennung erlangen kann.

Die KARTAC beantragt daher, den Zweckartikel (Art. 1 Abs. 2 lit b VE E-ID-Gesetz) wie folgt zu ergänzen (Ergänzung = unterstrichen):

> „Es hat zum Zweck:
>
> a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
>
> b. eine weite Verbreitung und Nutzung, die Standardisierung und die Interoperabilität der E-ID auf nationaler und internationaler Ebene sicherzustellen."

- **Antrag: Den Begriff „Attribute" in Art. 2 VE ID-Gesetz definieren (Art. 2 lit. k VE E-ID-Gesetz)**

  Vorentwurf und Erläuternder Bericht gehen davon aus, dass neben den von der Identitätsstelle zum Abgleich der Daten zur Verfügung gestellten Identitätsmerkmalen auch noch weitere Attribute mit der E-ID verbunden werden können. Die KARTAC begrüsst diese Möglichkeit, da sie einen gewichtigen Beitrag zur Verbreitung der E-ID leisten kann. Auf dieser Ausgangslage erscheint es angebracht, den Begriff "Attribute" im Gesetz entsprechend zu definieren.

  Die KARTAC beantragt, Art. 2 VE E-ID-Gesetz wie folgt um lit. k zu ergänzen (Ergänzung = unterstrichen):

> „In diesem Gesetz bedeuten:
> a. [...]
> k. *Attribute*: Andere als von der Identitätsstelle zur Verfügung gestellte Merkmale, die einer Person zugeordnet werden können."

2.2 Ausstellung von E-ID (Art. 3 ff. VE E-ID-Gesetz)

- **Antrag: Weitgehenden Kontrahierungszwang vorsehen (Art. 3 Abs. 1 VE E-ID-Gesetz)**

  Aufgrund der in Art. 3 Abs. 1 verwendeten Kann-Vorschrift besteht für den IdP kein Kontrahierungszwang. Dies wird im Erläuterungsbericht explizit bestätigt. Der IdP ist also nicht verpflichtet, ein Vertragsverhältnis einzugehen und eine E-ID auszustellen, auch wenn eine Person die Voraussetzungen für die Abgabe einer E-ID erfüllt. Warum dieser Ansatz verfolgt wird, wird in den Vernehmlassungsunterlagen nicht näher ausgeführt. Der KARTAC erschliesst sich Sinn und Zweck dieser Konzeption nicht. Im Gegenteil – sie erscheint nicht zielführend. Genauso wie ein Staat seinem Bürger bei gegebenen Voraussetzungen die Ausstellung eines Passes oder einer Identitätskarte nicht vorenthalten darf, soll auch ein IdP verpflichtet sein, einer berechtigten Person, welche entsprechend Antrag stellt, eine E-ID auszustellen. Andernfalls besteht das Risiko, dass aus sachfremden Beweggründen – zum Beispiel wirtschaftlichen oder überwiegend privaten Interessen – einer berechtigten Personen willkürlich der Zugang zu einer E-ID verwehrt bleibt oder über Gebühr erschwert wird.

Da offenbar auch keine Pflicht zur Begründung einer Ablehnung seitens des IdP besteht, stünde der Antragssteller einem negativen Bescheid seitens des IdP schutzlos gegenüber.

Dieser offensichtliche Missstand ist mit der Einführung eines weitgehenden Kontrahierungszwangs zu beheben. Die IdP sollen verpflichtet werden, sämtlichen bezugsberechtigten Personen auf deren Ersuchen hin eine E-ID auszustellen. Die Gründe für eine zulässige Verweigerung sind präzise festzulegen.

Die Konzeption von Art. 3 Abs. 1 VE E-ID-Gesetz, wonach der IdP nicht verpflichtet sein soll, ein Vertragsverhältnis einzugehen und eine E-ID auszustellen, soll durch das System eines weitgehenden Kontrahierungszwangs ersetzt werden.

- **Antrag: Kontinuität in der E-ID-Nutzung bei Geschäftsaufgabe eines IdP sicherstellen (Art. 4 Abs. 3 und Art. 11 Abs. 3 VE E-ID-Gesetz)**

  Der Vorentwurf sieht in Art. 4 Abs. 3 vor, dass die Anerkennung der IdP spätestens nach 3 Jahren erneuert werden muss, womit das Risiko besteht, dass die Anerkennung nicht weitergeführt wird. Art. 11 VE E-ID-Gesetz regelt das Erlöschen der Anerkennung infolge Konkurs oder Aufgabe der Geschäftstätigkeit. In all diesen Fällen der freiwilligen oder erzwungenen Geschäftsaufgabe eines IdP stellt der Vorentwurf nicht sicher, dass die Inhaberinnen und Inhaber von E-ID, welche der jeweilige IdP ausgestellt hat, ihre E-ID weiterhin nutzen können. Ebenso wenig ist sichergestellt, dass Betreiber von E-ID verwendenden Diensten weiterhin die bereits erhaltenen Datensätze abrufen können. Vielmehr findet der in Art. 3 VE E-ID-Gesetz fehlende Kontrahierungszwang seine Fortsetzung in Art. 11, indem kein IdP in die Pflicht genommen werden soll, die E-ID-Systeme bzw. Kundinnen und Kunden eines zukünftig nicht mehr bestehenden IdP zu übernehmen. Das erachtet die KARTAC als nicht sachgerecht und nicht zielführend: Insbesondere ist es dem Vertrauen der E-ID berechtigten Personen und der möglichen Betreiber von E-ID verwendenden Diensten in das E-ID-System und in die Rechtssicherheit abträglich.

  Angezeigt ist daher eine gesetzliche Regelung, welche IdP verpflichtet, Inhaberinnen und Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc" (gegen entsprechende Entschädigung, z.B. durch den Bund) zu übernehmen. Will der Gesetzgeber nicht so weit gehen, ist auf Gesetzesebene im Minimum sicherzustellen, dass von der Geschäftsaufgabe eines IdP betroffene Inhaberinnen und Inhaber einer E-ID von anderen IdP eine E-ID ausgestellt erhalten, ohne den gesamten Ausstellungsprozess gemäss Art. 6 VE E-ID-Gesetz erneut durchlaufen zu müssen. Dabei ist die ununterbrochene Nutzungsmöglichkeit der bisherigen E-ID bis zur Ausstellung einer neuen sicherzustellen (für die Inhaberinnen und Inhaber wie für die Betreiber von E-ID-verwendenden Diensten).

  Auf gesetzlicher Ebene ist 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 (durch die Inhaberinnen und Inhaber der E-ID wie durch die Betreiber von E-ID-verwendenden Diensten).

- **Antrag: Datenhaltung durch den IdP ausserhalb der Schweiz zulassen (Art. 4 Abs. 2 lit. f VE E-ID-Gesetz)**

  Der Vorentwurf sieht in Art. 4 Abs. 2 lit. f vor, dass die IdP die E-ID-System-Daten in der Schweiz und nach schweizerischem Recht halten und bearbeiten müssen. Diese absolute Anforderung wird nach Ansicht der KARTAC den heutigen Realitäten – worin

z.B. Cloud-Lösungen eine immer grössere Rolle spielen – nicht mehr gerecht. Der Gesetzgeber sollte hier – ohne bei den Sicherheitsanforderungen Abstriche zu machen – mehr Flexibilität zeigen und auch eine Datenhaltung ausserhalb der Schweiz zulassen, sofern die Daten bezüglich Datensicherheit und Datenschutz adäquat nach schweizerischem Recht bearbeitet und gehalten werden. Dies lässt sich umso mehr rechtfertigen, als mit der angestrebten internationalen Interoperabilität des schweizerischen E-ID-Systems künftig auch Schweizer E-ID bei Betreiber von E-ID-verwendenden Diensten im Ausland zum Einsatz kommen werden, was zwangsläufig einen gewissen Datenverkehr ins Ausland mit sich bringt.

Die KARTAC beantragt, Art. 4 Abs. 2 lit f.VE E-ID-Gesetz wie folgt abzufassen (Weglassungen = durchgestrichen / Ergänzung = unterstrichen):

> „IdP werden anerkannt, wenn sie:
> a. [...]
> f. die E-ID-System-Daten bezüglich Datensicherheit und Datenschutz adäquat nach Schweizer Recht ~~in der Schweiz nach schweizerischem Recht~~ halten und bearbeiten;"

- **Antrag: Gleichwertige Anerkennungsverfahren als hinreichend zulassen (Art. 4 Abs. 3 VE E-ID-Gesetz)**

  Die KARTAC erachtet ein periodisch wiederholtes Anerkennungsverfahren für IdP als sinnvoll. Dabei ist jedoch zu beachten, dass Banken (welche als IdP tätig sind) bereits jährlich andere Audits und Anerkennungsverfahren zu durchlaufen haben und mit dem Anerkennungsverfahren für IdP ein weiteres hinzukäme, welches gleiche oder ähnliche Bereiche abdecken dürfte. Aus Gründen der Prozessökonomie sollten die verschiedenen Anerkennungsverfahren harmonisiert werden. Bis dies realisiert ist, soll ein Anerkennungsverfahren jeweils auch für einen anderen Bereich gelten, sofern eine gewisse Gleichwertigkeit vorliegt.

  Die KARTAC beantragt, Art. 4 Abs. 3 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

  > „Die Anerkennung muss spätestens nach drei Jahren erneuert werden. Wurde eine gleichwertige Anerkennung bereits nach einem anderen Gesetz durchgeführt, muss sie nach diesem Gesetz nicht wiederholt werden."

- **Antrag: E-ID muss Anforderungen nach der Geldwäschereigesetzgebung und nach den einschlägigen Standesregeln gerecht werden (Art. 5 VE E-ID-Gesetz)**

  Für einen adäquaten Nutzen der E-ID (und damit eine hohe Nachfrage besteht) müssen die Voraussetzungen an die E-ID derart ausgestaltet sein, dass sie die Anforderungen nach Art. 3 des Geldwäschereigesetzes, nach der Geldwäschereiverordnung-FINMA und nach den einschlägigen Standesregeln (insbesondere Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken/VSB 16) an eine rechtskonforme Identifikation erfüllen. Die Akzeptanz der E-ID als rechtsgültiges Identifikationsmittel muss darüber hinaus insbesondere auch bei der Finanzmarktaufsicht gegeben sein. Nur so wird es gelingen, die E-ID im täglichen wirtschaftlichen Leben genügend zu verankern.

  In diesem Sinne begrüsst die KARTAC die Ausführungen im Erläuternden Bericht (Seite 35 f.), wonach eine E-ID als beweiskräftiges Identifikationsdokument dienen soll und insbesondere Finanzinstitute und Spielcasinos, die dem Geldwäschereigesetz unterstehen, eine sichere elektronische Identifikation mit der E-ID sollen vornehmen können.

Allerdings regelt das Geldwäschereigesetz selbst nicht abschliessend, was ein beweiskräftiges Dokument ist, sondern überlässt dies der Geldwäschereiverordnung der FINMA. Dazu führt der Erläuternde Bericht aus (Seite 35 f.): „Gegebenenfalls ist diese Verordnung so anzupassen, dass eine E-ID im elektronischen Geschäftsverkehr mit Finanzinstituten und Casinos eingesetzt werden kann." Für die KARTAC ist es zwingend, dass die notwendigen Anpassungen an der Geldwäschereiverordnung der FINMA – aber auch an den Standesregeln – auf den Zeitpunkt der Einführung der E-ID vorgenommen sind.

Es sind alle Voraussetzungen dafür zu schaffen, dass die E-ID die Anforderungen nach der Geldwäschereigesetzgebung und nach den einschlägigen Standesregeln an eine rechtskonforme Identifikation erfüllen bzw. dass die einschlägigen Rechtserlasse die E-ID als rechtsgültige Identifikationsmittel bzw. beweiskräftige Dokumente anerkennen.

- **Antrag: Akzeptanz einer bereits vorgenommenen Identifikation nach Geldwäschereigesetzgebung (Art. 5 Abs. 2 VE E-ID-Gesetz)**

  Art. 5 Abs. 2 VE E-ID-Gesetz legt unter lit. a fest, dass sich die verschiedenen Sicherheitsniveaus insbesondere in Bezug auf die Identifizierung und Authentifizierung der Inhaberin und des Inhabers bei der Registrierung unterscheiden sollen. Der Erläuterungsbericht führt hierzu aus, dass die Registrierung bei den Sicherheitsniveaus „substanziell" und „hoch" mit persönlicher Vorsprache oder mittels Videoidentifikation zu erfolgen hat.

  Unabhängig von den noch zu erlassenden Ausführungsbestimmungen auf Verordnungsstufe (Art. 5 Abs. 4 VE E-ID-Gesetz) ist es für die KARTAC wichtig, dass auf Gesetzesstufe festgehalten wird, dass sich ein IdP auf eine bereits nach der Geldwäschereigesetzgebung rechtsgültig erfolgte Identifikationen verlassen darf. Es wäre – sowohl für den IdP wie für den E-ID-Antragsteller – ineffizient und in der Praxis untauglich, wenn ein IdP, der gleichzeitig als Finanzintermediär gemäss Geldwäschereigesetzgebung qualifiziert und die Identifikation einer Person nach der Geldwäschereigesetzgebung vorgenommen hat, dieselbe Person für die Ausstellung einer E-ID nochmals identifizieren müsste. Dies bedeutet auch, dass an die Identifikation nach E-ID-Gesetz keine höheren Anforderungen gestellt werden dürfen als an die Identifikation nach Geldwäschereigesetzgebung. So soll sich beispielsweise eine „persönliche Vorsprache" nach Geldwäschereigesetzgebung nicht von einer „persönlichen Vorsprache" nach E-ID-Gesetz unterscheiden. Und eine vorbestehende Identifikation nach Geldwäschereigesetzgebung innerhalb eines Konzerns ist der Identifikation durch den konzerninternen IdP gleichzustellen (d.h. es bedarf keiner erneuten Identifikation durch den IdP, wenn die bereits nach GwG identifizierte Person beim IdP eine E-ID beantragt / siehe dazu auch den unten stehenden Antrag zu Art. 6 Abs. 3bis VE E-ID-Gesetz).

  Ergänzend ist hierzu festzuhalten, dass aufgrund einer der Identifikation nachfolgenden Übermittlung der Personenidentifizierungsdaten durch die Identitätsstelle bei der Ausstellung einer E-ID sogar ein vergleichsweise höheres Sicherheitsniveau besteht. Denn durch diesen Abgleich können beispielweise gefälschte Ausweispapiere immer als solche erkannt werden, was im Rahmen der Identifikation nach Geldwäschereigesetzgebung nicht ohne weiteres sichergestellt ist.

Im E-ID-Gesetz ist explizit zu regeln, dass sich ein IdP auf eine bestehende Identifikation nach zum im fraglichen Zeitpunkt geltender Geldwäschereigesetzgebung verlassen darf, unabhängig davon ob er diese selber vorgenommen hat oder ob diese unter Anwendung der in der Geldwäschereigesetzgebung festgelegten Pflichten innerhalb des Konzerns oder durch einen im Sinne der Bankenregulierung beauftragen Dritten erfolgt ist.

- **Antrag: Freie Zuordnung von Attributen (Art. 5 Abs. 3bis VE E-ID-Gesetz)**

  Gemäss Art. 7 Abs. 4 VE E-ID-Gesetz kann der IdP einer E-ID weitere Daten (sogenannte Attribute) zuordnen (siehe dazu auch den oben stehenden Antrag zu Art. 2 lit. k VE E-ID-Gesetz). Da es sich bei den Attributen um Daten handelt, die üblicherweise nicht von einer staatlichen Stelle stammen, sollte es nach Auffassung der KARTAC den beteiligten Personen überlassen bleiben, unter welchem Sicherheitsniveau die einzelnen Attribute verfügbar gemacht werden. Konkret heisst dies, dass es möglich sein muss, dass die Attribute je nach vertraglicher Abmachung zwischen IdP und E-ID-Nutzer auf sämtlichen Sicherheitsniveaus eingesetzt werden können.

  Die KARTAC beantragt, Art. 5 VE E-ID-Gesetz wie folgt um einen Absatz 3bis zu ergänzen (Ergänzung = unterstrichen):

  3 „Eine für ein bestimmtes Sicherheitsniveau ausgestellte E-ID kann auch auf einem tieferen Sicherheitsniveau eingesetzt werden.

  3bis Attribute gemäss Art. 7 Abs. 4 können unabhängig vom Sicherheitsniveau eingesetzt und geteilt werden."

- **Antrag: Massvollen Mindestanforderungen an die Identifizierung und Authentifizierung (Art. 5 Abs. 4 VE E-ID-Gesetz)**

  Wie bereits beim oben stehenden Antrag zu Art. 1 Abs. 2 lit. b VE E-ID-Gesetz ausgeführt, soll sich der Bundesrat bei der Ausarbeitung der E-ID-Verordnung an der zentralen Zielsetzung der weiten Verbreitung und Nutzung der E-ID orientieren. Das bedeutet insbesondere auch, dass der Ausstellungsprozess in Bezug auf die Identifizierung und Authentifizierung zwar sicher, aber auch zweck- bzw. verhältnismässig ausgestaltet sein muss. Die Erfahrungen aus der Praxis zeigen dabei, dass beispielsweise das Erfordernis der persönlichen Vorsprache von den Antragstellenden in der Regel als (zu) grosse Hürde angesehen wird. Eine Video- bzw. eine Online-Identifikation soll deshalb die jeweiligen Mindestanforderungen an eine Identifikation erfüllen (siehe dazu auch den nachfolgenden Antrag zu Art. 6 VE E-ID-Gesetz).

  Um dies zu verdeutlichen, beantragt die KARTAC, Art. 5 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

  „Der Bundesrat regelt die verschiedenen Sicherheitsniveaus, insbesondere die massvollen Mindestanforderungen an die Identifizierung und Authentifizierung."

- **Antrag: Prozessschritt der Prüfung von Identität und Authentizität des Antragstellers im Gesetz explizit aufführen (Art. 6 Abs. 3bis VE E-ID-Gesetz)**

  Stellt eine Person Antrag auf eine E-ID, muss der IdP die Identität und die Authentizität des Antragstellers prüfen, bevor er ihm eine E-ID zuweist. Dieser Schritt wird zwar vom Gesetz impliziert, jedoch nicht explizit aufgeführt. Angesichts der Bedeutung dieses Prozessschritts ist die KARTAC der Auffassung, dass eine ausdrückliche Regelung auf Gesetzesstufe angezeigt ist.

Je nach Sicherheitsniveau ist für die E-ID-Ausstellung eine persönliche Vorsprache vorgesehen. Da – wie bereits oben ausgeführt – eine solche vom Antragstellenden in der Praxis oft als (zu) grosse Hürde angesehen wird, soll auf Gesetzesebene festgehalten werden, dass der persönlichen Vorsprache eine Videoidentifikation oder eine andere gleichwertige Identifizierung gleichgestellt ist. Mit letzterem soll sichergestellt werden, dass in der Praxis dem technischen Fortschritt Rechnung getragen werden kann.

Wie bereits oben stehend zu Art. 5 Abs. 2 VE E-ID-Gesetz ausgeführt, soll im E-ID-Gesetz explizit festgehalten sein, dass sich ein IdP auf eine bestehende (zur Identifikation nach E-ID-Gesetz gleichwertige) Identifikation verlassen darf, unabhängig davon ob er diese selber vorgenommen hat oder ob diese innerhalb des Konzerns oder durch einen beauftragen Dritten erfolgt ist. Nach zum im fraglichen Zeitpunkt geltender Geldwäschereigesetzgebung bereits rechtsgenüglich identifizierte Personen sollen nicht noch einmal identifiziert werden müssen. Nach Auffassung der KARTAC bietet sich die Chance, diesen Grundsatz in Art. 6 VE E-ID-Gesetz zu verankern.

Die KARTAC beantragt, Art. 6 VE E-ID-Gesetz wie folgt um einen Absatz 3bis zu ergänzen (Ergänzung = unterstrichen):

3	„Er beantragt bei der Schweizerischen Stelle [...].
3bis	Er identifiziert und authentifiziert die antragstellende Person. Wo dafür eine persönliche Vorsprache erforderlich ist, kann dieses Erfordernis auch mittels Videoidentifikation oder einer anderen gleichwertigen digitalen Identifikation erfüllt werden. Eine bereits erfolgte zu diesem Gesetz gleichwertige Identifikation muss nicht wiederholt werden, wenn sie im fraglichen Zeitpunkt der geltenden Geldwäschereigesetzgebung entspricht."

- **Antrag: Gesetzliche Verankerung, dass eine Person mehrere E-ID besitzen kann (Art. 6 Abs. 4 VE E-ID-Gesetz)**

  Der Erläuternde Bericht verweist zu Recht auf die Möglichkeit, dass eine Person mehrere E-ID besitzen kann (z.B. je eine E-ID pro Sicherheitsniveau). Aus Sicht der KARTAC erscheint es angezeigt, diese Möglichkeit im E-ID-Gesetz zu erwähnen – inkl. Hinweis, dass die verschiedenen E-ID von unterschiedlichen IdP stammen können.

  Die KARTAC beantragt, Art. 6 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

  „Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person. Eine Person kann mehrere E-ID von einem oder mehreren IdP besitzen."

- **Antrag: Zentrale Führung von Signaturmitteln und Identifizierungseinheit ermöglichen (Art. 6 Abs. 4bis VE E-ID-Gesetz)**

  Der Erläuternde Bericht (Seite 34) geht davon aus, dass die E-ID mit einem Gerät verknüpft wird bzw. darauf angebracht wird. Gleichzeitig wird auf technische Standards im Rahmen der eIDAS-Verordnung verwiesen. Dort findet sich der Standard „CEN 419.241". Dieser ermöglicht es, Zertifikate für e-Signaturen zentral zu verwalten und bei Bedarf abzurufen. So könnte der Inhaber einer E-ID davon entbunden werden, für den Einsatz seiner E-ID ein bestimmtes Gerät zur Hand haben bzw. mitführen zu müssen. Vielmehr könnte er das Zertifikat mit den entsprechenden Zugangsmitteln (Zwei-Faktor-Authentifizierung) einholen. Dies würde mit den Anforderungen bezüglich E-Signatur korrelieren.

Die KARTAC beantragt daher, Art. 6 VE E-ID-Gesetz um einen Abs. 4bis zu ergänzen (Ergänzung = unterstrichen):

4 „Er ordnet die Personenidentifizierungsdaten [...]
„4bis Er kann Signaturmittel und Identifizierungseinheit zentral führen."

- **Antrag: Von der Identitätsstelle zuzuordnende Daten für jedes Sicherheitsniveau verbindlich festlegen (Art. 7 Abs. 2 VE E-ID-Gesetz)**

  Durch die in Art. 7 Abs. 2 VE E-ID-Gesetz gewählte Kann-Formulierung ist offen, ob und welche zusätzlichen Personenidentifizierungsdaten von der identitätsstelle einer E-ID zugeordnet werden. Für Betreiber von E-ID-verwendenden Diensten bestehen damit Unsicherheiten in Bezug auf den Inhalt der jeweiligen E-ID bzw. die bei der Identitätsstelle geprüften Daten. Dies hätte zur Folge, dass die Betreiber von E-ID-verwendenden Diensten den Umfang der geprüften bzw. zugeordneten Daten von IdP zu IdP gesondert zu ermitteln hätten. Dies ist nicht praktikabel. Damit Klarheit und Rechtssicherheit besteht, sind die von der Identitätsstelle einer E-ID zuzuordnenden Daten in Art. 7 VE E-ID-Gesetz für jedes Sicherheitsniveau (Art. 5 Abs. 1 VE E-ID-Gesetz) verbindlich festzulegen.

Die von der Identitätsstelle einer E-ID zuzuordnenden Personenidentifizierungsdaten sind für jedes Sicherheitsniveau auf Gesetzesstufe verbindlich zu definieren.

- **Antrag: Heimatort als zusätzlichen Inhalt einer E-ID aufführen (Art. 7 Abs. 2 VE E-ID-Gesetz)**

  Die Schweizer Ausweisdokumente beinhalten den Heimatort und nicht den Geburtsort. Damit Konsistenz zwischen physischem Ausweis und E-ID besteht, ist in Art. 7 Abs. 2 VE E-ID-Gesetz neben dem Geburtstort auch der Heimatort aufzuführen.

In Art. 7 Abs. 2 VE E-ID-Gesetz ist neben dem Geburtstort auch der Heimatort aufzuführen.

- **Antrag: Art. 7 Abs. 4 VE E-ID-Gesetz um den Begriff „Attribute" ergänzen**

  Im Sinne des oben zu Art. 2 lit. k VE E-ID-Gesetz gestellten Antrags (Definition des Begriffs „Attribute") ist Art. 7 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

„Der IdP kann einer E-ID weitere Daten (Attribute) zuordnen.

- **Antrag: Weitergabe von Personenidentifizierungsdaten flexibler regeln (Art. 10 Abs. 3 VE E-ID-Gesetz)**

  Art. 10 Abs. 3 VE E-ID-Gesetz legt fest, dass namentlich Betreiber von E-ID verwendeten Diensten weder die Personenidentifizierungsdaten gemäss Art. 7 Abs. 2 VE E-ID-Gesetz noch die darauf basierenden Nutzungsprofile Dritten bekannt geben dürfen. Im Erläuternden Bericht wird dazu ausgeführt, dass weder der Handel noch die unentgeltliche Weitergabe von Daten – auch nicht innerhalb eines Konzerns – erlaubt sein sollen. Diese Bestimmung in ihrer absoluten Form erachtet die KARTAC als zu weitgehend, nicht kompatibel mit der Geldwäschereigesetzgebung und nicht praktikabel.

  Was den Bereich der Geldwäschereibekämpfung betrifft, ist dort eine Delegation der Identifizierung der Vertragspartei ausdrücklich erlaubt.

Die Geldwäschereiverordnung-FINMA schreibt diesbezüglich vor, dass der delegierende Finanzintermediär Kopien der Unterlagen, d.h. auch der Identifikationsdokumente, zu seinen Akten zu nehmen hat[3]. Nimmt nun ein ordentlich ausgewählter, instruierter und überwachter Dritter eine Identifizierung nach Geldwäschereigesetzgebung unter Zuhilfenahme eines E-ID verwendeten Dienstes vor, so muss es ihm vernünftigerweise gestattet sein, die Kopien der Identifikationsdokumente dem Finanzintermediär (im Einklang mit den Vorschriften der Geldwäschereiverordnung-FINMA bzw. der VSB) zukommen zu lassen. Dies wird mit Art. 10 Abs. 3 VE E-ID-Gesetz verunmöglicht[4]. Analog präsentiert sich die Situation bei der konzerninternen Identifizierung[5], wo ebenfalls verlangt ist, dass Kopien der Identifikationsdokumente erstellt werden.

Bezüglich des vorgesehenen Verbots der Weitergabe der Daten innerhalb eines Konzerns ist ganz allgemein darauf hinzuweisen, dass eine solche Einschränkung der heutigen Realität nicht entspricht und nicht praktikabel wäre. So wäre z.B. eine konzernzentrale Verwaltung von Kundeninformationen nicht mehr möglich. Zusätzlich ist die vorgesehene Bestimmung nicht kundenfreundlich: Bietet ein Konzern seine Produkte z.B. über mehrere Konzerngesellschaften an, so müsste eine Kunde für jedes Produkt separat identifiziert werden. Eine Authentifizierung würde nicht ausreichen.

Die KARTAC plädiert daher dafür, dass anstelle des in Art. 10 Abs. 3 VE E-ID-Gesetz stipulierten absoluten Verbotes der Weitergabe von Daten das etablierte datenschutzrechtliche Prinzip zur Anwendung kommen, dass es der Inhaberin oder dem Inhaber der E-ID überlassen bleibt zu bestimmen, wie mit ihren/seinen Daten zu verfahren ist. Ein entsprechendes Akzept seitens der künftigen E-ID-Inhaberin oder des künftigen Inhabers könnte z.B. im Rahmen des in Art. 6 Abs. 1 VE E-ID-Gesetz angesprochenen Antragsprozesses rechtsgenüglich eingeholt werden und Grundlage für eine weitergehende Nutzung von Daten im Einverständnis mit der betroffenen Person sein.

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 ist zu ersetzen. An dessen Stelle ist ein 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 zubilligt.

2.3 Anbieterinnen von Identitätsdienstleistungen / IdP (Art. 17 f. VE E-ID-Gesetz)

- **Antrag: Orientierung an internationalen Standards bei der Bestimmung der technischen Standards (Art. 18 Abs. 2 VE E-ID-Gesetz)**

  Damit eine Interoperabilität ggf. auch mit ausländischen Systemen hergestellt werden kann, ist es notwendig, dass die Standards und Schnittstellen entsprechend dem im Ausland Üblichen ausgestaltet werden. Dieses Erfordernis soll in der Delegationsnorm von Art. 18 Abs. 2 VE E-ID-Gesetz aufgeführt werden.

2	„Der Bundesrat bestimmt die technischen Standards und definiert die Schnittstellen. Er orientiert sich dabei an internationalen Standards."

[3] Art. 29 Abs. 2 GwV-FINMA, analog Art. 43 Abs. 2 VSB 16

[4] Art. 7 Abs. 2 lit. e VE E-ID-Gesetz nennt die Staatsangehörigkeit, welche für die Identifizierung einer Vertragspartei wesentlich ist. Eine Weiterleitung dieses wichtigen Attributes wäre gemäss Art. 10 Abs. 3 VE E-ID-Gesetz nicht möglich.

[5] Art. 28 Abs. 2 lit. a GwV-FINMA in Verbindung mit Art. 29 Abs. 2 GwV-FINMA, Art. 19 VSB 16

Die KARTAC dankt Ihnen im Namen ihrer Mitglieder für die Entgegennahme und Prüfung unserer Ausführungen und Anliegen. Für Rückfragen und Erläuterungen stehen wir Ihnen gerne zur Verfügung

Freundliche Grüsse

KARTAC
Interessengemeinschaft der Zahlkartenindustrie

Uwe Behr
Präsident

Beat Steinmann
Sekretär

P.O. Box 360, CH 8024 Zürich

per Email zu Handen: copiur@bj.admin.ch

Frau Bundesrätin
Simonetta Sommaruga
Eidg. Justiz- und Polizeidepartement
3003 Bern

22. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Namens der Swiss Data Alliance bedanken wir uns für die Möglichkeit, unsere Position zum Entwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) darzulegen und reichen Ihnen hiermit unsere Stellungnahme ein.

1. Legitimation

Die Swiss Data Alliance, gegründet am 22. März 2017, ist ein Verein mit Sitz in Zürich.

Gründer sind die folgenden Vereine: der Schweizerische Verband Telekommunikation asut, der Schweizerische Verband der ICT-Anbieter Swico, der Verein Daten und Gesundheit, die Swiss Alliance for Data-Intensive Services und der Verein Opendata.ch. Diese Verbände repräsentieren zusammen mehr als 450 Unternehmungen aus den Bereichen Informatik und Telekommunikation sowie zahlreiche Organisationen, Institutionen und Privatpersonen.

Swiss Data Alliance setzt sich für eine zukunftsorientierte Datenpolitik ein, damit Daten ihr innovatives Potenzial in der Schweiz voll entfalten können. Das Kernelement einer funktionierenden Dateninfrastruktur ist ein staatlicher elektronischer Identitätsnachweis. Unser ausführlicheres Positionspapier zu diesem Thema finden Sie unter http://www.swissdataalliance.ch.

2. Antrag zur Überarbeitung

Eine Arbeitsgruppe von Experten der Swiss Data Alliance hat sich in den letzten Wochen mit der Vorlage beschäftigt und ist dabei zum Schluss gekommen, dass der vom Bundesrat vorgelegte Entwurf und das darin abgebildete Konzept (namentlich das „Konzept 2016“ des fedpol „Staatlich anerkannte elektronische Identifizierungsmittel (E-ID)“) in die falsche Richtung geht. Swiss Data Alliance weist den Vorentwurf in der vorliegenden Form deshalb zur Überarbeitung zurück.

Die seither geführten Gespräche mit den betroffenen Kreisen haben gezeigt, dass die Analyse von Swiss Data Alliance auf breite Zustimmung stösst. Namentlich haben wir gesehen, dass in den folgenden Punkten in weiten Kreisen Einigkeit besteht: (i) der staatliche elektronische Identitätsnachweis (staatliche E-ID) soll eine Staatsaufgabe sein; (ii) der Staat gibt die staatliche E-ID entweder alleine heraus oder beauftragt maximal einen Dritten, diese hoheitliche Aufgabe im Auftrag des Staates wahrzunehmen; (iii) die Nutzung der staatlichen E-ID soll für bestimmte Anwendungen zwingend sein (z.B. in den hoheitlichen Anwendungsbereichen E-Government und E-Health).

3. Grundsätzliche Überlegungen zur Überarbeitung

a) Bedürfnis nach einem digitalen Ausweis

Die digitale Welt verlangt für eine Vielzahl von Dienstleistungen unsere Identifikation als Nutzer. Manchmal genügen dazu einige Angaben zur Person, z.B. eine gültige Email-Adresse oder bloss eine Kreditkartennummer. Manchmal sind aber Informationen nötig, die von einer staatlichen Stelle beglaubigt sein müssen, weil die Applikation besonders heikel ist. Beispiele sind das elektronische Patientendossier, das E-Voting oder ein Strafregisterauszug. Wie in der nicht-digitalen Welt benötigen wir dann einen amtlichen Ausweis, welcher unsere Identität staatlich nachweist.

b) Glaubwürdigkeit der Eidgenossenschaft

In der nicht-digitalen Welt hat der Staat dazu bereits vor langer Zeit hoheitliche Institutionen und Verfahren eingerichtet, über welche wir einen solchen amtlichen Ausweis beziehen können. Die Glaubwürdigkeit der Schweizer Ausweispapiere, insbesondere des Schweizer Passes, ist legendär und Basis für zahllose Geschäftstransaktionen. Wir vertrauen dem Schweizer Pass, weil er vom Staat und nicht von einer privaten Unternehmung oder Organisation ausgestellt wird.

Glaubwürdigkeit und Vertrauen sind auch in der digitalen Welt elementar für den Aufbau erfolgreicher Geschäftsbeziehungen. Wir wissen, dass dieses Vertrauen bei digitale Dienstleistungen leider nicht immer gerechtfertigt ist. Wir müssen uns stets kritisch fragen, welche persönlichen Angaben wir zu welchem Zweck zur Verfügung stellen wollen und welches Risiko wir dabei eingehen.

Besonders kritisch wird es dann, wenn der staatliche Nachweis unserer elektronischen Identität verlangt wird. Hier kann für uns selber, aber auch für den Dienstleister, nur die höchste Vertrauensstufe ausreichend sein. Der staatliche Nachweis der elektronischen Identität muss daher genau wie bei den nicht-digitalen amtlichen Ausweispapieren eine hoheitliche Aufgabe bleiben, welche der Staat selber wahrnimmt. Nur dann ist die höchste Stufe des Vertrauens und der Glaubwürdigkeit gewährleistet, welche gewisse elektronische Geschäfte erfordern.

Wir wollen auf unser elektronisches Patientendossier nicht mit dem Ausweis eines Transportunternehmens zugreifen und wir wollen auch unsere Steuerunterlagen nicht mit dem Ausweis einer Bank einreichen. Wir wollen unsere staatliche elektronische Identität nicht von einem Detailhändler oder einer Versicherung, sondern nur vom Staat selbst beziehen.

4. Zum Vorentwurf

Der vorliegende Entwurf für ein Bundesgesetz über anerkannte elektronische Identifikationsmittel (EID-Gesetz) schlägt vor, die staatliche elektronische Identifikation an Unternehmen und Organisationen abzugeben, welche dafür zertifiziert werden. Die Swiss Data Alliance ist der Ansicht, dass dieses Konzept zum Scheitern verurteilt ist. Die Unternehmen und Organisationen, welche sich als Ausgabestelle für staatliche elektronische Ausweise zertifizieren lassen, mögen noch so glaubwürdig sein – die Nutzer werden ihnen nie dasselbe Vertrauen schenken wie einer staatlichen Stelle, welche diese Aufgabe hoheitlich wahrnimmt. Dieses ungeteilte Vertrauen ist aber die Basis für einen erfolgreichen elektronischen Schweizer Pass und damit Grundlage für den Erfolg der digitalen Wirtschaft und Verwaltung in der Schweiz. Es gibt zahllose Aufgaben, welche die Wirtschaft besser lösen kann als der Staat. Die hoheitliche Abgabe von analogen und elektronischen Identitätsausweisen gehört nicht dazu. Detaillierte Begründungen hierzu entnehmen Sie bitte unserem Positionspapier unter http://www.swissdataalliance.ch. Am Vorentwurf kritisiert Swiss Data Alliance namentlich Folgendes:

Falscher Fokus: Im Vorentwurf wird der Begriff der E-ID-Dienstleistungen zu weit verstanden. Es ist richtig, dass der Staat keine der Privatwirtschaft vorzubehaltenden Dienstleistungen („E-ID verwendende Dienste“) anbieten sollte. Er soll sich auf den eng zu verstehenden Kernbereich beschränken. Aber dieser Kernbereich ist eine staatliche Aufgabe.

Beschreibung „E-ID“ schärfen: Ob ein separates E-ID-System als neues „Register“ aufzubauen ist, ist noch in keiner Weise geklärt. Denkbar ist, dass nur ein blosser Abfrageservice eingerichtet wird, der auf bereits bestehende Register zugreift.

Die E-ID darf keine Nummer sein: Weiter ist die Beschreibung, was die E-ID ausmacht, unvollständig. Zentral – gerade aus Gründen des Datenschutzes und zum Schutz vor Überwachung des Bürgers im Staat – ist hervorzuheben, dass die staatliche E-ID gerade keine Nummer ist. Einmalige, zeitlich limitiert gültige transaktionsbezogene Nummern (Authentisierungscodes) sollen generiert werden können; aber es wäre falsch, die E-ID als neue permanente zentrale Personennummer einzuführen.

Systembedingte Strukturierungsnummern sind nicht zu kommunizieren: Der Vorentwurf geht deswegen mit der „E-ID-Registrierungsnummer“ (einer Person eindeutig zugeordnete Identifikationsnummer) in die falsche Richtung. Ein neues Register, falls tatsächlich benötigt, müsste wohl über eine Nummer erschlossen werden, und zwar für jeden neu anzulegenden Eintrag, der über die AHVN13 gespiesen wird (aus den Registern ISA, ZEMIS und Infostar sowie gegebenenfalls ZAS-UPI); diese Nummer könnte durchaus als „E-ID-Registrierungsnummer“ bezeichnet werden. Die E-ID-Registrierungsnummer wäre aber auf jeden Fall nur eine verwaltungsintern zu benutzende technische Ordnungsnummer zur Führung und zum Aufbau des E-ID-Systems. Diese Angabe darf nicht nach aussen bekannt gegeben werden, zumal eine Bekanntgabe nach aussen für das Funktionieren des E-ID-Systems nicht erforderlich ist.

Rechtsunsicherheit über Datenhoheit: Aus Wirtschaftssicht ist sodann hervorzuheben, dass Art. 10 des Vorentwurfs erhebliche Konsequenzen auf den bereits bestehenden Datenbestand bei privaten Unternehmen haben könnte[1]. Würde sich ein privates Unternehmen nach dem Konzept des Vorentwurfs als IdP melden, müsste es gewärtigen, einen Grossteil seiner Daten nicht mehr verwerten zu können, soweit er mit dem Katalog gemäss Art. 7 des Vorentwurfs übereinstimmt: Wie ist der bestehende Datenbestand abzugrenzen gegenüber jenem, den das Unternahmen „als IdP“ erwirbt? Entweder ist Artikel 10 des Vorentwurfs ein Papiertiger oder aber ein Brocken mit verheerender Wirkung.

Zeitverlust: Insgesamt führt das Konzept des Vorentwurfs zum Risiko, dass der Schweiz noch lange Zeit ein einheitlicher Standard fehlen wird (nicht zuletzt wegen der zu befürchtenden Marktzersplitterung). Das ist mit Blick auf die Digitalisierung, die heute, im Hier und Jetzt stattfindet und bereits pulsiert, unannehmbar. Die Schweiz würde mit dem vorliegenden Gesetzesentwurf gebremst. Dies muss um jeden Preis verhindert werden. Deswegen braucht es sofort eine „E-ID für alle“.

5. Konstruktiver Gegenvorschlag

a) Was ist die E-ID?

Swiss Data Alliance hat im Rahmen ihrer Kontakte in der Privatwirtschaft festgestellt, dass die E-ID zu kompliziert „gedacht wurde“. Deswegen ging der Blick aufs Wesentliche verloren und die Beschreibung, was eine E-ID eigentlich ist oder sein sollte, fällt nicht allen leicht. Um diesem Umstand zu begegnen, hat die Swiss Data Alliance eine Lösungsskizze erstellt, die klärt, was von einer staatlichen E-ID erwartet wird. Sie finden diese Lösungsskizze in Anhang 1.

b) Grundzüge der alternativen Regelung

Aus Sicht der Swiss Data Alliance sollte in Bezug auf den staatlichen elektronischen Identitätsnachweis Folgendes gelten:

- der **staatliche elektronische Identitätsnachweis** ist eine **hoheitliche Aufgabe des Bundes**. Die Staatsaufgabe besteht darin, innerhalb der Verwaltung und für Dritte, auf Anfrage die Korrektheit

[1] Art. 10 des Vorentwurfs stellt die folgenden Verwertungsschranken auf: „IdP dürfen **von der Identitätsstelle übermittelte** Personenidentifizierungsdaten nur bearbeiten, um nach diesem Gesetz Identifizierungen und Authentifizierungen durchzuführen.“ (Art. 10 Abs. 1); „Weder anerkannte IdP noch Betreiberinnen von E-ID-verwendenden Diensten dürfen **die Personenidentifizierungsdaten gemäss Artikel 7 Absatz 2** oder **die darauf basierenden Nutzungsprofile** Dritten bekannt geben“ (Art. 10 Abs. 3). [Hervorhebungen jeweils nicht im Original]

der Personenidentifizierungsdaten sowie die Authentizität der zu identifizierenden Person zu prüfen (daraus leitet sich der von Swiss Data Alliance verwendete Begriff des „staatlichen elektronischen Identitätsnachweises“ ab).

- die **staatliche E-ID ist keine Nummer**, sondern die Gesamtheit der vom Staat (entsprechend Art. 7 des Vorentwurfs) bestimmten Personenidentifizierungsdaten, welche der Staat als Eigenschaften einer bestimmten Person verifiziert und in den dazu bestimmten Registern gespeichert hat. Das staatliche E-ID-System benötigt von Seiten einer abfragenden Applikation keine einheitliche, auf einen Einzelnen bezogene Nummer, sondern nur einen transaktionsbezogenen Code, welche diese von der zu identifizierenden Person erhält.
- der **Bund sollte die staatliche E-ID ausgeben und verwalten**. Die Befürchtung des Bundes, mit der technologischen Entwicklung nicht mithalten zu können, sieht die Swiss Data Alliance nicht als validen Grund an, die Bestätigung der E-ID als Staatsaufgabe zu verneinen. Auch das Kostenargument (Erläuternder Bericht zum Vorentwurf, Ziffer 1.3.1) überzeugt nicht.
- **Sourcing für das E-ID-System**: Der Bund sollte eine Public-Private-Partnership prüfen oder einen Dienstleister mandatieren, das staatliche E-ID-System technisch zu betreiben. Im Umfeld der Ausgabe von Ausweisdokumenten (namentlich im Kontext des Ausweisgesetzes) bestehen bereits vergleichbare Systeme. Ausserhalb des Sourcing-Bereichs liegen Mehrwertdienste. Solche Mehrwertdienste kann jeder (auch der Dienstleister, mit dem der Bund zusammenarbeitet) auf eigene Rechnung, auf eigenes Risiko und zum eigenen Vorteil anbieten.
- **Spezifikation des E-ID-Systems**: Das vom Bund zu betreibende System besteht aus Datenschnittstellen zu den bestehenden Personenregistern, Sicherheitselementen, einer externen Schnittstelle (API) und einem Dienst, der eine Überprüfung von Personenidentifizierungsdaten und deren Zuordnung zu einer bestimmten Person (Authentifizierung) ermöglicht.
- **Spezifikation der Schnittstelle (API und evtl. Webzugang) und Nutzungsbedingungen**: die Swiss Data Alliance regt an, vertieft zu prüfen, inwiefern Anbieter von die E-ID verwendenden Diensten sich mittels eines verwaltungsrechtlichen Vertrags verpflichten müssen, bestimmte Nutzungsbedingungen zur Verwendung der Schnittstelle zu akzeptieren.
- **Ausweisdokumente**: Ergänzend zum E-ID-System, aber nur als Add-On, können Ausweisdokumente mit maschinenlesbaren Personenidentifizierungsdaten ausgegeben werden. Die Anbindung an Ausweisdokumente ist eine Erweiterung, und nicht Kerngehalt eines funktionierenden E-ID-Systems des Bundes.

Die Swiss Data Alliance unterbreitet im Anhang eine Lösungsskizze für die staatliche E-ID, die aufzeigt, wie die vorstehenden Überlegungen technisch umgesetzt werden können (Anhang 1).

c) Zur gesetzlichen Grundlage insbesondere

Es stellt sich die Frage, ob eine neue formell-gesetzliche Grundlage zu schaffen ist, um das staatliche E-ID-System aufzubauen. Da der Erlass einer solchen formell-gesetzlichen Grundlage normalerweise einige Zeit in Anspruch nimmt, ist die Frage von grosser Bedeutung.

Sofern das E-ID-System aus einem blossen Abfrageservice auf bestehende Register besteht, hält die Swiss Data Alliance für möglich, dass die bestehenden Registergesetze als Basis für eine Verordnung des Bundesrats ausreichen (Ausweisgesetz, Ausländergesetz, Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich, BGIAA; Zivilgesetzbuch und Zivilstandsverordnung sowie ZAS-Verordnung mit deren gesetzlichen Grundlagen). Jedenfalls sollte dieser Aspekt nochmals durchdacht werden (namentlich mit Blick auf die Notwendigkeit der Verwendung der AHVN13, des Verbots von Parallelregistern und der datenschutzrechtlich erforderten Regelung von Abfragediensten). Zu beachten ist insbesondere, dass Abfragen nach dem in Anhang 1 vorgeschlagenen Modell mit Zustimmung der betroffenen Person im Einzelfall erfolgen.

Wenn mit dem „E-ID-Gesetz“ ein neuer Erlass begründet werden sollte, empfiehlt die Swiss Data Alliance aber auf jeden Fall, ihn zu vereinfachen und zu entschlacken. Mit dem in dieser Eingabe dargestellten Ansatz sollte dies möglich sein. Auf Wunsch führen wir gerne Ergänzendes dazu aus.

Bei Schaffung eines neuen Erlasses sollte die verfassungsrechtliche Herleitung zudem nicht allein in Art. 95 und Art 122 BV gesucht werden (so der Vorentwurf), weil sonst z.B. die Regelung in Art. 13 des Vorentwurfs nicht begründet werden könnte (Art. 13 des Vorentwurfs betrifft nur den Bereich eGovernment, der sich mit der Regelung allein aus der zivilrechtlichen Optik kaum rechtfertigen liesse). Es bieten sich allerdings mit den Bestimmungen zum Registerrecht (Art. 65 Abs. 2 BV) und jenen zum Ausweisrecht auf Basis der Bestimmungen zum Bürgerrecht, Ausländerrecht, Asylrecht und Beziehungen zum Ausland (Art. 38, Art. 121 und Art. 166 BV) sinnvolle Ergänzungen an.

d) Zur Gebührenfrage insbesondere

Staatliche Grundversorgung soll grundsätzlich gebührenfrei zur Verfügung gestellt werden. Jeder und jede Anspruchsberechtigte sollen eine staatliche E-ID ausgestellt erhalten, ohne dafür bezahlen zu müssen. Die Nutzer und Nutzerinnen müssen die E-ID im E-ID-System allenfalls aktivieren (in Form einer Bestätigung), ansonsten steht die E-ID aber im Sinne eines Automatismus für jede bzw. jeden Anspruchsberechtigten voraussetzungslos zur Verfügung.

e) Einzelfragen

Ergänzend zeigen wir auf, wie mögliche ergänzende Fragen zum konstruktiven Gegenvorschlag der Swiss Data Alliance zu beantworten sind:

Warum braucht die Schweiz eine staatliche E-ID?
eGovernment, eHealth, eVoting, eCommerce etc. setzen voraus, dass sich die Nutzer über ihre Identität ausweisen. Die E-ID stellt die transaktionsbezogene Identifizierung sicher. Eine E-ID des Bundes bildet somit die Basisinfrastruktur für eine digitale Schweiz. Die staatliche E-ID ermöglicht den längst fälligen Durchbruch aller aufgeführten eThemen.

Was ist die Grundvoraussetzung für die staatliche E-ID?
Vertrauen gegenüber dem Herausgeber einer elektronischen Identität ist der Schlüsselfaktor für die Verbreitung und Nutzung einer staatlichen E-ID. Der Bund geniesst in der Schweiz das höchste Vertrauen und mehr als private Anbieter. Der Bund ist am besten geeignet, eine staatliche E-ID anzubieten.

Warum ist die E-ID eine hoheitliche Aufgabe?
Der Bund muss seine hoheitliche Aufgabe so wie in der physischen Welt (Pass, Identitätskarte) auch in der digitalen Welt (E-ID) wahrnehmen. Nur mit einer staatlichen E-ID des Bundes wird diese von den Berechtigten auch in allen Lebenslagen und für alle Arten von Geschäften eingesetzt werden. Zudem ist nur der Bund in der Lage, das Angebot der staatlichen E-ID langfristig sicherzustellen, da davon auszugehen ist, dass zahlreiche Anbieter wieder vom Markt verschwinden werden.

Warum ist der europäische Einbezug in die Schweizer E-ID von Bedeutung?
Trotz E-ID kann sich die Schweiz mit ihrer elektronischen Identität nicht abschotten und es muss sichergestellt sein, dass die Integration in das System der EU (eIDAS) gewährleistet ist. Diese Integration kann nur der Bund direkt mit der EU abstimmen. Diese Aufgabe sollte nicht privaten Anbietern überlassen werden.

Soll jeder Bürger/Einwohner der Schweiz und jeder Auslandschweizer eine staatliche E-ID haben?
Ja. Nur wenn alle Unternehmen (egal ob KMU oder Grossunternehmen) davon ausgehen können, dass alle ihre (potentiellen) Kunden einen staatlichen elektronischen Identitätsnachweis besitzen, können sie entsprechend neue Geschäftsmodelle entwickeln.

Warum muss der Bund die Aufgabe und die Verantwortung als Herausgeber einer staatlichen E-ID wahrnehmen?
Nur der Bund kann sicherstellen, dass es eine E-ID für alle Berechtigten gibt, auf deren Basis andere Anbieter weitere Dienste herausgeben können. In diesem Sinne ist die Herausgabe einer E-ID des Bundes auch nicht als Konkurrenzprodukt zu verstehen. Es sollen alle davon profitieren, nicht nur einzelne

Grossunternehmen. Allenfalls kann der Bund einen Dritten mandatieren, die Herausgabe der E-ID für ihn wahrzunehmen.

Warum sollte der Bund möglichst bald eine E-ID herausgeben?
Der vorgeschlagene Zeitplan sieht vor, dass ab ca. 2021 der Bund Anbieter von elektronischen Identitäten zertifizieren wird. Dies ist viel zu spät. Innovationsfähige Unternehmen haben jetzt Ideen und wollen diese jetzt verwirklichen. Zuwarten führt zu Verlangsamung oder einer Abwanderung von Innovation ins Ausland. Das Vorhandensein der E-ID in der Schweiz gehört zum Mindeststandard einer in der Digitalen Welt leistungsfähigen Volkswirtschaft.

Hat nicht bereits das Vorhaben „SuisseID" bewiesen, dass der Bund solche Angebote nicht tragen sollte?
Nein. Der Bund hat zwar zu Beginn die SuisseID mitfinanziert, angeboten wird sie jedoch privatwirtschaftlich durch die Schweizerische Post/SwissSign und die Quo Vadis Trustlink Schweiz AG.

Warum ist der Weg über die Privatwirtschaft nicht angezeigt?
Der "private Weg" führt zu verschiedenen, sich konkurrenzierenden Angeboten und damit zu Unübersichtlichkeit. Wir wollen auf unser elektronisches Patientendossier nicht mit dem Ausweis eines Transportunternehmens zugreifen und wir wollen auch unsere Steuerunterlagen nicht mit dem Ausweis einer Bank einreichen. Wir wollen unsere staatliche elektronische Identität nicht von einem Detailhändler oder einer Versicherung, sondern nur vom Staat selbst beziehen.

Warum muss der Bund die Kosten für die Entwicklung der E-ID übernehmen?
Die Herausgabe eines amtlichen Ausweises, ob auf Papier oder in elektronischen Form, ist eine hoheitliche Aufgabe. Der Entscheid zur staatlichen E-ID sollte sich zunächst nicht an kommerziellen oder technischen Aspekten orientieren. Im Vordergrund stehen das Grundrecht auf einen staatlichen Ausweis, Grundsätze von Rechtsgleichheit und Fairness in der digitalen Welt sowie das Potential, für alle zur Verfügung stehende, nichtdiskriminierende und sichere Mindestinfrastrukturen / Dateninfrastrukturen zu schaffen.

Sind die Kosten nicht zu hoch?
Die Kosten können minimiert werden, wenn die staatliche E-ID so einfach wie nur möglich ausgestaltet wird. Die staatliche E-ID sollte also strikt auf die Kernfunktion des staatlichen elektronischen Identitätsnachweises beschränkt werden. Alle Optionen für weitere E-ID-Dienste sollten dem Markt überlassen werden.

6. Abschliessende Bemerkungen und weiteres Vorgehen

Wir setzen uns dafür ein, dass der Vorentwurf des E-ID-Gesetzes überarbeitet wird. Gleichzeitig sollte die Privatwirtschaft erneut einbezogen werden, damit die Spezifikation des staatlichen elektronischen Identitätsnachweises im Sinne eines von der Privatwirtschaft mitgetragenen staatlichen Service definiert und entwickelt werden kann. Die Swiss Data Alliance hat verschiedene private Anbieter im Markt in diesem Sinne bereits kontaktiert und zusammengeführt. Auf diesen konstruktiven Vorarbeiten kann aufgebaut werden.

Für vertiefende Erläuterungen unserer Sichtweise zu diesen Fragen im direkten Gespräch stehen wir gerne zur Verfügung.

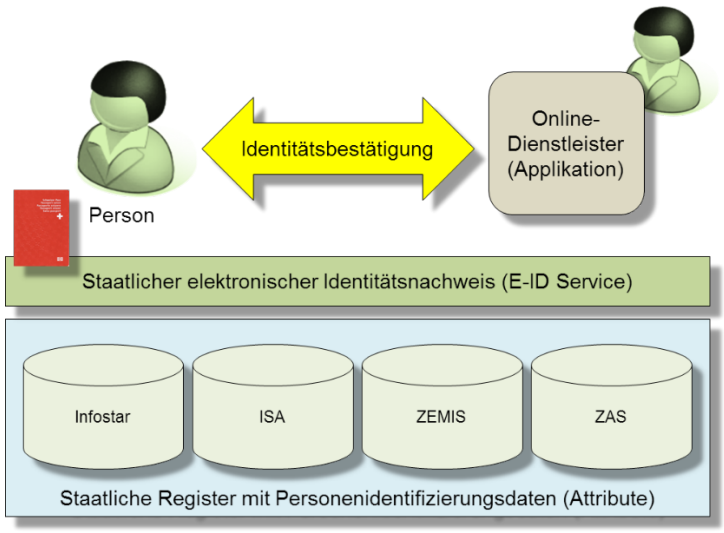
Mit vorzüglicher Hochachtung

André Golliez, Präsident Christian Laux, Vizepräsident

Anhang 1 Der staatliche elektronische Identitätsnachweis (Lösungsskizze)

Der staatliche elektronische Identitätsnachweis
Lösungsskizze

Voraussetzungen

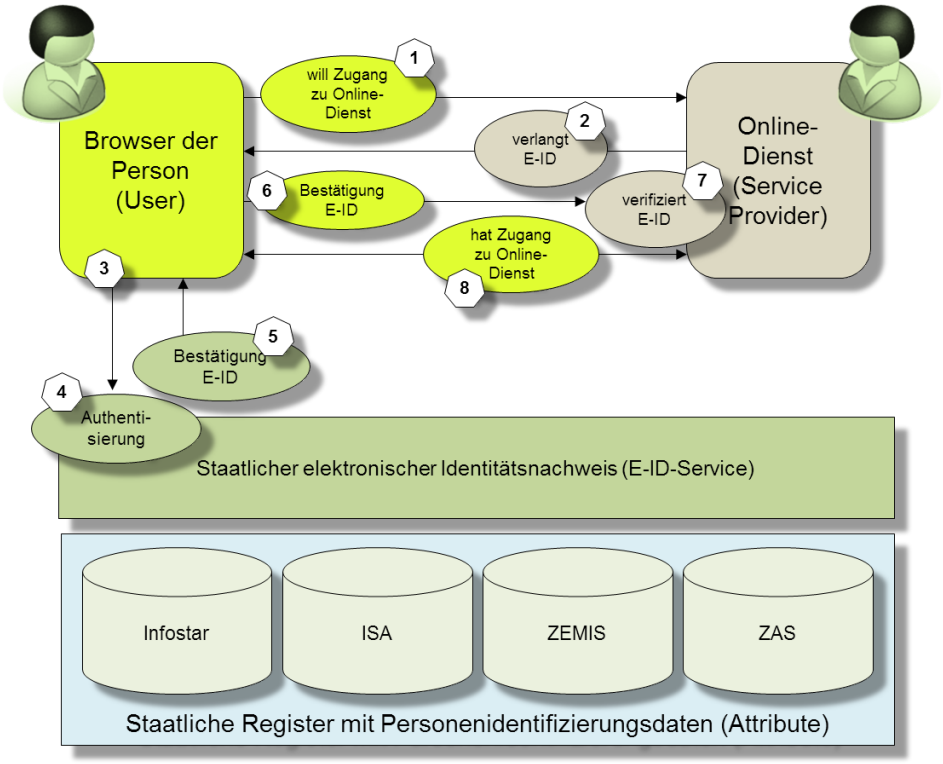


Der staatliche elektronische Identitätsnachweis beruht auf den folgenden Voraussetzungen:

1. Der staatliche elektronische Identitätsnachweis einer Person gegenüber einem Online-Dienstleister («Identitätsbestätigung» oder «Authentisierung») beruht auf den staatlich beglaubigten Personenidentifizierungsdaten (Attribute), welche in den bestehenden staatlichen Registern geführt werden (Infostar, ISA, ZEMIS und ZAS).
2. Die Verwaltung dieser Attribute ist für diese Register rechtlich bereits geregelt. Zusätzlich zu den bestehenden Verwendungszwecken dieser Daten wird deren Nutzung für den staatlichen elektronischen Identitätsnachweis zugelassen.
3. Für den staatlichen elektronischen Identitätsnachweis stehen die Attribute aus diesen Registern im Rahmen eines gemeinsamen E-ID-Service zur Verfügung und können dort von der Person selbst sowie den nachfragenden Online-Dienstleistern, sofern dazu berechtigt, abgefragt werden (Ablauf der Identitätsbestätigung siehe unten).
4. Jede Person hat für ihre Attribute einen Lesezugriff und kann von ihnen eine Kopie zur freien Verwendung und Weitergabe anfertigen. Die Person wird für diesen Zugriff durch die für den staatlichen elektronischen Identitätsnachweis zuständige Stelle autorisiert. Zudem hat jede Person die Möglichkeit, die Abfrage ihrer Attribute durch Dritte nachzuvollziehen («Logfile»).
5. Jede Anbieterin eines den staatlichen E-ID-Service verwendenden Online-Dienstes ist grundsätzlich berechtigt, von einer Person einen staatlichen elektronischen Identitätsnachweis zu verlangen, als Voraussetzung für die Nutzung der betreffenden Applikation.
6. Jede Person ist grundsätzlich frei, ob und in welchem Umfang sie den staatlichen elektronischen Identitätsnachweis gegenüber einer bestimmten Applikation erbringen will oder ob sie lieber auf die Nutzung der Applikation verzichtet.

7. Der staatliche elektronische Identitätsnachweis ist in der Lage, jeder abfragenden Applikation gegenüber die Identität einer bestimmten Person nachzuweisen, welche dieser Identifizierung zugestimmt hat.

Möglicher Ablauf der staatlichen elektronischen Identitätsbestätigung[1]



Die staatliche elektronische Identitätsbestätigung auf Basis der vorhandenen Personenregister kann wie folgt ablaufen :

1. Eine Person (User) will den Online-Dienst eines Service Providers nutzen und macht die dazu notwendigen Angaben (z.B. Name, Vorname, Adresse bzw. ein beim E-ID-Service vom User hinterlegter eindeutiger Benutzername).
2. Der Online-Dienst verlangt vom User den staatlichen Nachweis seiner Identität (E-ID) und generiert dafür eine entsprechende Anfrage an den E-ID Service.
3. Der Browser des Users leitet die Anfrage an den staatlichen E-ID-Service weiter.
4. Der staatliche E-ID-Service überprüft die Anfrage und authentisiert die betreffende Person.
5. Der staatliche E-ID-Service generiert eine Bestätigung der E-ID und schickt diese an den Browser des Users.
6. Der Browser des Users leitet die Bestätigung der E-ID an den Online-Dienst weiter.
7. Der Online-Dienst verifiziert die Bestätigung der E-ID.
8. Der User wurde erfolgreich identifiziert und hat nun Zugang zum Online-Dienst.

[1] Dieser Ablauf des staatlichen elektronischen Identitätsbestätigung orientiert sich am internationalen Standard SAML (siehe für eine vereinfachende Erläuterung hierzu https://blog.surf.nl/en/saml-for-dummies). Für die Abfrage von spezifischen Attributen beim E-ID Service direkt durch den Online-Dienst (Service Provider) wäre zudem OAuth einsetzbar. Zudem ist der eCH-Standard eCH-0170 (Qualitätsmodell zur Authentifizierung von Subjekten) sowie das zugehörige IAM Glossar eCH-297 zu berücksichtigen.

SWISS FINTECH INNOVATIONS

Per eMail: **copiur@bj.admin.ch**

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

Zürich, 29. Mai 2017

Vorentwurf Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) – Stellungnahme von Swiss Fintech Innovations

Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 22. Februar 2017 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartement (EJPD) betreffend Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Wir danken Ihnen und benützen die Gelegenheit zur Stellungnahme hiermit gerne.

Der Verband **Swiss Fintech Innovations** (SFTI, www.swissfintechinnovations.ch) vertritt die Interessen seiner Mitglieder im Bereich der Digitalisierung und Innovation in der Finanzindustrie. Zu den Mitgliedern des Verbands gehören derzeit: AXA Winterthur, Credit Suisse, CSS, Generali Versicherungen, Helvetia, Hypothekarbank Lenzburg, Lombard Odier, Luzerner Kantonalbank, Raiffeisen, Schroders, SIX Group, Swiss Life, Swiss Fintech Innovation Lab an der Universität Zürich, SYZ Group, Vontobel, Zürcher Kantonalbank und Zuger Kantonalbank. Unsere Arbeitsgruppe „Regulations“ beschäftigt sich mit Gesetzgebung und Regulation rund um Innovation und Digitalisierung in der Finanzindustrie.

Unsere **Stellungnahme** lässt sich wie folgt zusammenfassen:

1. Das vordringlichste Ziel ist die schnelle Einführung einer breit akzeptierten E-ID mit einem hohen Sicherheitsstandard.

2. Die vorgeschlagene Aufteilung der Aufgaben, Kompetenzen und Verantwortlichkeiten zwischen staatlichen Stellen und privaten Unternehmen trägt den bereits weit fortgeschrittenen Projekten privater Unternehmen Rechnung und unterstützt damit eine schnelle Einführung.

3. Damit auch das Ziel einer breiten Akzeptanz erreicht werden kann, muss sichergestellt werden, dass der Geschäftsverkehr aller Schweizer Bürger (bzw. auch Ausländer gemäss Definition E-ID-Gesetz) mit dem Staat per E-ID erfolgen kann.

4. Anträge zu einzelnen Gesetzesbestimmungen beinhalten Präzisierungen zur Erhöhung der Rechtssicherheit

Inhalt

1 Ziel: schnelle Einführung mit hohem Sicherheitsstandard

Für SFTI steht die schnelle Einführung einer E-ID mit hohem Sicherheitsstandard im Vordergrund. Eine solche E-ID ist die Grundlage für die meisten digitalen Dienste und Anwendungen, sowohl in der Privatwirtschaft als auch im staatlichen Bereich. Seit dem ersten Anlauf 2004 ist viel Zeit vergangen und die Schweiz ist im internationalen Vergleich unterdurchschnittlich unterwegs (vgl. E-Government-Benchmark-Bericht der EU).

Die vorgeschlagene Kaskade von drei E-ID-Sicherheitsniveaus ermöglicht es unseres Erachtens, branchenspezifisch und je nach Anwendungsfall ein ausgewogenes Verhältnis zwischen Sicherheit und Benutzerfreundlichkeit zu finden.

2 Aufgabenteilung Staat-Private

Grundsätzlich unterstützt SFTI die Stossrichtung des Vorentwurfs. Die vorgeschlagene Aufteilung der Aufgaben, Kompetenzen und Verantwortlichkeiten zwischen staatlichen Stellen und privaten Unternehmen trägt den bereits weit fortgeschrittenen Projekten privater Unternehmen Rechnung und unterstützt damit eine schnelle Einführung.

Zu erwähnen sind in diesem Zusammenhang vor allem die folgenden Projekte:

1) Identity Network Switzerland (IDV Schweiz mit SECO)

2) Six Novena

3) SwissSign – Swiss-ID Produkte und Services

4) UBS, CS und Swisscom (the „Notakey“ PoC)

Die Arbeitsgruppe DITP des SFTI hat diese vier Projekte in einem Blueprint zusammengefasst (vgl. Beilage).

Art. 6: Ergänzung der privaten Anbieter von E-ID mit staatlichen Stellen

Der Vorentwurf des E-ID-Gesetzes sieht als IdP nur private Anbieter vor, welche bei Erfüllen bestimmter Kriterien eine Bewilligung erhalten (Art. 4). Dieses Bewilligungskonzept schliesst nicht aus, parallel dazu auch geeignete staatliche Stellen mit derselben Funktion zu betrauen. Passbüros

Swiss Fintech Innovations | c/o Universität Zürich | Binzmühlestrasse 14 | CH-8050 Zürich | T +41 77 432 76 54
www.swissfintechinnovations.ch | office@swissfintechinnovations.ch

erscheinen uns in dieser Hinsicht als besonders prädestiniert. Eine solche Ausgestaltung des VE-E-ID-Gesetzes würde es ermöglichen, dass eine bestimmte Person bei einer anerkannten, vertrauenswürdigen Stelle gleichzeitig und damit sehr effizient physische und elektronische Identifikationsmittel beziehen könnte. Dies würde als Portal-Ergänzung die Marktdurchdringung erhöhen und damit der für das Gelingen des E-ID-Konzeptes essenziellen Verbreitung dienen. Mit Blick auf diese Vorteile sind unseres Erachtens die damit für den Staat anfallenden Mehrkosten hinzunehmen.

Demzufolge empfehlen wir, die Gesetzessystematik dahingehend anzupassen, dass neben bewilligten privaten Unternehmen auch geeignete staatliche Stellen die Funktion des IdP wahrnehmen.

3 Sicherstellen der Akzeptanz der E-ID durch Behörden

Zu einer breiten Akzeptanz der E-ID dürfte vor allem die **Festlegung des EJPD als gesetzlich definierte Identitätsstelle** und Herrscherin über die vollständigen Datensätze führen (Art. 19 f.). Das EJPD kann die Daten nur mit dem Einverständnis der antragstellenden Person herausgeben. Die Identity Provider (IdP) können, solange sie vertrauenswürdig sind und die Bewilligungsvoraussetzungen weiterhin erfüllen (Art. 4 E-ID-Gesetz), auf die funktionsgemäss notwendigen Datensätze zugreifen und die Aktualisierung der Datensätze sicherstellen (Art. 8).

Mindestens ebenso wichtig sind aus Sicht von SFTI aber auch die **Interoperabilität** der anerkannten E-ID und E-ID-Systeme, was einen hohen Kundennutzen sicherstellt. Dies wird in Art. 18 VE-E-ID-Gesetz so vorgeschrieben.

Für den Fall, dass kein IdP für die Ausstellung der Sicherheitsniveaus substanziell oder hoch anerkannt ist, sieht Art. 13 Abs. 1 VE-E-ID-Gesetz lediglich vor, dass der Bundesrat den Betrieb durch eine Bundesbehörde vorsehen *kann*. **Die Sicherstellung von Systemkontinuität durch subsidiäres E-ID-System des Bundes stellt für SFTI jedoch eine weitere wichtige Voraussetzung für die Akzeptanz des gesamten E-ID-Systems dar. Entsprechend unterstützt SFTI den Antrag der Bankiervereinigung zur Anpassung von Art. 13 Abs. 1 VE-E-ID-Gesetz:**

Die Sicherheitsniveaus substanziell und hoch sind für die breite Akzeptanz des E-ID-Konzeptes durch die Wirtschaft von entscheidender Bedeutung. Dies trifft in besonderem Masse auf die Finanzdienstleistungsbranche zu, welche gemäss zahlreichen aufsichtsrechtlichen Vorgaben alle direkt oder indirekt kundenidentifizierenden Daten streng vor unberechtigter Einsichtnahme Dritter zu schützen haben (vgl. insbesondere Bankkundengeheimnis gemäss Art. 47 BankG und die Anforderungen von FINMA-RS 2008/21 operationelle Risiken Banken, insbesondere Anhang 3). Damit sich das E-ID-Konzept im Markt durchsetzt, muss deshalb sichergestellt sein, dass diese qualifizierten Sicherheitsniveaus tatsächlich und dauernd zur Verfügung stehen. Dies lässt sich nur dadurch bewerkstelligen, dass die blosse Kann-Vorschrift durch eine Muss-Vorschrift ersetzt wird. Demzufolge ist Art. 13 Abs. 1 VE E-ID Gesetz wie folgt anzupassen:

> *„Falls kein IdP für die Ausstellung von E-ID der Sicherheitsniveaus substantiell oder hoch anerkannt ist, ~~kann~~ bezeichnet der Bundesrat eine Verwaltungseinheit ~~bezeichnen~~, die ~~für die Bedürfnisse von Behörden~~ ein E-ID-System betreibt und E-ID herausgibt.“*

Swiss Fintech Innovations | c/o Universität Zürich | Binzmühlestrasse 14 | CH-8050 Zürich | T +41 77 432 76 54
www.swissfintechinnovations.ch | office@swissfintechinnovations.ch

4 Zu einzelnen Gesetzesbestimmungen

SFTI unterstützt ausdrücklich die Änderungsanträge der Bankiervereinigung zu den folgenden drei vorgeschlagenen Gesetzesbestimmungen.

4.1 Art. 10 Abs. 1 Offenere Formulierung der Datenbearbeitung

Es ist schwierig, die angemessene Nutzung der Personenidentifizierungsdaten durch einen IdP heute schon abschliessend vorauszusehen. Es wäre beispielsweise möglich, dass der IdP eine „SAML Assertion" (Security Assertion Markup Language) zu Handen eines Service Providers nur dann ausstellt, wenn die Personenidentifizierungsdaten gewisse Kriterien erfüllen (z.B. Alterslimite oder Aufenthaltsstatus). Dies würde eine Autorisierung seitens des IdP darstellen und wäre gemäss vorgeschlagener Formulierung von Art.10 VE-E-ID-Gesetz ausgeschlossen.

Weiter könnten in Zukunft in Zusammenhang mit einer E-ID verschiedene weitere Datenpakete bzw. Dienste angeboten werden, wie beispielsweise bestätigte Auskünfte zur Bonität, welche der Nutzer an Dritte weitergeben möchte.

Die explizite Eingrenzung der Datenbearbeitung für den IdP auf die zwei Anwendungsfälle „Identifizierung" und „Authentifizierung" ist deshalb möglicherweise mit Blick auf die Herausforderungen und Bedürfnisse des praktischen Alltags zu einschränkend. Wir empfehlen deshalb eine offenere Formulierung. Die Streichung des Wörtchens „nur" ermöglicht bei Bedarf die angemessene Erweiterung des Kreises sinnvoller Nutzungen, welche im Bedarfsfall selbstverständlich zwischen den Beteiligten vertraglich zu regeln wäre. Demzufolge muss Art. 10 Abs. 1 VE-E-ID-Gesetz neu wie folgt lauten:

> *„IdP dürfen von der Identitätsstelle übermittelte Personenidentifizierungsdaten ~~nur~~ bearbeiten, um nach diesem Gesetz Identifizierungen und Authentifizierung durchzuführen".*

4.2 Art. 20 Abs. 4^{neu} Sicherstellung Eindeutigkeit von E-ID-Registrierungsnummern

Eine natürliche Person kann gleichzeitig bei mehreren IdP über eine E-ID verfügen und für die initiale Identifikation unterschiedliche Ausweise verwenden. In solchen Fällen kann nur die Identitätsstelle sicherstellen, dass eine bereits bestehende E-ID-Registrierungsnummer wiederverwendet und für dieselbe natürliche Person nicht eine zweite E-ID-Registrierungsnummer generiert wird.

Wir empfehlen deshalb in Art. 20 VE-E-ID-Gesetz einen zusätzlichen Absatz 4, der die Eindeutigkeit der E-ID-Registrierungsnummer wie folgt adressiert:

> *„Die Identitätsstelle stellt sicher, dass für eine natürliche Person nur eine E-ID-Registrierungsnummer ausgestellt wird."*

Die bestehenden Abs. 4 und 5 von Art. 20 VE-E-ID-Gesetz werden dadurch zu Abs. 5 und 6.

4.3 Art. 9 Abs. 1bis ZertES (Anhang zum VE-E-ID-Gesetz)

Während das E-ID-Gesetz die Identifizierung bzw. Authentifizierung der Identität von Kommunikationspartnern regelt, stellt die ZertES ergänzend die für den verbindlichen Rechtsverkehr notwendigen Zertifikate zur Verfügung. Aus dem Zusammenspiel dieser Regeln ergibt sich ein in sich stimmiges Gesamtkonzept.

Swiss Fintech Innovations | c/o Universität Zürich | Binzmühlestrasse 14 | CH-8050 Zürich | T +41 77 432 76 54
www.swissfintechinnovations.ch | office@swissfintechinnovations.ch

Die im Zusammenhang mit dem neuen E-ID-Gesetz geplante Änderung des Bundesgesetzes über die elektronische Signatur (ZertES) sieht im Anhang zum VE-E-ID-Gesetz vorgeschlagenen Art. 9 Abs. 1^{bis} ZertES vor, dass bei Verwendung einer E-ID die persönliche Vorsprache generell entfällt. Dies geht einerseits sachlich zu weit, weil im Falle tiefer Sicherheitsniveaus für eine eindeutige Identifikation und Authentifikation nicht auf eine persönliche Vorsprache verzichtet werden kann. Das Risiko, dass eine E-ID so missbräuchlich oder zu rechtswidrigen Zwecken verwendet wird, wäre zu hoch. Eine auf solch schwacher Basis ausgestellte E-ID widerspräche auch den einschlägigen Vorgaben des Bankenaufsichtsrecht und der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Korruption (vgl. illustrativ Art. 4 ff. VSB 16).

Andererseits ist die Regelung in Art. 9 Abs. 1^{bis} ZertES auch am falschen Ort eingefügt. So sieht die Verordnung über die elektronische Signatur, VZertES, in ihrem Art. 7 bereits die Bestimmungen vor, welche in Zusammenhang mit elektronischen Zertifikaten von der Pflicht des persönlichen Erscheinens befreien. Diese Regeln sind zu koordinieren.

Die von Art. 9 Abs. 1^{bis} ZertES angeordnete Rechtsfolge darf sich demzufolge einerseits nur auf die Sicherheitsniveaus *„substanziell“* und *„hoch“*, nicht aber auf das tiefste Sicherheitsniveau *„niedrig“* erstrecken und muss andererseits mit der Bestimmung von Art. 7 VZertES koordiniert werden.

Wir bitten Sie um Berücksichtigung unserer eingangs formulierten Anliegen. Gerne stehen wir Ihnen zur Diskussion und für die weitere Zusammenarbeit jederzeit zur Verfügung.

Für die Arbeitsgruppe Regulations von SFTI:

Sig. Noemi Heusler Geschäftsstellenleiterin	Sig. Werner Wyss Mitglied der AG Fintech Regulations	Sig. Dr. Cornelia Stengel Mitglied der AG Fintech Regulations

Beilage: Blueprint for Technology Initiatives for a Swiss Digital ID

Swiss Fintech Innovations | c/o Universität Zürich | Binzmühlestrasse 14 | CH-8050 Zürich | T +41 77 432 76 54
www.swissfintechinnovations.ch | office@swissfintechinnovations.ch

Haus der Kantone, Speichergasse 6, CH-3011 Bern
Telefon: +41 (0)31 320 00 00

E-Mail: urs.jermann@sik.ch
Internet: www.sik.ch Intranet: intranet.sik.ch

Schweizerische Informatikkonferenz

Conférence suisse sur l'informatique

Conferenza svizzera sull'informatica

Eidgenössisches Justiz- und Polizeidepartement
Bundeshaus West
CH-3003 Bern
per Email: copiur@bj.admin.ch

cc: Vorstand, Delegierte und Beobachter der SIK

Bern, 25. Mai 2017

Stellungnahme zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Die Schweizerische Informatikkonferenz (SIK) dankt für die Möglichkeit, zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung zu nehmen. Die SIK begrüsst das Bestreben des EJPDs, ein elektronisches und staatlich anerkanntes Identifikationsmittel (eID) einzuführen. Die SIK unterstützt die unterbreitete Vorlage. Gerade für die Abwicklung von wichtigen Online-Geschäften mit der Verwaltung ist eine sichere elektronische Identität möglichst schnell nötig.

Um die Digitalisierung der öffentlichen Verwaltungen der Schweiz wirtschaftlich und effizient umsetzen zu können, braucht es zudem einen eindeutigen Personenidentifikator. Der Bundesrat hat an seiner Sitzung vom 1. Februar 2017 seine Absicht bestätigt, die systematische Verwendung der AHV-Nummer durch die Behörden von Bund, Kantonen und Gemeinden künftig zu erleichtern (vgl. Medienmitteilung vom 1. Februar 2017). Deshalb ist es essentiell, dass die Identitätsstelle die Versichertennummer für den im Vorentwurf vorgesehenen Zweck systematisch verwenden darf.

Der geplante Einführungszeitpunkt einer E-ID Ende 2019 bzw. im Verlauf des Jahres 2020 ist aufgrund dringend benötigter IAM-Lösungen sehr spät. Es besteht die Gefahr, dass die geplante Inbetriebnahme des Identitätsverbunds Schweiz (IDV), die dazugehörigen Kantonsprojekte 2018 und die resultierende E-ID-Verordnung unterschiedliche Wege einschlagen. Auch für andere laufende E-Government-Projekte ist 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 abstimmt werden. In der Botschaft sind die Zusammenhänge und Abhängigkeiten dieser Projekte zur E-ID aufzuzeigen.

Freundliche Grüsse

Schweizerische Informatikkonferenz

RR Marcel Schwerzmann
Präsident

Urs Jermann
Geschäftsleiter

Maison des cantons, Speichergasse 6, CH-3011 Berne
Telefon: +41 (0)31 320 00 00

E-Mail: urs.jermann@sik.ch
Internet: www.sik.ch Intranet: intranet.sik.ch

Schweizerische Informatikkonferenz

Conférence suisse sur l'informatique

Conferenza svizzera sull'informatica

Département fédéral de justice et police
Palais fédéral ouest
CH-3003 Berne
par Email: copiur@bj.admin.ch

cc: Comité directeur, Délégués et Observateurs CSI

Berne, 25 mai 2017

Prise de position sur l'avant-projet de loi fédérale sur les moyens d'identification électronique reconnus (Loi e-ID)

La Conférence suisse sur l'informatique (SIK) est reconnaissante de pouvoir prendre position à l'occasion de l'avant-projet de loi fédérale sur les moyens d'identification électronique reconnus (Loi e-ID). La CSI appuie la tendance du DFJP, de mettre en place des moyens électroniques d'identification reconnus au niveau national (e-ID). La CSI soutient la proposition avancée. En particulier, pour le traitement des affaires en ligne importantes avec l'administration, il est nécessaire de disposer d'une identité électronique sécurisée le plus rapidement possible.

Afin de mettre en œuvre la digitalisation des administrations publiques suisses sur le plan économique et ceci le plus efficacement possible, un identifiant personnel unique est également nécessaire. Le Conseil fédéral a confirmé son intention, lors de sa réunion du 1er février 2017, de continuer à faciliter l'utilisation systématique du numéro d'AVS par la Confédération, les cantons et les communes (voir communiqué de presse du 1er février 2017). Par conséquent, il est essentiel que l'office délivrant les identités puisse utiliser systématiquement le numéro d'assurance sociale aux fins prévues dans l'avant-projet.

La date de lancement prévue d'une e-ID à la fin 2019 respectivement au cours de l'année 2020 est très en retard en raison de la mise en place de solutions IAM urgemment nécessaires. Il existe un risque que l'identité prévue par la fédération suisse d'identités (FSI), les projets correspondants des cantons en 2018 et l'ordonnance e-ID résultant prennent des chemins différents. Pour les autres projets d'e-gouvernement en cours, il est important que ce domaine soit au plus tôt abordé et qu'une mise en œuvre commune soit planifiée. Il faut veiller à ce que les projets au niveau fédéral comme IDV puissent être coordonnés très étroitement avec la législation de l'e-ID. Dans le message, les relations et les dépendances de ces projets sur l'e-ID sont à souligner.

Avec mes meilleures salutations

Conférence suisse sur l'informatique

<Le document original en allemand fait foi>

CE Marcel Schwerzmann
Président

Urs Jermann
Secrétaire général

Swiss Payment Association

Ohmstrasse 11, 8050 Zürich
office@swiss-p-a.ch, +41 (0)58 426 25 55

Bundesamt für Justiz
Frau Sandra Eberle
Herr Urs Paul Holenstein
Bundesrain 20
3003 Bern

Per Mail: copiur@bj.admin.ch

Zürich, 24. Mai 2017

Vernehmlassung zum Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz):
Stellungnahme der Swiss Payment Association

Sehr geehrte Frau Eberle
Sehr geehrter Herr Holenstein
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 22. Februar 2017 eröffnete Vernehmlassung zum Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) und bedanken uns für die Möglichkeit zur Stellungnahme.

Vorab gestatten wir uns den Hinweis, dass der Swiss Payment Association (SPA) alle Schweizer Herausgeber[1] (Issuer) von Kreditkarten der internationalen Kartenorganisationen angehören. Als Branchenorganisation vertritt die SPA die Positionen ihrer Mitglieder im Dialog mit all deren Anspruchsgruppen.

Management Summary

Oberste Zielsetzung der unterbreiteten Gesetzes-Vorlage muss es sein, optimale Rahmenbedingungen für eine **weite Verbreitung und eine hohe Nutzung von elektronischen Identifizierungseinheiten** (E-ID) zu schaffen. Ein möglichst einfacher Zugang zu den E-ID, verhältnismässige Gebühren, ein breites E-ID-Einsatzspektrum und durch das übergeordnete Recht abgesteckte massvolle Verordnungsbestimmungen sind wichtige Voraussetzungen dafür.

Die Grundversorgung der Bevölkerung mit E-ID muss sichergestellt sein. Der uneingeschränkte Zugang zu und die dauernde Verfügbarkeit der E-ID stellen eine absolute Notwendigkeit dar. Instrumente dafür sind ein Kontrahierungszwang für den Identity Provider

[1] Mitglieder der Swiss Payment Association sind die Schweizer Kreditkarten-Herausgeber BonusCard.ch AG, Cembra Money Bank AG, Cornèr Bank AG, PostFinance AG, Swisscard AECS GmbH, UBS Switzerland AG und Viseca Card Services SA.

(IdP) und die Sicherstellung der Kontinuität der E-ID-Services für den Fall, dass ein IdP seine Dienstleistungen nicht mehr erbringen darf, kann oder will.

Die internationale Interoperabilität bzw. die internationale Anwendbarkeit der schweizerischen E-ID ist zeitnah sicherzustellen. Damit die E-ID – als Online-Ausweise im grenzenlosen Internet – für die Bevölkerung einen hohen Nutzen schaffen, müssen sie möglichst auch international zum Einsatz gebracht werden können. Dafür erforderliche bilaterale Abkommen – insbesondere mit der EU/einzelnen europäischen Staaten – sind möglichst rasch abzuschliessen.

1. Grundsätzliche Ausführungen

1.1 Oberstes Ziel: Weite Verbreitung und hohe Nutzung der E-ID

Aus Sicht der SPA muss es die oberste Zielsetzung der unterbreiteten Gesetzes-Vorlage sein, optimale Rahmenbedingungen für eine weite Verbreitung und eine hohe Nutzung von elektronischen Identifizierungseinheiten zu schaffen. Nachdem dies bei früheren ähnlichen Vorhaben (z.B. SuisseID) nicht gelungen ist, darf die vorliegende Chance nicht erneut vertan werden, andernfalls das volkswirtschaftliche Schadenspotenzial erheblich sein dürfte. Damit die Schweiz die Chancen der Digitalisierung in allen Lebensbereichen konsequent nutzen und volkswirtschaftliche Gewinne erzielen kann, ist eine möglichst weite Ausbreitung und hohe Verwendung der E-ID unerlässlich. Die SPA hat daher die unterbreitete Gesetzesvorlage ganz besonders unter dem Aspekt der hohen Verbreitung/Nutzung geprüft und wird in der vorliegenden Stellungnahme verschiedentlich darauf zu sprechen kommen.

1.2 Unterstützung für die Initiative des Bundesrats

Die SPA begrüsst die Anstrengungen des Bundesrats, die erforderlichen rechtlichen und organisatorischen Rahmenbedingungen für die Anerkennung von E-ID und deren Anbieter zu schaffen. Damit wird eine zentrale Voraussetzung dafür realisiert, dass künftig auch anspruchsvolle Geschäfte mit vernünftigem Aufwand sicher online abgewickelt werden können. Ziel muss es sein, mit umfassend verfügbaren, breit akzeptierten bzw. genutzten und vielfältig einsetzbaren E-ID die digitale Abwicklung auch anspruchsvoller Geschäfts- und Verwaltungsprozesse zu ermöglichen bzw. effizient und effektiv auszugestalten.

1.3 Zweckmässige Aufgabenteilung zwischen Staat und Privaten

Die SPA begrüsst das Konzept, wonach eine Aufgabenteilung zwischen Staat und privaten Anbietern vorgenommen werden soll und private Identifizierungsdienstleister von einer staatlichen Anerkennungsstelle eine Zulassung zur Herausgabe von staatlich anerkannten elektronischen Identifizierungsmitteln erlangen können. Diese Konzeption verspricht einen zügigen und effizienten Aufbau bzw. Betrieb des Systems, eine zeitgerechte Weiterentwicklung desselben entlang rasch voranschreitender digitaler Entwicklungen und den Schutz bereits getätigter privater Investitionen in existierende oder sich im Aufbau befindliche elektronische Identifizierungsinstrumente.

1.4 Sicherstellung der Grundversorgung der Bevölkerung mit E-ID

Mit der vorgesehenen (von der SPA unterstützten) teilweisen Auslagerung einer bisher rein staatlichen Aufgabe (Herausgabe von Pässen und Identitätskarten) an Private ist u.a. das Risiko verbunden, dass nicht für jede/n Berechtigte/n Zugang zu einer E-ID besteht bzw.

dass eine solche nicht ständig verfügbar ist. Der uneingeschränkte Zugang zu und die dauernde Verfügbarkeit der E-ID stellen jedoch eine absolute Notwendigkeit dar; dies ganz besonders unter dem Aspekt, dass die E-ID in Kombination mit z.B. der elektronischen Signatur das Potential besitzen, sich zum zentralen Identifizierungsmittel der näheren Zukunft zu entwickeln. Ohne eine jederzeit verfügbare E-ID kann eine Person zukünftig dauernd oder vorübergehend von wesentlichen Teilen des wirtschaftlichen Lebens ausgeschlossen bleiben. Für die SPA ist es deshalb von zentraler Bedeutung, das E-ID-Gesetz so auszugestalten, dass die Grundversorgung der Bevölkerung mit E-ID bestmöglich und nachhaltig sichergestellt wird. Dazu gehören die gesetzliche Verankerung eines Kontrahierungszwangs für den Identity Provider (IdP) und die Sicherstellung der Kontinuität der E-ID-Services für den Fall, dass ein IdP seine Dienstleistungen nicht mehr erbringen darf, kann oder will. Beide Themen-Bereiche regelt der Vorentwurf nicht oder nicht ausreichend.

1.5 Keine prohibitiven Gebühren

Es ist vorgesehen, die beiden neuen Bundesstellen (Identitätsstelle und Anerkennungsstelle) über Gebühren zu finanzieren. Wie vorstehend angesprochen, ist es – ganz besonders auch aus einem volkswirtschaftlichen Blickwinkel heraus – von entscheidender Bedeutung, dass die E-ID in der Bevölkerung eine grosse Ausbreitung erfährt bzw. dass jedermann nicht nur theoretisch sondern auch faktisch Zugang zu einer E-ID hat. Ein zu hoher Endkunden-Preis für den Erwerb bzw. Betrieb einer E-ID stünde dieser zentralen Zielsetzung diametral entgegen. Bei der Gebühren-Festsetzung ist daher 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.

1.6 Zeitnahe Sicherstellung von internationaler Interoperabilität bzw. Anwendbarkeit der schweizerischen E-ID

Damit die E-ID – als Online-Ausweise im grenzenlosen Internet – für die Bevölkerung einen möglichst hohen Nutzen schaffen (und damit auch nachgefragt werden bzw. eine weite Verbreitung erfahren), müssen sie möglichst auch international – ganz besonders europäisch – zum Einsatz gebracht werden können. Gemäss Erläuterndem Bericht zum Vorentwurf für ein E-ID-Gesetz berücksichtigt der Vorentwurf insbesondere die Vorgaben für die EU-Kompatibilität gemäss eIDAS-Verordnung[2]. So wird u.a. auf Seite 13 festgehalten: „In der eIDAS-Verordnung und den entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das Konzept für schweizerisch anerkannte E-ID-Systeme richtet sich an diesen internationalen Vorgaben aus, sodass die schweizerischen E-ID auch im internationalen Kontext eingesetzt werden könnten." Zu beachten ist diesbezüglich allerdings, dass schweizerische E-ID nur dann europaweite Anerkennung erlangen, wenn die Schweiz dazu ein bilaterales Abkommen mit der EU oder bilaterale Abkommen mit einzelnen Mitgliedstaaten schliesst. Auch wenn der bilaterale Weg zwischen der EU und der Schweiz faktisch nach wie vor blockiert erscheint, ist es aus Sicht der SPA für den Erfolg – und damit für die Etablierung – der schweizerischen E-ID unerlässlich, dass der Bundesrat

[2] 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/EG1

nach Erlass des E-ID-Gesetzes rasch und mit Nachdruck auf ein Anerkennungs-Abkommen mit der EU drängt.

1.7 Regelung von Eckwerten und Leitplanken anstelle von Prozessen

Der unterbreitete Vorentwurf fokussiert stark auf die Regelung von Prozessen. In der digitalen Welt, welche einem permanenten und raschen Wandel unterzogen ist, kann sich dies als Hemmschuh erweisen, wenn es darum geht, mit neuen Entwicklungen angemessen Schritt zu halten. Die SPA schlägt daher vor, im Gesetz verstärkt Eckwerte und Leitplanken in generischer Weise festzulegen und auf die Umschreibung von Prozessen zu verzichten bzw. diese – bei Bedarf – auf Verordnungsstufe zu umreissen. Das Gesetz soll möglichst viele Prinzipien und möglichst keine Regeln enthalten. Damit kann sichergestellt werden, dass das Gesetz auf lange Sicht eine verlässliche, aber dennoch genügend flexible Grundlage für den innovativen Einsatz von E-ID schafft.

1.8 Regelungen auf Verordnungsstufe zugunsten einer weiten Verbreitung und hohen Nutzung der E-ID

In der digitalen Welt, die einem ständigen Wandel unterworfen ist, ist es zweckmässig, gute Voraussetzungen für die zeitgerechte Weiterentwicklung der regulatorischen Rahmenbedingungen bzw. die Berücksichtigung neuer Realitäten zu schaffen. Der Vorentwurf wird diesem Anspruch insofern gerecht, als er dem Bundesrat eine breite Palette an Themen zuweist, welche auf Verordnungsstufe – und damit in einem vergleichsweise raschen Rechtsetzungsverfahren – geregelt bzw. detailliert werden können. Dabei sind aus Sicht der SPA allerdings folgende zwei zentralen Punkte zu beachten: Zum einen sind in den einzelnen Themen auf Gesetzesstufe klare Leitplanken bzw. Schranken für den Verordnungsgeber zu setzen, zum anderen hat der Verordnungsgeber seine Rechtsetzungskompetenz dem Zweck und den Zielen des übergeordneten Gesetzes entsprechend auszuüben. Vorliegend bedeutet dies nach Auffassung der SPA insbesondere, dass auch der Bundesrat so regulieren soll, dass optimale Rahmenbedingungen für eine weite Verbreitung und eine hohe Nutzung von E-ID geschaffen werden.

1.9 Änderung anderer Erlasse: Umfassende Beseitigung von rechtlichen Hindernissen für den E-ID-Einsatz

Die SPA ist der Auffassung, dass die im Anhang zur E-ID-Gesetzes-Vorlage enthaltene Auflistung anderer Erlasse, welche geändert werden sollen, zu eng gehalten ist. Für den Erfolg bzw. die erforderliche hohe Verbreitung von E-ID ist es zwingend, dass diese in den verschiedensten Lebenssituationen bzw. in den unterschiedlichsten Geschäfts- und Verwaltungsprozessen zur Anwendung kommen können. Es ist deshalb darauf zu achten, dass in der gesamten Schweizer Rechtsordnung die nötigen Voraussetzungen für die Einsetzbarkeit von E-ID geschaffen werden bzw. dass rechtliche Hürden, welche dem entgegenstehen, umfassend beseitigt werden.

2. Ausführungen zu einzelnen Gesetzesartikeln und Anträge der Swiss Payment Association

Nachstehend finden sich zu ausgewählten Artikeln des Vorentwurfs zu einem E-ID-Gesetz die Einschätzungen und Anträge der SPA:

2.1 Allgemeine Bestimmungen (Art. 1 f. VE E-ID-Gesetz)

- **Antrag: „Weite Verbreitung und Nutzung“ in die Zweckbestimmung aufnehmen (Art. 1 Abs. 2 lit. b VE E-ID-Gesetz)**

  Das Ziel einer möglichst umfassenden Verbreitung der E-ID soll in den Zweckartikel des E-ID-Gesetzes aufgenommen werden. Wie bereits in den grundsätzlichen Ausführungen dargelegt, muss es das oberste Ziel des Gesetzgebers sein, ein Instrument zur Verfügung zu stellen, dass von der Bevölkerung breit angenommen und rege genutzt wird. Dies bedingt einerseits eine einfache aber dennoch sichere Handhabung der E-ID und anderseits ein möglichst weites Anwendungsfeld derselben sowohl im öffentlichen als auch im privaten Sektor. Die Aufnahme des zusätzlichen Ziels der „weiten Verbreitung und Nutzung der E-ID“ in den Zweckartikel soll insbesondere auch den Bundesrat bei der Ausarbeitung der E-ID-Verordnung leiten.

  Die SPA beantragt, den Zweckartikel (Art. 1 Abs. 2 lit b VE E-ID-Gesetz) wie folgt zu ergänzen (Ergänzung = unterstrichen):

  > „Es hat zum Zweck:
  >
  > a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
  >
  > b. <u>eine weite Verbreitung und Nutzung</u>, die Standardisierung und die Interoperabilität der E-ID sicherzustellen.“

- **Antrag: „Nationale und internationale Interoperabilität“ in die Zweckbestimmung aufnehmen (Art. 1 Abs. 2 lit. b VE E-ID-Gesetz)**

  Inhaberinnen und Inhaber einer E-ID sollen diese bei allen E-ID-verwendenden Diensten einsetzen können, und zwar unabhängig davon, ob der Betreiber eines E-ID-verwendenden Dienstes mit demjenigen IdP eine Vereinbarung hat, der die E-ID ausgestellt hat. Dieser zentrale Aspekt der Interoperabilität fokussiert primär auf den nationalen Bereich. Daneben ist es für die breite Einsatzbarkeit (und damit die weite Verbreitung) der E-ID genauso wichtig, dass die Interoperabilität auch zwischen den einzelnen länderspezifischen Systemen sichergestellt wird. Zu diesem Zweck sind von der Schweizer E-ID-Lösung die massgeblichen internationalen Standards zu beachten bzw. es sind adäquate Lösungen dazu zu treffen, insbesondere was die EU anbelangt. Damit werden die Voraussetzungen dafür geschaffen, dass die schweizerische E-ID zumindest europaweite Anerkennung erlangen kann.

  Die SPA beantragt daher, den Zweckartikel (Art. 1 Abs. 2 lit b VE E-ID-Gesetz) wie folgt zu ergänzen (Ergänzung = unterstrichen):

  > „Es hat zum Zweck:
  >
  > a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
  >
  > b. eine weite Verbreitung und Nutzung, die Standardisierung und die Interoperabilität der E-ID <u>auf nationaler und internationaler Ebene</u> sicherzustellen.“

- **Antrag: Den Begriff „Attribute“ in Art. 2 VE ID-Gesetz definieren (Art. 2 lit. k VE E-ID-Gesetz)**

  Vorentwurf und Erläuternder Bericht gehen davon aus, dass neben den von der Identitätsstelle zum Abgleich der Daten zur Verfügung gestellten Identitätsmerkmalen auch noch weitere Attribute mit der E-ID verbunden werden können. Die SPA begrüsst diese

Möglichkeit, da sie einen gewichtigen Beitrag zur Verbreitung der E-ID leisten kann. Auf dieser Ausgangslage erscheint es angebracht, den Begriff "Attribute" im Gesetz entsprechend zu definieren.

Die SPA beantragt, Art. 2 VE E-ID-Gesetz wie folgt um lit. k zu ergänzen (Ergänzung = unterstrichen):

„In diesem Gesetz bedeuten: a. […] k. *Attribute*: Andere als von der Identitätsstelle zur Verfügung gestellte Merkmale, die einer Person zugeordnet werden können."

2.2 Ausstellung von E-ID (Art. 3 ff. VE E-ID-Gesetz)

- **Antrag: Weitgehenden Kontrahierungszwang vorsehen (Art. 3 Abs. 1 VE E-ID-Gesetz)**

  Aufgrund der in Art. 3 Abs. 1 verwendeten Kann-Vorschrift besteht für den IdP kein Kontrahierungszwang. Dies wird im Erläuterungsbericht explizit bestätigt. Der IdP ist also nicht verpflichtet, ein Vertragsverhältnis einzugehen und eine E-ID auszustellen, auch wenn eine Person die Voraussetzungen für die Abgabe einer E-ID erfüllt. Warum dieser Ansatz verfolgt wird, wird in den Vernehmlassungsunterlagen nicht näher ausgeführt. Der SPA erschliesst sich Sinn und Zweck dieser Konzeption nicht. Im Gegenteil – sie erscheint nicht zielführend. Genauso wie ein Staat seinem Bürger bei gegebenen Voraussetzungen die Ausstellung eines Passes oder einer Identitätskarte nicht vorenthalten darf, soll auch ein IdP verpflichtet sein, einer berechtigten Person, welche entsprechend Antrag stellt, eine E-ID auszustellen. Andernfalls besteht das Risiko, dass aus sachfremden Beweggründen – zum Beispiel wirtschaftlichen oder überwiegend privaten Interessen – einer berechtigten Personen willkürlich der Zugang zu einer E-ID verwehrt bleibt oder über Gebühr erschwert wird. Da offenbar auch keine Pflicht zur Begründung einer Ablehnung seitens des IdP besteht, stünde der Antragssteller einem negativen Bescheid seitens des IdP schutzlos gegenüber.

  Dieser offensichtliche Missstand ist mit der Einführung eines weitgehenden Kontrahierungszwangs zu beheben. Die IdP sollen verpflichtet werden, sämtlichen bezugsberechtigten Personen auf deren Ersuchen hin eine E-ID auszustellen. Die Gründe für eine zulässige Verweigerung sind präzise festzulegen.

Die Konzeption von Art. 3 Abs. 1 VE E-ID-Gesetz, wonach der IdP nicht verpflichtet sein soll, ein Vertragsverhältnis einzugehen und eine E-ID auszustellen, soll durch das System eines weitgehenden Kontrahierungszwangs ersetzt werden.

- **Antrag: Kontinuität in der E-ID-Nutzung bei Geschäftsaufgabe eines IdP sicherstellen (Art. 4 Abs. 3 und Art. 11 Abs. 3 VE E-ID-Gesetz)**

  Der Vorentwurf sieht in Art. 4 Abs. 3 vor, dass die Anerkennung der IdP spätestens nach 3 Jahren erneuert werden muss, womit das Risiko besteht, dass die Anerkennung nicht weitergeführt wird. Art. 11 VE E-ID-Gesetz regelt das Erlöschen der Anerkennung infolge Konkurs oder Aufgabe der Geschäftstätigkeit. In all diesen Fällen der freiwilligen oder erzwungenen Geschäftsaufgabe eines IdP stellt der Vorentwurf nicht sicher, dass die Inhaberinnen und Inhaber von E-ID, welche der jeweilige IdP ausgestellt hat, ihre E-ID weiterhin nutzen können. Ebenso wenig ist sichergestellt, dass Betreiber von E-ID verwendenden Diensten weiterhin die bereits erhaltenen Datensätze abrufen können. Viel-

mehr findet der in Art. 3 VE E-ID-Gesetz fehlende Kontrahierungszwang seine Fortsetzung in Art. 11, indem kein IdP in die Pflicht genommen werden soll, die E-ID-Systeme bzw. Kundinnen und Kunden eines zukünftig nicht mehr bestehenden IdP zu übernehmen. Das erachtet die SPA als nicht sachgerecht und nicht zielführend: Insbesondere ist es dem Vertrauen der E-ID berechtigten Personen und der möglichen Betreiber von E-ID verwendenden Diensten in das E-ID-System und in die Rechtssicherheit abträglich.

Angezeigt ist daher eine gesetzliche Regelung, welche IdP verpflichtet, Inhaberinnen und Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc" (gegen entsprechende Entschädigung, z.B. durch den Bund) zu übernehmen. Will der Gesetzgeber nicht so weit gehen, ist auf Gesetzesebene im Minimum sicherzustellen, dass von der Geschäftsaufgabe eines IdP betroffene Inhaberinnen und Inhaber einer E-ID von anderen IdP eine E-ID ausgestellt erhalten, ohne den gesamten Ausstellungsprozess gemäss Art. 6 VE E-ID-Gesetz erneut durchlaufen zu müssen. Dabei ist die ununterbrochene Nutzungsmöglichkeit der bisherigen E-ID bis zur Ausstellung einer neuen sicherzustellen (für die Inhaberinnen und Inhaber wie für die Betreiber von E-ID-verwendenden Diensten).

Auf gesetzlicher Ebene ist 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 (durch die Inhaberinnen und Inhaber der E-ID wie durch die Betreiber von E-ID-verwendenden Diensten).

- **<u>Antrag: Datenhaltung durch den IdP ausserhalb der Schweiz zulassen (Art. 4 Abs. 2 lit. f VE E-ID-Gesetz)</u>**

  Der Vorentwurf sieht in Art. 4 Abs. 2 lit. f vor, dass die IdP die E-ID-System-Daten in der Schweiz und nach schweizerischem Recht halten und bearbeiten müssen. Diese absolute Anforderung wird nach Ansicht der SPA den heutigen Realitäten – worin z.B. Cloud-Lösungen eine immer grössere Rolle spielen – nicht mehr gerecht. Der Gesetzgeber sollte hier – ohne bei den Sicherheitsanforderungen Abstriche zu machen – mehr Flexibilität zeigen und auch eine Datenhaltung ausserhalb der Schweiz zulassen, sofern die Daten bezüglich Datensicherheit und Datenschutz adäquat nach schweizerischem Recht bearbeitet und gehalten werden. Dies lässt sich umso mehr rechtfertigen, als mit der angestrebten internationalen Interoperabilität des schweizerischen E-ID-Systems künftig auch Schweizer E-ID bei Betreiber von E-ID-verwendenden Diensten im Ausland zum Einsatz kommen werden, was zwangsläufig einen gewissen Datenverkehr ins Ausland mit sich bringt.

  Die SPA beantragt, Art. 4 Abs. 2 lit f.VE E-ID-Gesetz wie folgt abzufassen (Weglassungen = durchgestrichen / Ergänzung = unterstrichen):

„IdP werden anerkannt, wenn sie: a. […] f. die E-ID-System-Daten bezüglich Datensicherheit und Datenschutz <u>adäquat nach Schweizer Recht</u> ~~in der Schweiz nach schweizerischem Recht~~ halten und bearbeiten;"

- **<u>Antrag: Gleichwertige Anerkennungsverfahren als hinreichend zulassen (Art. 4 Abs. 3 VE E-ID-Gesetz)</u>**

  Die SPA erachtet ein periodisch wiederholtes Anerkennungsverfahren für IdP als sinnvoll. Dabei ist jedoch zu beachten, dass Banken (welche als IdP tätig sind) bereits jähr-

lich andere Audits und Anerkennungsverfahren zu durchlaufen haben und mit dem Anerkennungsverfahren für IdP ein weiteres hinzukäme, welches gleiche oder ähnliche Bereiche abdecken dürfte. Aus Gründen der Prozessökonomie sollten die verschiedenen Anerkennungsverfahren harmonisiert werden. Bis dies realisiert ist, soll ein Anerkennungsverfahren jeweils auch für einen anderen Bereich gelten, sofern eine gewisse Gleichwertigkeit vorliegt.

Die SPA beantragt, Art. 4 Abs. 3 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

„Die Anerkennung muss spätestens nach drei Jahren erneuert werden. Wurde eine gleichwertige Anerkennung bereits nach einem anderen Gesetz durchgeführt, muss sie nach diesem Gesetz nicht wiederholt werden."

- **Antrag: E-ID muss Anforderungen nach der Geldwäschereigesetzgebung und nach den einschlägigen Standesregeln gerecht werden (Art. 5 VE E-ID-Gesetz)**

  Für einen adäquaten Nutzen der E-ID (und damit eine hohe Nachfrage besteht) müssen die Voraussetzungen an die E-ID derart ausgestaltet sein, dass sie die Anforderungen nach Art. 3 des Geldwäschereigesetzes, nach der Geldwäschereiverordnung-FINMA und nach den einschlägigen Standesregeln (insbesondere Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken/VSB 16) an eine rechtskonforme Identifikation erfüllen. Die Akzeptanz der E-ID als rechtsgültiges Identifikationsmittel muss darüber hinaus insbesondere auch bei der Finanzmarktaufsicht gegeben sein. Nur so wird es gelingen, die E-ID im täglichen wirtschaftlichen Leben genügend zu verankern.

  In diesem Sinne begrüsst die SPA die Ausführungen im Erläuternden Bericht (Seite 35 f.), wonach eine E-ID als beweiskräftiges Identifikationsdokument dienen soll und insbesondere Finanzinstitute und Spielcasinos, die dem Geldwäschereigesetz unterstehen, eine sichere elektronische Identifikation mit der E-ID sollen vornehmen können. Allerdings regelt das Geldwäschereigesetz selbst nicht abschliessend, was ein beweiskräftiges Dokument ist, sondern überlässt dies der Geldwäschereiverordnung der FINMA. Dazu führt der Erläuternde Bericht aus (Seite 35 f.): „Gegebenenfalls ist diese Verordnung so anzupassen, dass eine E-ID im elektronischen Geschäftsverkehr mit Finanzinstituten und Casinos eingesetzt werden kann." Für die SPA ist es zwingend, dass die notwendigen Anpassungen an der Geldwäschereiverordnung der FINMA – aber auch an den Standesregeln – auf den Zeitpunkt der Einführung der E-ID vorgenommen sind.

Es sind alle Voraussetzungen dafür zu schaffen, dass die E-ID die Anforderungen nach der Geldwäschereigesetzgebung und nach den einschlägigen Standesregeln an eine rechtskonforme Identifikation erfüllen bzw. dass die einschlägigen Rechtserlasse die E-ID als rechtsgültige Identifikationsmittel bzw. beweiskräftige Dokumente anerkennen.

- **Antrag: Akzeptanz einer bereits vorgenommenen Identifikation nach Geldwäschereigesetzgebung (Art. 5 Abs. 2 VE E-ID-Gesetz)**

  Art. 5 Abs. 2 VE E-ID-Gesetz legt unter lit. a fest, dass sich die verschiedenen Sicherheitsniveaus insbesondere in Bezug auf die Identifizierung und Authentifizierung der Inhaberin und des Inhabers bei der Registrierung unterscheiden sollen. Der Erläuterungsbericht führt hierzu aus, dass die Registrierung bei den Sicherheitsniveaus „substanziell" und „hoch" mit persönlicher Vorsprache oder mittels Videoidentifikation zu erfolgen hat.

  Unabhängig von den noch zu erlassenden Ausführungsbestimmungen auf Verordnungsstufe (Art. 5 Abs. 4 VE E-ID-Gesetz) ist es für die SPA wichtig, dass auf Geset-

zesstufe festgehalten wird, dass sich ein IdP auf eine bereits nach der Geldwäschereigesetzgebung rechtsgültig erfolgte Identifikationen verlassen darf. Es wäre – sowohl für den IdP wie für den E-ID-Antragsteller – ineffizient und in der Praxis untauglich, wenn ein IdP, der gleichzeitig als Finanzintermediär gemäss Geldwäschereigesetzgebung qualifiziert und die Identifikation einer Person nach der Geldwäschereigesetzgebung vorgenommen hat, dieselbe Person für die Ausstellung einer E-ID nochmals identifizieren müsste. Dies bedeutet auch, dass an die Identifikation nach E-ID-Gesetz keine höheren Anforderungen gestellt werden dürfen als an die Identifikation nach Geldwäschereigesetzgebung. So soll sich beispielsweise eine „persönliche Vorsprache" nach Geldwäschereigesetzgebung nicht von einer „persönlichen Vorsprache" nach E-ID-Gesetz unterscheiden. Und eine vorbestehende Identifikation nach Geldwäschereigesetzgebung innerhalb eines Konzerns ist der Identifikation durch den konzerninternen IdP gleichzustellen (d.h. es bedarf keiner erneuten Identifikation durch den IdP, wenn die bereits nach GwG identifizierte Person beim IdP eine E-ID beantragt / siehe dazu auch den unten stehenden Antrag zu Art. 6 Abs. 3bis VE E-ID-Gesetz).

Ergänzend ist hierzu festzuhalten, dass aufgrund einer der Identifikation nachfolgenden Übermittlung der Personenidentifizierungsdaten durch die Identitätsstelle bei der Ausstellung einer E-ID sogar ein vergleichsweise höheres Sicherheitsniveau besteht. Denn durch diesen Abgleich können beispielsweise gefälschte Ausweispapiere immer als solche erkannt werden, was im Rahmen der Identifikation nach Geldwäschereigesetzgebung nicht ohne weiteres sichergestellt ist.

Im E-ID-Gesetz ist explizit zu regeln, dass sich ein IdP auf eine bestehende Identifikation nach zum im fraglichen Zeitpunkt geltender Geldwäschereigesetzgebung verlassen darf, unabhängig davon ob er diese selber vorgenommen hat oder ob diese unter Anwendung der in der Geldwäschereigesetzgebung festgelegten Pflichten innerhalb des Konzerns oder durch einen im Sinne der Bankenregulierung beauftragen Dritten erfolgt ist.

- **<u>Antrag: Freie Zuordnung von Attributen (Art. 5 Abs. 3bis VE E-ID-Gesetz)</u>**

  Gemäss Art. 7 Abs. 4 VE E-ID-Gesetz kann der IdP einer E-ID weitere Daten (sogenannte Attribute) zuordnen (siehe dazu auch den oben stehenden Antrag zu Art. 2 lit. k VE E-ID-Gesetz). Da es sich bei den Attributen um Daten handelt, die üblicherweise nicht von einer staatlichen Stelle stammen, sollte es nach Auffassung der SPA den beteiligten Personen überlassen bleiben, unter welchem Sicherheitsniveau die einzelnen Attribute verfügbar gemacht werden. Konkret heisst dies, dass es möglich sein muss, dass die Attribute je nach vertraglicher Abmachung zwischen IdP und E-ID-Nutzer auf sämtlichen Sicherheitsniveaus eingesetzt werden können.

  Die SPA beantragt, Art. 5 VE E-ID-Gesetz wie folgt um einen Absatz 3bis zu ergänzen (Ergänzung = unterstrichen):

3	„Eine für ein bestimmtes Sicherheitsniveau ausgestellte E-ID kann auch auf einem tieferen Sicherheitsniveau eingesetzt werden.
3bis	<u>Attribute gemäss Art. 7 Abs. 4 können unabhängig vom Sicherheitsniveau eingesetzt und geteilt werden."</u>

- **<u>Antrag: Massvollen Mindestanforderungen an die Identifizierung und Authentifizierung (Art. 5 Abs. 4 VE E-ID-Gesetz)</u>**

  Wie bereits beim oben stehenden Antrag zu Art. 1 Abs. 2 lit. b VE E-ID-Gesetz ausgeführt, soll sich der Bundesrat bei der Ausarbeitung der E-ID-Verordnung an der zentralen

Zielsetzung der weiten Verbreitung und Nutzung der E-ID orientieren. Das bedeutet insbesondere auch, dass der Ausstellungsprozess in Bezug auf die Identifizierung und Authentifizierung zwar sicher, aber auch zweck- bzw. verhältnismässig ausgestaltet sein muss. Die Erfahrungen aus der Praxis zeigen dabei, dass beispielsweise das Erfordernis der persönlichen Vorsprache von den Antragstellenden in der Regel als (zu) grosse Hürde angesehen wird. Eine Video- bzw. eine Online-Identifikation soll deshalb die jeweiligen Mindestanforderungen an eine Identifikation erfüllen (siehe dazu auch den nachfolgenden Antrag zu Art. 6 VE E-ID-Gesetz).

Um dies zu verdeutlichen, beantragt die SPA, Art. 5 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

„Der Bundesrat regelt die verschiedenen Sicherheitsniveaus, insbesondere die massvollen Mindestanforderungen an die Identifizierung und Authentifizierung.“

- **Antrag: Prozessschritt der Prüfung von Identität und Authentizität des Antragstellers im Gesetz explizit aufführen (Art. 6 Abs. 3bis VE E-ID-Gesetz)**

  Stellt eine Person Antrag auf eine E-ID, muss der IdP die Identität und die Authentizität des Antragstellers prüfen, bevor er ihm eine E-ID zuweist. Dieser Schritt wird zwar vom Gesetz impliziert, jedoch nicht explizit aufgeführt. Angesichts der Bedeutung dieses Prozessschritts ist die SPA der Auffassung, dass eine ausdrückliche Regelung auf Gesetzesstufe angezeigt ist.

  Je nach Sicherheitsniveau ist für die E-ID-Ausstellung eine persönliche Vorsprache vorgesehen. Da – wie bereits oben ausgeführt – eine solche vom Antragstellenden in der Praxis oft als (zu) grosse Hürde angesehen wird, soll auf Gesetzesebene festgehalten werden, dass der persönlichen Vorsprache eine Videoidentifikation oder eine andere gleichwertige Identifizierung gleichgestellt ist. Mit letzterem soll sichergestellt werden, dass in der Praxis dem technischen Fortschritt Rechnung getragen werden kann.

  Wie bereits oben stehend zu Art. 5 Abs. 2 VE E-ID-Gesetz ausgeführt, soll im E-ID-Gesetz explizit festgehalten sein, dass sich ein IdP auf eine bestehende (zur Identifikation nach E-ID-Gesetz gleichwertige) Identifikation verlassen darf, unabhängig davon ob er diese selber vorgenommen hat oder ob diese innerhalb des Konzerns oder durch einen beauftragen Dritten erfolgt ist. Nach zum im fraglichen Zeitpunkt geltender Geldwäschereigesetzgebung bereits rechtsgenüglich identifizierte Personen sollen nicht noch einmal identifiziert werden müssen. Nach Auffassung der SPA bietet sich die Chance, diesen Grundsatz in Art. 6 VE E-ID-Gesetz zu verankern.

  Die SPA beantragt, Art. 6 VE E-ID-Gesetz wie folgt um einen Absatz 3bis zu ergänzen (Ergänzung = unterstrichen):

3	„Er beantragt bei der Schweizerischen Stelle […].
3bis	Er identifiziert und authentifiziert die antragstellende Person. Wo dafür eine persönliche Vorsprache erforderlich ist, kann dieses Erfordernis auch mittels Videoidentifikation oder einer anderen gleichwertigen digitalen Identifikation erfüllt werden. Eine bereits erfolgte zu diesem Gesetz gleichwertige Identifikation muss nicht wiederholt werden, wenn sie im fraglichen Zeitpunkt der geltenden Geldwäschereigesetzgebung entspricht.“

- **Antrag: Gesetzliche Verankerung, dass eine Person mehrere E-ID besitzen kann (Art. 6 Abs. 4 VE E-ID-Gesetz)**

  Der Erläuternde Bericht verweist zu Recht auf die Möglichkeit, dass eine Person mehrere E-ID besitzen kann (z.B. je eine E-ID pro Sicherheitsniveau). Aus Sicht der SPA erscheint es angezeigt, diese Möglichkeit im E-ID-Gesetz zu erwähnen – inkl. Hinweis, dass die verschiedenen E-ID von unterschiedlichen IdP stammen können.

  Die SPA beantragt, Art. 6 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

  „Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person. Eine Person kann mehrere E-ID von einem oder mehreren IdP besitzen."

- **Antrag: Zentrale Führung von Signaturmitteln und Identifizierungseinheit ermöglichen (Art. 6 Abs. 4bis VE E-ID-Gesetz)**

  Der Erläuternde Bericht (Seite 34) geht davon aus, dass die E-ID mit einem Gerät verknüpft wird bzw. darauf angebracht wird. Gleichzeitig wird auf technische Standards im Rahmen der eIDAS-Verordnung verwiesen. Dort findet sich der Standard „CEN 419.241". Dieser ermöglicht es, Zertifikate für e-Signaturen zentral zu verwalten und bei Bedarf abzurufen. So könnte der Inhaber einer E-ID davon entbunden werden, für den Einsatz seiner E-ID ein bestimmtes Gerät zur Hand haben bzw. mitführen zu müssen. Vielmehr könnte er das Zertifikat mit den entsprechenden Zugangsmitteln (Zwei-Faktor-Authentifizierung) einholen. Dies würde mit den Anforderungen bezüglich E-Signatur korrelieren.

  Die SPA beantragt daher, Art. 6 VE E-ID-Gesetz um einen Abs. 4bis zu ergänzen (Ergänzung = unterstrichen):

  4 „Er ordnet die Personenidentifizierungsdaten […]

  „4bis Er kann Signaturmittel und Identifizierungseinheit zentral führen."

- **Antrag: Von der Identitätsstelle zuzuordnende Daten für jedes Sicherheitsniveau verbindlich festlegen (Art. 7 Abs. 2 VE E-ID-Gesetz)**

  Durch die in Art. 7 Abs. 2 VE E-ID-Gesetz gewählte Kann-Formulierung ist offen, ob und welche zusätzlichen Personenidentifizierungsdaten von der identitätsstelle einer E-ID zugeordnet werden. Für Betreiber von E-ID-verwendenden Diensten bestehen damit Unsicherheiten in Bezug auf den Inhalt der jeweiligen E-ID bzw. die bei der Identitätsstelle geprüften Daten. Dies hätte zur Folge, dass die Betreiber von E-ID-verwendenden Diensten den Umfang der geprüften bzw. zugeordneten Daten von IdP zu IdP gesondert zu ermitteln hätten. Dies ist nicht praktikabel. Damit Klarheit und Rechtssicherheit besteht, sind die von der Identitätsstelle einer E-ID zuzuordnenden Daten in Art. 7 VE E-ID-Gesetz für jedes Sicherheitsniveau (Art. 5 Abs. 1 VE E-ID-Gesetz) verbindlich festzulegen.

  Die von der Identitätsstelle einer E-ID zuzuordnenden Personenidentifizierungsdaten sind für jedes Sicherheitsniveau auf Gesetzesstufe verbindlich zu definieren.

- **Antrag: Heimatort als zusätzlichen Inhalt einer E-ID aufführen (Art. 7 Abs. 2 VE E-ID-Gesetz)**

  Die Schweizer Ausweisdokumente beinhalten den Heimatort und nicht den Geburtsort. Damit Konsistenz zwischen physischem Ausweis und E-ID besteht, ist in Art. 7 Abs. 2 VE E-ID-Gesetz neben dem Geburtstort auch der Heimatort aufzuführen.

In Art. 7 Abs. 2 VE E-ID-Gesetz ist neben dem Geburtstort auch der Heimatort aufzuführen.

- **Antrag: Art. 7 Abs. 4 VE E-ID-Gesetz um den Begriff „Attribute" ergänzen**

  Im Sinne des oben zu Art. 2 lit. k VE E-ID-Gesetz gestellten Antrags (Definition des Begriffs „Attribute") ist Art. 7 Abs. 4 VE E-ID-Gesetz wie folgt zu ergänzen (Ergänzung = unterstrichen):

„Der IdP kann einer E-ID weitere Daten (Attribute) zuordnen.

- **Antrag: Weitergabe von Personenidentifizierungsdaten flexibler regeln (Art. 10 Abs. 3 VE E-ID-Gesetz)**

  Art. 10 Abs. 3 VE E-ID-Gesetz legt fest, dass namentlich Betreiber von E-ID verwendeten Diensten weder die Personenidentifizierungsdaten gemäss Art. 7 Abs. 2 VE E-ID-Gesetz noch die darauf basierenden Nutzungsprofile Dritten bekannt geben dürfen. Im Erläuternden Bericht wird dazu ausgeführt, dass weder der Handel noch die unentgeltliche Weitergabe von Daten – auch nicht innerhalb eines Konzerns – erlaubt sein sollen. Diese Bestimmung in ihrer absoluten Form erachtet die SPA als zu weitgehend, nicht kompatibel mit der Geldwäschereigesetzgebung und nicht praktikabel.

  Was den Bereich der Geldwäschereibekämpfung betrifft, ist dort eine Delegation der Identifizierung der Vertragspartei ausdrücklich erlaubt. Die Geldwäschereiverordnung-FINMA schreibt diesbezüglich vor, dass der delegierende Finanzintermediär Kopien der Unterlagen, d.h. auch der Identifikationsdokumente, zu seinen Akten zu nehmen hat[3]. Nimmt nun ein ordentlich ausgewählter, instruierter und überwachter Dritter eine Identifizierung nach Geldwäschereigesetzgebung unter Zuhilfenahme eines E-ID verwendeten Dienstes vor, so muss es ihm vernünftigerweise gestattet sein, die Kopien der Identifikationsdokumente dem Finanzintermediär (im Einklang mit den Vorschriften der Geldwäschereiverordnung-FINMA bzw. der VSB) zukommen zu lassen. Dies wird mit Art. 10 Abs. 3 VE E-ID-Gesetz verunmöglicht[4]. Analog präsentiert sich die Situation bei der konzerninternen Identifizierung[5], wo ebenfalls verlangt ist, dass Kopien der Identifikationsdokumente erstellt werden.

  Bezüglich des vorgesehenen Verbots der Weitergabe der Daten innerhalb eines Konzerns ist ganz allgemein darauf hinzuweisen, dass eine solche Einschränkung der heutigen Realität nicht entspricht und nicht praktikabel wäre. So wäre z.B. eine konzernzentrale Verwaltung von Kundeninformationen nicht mehr möglich. Zusätzlich ist die vorgesehene Bestimmung nicht kundenfreundlich: Bietet ein Konzern seine Produkte z.B. über mehrere Konzerngesellschaften an, so müsste eine Kunde für jedes Produkt separat identifiziert werden. Eine Authentifizierung würde nicht ausreichen.

[3] Art. 29 Abs. 2 GwV-FINMA, analog Art. 43 Abs. 2 VSB 16

[4] Art. 7 Abs. 2 lit. e VE E-ID-Gesetz nennt die Staatsangehörigkeit, welche für die Identifizierung einer Vertragspartei wesentlich ist. Eine Weiterleitung dieses wichtigen Attributes wäre gemäss Art. 10 Abs. 3 VE E-ID-Gesetz nicht möglich.

[5] Art. 28 Abs. 2 lit. a GwV-FINMA in Verbindung mit Art. 29 Abs. 2 GwV-FINMA, Art. 19 VSB 16

Die SPA plädiert daher dafür, dass anstelle des in Art. 10 Abs. 3 VE E-ID-Gesetz stipulierten absoluten Verbotes der Weitergabe von Daten das etablierte datenschutzrechtliche Prinzip zur Anwendung kommen, dass es der Inhaberin oder dem Inhaber der E-ID überlassen bleibt zu bestimmen, wie mit ihren/seinen Daten zu verfahren ist. Ein entsprechendes Akzept seitens der künftigen E-ID-Inhaberin oder des künftigen Inhabers könnte z.B. im Rahmen des in Art. 6 Abs. 1 VE E-ID-Gesetz angesprochenen Antragsprozesses rechtsgenüglich eingeholt werden und Grundlage für eine weitergehende Nutzung von Daten im Einverständnis mit der betroffenen Person sein.

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 ist zu ersetzen. An dessen Stelle ist ein 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 zubilligt.

2.3 Anbieterinnen von Identitätsdienstleistungen / IdP (Art. 17 f. VE E-ID-Gesetz)

- **Antrag: Orientierung an internationalen Standards bei der Bestimmung der technischen Standards (Art. 18 Abs. 2 VE E-ID-Gesetz)**

  Damit eine Interoperabilität ggf. auch mit ausländischen Systemen hergestellt werden kann, ist es notwendig, dass die Standards und Schnittstellen entsprechend dem im Ausland Üblichen ausgestaltet werden. Dieses Erfordernis soll in der Delegationsnorm von Art. 18 Abs. 2 VE E-ID-Gesetz aufgeführt werden.

2	"Der Bundesrat bestimmt die technischen Standards und definiert die Schnittstellen. Er orientiert sich dabei an internationalen Standards."

Wir danken Ihnen für die Prüfung unserer Ausführungen sowie für die Berücksichtigung unserer Überlegungen und Anliegen. Bei allfälligen Rückfragen stehen wir Ihnen gerne zur Verfügung. Wenden Sie sich bitte an den Rechtsunterzeichneten (thomas.hodel@swiss-p-a.ch / 058 426 25 50).

Freundliche Grüsse

Swiss Payment Association

Dr. Daniel Bürchler
Vizepräsident

Dr. Thomas Hodel
Geschäftsführer

Swico
Josefstrasse 218
CH-8005 Zürich

Tel. +41 44 446 90 90
www.swico.ch
info@swico.ch

Eidgenössisches Justiz-
und Polizeidepartement EJPD
Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

Zürich, 29. Mai 2017

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

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Namens des Swico bedanken wir uns für die Möglichkeit, unsere Position zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) darzulegen und reichen Ihnen hiermit unsere Stellungnahme ein.

1. Legitimation und Betroffenheit

Swico ist der Verband der ICT-Anbieter der Schweiz. Swico vertritt die Interessen von 450 ICT-Anbieterfirmen, welche 56'000 Mitarbeitende beschäftigen und einen Umsatz von jährlich CHF 40 Milliarden erwirtschaften.

Swico ist Mitgründer des Vereins Swiss Data Alliance. Swiss Data Alliance setzt sich für eine zukunftsorientierte Datenpolitik ein, damit Daten ihr innovatives Potenzial in der Schweiz voll entfalten können. Das Kernelement einer funktionierenden Dateninfrastruktur ist ein staatlicher elektronischer Identitätsnachweis.

Die Einführung eines elektronischen Identitätsnachweises hat direkte Auswirkungen auf die ICT-Branche insgesamt und damit verwandter Branchen. Unsere Mitglieder sind daher von dieser Vorlage unmittelbar und ganz besonders betroffen und Swico zu vorliegender Stellungnahme legitimiert.

2. Grundsätzliches

2.1 Antrag für die Überarbeitung

Swico unterstützt die Stellungnahme der Swiss Data Alliance und insbesondere auch die Feststellung, dass der vom Bundesrat vorgelegte Entwurf und das darin abgebildete Konzept (namentlich das „Konzept 2016" des fedpol „Staatlich anerkannte elektronische Identifizierungsmittel (E-ID)") in die falsche Richtung gehen. Deshalb beantragen wir die Rückweisung der Vorlage zur Überarbeitung im Sinne der nachstehenden Ausführungen.

2.2 Bedürfnis nach einem digitalen Ausweis

Die digitale Welt verlangt für eine Vielzahl von Dienstleistungen unsere Identifikation als Nutzer. Manchmal genügen dazu einige Angaben zur Person, z.B. eine gültige Email-Adresse oder bloss eine Kreditkartennummer. Manchmal sind aber Informationen nötig, die von einer staatlichen Stelle beglaubigt sein müssen, weil die Applikation besonders heikel ist. Beispiele sind das elektronische Patientendossier, das E-Voting oder ein Strafregisterauszug. Wie in der nicht-digitalen Welt benötigen wir dann einen amtlichen Ausweis, welcher unsere Identität staatlich nachweist.

2.3 Vertrauen in den staatlichen Identitätsnachweis

Wie auch im erläuternden Bericht zur Vernehmlassungsvorlage festgestellt wird, geniesst der Staat auf allen föderalen Ebenen besonderes Vertrauen für die Bestätigung der Identität einer Person (vgl. Bericht S. 7).

In der nicht-digitalen Welt hat der Staat dazu bereits vor langer Zeit hoheitliche Institutionen und Verfahren eingerichtet, über welche wir einen solchen amtlichen Ausweis beziehen können. Die Glaubwürdigkeit der Schweizer Ausweispapiere, insbesondere des Schweizer Passes, ist legendär und Basis für zahllose Geschäftstransaktionen. Wir vertrauen dem Schweizer Pass, weil er vom Staat und nicht von einer privaten Unternehmung oder Organisation ausgestellt wird. Glaubwürdigkeit und Vertrauen sind auch in der digitalen Welt elementar für den Aufbau erfolgreicher Geschäftsbeziehungen. Wir wissen, dass dieses Vertrauen bei digitalen Dienstleistungen leider nicht immer gerechtfertigt ist. Wir müssen uns stets kritisch fragen, welche persönlichen Angaben wir zu welchem Zweck zur Verfügung stellen wollen und welches Risiko wir dabei eingehen. Besonders kritisch wird es dann, wenn der staatliche Nachweis unserer elektronischen Identität verlangt wird. Hier kann für uns selber, aber auch für den Dienstleister, nur die höchste Vertrauensstufe ausreichend sein. Der staatliche Nachweis der elektronischen Identität muss daher genau wie bei den nichtdigitalen amtlichen Ausweispapieren eine hoheitliche Aufgabe bleiben, welche der Staat selber wahrnimmt. Nur dann ist die höchste Stufe des Vertrauens und der Glaubwürdigkeit gewährleistet, welche gewisse elektronische Geschäfte erfordern. Wir wollen auf unser elektronisches Patientendossier nicht mit dem Ausweis eines Transportunternehmens zugreifen und wir wollen auch unsere Steuerunterlagen nicht mit dem Ausweis einer Bank einreichen. Wir wollen unsere staatliche elektronische Identität nicht von einem Detailhändler oder einer Versicherung, sondern nur vom Staat selbst beziehen.

3. Zum Vorentwurf im Besonderen

Der Vorentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) schlägt vor, die staatliche elektronische Identifikation an Unternehmen und Organisationen abzugeben, welche dafür zertifiziert werden. Swico ist der Ansicht, dass dieses Konzept zum Scheitern verurteilt ist. Die Unternehmen und Organisationen, welche sich als Ausgabestelle für staatliche elektronische Ausweise zertifizieren lassen, mögen noch so glaubwürdig sein – die Nutzer werden ihnen nie dasselbe Vertrauen schenken wie einer staatlichen Stelle, welche diese Aufgabe hoheitlich wahrnimmt. Dieses ungeteilte Vertrauen ist aber die Basis für einen erfolgreichen elektronischen Schweizer Pass und damit Grundlage für den Erfolg der digitalen Wirtschaft und Verwaltung in der Schweiz. Es gibt zahllose Aufgaben, welche die Wirtschaft besser lösen kann als der Staat. Die hoheitliche Abgabe von analogen und elektronischen Identitätsausweisen gehört nicht dazu.

Am Vorentwurf bestehen v.a. die folgenden Kritikpunkte:

3.1 Falscher Fokus

Der Begriff der E-ID-Dienstleistungen wird im Vorentwurf zu weit verstanden. Es ist richtig, dass der Staat keine der Privatwirtschaft vorzubehaltenden Dienstleistungen („E-ID verwendende Dienste") anbieten sollte. Er soll sich auf den eng zu verstehenden Kernbereich beschränken. Aber dieser Kernbereich ist eine staatliche Aufgabe.

3.2 Beschreibung „E-ID" schärfen

Ob ein separates E-ID-System als neues „Register" aufzubauen ist, ist noch in keiner Weise geklärt. Denkbar ist, dass nur ein blosser Abfrageservice eingerichtet wird, der auf bereits bestehende Register zugreift.

3.3 Die E-ID darf keine Nummer sein

Weiter ist die Beschreibung, was die E-ID ausmacht, unvollständig. Zentral - gerade aus Gründen des Datenschutzes und zum Schutz vor Überwachung des Bürgers im Staat - ist hervorzuheben, dass die staatliche E-ID gerade keine Nummer ist. Einmalige, zeitlich limitiert gültige transaktionsbezogene Nummern (Authentisierungscodes) sollen generiert werden können; aber es wäre falsch, die E-ID als neue permanente zentrale Personennummer einzuführen.

3.4 Systembedingte Strukturierungsnummern sind nicht zu kommunizieren

Der Vorentwurf geht mit der „E-ID-Registrierungsnummer" (einer Person eindeutig zugeordnete Identifikationsnummer) in die falsche Richtung. Ein neues Register, falls tatsächlich benötigt, müsste wohl über eine Nummer erschlossen werden, und zwar für jeden neu anzulegenden Eintrag, der über die AHVN13 gespiesen wird (aus den Registern ISA, ZEMIS und Infostar sowie gegebenenfalls ZAS-UPI); diese Nummer könnte durchaus als „E-ID-Registrierungsnummer" bezeichnet werden. Die E-ID-Registrierungsnummer wäre aber auf jeden Fall nur eine verwaltungsintern zu benutzende technische Ordnungsnummer zur Führung und zum Aufbau des E-ID-Systems. Diese Angabe darf nicht nach aussen bekannt gegeben werden, zumal eine Bekanntgabe nach aussen für das Funktionieren des E-ID-Systems nicht erforderlich ist.

3.5 Rechtsunsicherheit über Datenhoheit

Aus Sicht der Wirtschaft ist sodann hervorzuheben, dass Art. 10 des Vorentwurfs erhebliche Konsequenzen auf den bereits bestehenden Datenbestand bei privaten Unternehmen haben könnte. Würde sich ein privates Unternehmen nach dem Konzept des Vorentwurfs als IdP melden, müsste es gewärtigen, einen Grossteil seiner Daten nicht mehr verwerten zu können, soweit er mit dem Katalog gemäss Art. 7 des Vorentwurfs übereinstimmt: Wie ist der bestehende Datenbestand abzugrenzen gegenüber jenem, den das Unternahmen „als IdP" erwirbt? Entweder ist Artikel 10 des Vorentwurfs ein Papiertiger oder aber ein Brocken mit verheerender Wirkung.

3.6 Zeitverlust

Insgesamt führt das Konzept des Vorentwurfs zum Risiko, dass der Schweiz noch lange Zeit ein einheitlicher Standard fehlen wird (nicht zuletzt wegen der zu befürchtenden Marktzersplitterung). Das ist mit Blick auf die Digitalisierung, die heute, im Hier und Jetzt stattfindet und bereits pulsiert, unannehmbar. Die Schweiz würde mit dem vorliegenden Gesetzesentwurf gebremst. Dies muss um jeden Preis verhindert werden. Deswegen braucht es sofort eine „E-ID für alle".

4. Unterstützung des Gegenvorschlages der Swiss Data Alliance

Die Swiss Data Alliance hat den nachfolgenden breit abgestützten, konstruktiven Gegenvorschlag verfasst, welchen Swico vollumfänglich unterstützt.

4.1 Grundzüge der alternativen Regelung

- Der staatliche elektronische Identitätsnachweis ist eine hoheitliche Aufgabe des Bundes. Die Staatsaufgabe besteht darin, innerhalb der Verwaltung und für Dritte, auf Anfrage die Korrektheit der Personenidentifizierungsdaten sowie die Authentizität der zu identifizierenden Person zu prüfen.
- Die staatliche E-ID ist keine Nummer, sondern die Gesamtheit der vom Staat (entsprechend Art. 7 des Vorentwurfs) bestimmten Personenidentifizierungsdaten, welche der Staat als Eigenschaften einer bestimmten Person verifiziert und in den dazu bestimmten Registern gespeichert hat. Das staatliche E-ID-System benötigt von Seiten einer abfragenden Applikation keine einheitliche, auf einen Einzelnen bezogene Nummer, sondern nur einen transaktionsbezogenen Code, welche diese von der zu identifizierenden Person erhält.
- Der Bund sollte die staatliche E-ID ausgeben und verwalten. Die Befürchtung des Bundes, mit der technologischen Entwicklung nicht mithalten zu können, ist kein valider Grund, die Bestätigung der E-ID als Staatsaufgabe zu verneinen. Auch das Kostenargument (Erläuternder Bericht zum Vorentwurf, Ziffer 1.3.1) überzeugt nicht.
- Sourcing für das E-ID-System: Der Bund sollte eine Public-Private-Partnership prüfen oder einen Dienstleister mandatieren, das staatliche E-ID-System technisch zu betreiben. Im Umfeld der Ausgabe von Ausweisdokumenten (namentlich im Kontext des Ausweisgesetzes) bestehen bereits vergleichbare Systeme. Ausserhalb des Sourcing-Bereichs liegen Mehrwertdienste. Solche Mehrwertdienste kann jeder (auch der Dienstleister, mit

dem der Bund zusammenarbeitet) auf eigene Rechnung, auf eigenes Risiko und zum eigenen Vorteil anbieten.

- Spezifikation des E-ID-Systems: Das vom Bund zu betreibende System besteht aus Datenschnittstellen zu den bestehenden Personenregistern, Sicherheitselementen, einer externen Schnittstelle (API) und einem Dienst, der eine Überprüfung von Personenidentifizierungsdaten und deren Zuordnung zu einer bestimmten Person (Authentifizierung) ermöglicht.
- Spezifikation der Schnittstelle (API und evtl. Webzugang) und Nutzungsbedingungen: Swico unterstützt den diesbezügliche Anregung der Swiss Data Alliance, d.h. vertieft zu prüfen, inwiefern Anbieter von die E-ID verwendenden Diensten sich mittels eines verwaltungsrechtlichen Vertrags verpflichten müssen, bestimmte Nutzungsbedingungen zur Verwendung der Schnittstelle zu akzeptieren.
- Ausweisdokumente: Ergänzend zum E-ID-System, aber nur als Add-On, können Ausweisdokumente mit maschinenlesbaren Personenidentifizierungsdaten ausgegeben werden. Die Anbindung an Ausweisdokumente ist eine Erweiterung, und nicht Kerngehalt eines funktionierenden E-IDSystems des Bundes.

Die Swiss Data Alliance hat im Anhang ihrer Stellungnahme eine Lösungsskizze für die staatliche E-ID vorgeschlagen, welche aufzeigt, wie die vorstehenden Überlegungen technisch umgesetzt werden können. Darauf verweisen wir vollumfänglich.

4.2 Zur gesetzlichen Grundlage insbesondere

Es stellt sich die Frage, ob eine neue formell-gesetzliche Grundlage zu schaffen ist, um das staatliche EID-System aufzubauen. Sofern das E-ID-System aus einem blossen Abfrageservice auf bestehende Register besteht, kann als möglich erachtet werden, dass die bestehenden Registergesetze als Basis für eine Verordnung des Bundesrats ausreichen (Ausweisgesetz, Ausländergesetz, Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich, BGIAA; Zivilgesetzbuch und Zivilstandsverordnung sowie ZAS-Verordnung mit deren gesetzlichen Grundlagen). Jedenfalls sollte dieser Aspekt nochmals durchdacht werden (namentlich mit Blick auf die Notwendigkeit der Verwendung der AHVN13, des Verbots von Parallelregistern und der datenschutzrechtlich erforderten Regelung von Abfragediensten). Sofern singulär nur für die ISA-Datenbank eine Verknüpfung mit der AHVN13 beabsichtigt wird, wäre auch die Regelung nur dieses Aspekts direkt im Ausweisgesetz möglich. Ein neuer formell-gesetzlicher Erlass wäre dann nicht nötig und eine Regelung auf Verordnungsstufe könnte genügen.

Wenn mit dem „E-ID-Gesetz" ein neuer Erlass begründet werden müsste, ist dieser zu vereinfachen und zu entschlacken, was mit dem Gegenvorschlag der Swiss Data Alliance auf jeden Fall möglich wäre. Bei Schaffung eines neuen Erlasses sollte die verfassungsrechtliche Herleitung zudem nicht allein in Art. 95 und Art 122 BV gesucht werden (so der Vorentwurf), weil sonst z.B. die Regelung in Art. 13 des Vorentwurfs nicht begründet werden könnte (Art. 13 des Vorentwurfs betrifft nur den Bereich eGovernment, der sich mit der Regelung allein aus der zivilrechtlichen Optik kaum rechtfertigen liesse). Es bieten sich allerdings mit den Bestimmungen zum Registerrecht (Art. 65 Abs. 2 BV) und jenen zum Ausweisrecht auf Basis der Bestimmungen zum Bürgerrecht, Ausländerrecht, Asylrecht und Beziehungen zum Ausland (Art. 38, Art. 121 und Art. 166 BV) sinnvolle Ergänzungen an. Allenfalls kann - im

Sinne einer Pflicht zum Tätigwerden des Staats zwecks Durchsetzung von Freiheitsrechten - auch der verfassungsrechtlich garantierte Anspruch auf Bewegungsfreiheit ins Feld geführt werden (Art. 10 Abs. 2 BV, verstanden als konstitutiv-institutionelles Freiheitsrecht).

4.3 Zur Gebührenfrage insbesondere

Staatliche Grundversorgung soll grundsätzlich gebührenfrei zur Verfügung gestellt werden. Jeder und jede Anspruchsberechtigte soll eine staatliche E-ID ausgestellt erhalten, ohne dafür bezahlen zu müssen. Die Nutzer und Nutzerinnen müssen die E-ID im E-ID-System allenfalls aktivieren (in Form einer Bestätigung), ansonsten steht die E-ID aber im Sinne eines Automatismus für jede bzw. jeden Anspruchsberechtigten voraussetzungslos zur Verfügung.

5. Fazit

Zusammenfassend ist es aus unserer Sicht unabdingbar, dass die initiale Feststellung der elektronischen Identität auf hoheitlichem Weg erfolgt. Die weitergehende Ausgestaltung, insbesondere was die Applikationen und Schnittstellen für Drittanbieter anbelangt, ist nicht Aufgabe des Staates, sondern von zertifizierten ID-Providern, welche sich dynamisch am Markt ausrichten. Der Bürger hat dann die Wahlfreiheit über die Angebote auf dem Markt zu entscheiden.

Wir danken Ihnen namens unserer Mitglieder für eine Berücksichtigung unserer Anliegen.

Freundliche Grüsse

Swico

Jean-Marc Hensch
Geschäftsführer

Christa Hofmann
Head Legal & Public Affairs

Gruber Daniel BJ

Von: Thomas Flatt <thomas.flatt@swissict.ch>
Gesendet: Freitag, 9. Juni 2017 10:36
An: Gruber Daniel BJ
Betreff: Re: Präsentation im Vorstand swissICT

Sehr geehrter Herr Gruber

Nochmals herzlichen Dank für Ihren Besuch bei uns und Danke für die lebhafte Präsentation/Diskussion, die Sie ermöglicht haben. Danke auch für Ihr Angebot, noch eine Vernehmlassungsantwort nachzureichen. Für eine vollständige, detaillierte Antwort ist es zu spät. Wir haben aber im Nachgang unsere Position wie folgt zusammengefasst:

1. Wir unterstützen das Gesetz im Grundsatz so wie es vorliegt – es ist, zumindest aus staatlicher Sicht, ein Ressourcen schonendes Vorgehen (s. auch Punkt 5)
2. Eine Einschränkung, wer die E-ID technisch herausgibt ist nicht notwendig. Es können sich also unserer Meinung nach mehrere private Anbieter etablieren.
3. Die Verantwortung, private Anbieter zu überwachen, bleibt aber beim Staat. Damit ist der Debatte, bezüglich hoheitlicher Verantwortung, Genüge getan.
4. Wir begrüssen die Kompatibilität mit der EU Gesetzgebung und die Möglichkeit einer zukünftigen Interoperabilität mit europäischen E-IDs
5. Wir bleiben bei unserer eher skeptischen Beurteilung bezüglich einer raschen Verbreitung der E-ID in der Praxis. Der Grenznutzen der staatlichen E-ID im Vergleich zu heute bereits angebotenen Lösungen ist klein. Doch hier werden wir gerne eines Besseren belehrt.

Beste Grüsse
Thomas Flatt

SWITCH

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Per E-Mail an:
copiur@bj.admin.ch

Zu Handen:
Frau Bundesrätin Sommaruga
Eidgenössisches Justiz- und Polizeidepartement EJPD

Dr. Andreas Dudler
Managing Director
Telefon: +41 44 268 15 15
Direktwahl: +41 44 268 15 13
E-Mail: andreas.dudler@switch.ch

Zürich, 29. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Namens SWITCH bedanken wir uns für die Möglichkeit im Vernehmlassungsverfahren zum Entwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung nehmen zu können.

1. Legitimation

SWITCH steht für mehr Leistung, Komfort und Sicherheit in der digitalen Welt. In Partnerschaft mit ihren Anspruchsgruppen in und ausserhalb der akademischen Welt entwickelt und verbessert die Stiftung ganzheitliche ICT-Lösungen in den Bereichen Network, Security, Identity Management und Cloud Computing. Seit den Anfängen des Internets ist SWITCH auch die Registry für Domain-Namen mit den Endung .ch und.li. Die Stiftung beschäftigt rund 100 Mitarbeitende an ihrem Sitz in Zürich.

Seit mehr als 10 Jahren betreibt SWITCH eine Sektorlösung für die Bereitstellung föderierter digitaler Identitäten an 400'000 Nutzer und 1'000 vertrauende Dienste der schweizerischen Hochschullandschaft.

2. Grundsätzliche Überlegungen

SWITCH bekräftigt, dass eine funktionierende und allgemein akzeptierte E-ID ein wichtiges Anliegen darstellt.

Unabhängig vom E-ID-Gesetz existieren weitere Lösungen rund um die digitale Identität. Diese decken, wie im Falle von SWITCH als Sektorlösung, spezifische Bedürfnisse ab. Für solche Identitätsdienste stehen zwei Anwendungsfälle im Vordergrund:

1. Der Identitätsdienst kann als E-ID-IdP die E-ID-Funktion selber anbieten.

2. Der Identitätsdienst kann als E-ID-verwendenden Dienst einen E-ID-Dienst Dritter nutzen.

Beide Anwendungsfälle sind potenziell wichtige Treiber für die Verbreitung der E-ID über reine eGovernment-Anwendungen hinaus und für das Entstehen eines E-ID-Ökosystems. Wir möchten diese Anwendungsfälle einzeln reflektieren.

2.1 Grundsätzliche Überlegungen für E-ID-IdP

Für Identitätsdienste ist wichtig festzuhalten, welche Attribute (als Basisattribute) den Regeln des E-ID-Gesetzes unterworfen sind und für welche diese Regeln nicht gelten. Im aktuellen Gesetzesentwurf steht, dass der E-ID-IdP einer E-ID weitere Daten zuordnen kann (Art 7, Abs. 4). Diese Bestimmung soll nicht so verstanden werden dürfen, dass zusätzliche Attribute bei der Identitätsstelle registriert und im Rahmen der Interoperabilität mit anderen E-ID-IdPs ausgetauscht werden müssen. Aus diesem Grund ist Art. 7, Abs. 4 entsprechend anzupassen oder zu streichen.

Eine Umsetzung auf der Basis des E-ID-Gesetzesentwurfs birgt in unserer Einschätzung erhebliche Risiken, schafft hohe Komplexität und wird keine schnelle Umsetzung erlauben:

- Vor der Inbetriebnahme eines E-ID Dienstes muss das regulatorische Umfeld geschaffen worden sein (insbesondere die Anerkennungsstelle) und die Marktteilnehmer müssen akkreditiert worden sein.

- Zudem muss das am Markt nicht erprobte (und im Bericht auch nicht näher beschriebene) "Roaming" (Art. 18, Interoperabilität) zwischen den verschiedenen Anbietern geklärt sein. Es ist davon auszugehen, dass die Eckwerte dieses "Roamings" in entsprechenden TAVs vor der Akkreditierung und deutlich vor der Markteinführung vorliegen müssen. Hierbei kann nicht davon ausgegangen werden, dass bei den Marktteilnehmern Einigkeit herrscht über das zu verwendende Business Modell für das "Roaming".

- Im Falle von sich gegenseitig ausschliessenden "Roaming" Modellen oder Business Modellen, ist unklar wie sich die Aufsichtsbehörden für ein Modell festlegen sollen, das dann in die TAV übernommen werden soll.

- Anbieter von Identitätsdienstleistungen werden sich erst nach Detailkenntnis des zugrunde liegenden "Roamings" zwischen den Anbietern entscheiden können, ob sie die Funktion der E-ID in die Roadmap ihrer Identitäten aufnehmen wollen oder nicht.

- Damit entpuppt sich der Aufbau des regulatorischen Umfeldes als recht komplexe Aufgabe und wird die Umsetzung einer E-ID markant verzögern.

- Es ist zur Zeit nicht abschätzbar, ob dieser Markt funktionieren wird.

2.2 Grundsätzliche Überlegungen für E-ID-verwendende Dienste

Um eine möglichst grosse Verbreitung E-ID-verwendender Dienste und die innovative Nutzung der E-ID zu fördern, sind folgende Aspekte zu beachten:

- Die Nutzung der durch den Inhaber der E-ID freigegebenen Basis-Attribute dürfen durch die E-ID-IdPs über die geltenden Gesetze hinaus nicht weiter eingeschränkt werden.

SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

- Die Nutzung der durch den Inhaber der E-ID freigegebenen Basis-Attribute durch E-ID-verwendende Dienste soll für letztere (unter gewissen Einschränkungen wie z.B. dem Nutzungsvolumen) grundsätzlich kostenlos und möglichst ohne weitere Hindernisse erfolgen.

3. Vorgehensvorschlag

SWITCH schlägt die Überarbeitung des Entwurfes vor:

- Zur Sicherstellung einer schnellen Umsetzung und zur Reduktion der Risiken sowie der Komplexität schlägt SWITCH vor, den Verzicht auf das Marktmodell zugunsten einer Umsetzung durch den Bund oder einer Vergabe durch den Bund an einen Dritten zu prüfen.
- Sollte das Marktmodell weiter verfolgt werden, schlägt SWITCH den Einsatz einer Expertengruppe vor, in der die verschiedenen Interessenvertreter (zumindest potenzielle E-ID-verwendende Dienste und E-ID-IdP, sowie die öffentliche Hand) die unter 2.1 erwähnten Aspekte klären. Gerne würde sich SWITCH für eine Teilnahme in einer solchen Expertengruppe zur Verfügung stellen. Nur wenn sich auf Basis der erarbeiteten Resultate mehrere Anbieter klar zur Integration einer E-ID-Funktion in ihre Identitätsdienste verpflichten und sich dazu auf ein "Roaming"-Modell einigen können, ist der privatwirtschaftliche Ansatz weiter zu verfolgen. Ansonsten ist ein staatlicher Ansatz (oder auch die Vergabe) zum Aufbau einer E-ID klar vorzuziehen.

Gerne stehen wir Ihnen zur Erläuterung unserer Sichtweise zur Verfügung. Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

Dr. Andreas Dudler
Managing Director

Christoph Graf
Programm Leiter SWITCH edu-ID

DJS JDS GDS

Demokratische Juristinnen und Juristen der Schweiz
Juristes Démocrates de Suisse
Giuristi e Giuriste Democratici Svizzeri
Giuristas e Giurists Democratics Svizzers

Schwanengasse 9
3011 Bern
Tel 078 617 87 17
info@djs-jds.ch

An die Vorsteherin des EJPD
Frau Bundesrätin Simonetta Sommaruga
3003 Bern

per E-Mail an copiur@bj.admin.ch

Bern, den 29. Mai 2017

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten, E-ID-Gesetz,
Vernehmlassungsfrist 29. Mai 2017

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Die Demokratischen Juristinnen und Juristen der Schweiz nehmen hiermit kurz Stellung zur Einführung elektronischer Identifizierungseinheiten (E-ID). Wir schliessen uns den Ausführungen des Vereins grundrechte.ch an, deren Stellungnahme Sie ebenfalls erhalten haben.

Eine E-ID ist ausschliesslich durch den Staat ohne Einbezug von Privaten zu vergeben und wir fordern, dass der vorliegende Entwurf in diesem Sinne vollständig zu überarbeiten ist.

Jede neue Datenbank erweckt neue Begehrlichkeiten wie Missbrauch, Manipulation, Erpressung, oder Handel mit Daten. Da es keine Garantie gibt, Datenbanken vor Angriffen von aussen hundertprozentig zu schützen, muss der Staat umso sorgfältiger mit den Personendaten seiner Bürgerinnen und Bürger umgehen.

Die E-ID darf auf keinen Fall die herkömmlichen Ausweispapiere (ID, Pass, Ausländerausweis) ersetzen. Die Wahlfreiheit, mit welcher Methode, mit welchem amtlichen Dokument sich jemand gegenüber öffentlichen Ämtern oder privaten Firmen ausweisen will, muss zwingend erhalten blei-

ben. Nur so kann das Grundrecht auf informationelle Selbstbestimmung auf lange Zeit gewahrt und geschützt werden.

Wenn überhaupt eine E-ID eingeführt werden soll darf dies auf gar keinen Fall an private profitorientierte Unternehmen ausgelagert werden. Der Staat ist die einzige Institution, die – analog der Ausstellung amtlicher Ausweise – dazu berechtigt sein darf. Es muss unbedingt gewährleistet bleiben, dass das Ausstellen eines rechtsgültigen ID Nachweises, in welcher Form auch immer, eine unveräusserliche Aufgabe des Staates bleibt und damit sichergestellt wird, dass kein Datenmissbrauch möglich ist.

Die Vorlage geht auch bezüglich der zu verarbeitenden Daten für eine E-ID zu weit. Es ist nicht ersichtlich, weshalb derart viele Personendaten quasi auf Vorrat gesammelt und den privaten Anbietern zur Verfügung gestellt werden sollen. Insbesondere die Versichertennummer nach Artikel 50c des Bundesgesetzes über die Alters- und Hinterlassenen-Versicherung sowie das Gesichtsbild und das Unterschriftsbild aus der nationalen Ausweisdatenbank sind hochsensible höchstpersönliche Daten und werden einzig für andere, ganz bestimmte eingeschränkte Zwecke unter Zusicherung der Vertraulichkeit erfasst.

Es gibt bereits genügend aktuelle Beispiele, wonach Personendaten längst nicht nur für den ursprünglich angegebenen Zweck verwendet werden. Die im Gesetzesentwurf vorgesehene Kontrolle durch die beim Bund angesiedelte Anerkennungsstelle ist ungenügend. Sie wäre kaum in der Lage, die korrekte Verwendung aller Personendaten sicher zu stellen – zumal diese sogar von den Identity Providern an Betreiber von E-ID-verwendende Dienste weitergegeben werden dürften.

Die Ausstellung einer E-ID muss auch unter diesem Kontrollaspekt eine reine Bundesaufgabe bleiben. Nur so kann sichergestellt werden, dass der Umgang mit diesen sensiblen Daten jederzeit auch einer parlamentarischen Aufsicht und Kontrolle unterstellt bleibt und das Gesetz, sofern notwendig, nachgebessert werden kann, ohne dass dadurch bestehende Verträge mit privaten Dritten verletzt würden.

Zusammenfassend halten wir fest, dass wir die Vorlage insgesamt ablehnen. Die Einführung einer E-ID muss zwingend eine staatliche Aufgabe bleiben. Sie darf unter keinen Umständen an private Dritte ausgelagert werden. Staatlich anerkannte Identitätsausweise müssen, in welcher Form auch immer, ausschliesslich vom Staat selbst ausgestellt und nachgeführt werden. Das Kostenargument darf hier nicht zum Tragen kommen.

Zudem muss der Bund sicherstellen, dass die Bürgerinnen und Bürger jederzeit das Recht haben selber zu entscheiden, mit welchem Dokument sie sich ausweisen wollen. Dies gilt auch für die Authentifizierungs-Vorgaben von privaten Firmen. Der Bund ist in der Pflicht diese anzuweisen, das Recht auf informationelle Selbstbestimmung, die digitale Selbstbestimmung zu wahren. Die im Bericht erwähnten Projekte „Passepartout fürs Internet“ von Credit Suisse, UBS und Swisscom sowie „SwissID“ von der Post und den SBB sehen eine Zwangsverpflichtung der KundInnen zu einer digitalen E-ID vor. Sie alle verletzen dieses Grundrecht. Der Bundesrat ist daher aufgefordert, die gesetzlichen Grundlagen zu schaffen bzw. das Datenschutzrecht so anzupassen, dass die Kundinnen und Kunden die Angebote auch ohne SwissID wahrnehmen können.

Mit der Bitte um Kenntnisnahme verbleibe ich,

Mit freundlichen Grüssen

Melanie Aebli
Geschäftsleiterin DJS

eGov schweiz
innovation and network

Per E-Mail zu Handen: copiur@bj.admin.ch
Frau Bundesrätin
Simonetta Sommaruga
Eidg. Justiz- und Polizeidepartement
3003 Bern

Bern, 24. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz).

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit, im Rahmen der Vernehmlassung zum neuen E-ID-Gesetz Stellung zu nehmen.

Einleitung und grundsätzliche Bemerkungen
Der Verein eGov-Schweiz, www.egov-schweiz.ch, wurde als PPP-Projekt (Anschubfinanzierung durch den Kanton Bern) zur Förderung der Innovation im eGovernment 2011 gegründet. Seine Vision, Ziele und Tätigkeiten basieren auf der nationalen E-Government-Strategie der Schweiz (Schwerpunkteplan), dem Wirtschaftsförderungsgesetz des Kantons Bern sowie dem politischen Willen, den Kanton Bern im Bereich eGovernment-Anwendungen vorwärts, in führende Position zu bringen. Unsere Mitglieder sind Hochschulen, Fachhochschulen und Industrieunternehmungen aus der ganzen Schweiz.

eGov-Schweiz bearbeitet mit dem Schwerpunktthema „Bürgerdossier“ ein Anliegen der Bevölkerung an den Staat für einen einheitlichen Zugang zu allen elektronischen Behördendaten auf allen föderalistischen Ebenen der Schweiz. In diesem Zusammenhang beauftragte der Verein die Studie „Zukunftsstandort digitale Schweiz - Voraussetzungen und Potenziale des elektronischen Bürgerdossiers für Schweizer Bürger/innen und Einwohner/innen“[i]. Im Rahmen dieser Studie wurde unter den Schlussfolgerungen mit dem Schritt 2: *„Elektronische Identität sicherstellen“. Jede/r Bürger/in und jede/r Einwohner/in muss über eine elektronische Identität verfügen, mit der er oder sie sich am eBürgerdossier anmelden kann. Die elektronische Identität muss so gestaltet sein, dass sie die ein-*

Verein eGov-Schweiz
c/o mundi consulting AG
Marktgasse 55, Postfach
3001 Bern

Tel +41 (0)31 326 76 76
Fax +41 (0)31 326 76 77

info@egov-schweiz.ch
http://www.egov-schweiz.ch

deutige Identifikation in der Schweiz sicherstellt und für die elektronische Signatur genutzt werden kann…." die Forderung nach einer E-ID bereits vor längerer Zeit publiziert.

Der Verein eGov-Schweiz begrüsst grundsätzlich die Einführung des E-ID-Gesetzes. Es ist uns wichtig, dass in einem ersten Schritt eine elektronische Identität – in relativ naher Zukunft - geschaffen wird.

Grundsätzliches zum Entwurf:
Der vorliegende Gesetzesentwurf legt eine Basis, welche es kontinuierlich auszubauen gilt. Nachfolgend zeigen wir die aus unserer Sicht die kritischen Herausforderungen, welche im Gesetz berücksichtigt werden sollten.

E-ID für juristische Personen bzw. UID-Einheiten:
Sowohl im privaten als auch im geschäftlichen Bereich finden viele elektronische Interaktionen zwischen Personen, Behörden, Organisationen und / oder Firmen statt. Ein Mensch – eine natürliche Person – bekleidet oftmals innerhalb einer juristischen Einheit eine Funktion, welche ihn berechtigt Interaktionen umzusetzen.
Im UID-Register sind alle in der Schweiz aktiven Firmen und Organisationen bereits registriert, ergänzend dazu gibt das Handelsregister Auskunft über die Funktionen bzw. Zeichnungsberechtigungen innerhalb der Organisationen.
Diese Grundlagen sollten eingesetzt werden, um die E-ID ebenfalls für juristische Personen auf der selben gesetzlichen Basis umzusetzen.
Diese Interaktionen zwischen Behörden und natürlichen Personen (G2C), Behörden und Behörden (G2G), juristischen Personen und Behörden (B2G), juristischen Personen und juristischen Personen (B2B) sowie juristischen Personen und natürlichen Personen (B2C) stellen die selben Anforderungen an eine E-ID wie die Interaktionen „nur" zwischen den natürlichen Personen.
Wichtig ist, dass die Integration der juristischen Personen ein sehr grosses Potential an Benutzern und Applikationen generiert. Wenn „nur" das Mengengerüst der natürlichen Personen der Schweiz zur Verfügung steht, wird die Anzahl eingesetzter E-ID nicht die kritische Masse erreichen. Da Dritte, private Organisationen die E-ID betreiben werden, steht die Geschäftsorientierung, der Value Add für die Firmen im Vordergrund und es besteht die Gefahr, dass die Anbieter das Angebot relativ schnell vom Markt entfernen werden. Die Gefahr einer „zweiten SuisseID" (gutes Konzept, keine Verbreitung und hohe Kosten) zu erleben, ist somit erheblich.

Einheitlicher Identifikator für eGovernment:
Der Bundesrat hat an seiner Sitzung vom 1. Februar 2017 seine Absicht bestätigt, die systematische Verwendung der AHV-Nummer durch die Behörden von Bund, Kantonen und Gemeinden künftig zu erleichtern und dies in einer Medienmitteilung kommuniziert.
Wie in den Schlussfolgerungen der Studie „Digitale Zukunft Schweiz" aufgezeigt wird, benötigt ein funktionierendes eGovernment auch einen einheitlichen Identifikator für alle betroffenen Natürlichen und Juristischen Personen sowie den betroffenen Behördeneinheiten.

Verein eGov-Schweiz
c/o mundi consulting AG
Marktgasse 55, Postfach
3001 Bern

Tel +41 (0)31 326 76 76
Fax +41 (0)31 326 76 77

info@egov-schweiz.ch
http://www.egov-schweiz.ch

Gemäss dem Erläuternden Bericht zum Vorentwurf, Kapitel 1.2.6 Abschnitt „Verhältnis des Personenidentifikators AHVN13 zur E-ID Registrierungsnummer“ kann die AHVN13 gemäss heutiger Praxis nur in Teilbereichen eingesetzt werden. Dies nur sofern die formalgesetzlichen Grundlagen bestehen.
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.

Der staatliche elektronische Identitätsnachweis ist eine hoheitliche Aufgabe
Die digitale Welt verlangt für verschiedenste Dienstleistungen unsere Identifikation als Nutzer. Teilweise genügen dazu wenige Angaben zur Person, eine gültige Email-Adresse oder bloss eine Kreditkartennummer. Manchmal sind aber Informationen nötig, die von einer staatlichen Stelle beglaubigt sein müssen. Beispiele dafür sind das elektronische Patientendossier, eVoting oder die Bestellung eines Strafregisterauszuges.
In der nicht-digitalen Welt hat der Staat hoheitliche Institutionen und Verfahren eingerichtet. Die Glaubwürdigkeit der Schweizer Ausweispapiere, insbesondere des Schweizer Passes, ist legendär und Basis für zahllose Geschäftstransaktionen. Wir vertrauen dem Schweizer Pass, weil er hoheitlich und nicht von einer privaten Unternehmung oder Organisation ausgestellt wird.
Glaubwürdigkeit und Vertrauen sind auch in der digitalen Welt elementar für den Aufbau erfolgreicher Geschäftsbeziehungen. Wir wissen, dass dieses Vertrauen bei digitalen Dienstleistungen leider nicht immer gerechtfertigt ist. Besonders kritisch wird es dann, wenn der staatliche Nachweis unserer elektronischen Identität verlangt wird. Hier kann für uns selber, aber auch für den Dienstleister, nur die höchste Vertrauensstufe ausreichend sein. Der staatliche Nachweis der elektronischen Identität muss daher eine hoheitliche Aufgabe bleiben, welche der Staat selber wahrnimmt oder an einen einzelnen Dienstleister delegiert.
Der vorliegende Entwurf für ein Bundesgesetz über anerkannte elektronische Identifikationsmittel (E- ID-Gesetz) schlägt vor, die staatliche elektronische Identifikation an Unternehmen und Organisationen abzugeben, welche dafür zertifiziert werden. Der Verein eGov-Schweiz ist überzeugt, dass dieser Weg nicht erfolgreich sein wird. Die Unternehmen und Organisationen, welche sich als Ausgabestelle für staatliche elektronische Ausweise zertifizieren lassen, mögen noch so glaubwürdig sein – die Nutzer werden ihnen nie dasselbe Vertrauen schenken wie einer staatlichen oder *einer* privaten Stelle, welche diese Aufgabe hoheitlich wahrnimmt. Dieses uneingeschränkte Vertrauen ist aber die Basis für eine erfolgreichen elektronischen Schweizer Pass und damit Grundlage für den Erfolg der digitalen Wirtschaft und Verwaltung in der Schweiz.

Harmonisierung und Internationale Interoperabilität
Aktuell bestehen für verschiedene Trust Service Provider (TSP) unterschiedliche Anerkennungssysteme (z.B. für qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, E-Health, E-Voting usw.), was insgesamt als sehr ineffizient erscheint und zu Widersprüchen führen kann. Eine Harmonisierung der Anerkennungssysteme und der entspre-

Verein eGov-Schweiz
c/o mundi consulting AG
Marktgasse 55, Postfach
3001 Bern

Tel +41 (0)31 326 76 76
Fax +41 (0)31 326 76 77

info@egov-schweiz.ch
http://www.egov-schweiz.ch

chenden Anerkennungsvoraussetzungen über alle TSP-Angebote hinweg tut Not. Dabei ist darauf zu achten, dass einer internationalen gegenseitigen Anerkennung (z.B. eIDAS) nichts im Wege steht.
Beim Einsatz der E-ID im Behördenumfeld setzt dies die flächendeckende Harmonisierung der betreffenden Gesetze voraus. Der Bürger erwartet universelle Einsatzmöglichkeiten insbesondere für E-Government, E-Health und E-Voting. Das E-ID Gesetz sollte eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz. Als minimale Anforderung sollte die E-ID für die folgenden Gesetze als Referenz für elektronische Identitäten und deren Sicherheitsniveaus dienen: ePDG, ZertES, FMG, DSG, div. Gesetze für die Finanz- und Versicherungsbranche, insbesondere. GwG (inkl. FINMA-GwV und RS Video) oder Konsumkreditgesetz, Verordnung des EJPD über die Anerkennung von Plattformen für die sichere Zustellung im Rahmen von rechtlichen Verfahren, Verordnung über das Vote Electronique (Veles).
Im vorliegenden Entwurf ist die internationale Interoperabilität und gegenseitige staatliche Anerkennung kein Thema. Diese Lücke sollte geschlossen werden. Die Regelung in Art. 20 ZertES kann als Vorbild dienen.

Freundliche Grüsse
eGov-Schweiz

Renato Gunc
Präsident

Christoph Beer
Geschäftsführer

[i] Studie „Zukunftsstandort digitale Schweiz“,
Herausgeber: Verein eGov Schweiz,
Konzept und wissenschaftliche Leitung: Prof. Dr. Matthias Finger
Autoren:
Prof. Dr. Matthias Finger, Prof. Dr. Annett Laube-Rosenpflanzer, Prof. Dr. Edy Portmann, Dr. Christian Jaag, Dr. Pascal Sieber, Dr. Denis Morel, Urs Stalder, Peter Nobs, Renato Gunc, Alfred Bertschinger und Georg Ständike
ISBN-Nummer: 978-3-906167-10-7

Verein eGov-Schweiz
c/o mundi consulting AG
Marktgasse 55, Postfach
3001 Bern

Tel +41 (0)31 326 76 76
Fax +41 (0)31 326 76 77

info@egov-schweiz.ch
http://www.egov-schweiz.ch

FMH

Frau
Simonetta Sommaruga
Bundesrätin, Vorsteherin EJPD
3003 Bern
copiur@bj.admin.ch
urspaul.holenstein@bj.admin.ch
sandra.eberle@bj.admin.ch

Bern, 18. Mai 2017

Stellungnahme der FMH zum Vorentwurf E-ID-Gesetz

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Der FMH Zentralvorstand dankt für den Einbezug ins Vernehmlassungsverfahren. Nach Anhörung aller in der Ärztekammer vertretenen Organisationen nimmt er wie folgt Stellung.

Allgemeine Bemerkungen

Die FMH begrüsst den Grundsatz eines E-ID Gesetzes.

In Bezug auf die eHealth-Anwendungen sind für einen erfolgreichen Einsatz von E-Identitäten gemäss dem künftigen E-ID Gesetz folgende Voraussetzungen zentral:

- Die E-Identität muss für Patienten mit der Patientenidentifikationsnummer gemäss EPDG verknüpft werden können.
- Viele Grenzgänger lassen sich in der Schweiz behandeln. Viele andere Patienten reisen aus Drittstaaten ein, um sich in der Schweiz behandeln zu lassen. Nicht alle in der Schweiz tätigen Gesundheitsfachpersonen verfügen über einen Schweizer Pass oder eine Aufenthaltsbewilligung; insbesondere können auch 90-Tage Dienstleister im Schweizer Gesundheitswesen tätig sein. Sowohl für Patienten wie für Gesundheitsfachpersonen muss deshalb eine für eHealth Anwendungen akzeptierte E-Identität auch für Personen geschaffen werden können, die weder Schweizer sind noch eine Aufenthaltsbewilligung haben.
- Für unterschiedliche Behandlungen sind im Gesundheitswesen unterschiedliche Sicherheitsniveaus der Patientenidentifikation und im eHealth-Bereich unterschiedliche Sicherheitsniveaus der Authentifizierung angemessen. One size doesn't fit all. Der Patient soll das für seine Behandlung angemessene Authentifizierungsniveau festlegen können (hohe Anforderungen an die Authentifizierung könnten zum Beispiel die grenzüberüberschreitende Zusammenarbeit von Gesundheitsfachpersonen verunmöglichen).

- Eine Regelungslücke besteht im Gesetzesentwurf bezüglich der Frage, wie lange die Nachvollziehbarkeit des Ausstellungsprozesses und des Widerrufs- oder Sperrungsprozess gewährleistet sein muss.

Vorbemerkung zur Unterscheidung zwischen Identifizierung und Authentifizierung

Gesetzesentwurf und Bericht unterscheiden nicht konsequent zwischen Identifizierung und Authentifizierung. Oft wird im Bericht „Identifizierung" geschrieben, wo „Authentifizierung" stehen müsste.[1] „Während Sie bei der Authentifizierung Ihre Daten an eine zweite Person weitergeben können, ist es bei einem Identifikationsverfahren nicht möglich Berechtigungen weiter zugeben, da die Identifizierungsdaten streng an Ihre Person gebunden sind."[2]

Das *Identifizieren* beruht auf der physischen Prüfung anhand biometrischer Angaben wie Passfoto, Unterschrift. Merkmale oder Attribute (genetischer Abdruck, Iris Scan), anhand welcher eine Identifikation vorgenommen wird, sind (bisher) nicht übertragbar.

Das *Authentifizieren* beruht auf dem Überzeugungsprozess, dass die Person A am fernen Ende des Datennetzes die vertraulich zu haltenden Informationen wie z:B. den privaten Schlüssel kennt, welcher zum öffentlichen Schlüssel im Zertifikat passt. Die Mittel zum Authentisieren lassen sich übertragen. Person A kann beispielsweise ihre sichere Signaturerstellungseinheit auf eine andere Person C übertragen, ohne dass Person B davon Kenntnis erhält. Person B wird meinen, dass sich Person A, wie im Zertifikat angegeben, angemeldet hat und nicht Person C.

Um beim Beispiel des elektronischen Zertifikats zu bleiben: Person B muss sich, um nach der Authentifizierung Dispositionen vorzunehmen, auf Folgendes verlassen können:

- Die Angaben im Zertifikat stimmen. D.h. der Aussteller des Zertifikats hat die Identifizierung und das Erfassen der Personenattribute sorgfältig vorgenommen;
- Person A ist sorgsam mit ihrer Signaturerstellungseinheit umgegangen, d.h. sie hat ihren privaten Schlüssel nicht einem Dritten zugänglich gemacht oder ihr übertragen;
- das Verfahren bei der Zuordnung vom öffentlichen Schlüssel im Zertifikat zum zugehörigen privaten (Authentisierungsverfahren) ist sicher.

Auch nach dem Authentifizieren bleibt immer eine Restunsicherheit, ob wirklich diejenige Person, deren Angaben im Zertifikat enthalten sind, sich angemeldet oder ein Dokument signiert hat.
– vergleichbar zur Ungewissheit, ob der registrierte Halter eines Fahrzeugs am Tag X auch der wirkliche Fahrer war. Die Botschaft Revision ZertES führte aus: Damit der Empfänger der „qualifizierten elektronischen „Signatur trotzdem ein hohes Vertrauen entgegen bringt, haften ihm sowohl die Zertifikatsanbieterin gemäss ZertES Artikel 17 (neu, bisher 16) als auch der Zertifikatsinhaber gemäss Artikel 59a OR für eine gewisse Sorgfalt bei der Wahrnehmung ihrer jeweiligen Pflichten."[3].

---

[1] Siehe u.a.
2.1.1. "Verschiedene Bundesstellen werden voraussichtlich von der E-ID guten Gebrauch machen können. Die E-ID wird dort angewendet werden, wo natürliche Personen im direkten Kontakt mit der Bundesverwaltung stehen und sich bei staatlichen Stellen sicher *identifizieren* sollen. Mit der *E-ID* steht verschiedensten Informationssystemen eine adäquate Lösung für die *sichere Identifizierung* und Authentifizierung der Personen zur Verfügung. Beispiele hierfür sind die Online-Bestellung von Auszügen aus dem Straf- oder Betreibungsregister oder die Online-Eingabe von Daten in land- und veterinärwirtschaftliche Informationssysteme."
2.3. Breit verfügbare anerkannte *elektronische Identifizierungsmittel* bilden einen wichtigen Eckstein in einem umfassenderen E-ID-Ökosystem, das Sicherheit und Vertrauen im elektronischen Geschäftsverkehr herstellen kann. Dadurch können anspruchsvolle Geschäfte mit dem Staat wie auch unter Privaten elektronisch und damit effizienter abgewickelt werden. Zudem eröffnen sich bedeutende neue Geschäftsfelder.
[2] http://www.defense.at/sicherheitsfragen/i-l/identifikation.html
[3] BBL 2014 S. 1015.

Deshalb sind auch im E-ID-Gesetz Haftungsfragen sowohl der Anbieterin der E-ID wie auch des Anwenders zentral für die Vertrauenswürdigkeit des Systems.

Zu den einzelnen Artikeln

Art. 1 Gegenstand und Zweck
[1] Dieses Gesetz regelt:
[…]

[2] Es hat zum Zweck:
a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
b. […]

Kommentar:

Die Bedürfnisse der sicheren und effizienten Patientenbehandlung sind nicht identisch mit denjenigen des sicheren elektronischen *Geschäfts*verkehrs. Siehe dazu weiter unten.

Art. 2 Begriffe
In diesem Gesetz bedeuten:
a. *elektronische Identifizierungseinheit:* eine elektronische Einheit, die zur Identifizierung und Authentifizierung einer natürlichen Person verwendet wird;

b. anerkannte elektronische Identifizierungseinheit (E-ID): eine elektroni-sche Identifizierungseinheit, die von einem IdP nach den Vorgaben dieses Gesetzes ausgestellt wird;

[...]

Kommentar:

Ad lit a „elektronische Einheit, die zur Identifizierung und Authentifizierung einer *natürlichen* Person verwendet wird": Die EU-Richtlinie erwähnt auch Ausweise für Serverbetreiber, oder für Website-Authentifizierungen (Art. 45 Abschnitt 8 EU-Richtlinie). Die für die Schweiz im VE E-ID-Gesetz vorgeschlagene Beschränkung überzeugt nicht. So muss zum Beispiel der Patient wissen können, ob er mit dem richtigen Patientendossier verbunden ist. Die Authentizität des Servicebetreibers sicherzustellen ist mindestens so wichtig wie die Authentifizierung der Gesundheitsfachperson, die auf das EPD zugreifen können soll.

Ad lit. b: Was ist die anerkannte elektronische Identifizierungseinheit E-ID: Ist sie eine Urkunde? ein Zertifikat? Etwas Drittes ? Diese Definition ist relevant für die Festlegung der Rechte und Pflichten des Inhabers wie auch im Zusammenhang mit dem Straftatbestand der Urkundenfälschung.

Art. 3 Persönliche Voraussetzungen
[1] IdP können folgenden Personen eine E-ID ausstellen:
a. Schweizerinnen und Schweizer, die zum Zeitpunkt der Ausstellung über einen gültigen Schweizer Ausweis gemäss Bundesgesetz vom 22. Juni 20013 über die Ausweise für Schweizer Staatsangehörige verfügen;

b. Ausländerinnen und Ausländer die zum Zeitpunkt der Ausstellung über einen gültigen Ausländerausweis gemäss Bundesgesetz vom 16. Dezem-ber 20054 über die Ausländerinnen und Ausländer verfügen.

Kommentar:

Zu Abs. 1: das „können … ausstellen" ist zu anzupassen. Der Bürger muss ein Recht haben, dass ihm eine E-ID ausgestellt wird, wenn er die Voraussetzungen erfüllt. Der Texte sollte somit lauten:

> **Art. 3** Persönliche Voraussetzungen
> [1] IdP ~~können~~ *stellen* folgenden Personen eine E-ID aus ~~stellen~~:

Das Gesundheitswesen fragt nicht nach dem Schweizer Pass. Weder alle in der Schweiz behandelten Patienten noch alle in der Schweiz tätigen Gesundheitsfachpersonen sind Schweizer oder Ausländer mit einem gültigen Aufenthaltsausweis. Auch der in Interlaken verunfallte chinesische Tourist muss als Patient ein EPD-Dossier eröffnen können, und der für ein Tumorboard in Lausanne konsiliarisch tätige Onkologe aus Quebec muss das EPD des Lausanner Patienten befüllen können.

Die vorgesehene Begrenzung des E-ID-Gesetzes auf Schweizer Bürger und Ausländer mit einem gültigen Aufenthaltsausweis erlaubt nicht, die Bedürfnisse von eHealth-Anwendungen abdecken zu können. Die Folge wäre, dass E-Identitäten für eHealth *neben* der E-Identität gemäss E-ID-Gesetz geschaffen werden müssten.

> **Art. 4** Anerkennung von IdP
> [1] IdP, die E-ID ausstellen wollen, brauchen eine Anerkennung der Anerkennungs-stelle (Art. 21).
> [2] IdP werden anerkannt, wenn sie:
> a. ihren Sitz in der Schweiz haben;
> b. über eine UID-Nummer gemäss Bundesgesetz vom 18. Juni 20105 über die Unternehmens-Identifikationsnummer (UIDG) verfügen;
> c. nachweisen, dass die für die E-ID-Systeme verantwortlichen Personen kein Risiko für die Sicherheit darstellen;
> d. Personen mit den erforderlichen Fachkenntnissen, Erfahrungen und Quali-fikationen beschäftigen;
> e. Gewähr bieten, dass die von ihnen betriebenen E-ID-Systeme die für das jeweilige Sicherheitsniveau vorgesehenen Sicherheitsanforderungen erfül-len;
> f. die E-ID-System-Daten in der Schweiz nach schweizerischem Recht hal-ten und bearbeiten;
> g. eine ausreichende Versicherung zur Deckung der Haftpflicht nach Artikel 24 oder gleichwertige finanzielle Sicherheiten nachweisen;
> h. die Einhaltung des anwendbaren Rechts, namentlich dieses Gesetzes und seiner Ausführungsbestimmungen, gewährleisten.

Kommentar:

Art. 4 ist zu ergänzen. Die internationalen Erfahrungen[4] zeigen, dass die Server, auf denen E-ID-Daten gespeichert werden, zudem in europäischen Händen sein müssen und nicht einer US-Firma gehören dürfen, da letztere offenbar verpflichtet werden können, die Daten in die USA zu transferieren, wo sie keinen unserem Land vergleichbaren Datenschutz geniessen.

[4] Vgl. etwa DeepMind-Royal Free deal is "cautionary tale" for healthcare in the algorithmic age ;Julia Powles, 16 Mar 2017, University of Cambridge – Research – News: A study of a deal which has allowed Google DeepMind access to millions of healthcare records argues that more needs to be done to regulate such agreements between public sector bodies and private technology firms.

Art. 5 Sicherheitsniveaus
[1] IdP können E-ID-Systeme mit unterschiedlichen, aufeinander aufbauenden Sicherheitsniveaus betreiben und entsprechend *E-ID ausstellen, die folgendes Mass an Vertrauen vermitteln*:
a. *niedrig*: Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;

b. *substanziell*: substanzielle Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;

c. *hoch*: Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung.

[2] Die verschiedenen Sicherheitsniveaus unterscheiden sich durch:
a. den *Ausstellungsprozess*, insbesondere in Bezug auf die Identifizierung und Authentifizierung der Inhaberin oder des Inhabers bei der Registrierung;

b. den Betrieb, insbesondere die Aktualisierung der Personenidentifizierungsdaten;

c. die *Anwendung*, insbesondere in Bezug auf die Identifizierung und Authentifizierung; und

d. weitere technische oder organisatorische Sicherheitsmassnahmen nach dem jeweiligen Stand der Technik.

[3] Eine für ein bestimmtes Sicherheitsniveau ausgestellte E-ID kann auch auf einem tieferen Sicherheitsniveau eingesetzt werden.
[4] Der Bundesrat regelt die verschiedenen Sicherheitsniveaus, insbesondere die Mindestanforderungen an die Identifizierung und Authentifizierung.

Kommentar:

Für die *Ausstellung* muss das Sicherheitsniveau immer hoch sein. Es geht nicht an, eine e-Identität für eine nicht sicher identifizierte Person auszustellen. Die Schweiz stellt in der analogen Welt auch keinen Pass und keine ID für jemanden aus, dessen Identität sie nicht mit hoher Sicherheit geprüft hat. Art. 5 Abs. 1 ist anzupassen.

Nur für die *Anwendung* treffend die Hinweise aus dem Bericht zu: (*1.2.5 Sicherheitsniveaus*)**: „**Nicht alle Geschäftsprozesse erfordern dasselbe Sicherheitsniveau. Zu hohe Sicherheitsanforderungen können in der Praxis als störend empfunden werden und Umgehungshandlungen begünstigen sowie höhere Kosten verursachen. […]“ „ Welches Sicherheitsniveau für welche Art der Anwendung in Frage kommt, wird in den jeweiligen Spezialerlassen festgehalten bzw. durch die privaten Betreiberinnen von E-ID-verwendenden Diensten definiert. So kann für E-Education ein anderes Sicherheitsniveau gewählt werden, als es für Vote électronique vorgeschrieben oder für E-Health-Anwendungen notwendig ist.“

Wie in den allgemeinen Bemerkungen ausgeführt, sind für unterschiedliche Behandlungen im Gesundheitswesen unterschiedliche Sicherheitsniveaus der Patientenidentifikation angemessen. Für Infusionen von Krebsmedikamenten ist die sichere Patientenidentifikation entscheidend, für die Grippekonsultation ist sie es nicht.

One size doesn‘t fit all glt auch für E-Health-Anwendungen: Der Patient soll die Möglichkeit haben, nach seinem persönlichen Bedürfnis ein unterschiedliches Sicherheitsniveau bezüglich Authentifikation vorzugeben – genauso, wie wir dies heute im elektronischen Kontakt zwischen Patienten und Gesundheitsinstitution erleben. Für ein VIP in psychiatrischer Behandlung wird die Geheimhaltung zentral sein – für einen chronischkranken Grenzgänger kann die möglichst niederschwellige Vernetzung von Gesundheitsfachpersonen in der Schweiz und im Ausland wichtiger sein; dafür wird er in Kauf nehmen, dass weniger strenge Authentifizierungsregeln gelten.

Dass der Bundesrat gemäss Abs. 4 für alle eHealth-Anwendungen ein Sicherheitsniveau festlegen soll, ist vor diesem Hintergrund nicht zielführend.

> **Art. 6 Ausstellungsprozess**
> 1 Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP.
>
> 2 Der IdP überprüft die persönlichen Voraussetzungen.
>
> 3 Er beantragt bei der Schweizerischen Stelle für elektronische Identität (Identitäts-stelle) mit dem Einverständnis der antragstellenden Person die Übermittlung der Personenidentifizierungsdaten nach Artikel 7 Absätze 1 und 2.
>
> 4 Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person.
>
> 5 Die Identitätsstelle protokolliert die Datenübermittlungen.

Kommentar:

Zu klären ist die Schnittstelle zum EPDG bezüglich der Erneuerung der Identitätsprüfung, vgl. Art. 25 EPDV.[5]

> **Art.** 8 Aktualisierung der Personenidentifizierungsdaten
> [1] Der IdP aktualisiert die von ihm geführten Personenidentifizierungsdaten durch eine automatisierte Abfrage anhand der E-ID-Registrierungsnummer bei der Identitätsstelle mindestens wie folgt:
> a. für E-ID des Sicherheitsniveaus niedrig: jährlich;
>
> b. für E-ID des Sicherheitsniveaus substanziell: quartalsweise;
>
> c. für E-ID des Sicherheitsniveaus hoch: wöchentlich.
> [2] Er ist verantwortlich, dass von ihm ausgestellte E-ID umgehend gesperrt oder widerrufen werden, wenn die E-ID-Registrierungsnummer nicht mehr verwendet werden darf. (Anm. Übersetzung: Er sperrt oder widerruft …)

Kommentar:

Der Ausstellungsprozess und die Bestimmung über die Aktualisierung der Personenidentifizierungsdaten wie auch die übrigen Gesetzesartikel regeln die für eHealth Anwendungen zentrale Schnittstelle zu den Stellen nicht, die die Eigenschaft als Gesundheitsfachperson bestätigen und bei Wegfall der Qualifikation widerrufen. Der Begriff berufliche Qualifikation kommt weder im VE-E-IDG noch im Bericht vor.

Das revidierte ZertES vom 18. März 2016 sieht in Art. 7 die Möglichkeit vor, dass Zertifikate als spezifische Attribute *berufliche Qualifikationen* enthalten können.

> 3 Das Zertifikat kann zudem die folgenden Elemente enthalten:
>
> a. *spezifische Attribute der Inhaberin oder des Inhabers des zugehörigen privaten kryptografischen Schlüssels, beispielsweise berufliche Qualifikationen*;

[5] EPDV Art. 25 Erneuerung der Gültigkeitsdauer des Identifikationsmittels
Nach Ablauf der Gültigkeit des Identifikationsmittels von höchstens 10 Jahren (vgl. Art. 22 Bst. d) muss dieses neu beantragt werden. Absatz 2 statuiert, dass abweichend von der Norm ISO/IEC 29115:2013 für die Erneuerung des Identifikationsmittels eine Identitätsprüfung gemäss dem Vertrauensniveau der Stufe 3 durchgeführt werden muss (vgl. Art. 23).

b. bei natürlichen Personen den Hinweis, dass sie zur Vertretung einer bestimmten UID-Einheit berechtigt ist;

c. den Geltungsbereich, für den das Zertifikat bestimmt ist;

d. die Obergrenze der Transaktionen, für die das Zertifikat bestimmt ist.

Begründet wurde dies in der ZertES-Botschaft [6] 2014 wie folgt: „Art. 7 […] Buchstabe a führt die optionalen Attribute auf und bringt zur Veranschaulichung als Beispiel *die in der Praxis öfters verwendete berufliche Qualifikation.“ [kursive Hervorhebung FMH]*

Die Erfahrungen mit unechten Ärzten in der Schweiz[7] zeigen, wie wichtig es ist, im Rahmen von eHealth unverzüglich das Attribut als anerkannte Gesundheitsfachperson entziehen zu können – auch wenn die Person nicht unter falscher Identität auftritt. In den in den letzten Jahren bekannt gewordenen Fällen[8] waren die Personen unter ihrer tatsächlichen Identität aufgetreten, aber ihre beruflichen Qualifikationen waren gefälscht bzw. nicht vorhanden.

Wenn E-Identitätsausweise nach diesem Gesetz im Rahmen von eHealth-Anwendungen eingesetzt werden sollen, ist die Koordination des Ausgabe- und Widerrufprozesses mit der Stelle, die die Qualifikation als Gesundheitsfachperson bestätigt, von zentraler Bedeutung.

5. Abschnitt: Anbieterinnen von Identitätsdienstleistungen (IdP)

Art. 17 Pflichten
1 Der IdP hat folgende Pflichten:
[…]
2 Er sorgt für einen Kundendienst, der es erlaubt, Meldungen über Störungen oder Verlust einer E-ID entgegenzunehmen und zu bearbeiten. Er meldet Fehler in den Personenidentifizierungsdaten der Identitätsstelle.

3 Besteht die Gefahr, dass eine Drittperson Zugang zu einer E-ID haben könnte, oder wird der Verlust oder der Verdacht auf Missbrauch gemeldet, so ist der IdP ver-pflichtet, die E-ID unverzüglich zu sperren.

Kommentar:

Nicht geregelt ist die Frage einer Publikation oder einer Zugänglichmachung des Widerrufs oder der Sperrung an E-ID-Anwender wie z.B. an das Patientendossier.

9. Abschnitt: Haftung

Art. 24
1 Die Haftung der Inhaberin und des Inhabers, der Betreiberin von E-ID-verwendenden Diensten sowie des IdP richtet sich nach dem Obligationenrecht7.
2 Die Haftung der Identitätsstelle und der Anerkennungsstelle richtet sich nach dem Verantwortlichkeitsgesetz vom 14. März 19588.

[6] 14.015 Botschaft zur Totalrevision des Bundesgesetzes über die elektronische Signatur (ZertES) vom 15. Januar 2014, BBl 2014, 1001, S. 1025f:

[7] Thomas Knellwolf, Sechs Jobs und ein Totenschein - Tages-Anzeiger; 14.06.2013 - Sie überlebt, verarztet Verletzte, birgt Tote. So erzählt sie es zumindest. Doch Dichtung und Wahrheit vermischen sich oft bei Lotte Zahm.

www.tagesanzeiger.ch/schweiz/Sechs-Jobs-und-ein-Totenschein/story/21277040

[8] „Lotte Zahm“ war Krankenpflegefachperson aber nicht Ärztin, der Zahntechniker in Biel war nicht Zahnarzt, der falsche Arzt im Tessin hatte keinen Studienabbschluss.

Kommentar:

Die Haftungsregelung durch Verweis auf OR bzw. Verantwortlichkeitsgesetz ist nicht kompatibel mit den unterschiedlichen Sicherheitsniveaus bei der Ausstellung der E-ID gemäss Art. 5 Abs. 1. Zudem ist sie nicht koordiniert mit der Haftung gemäss ZertES. Es müsste wie in Art. 17 Abs. 3 ZertES sichergestellt werden, dass auch im E-ID-Gesetz der Anbieter die Haftung **weder für eigenes Verhalten noch für jenes ihrer Hilfspersonen wegbedingen** kann.

ZertES in der Fassung 2016:

7. Abschnitt: Haftung

Art. 17 Haftung der Anbieterin von Zertifizierungsdiensten
1 Die anerkannte Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber eines gültigen geregelten Zertifikats und Drittpersonen, die sich auf ein solches Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsbestimmungen nicht nachgekommen ist.
2 Sie trägt die Beweislast dafür, den Pflichten aus diesem Gesetz und den Ausführungsbestimmungen nachgekommen zu sein.
3 **Sie kann ihre Haftung aus diesem Gesetz weder für eigenes Verhalten noch für jenes ihrer Hilfspersonen wegbedingen**. Sie haftet jedoch nicht für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung (Art. 7 Abs. 3 Bst. c und d) ergeben

Art. 18 Haftung der Anerkennungsstelle
Die Anerkennungsstelle haftet der Inhaberin oder dem Inhaber eines gültigen geregelten Zertifikats und Drittpersonen, die sich auf ein solches Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anerkennungsstelle ihren Pflichten aus diesem Gesetz und den Ausführungsbestimmungen nicht nachgekommen ist. Artikel 17 Absätze 2 und 3 gilt sinngemäss.

Die EU kennt ebenfalls unterschiedliche Sicherheitsniveaus – aber konsequenterweise eine differenzierte Haftungsregelung:

Artikel 13

Haftung und Beweislast

(1) Unbeschadet des Absatzes 2 haften Vertrauensdiensteanbieter für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind.

Die Beweislast für den Nachweis des Vorsatzes oder der Fahrlässigkeit seitens eines nichtqualifizierten Vertrauensdiensteanbieters liegt bei der natürlichen oder juristischen Person, die den in Unterabsatz 1 genannten Schaden geltend macht.

Bei einem qualifizierten Vertrauensdiensteanbieter wird von Vorsatz oder Fahrlässigkeit ausgegangen, es sei denn, der qualifizierte Vertrauensdiensteanbieter weist nach, dass der in Unterabsatz 1 genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.

(2) Unterrichten Vertrauensdiensteanbieter ihre Kunden im Voraus hinreichend über Beschränkungen der Verwendung der von ihnen erbrachten Dienste und sind diese Beschränkungen für dritte Beteiligte ersichtlich, so haften die Vertrauensdiensteanbieter nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

(3) Die Absätze 1 und 2 werden im Einklang mit den nationalen Vorschriften über die Haftung angewendet. ▼B
2014R0910 — DE — 17.09.2014 — 000.003 — 26

Zur Änderung anderer Gesetze:

4. Bundesgesetz vom 18. März 2016[16] über die elektronische Signatur

Art. 9 Abs. 1bis

[1bis] Wird der Identitätsnachweis durch eine E-ID gemäss E-ID-Gesetz vom ….[17] erbracht, entfällt die persönliche Vorsprache.

Kommentar:

Diese Regelung ist nicht kompatibel mit den verschiedenen Sicherheitsniveaus gemäss Art. 5 Abs. 1 des vorliegenden Gesetzesentwurfs.

Freundliche Grüsse

Dr. med. Jürg Schlup
Präsident FMH

Dr. med. Yvonne Gilli
Mitglied Zentralvorstand,
Departementsverantwortliche Digitalisierung und eHealth

IG eHealth, Amthausgasse 18, 3011 Bern

Frau
Bundesrätin Simonetta Sommaruga
Vorsteherin des EJPD
3003 Bern
copiur@bj.admin.ch, urspaul.holenstein@bj.admin.ch, sandra.eberle@bj.admin.ch

Bern, 29. Mai 2017

Stellungnahme der IG eHealth zum Vorentwurf des E-ID-Gesetzes

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren

Die IG eHealth bezieht gerne als Vertreterin der Healthcare-Industrie Stellung zum Vorentwurf des E-ID-Gesetzes. Eine gesetzliche Regelung für eine flächendeckende elektronische Identität fehlt heute. Eine E-ID wird viele Prozesse in der Schweiz vereinfachen, durchgängig machen und Effizienzgewinne ermöglichen. Die Öffentlichkeit erwartet vielfältige Einsatzmöglichkeiten im eHealth, eGovernment, eDemocracy und in weiteren Anwendungen. So muss das E-ID-Gesetz z.B. Anwendung finden im ePatientendossiergesetz EPDG, ZertES, VEIeS, FMG und Finanzmarktregulierungen. Die IG eHealth setzt sich dafür ein, dass die E-ID in Prozessen des Gesundheitswesens breite Verwendung finden kann. Wir legen den Fokus unserer Eingabe deshalb auf das Gesundheitswesen.

Einleitung

Die IG eHealth begrüsst die Schaffung eines Spezialgesetzes und unterstützt den im Gesetz genannten Zweck (sicherer elektronischer Geschäftsverkehr zwischen Privaten und Behörden, Standardisierung und Interoperabilität E-ID).

Konkrete Anliegen

Aus unserer Sicht ist es zentral, dass die E-ID für eHealth-Anwendungen (ePatientendossier, Register, u.a.) eingesetzt werden kann.

- Es wäre begrüssenswert, wenn das Erstellen einer E-ID auch durch die staatlichen Ausweis-Ausstellungsprozesse gefördert würde. Eine möglichst flächendeckende E-ID wird vor allem Kosten mit öffentlichen Stellen senken.
- Damit die E-ID im Verkehr mit möglichst allen Behörden eingesetzt werden kann, muss im Gesetz eine zentrale Akzeptanznorm definiert werden. Es kann nicht sein, dass in jedem Gesetz andere Bedingungen/Voraussetzungen beschrieben werden und so eine einzige E-ID gar nicht möglich ist. Die E-ID soll in der gesamten Rechtsordnung für alle Behörden und alle öffentlichen e-Aufgaben (auch im Privatrecht geregelte wie das EPDG) zentral das Thema E-Identifikation regeln. Sollte eine zentrale Regelung nicht möglich sein, muss eine Harmonisierung der Gesetze vorgesehen werden.

- Es ist eine bedarfsgerechte Aktualisierung der Personenidentifizierungsdaten vorzusehen. Das vorgesehene Gebührenmodell wirkt kontraproduktiv auf eine bedarfsgerechte Aktualisierung. Aktuelle Personenidentifikationsdaten sind aber ein wichtiges Qualitätsmerkmal einer ID.
- Viele Sektoren benötigen international funktionierende Identifikationsprozesse. Viele Patienten aus dem nahen Ausland sind regelmässig in der Schweiz. Die internationale Interoperabilität ist anzustreben. Die Regelung in Art. 20 ZertES kann als Vorbild dienen.
- In der Gesamtrechtsordnung ist ein konsistenter Umgang mit der AHVN13 erwünscht. Das ATSG erlaubt die Verwendung nur sehr restriktiv. Insbesondere das EPDG hat die Verwendung von Versichertennummer verboten, aber eine E-ID ist definiert. Daher gilt es hier darauf zu achten, dass keine Inkompatibilität entsteht, die dann die Nutzung der E-ID für ein Patientendossier verunmöglichen würde.
- Im Artikel 3 schlagen wir vor, statt der Kann-Formulierung eine Verpflichtung zu statuieren: Die BürgerInnen sollen das Recht erhalten, eine E-ID zu erhalten.
- In der Gesetzgebung bestehen für verschiedene so genannte Trust Service Provider unterschiedliche Anerkennungssysteme (wie qualifizierte Zertifikate, IdP, E-Health). Um Ineffizienzen zu verhindern, müssen Anerkennungssysteme und Voraussetzungen harmonisiert werden.

Finanzierung

Erlauben Sie uns eine Schlussbemerkung zur Finanzierung. Bisherige E-ID-Angebote, die mit Kosten für den Anwender verbunden waren, konnten sich nicht durchsetzen. Der Aufbau und der Betrieb einer staatlichen Identitätsstelle kann als Infrastrukturaufgabe interpretiert werden, die ganz oder mehrheitlich vom Bund übernommen werden sollte. Auf eine Gebührenfinanzierung ist zu verzichten. Mit einer staatlich anerkannten E-ID kann ein Vielfaches an Kosten in E-Government-Prozessen eingespart werden. Es ist im Eigeninteresse des Staates, hier ein möglichst flächendeckendes Identifikationsinstrument einzuführen.

Die IG eHealth bedankt sich für die Prüfung und gegebenenfalls die Berücksichtigung unserer Anliegen.

Mit bestem Dank und freundlichen Grüssen

Im Namen des Vorstandes

Urs Stromer
Präsident IG eHealth

Walter Stüdeli
Geschäftsführer IG eHealth

Die IG eHealth

IG eHealth Die Interessengemeinschaft eHealth will die Umsetzung von eHealth in der Schweiz beschleunigen, damit Qualitäts- und Sicherheitslücken in der Behandlung verhindert und administrative Prozesse verbessert werden. Die IG eHealth setzt sich für bessere Rahmenbedingungen von eHealth in der Schweiz ein und leistet fachliche Unterstützung bei der Erarbeitung der gesetzlichen Grundlagen. Die IG ist im steten Dialog mit allen Stakeholdern im Gesundheitswesen. Sie vertritt die Industrie im «Beirat der Umsetzer und User» von eHealthSuisse (ehemals Projektleitungsgremium eHealth Suisse des Bundes und der Kantone), welcher die Strategie eHealth Schweiz umsetzt.
www.ig-ehealth.ch

Inclusion Handicap
Mühlemattstrasse 14a
3007 Bern

info@inclusion-handicap.ch
www.inclusion-handicap.ch

INCLUSION. HANDICAP

Dachverband der Behindertenorganisationen Schweiz

Association faîtière des organisations suisses de personnes handicapées

Mantello svizzero delle organizzazioni di persone con disabilità

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Email an: copiur@bj.admin.ch

Bern, 31. Mai 2017

BUNDESGESETZ ÜBER ANERKANNTE ELEKTRONISCHE IDENTIFIZIERUNGSEINHEITEN (E-ID-GESETZ): VERNEHMLASSUNG

Stellungnahme zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin Sommaruga

Inclusion Handicap ist der Dachverband der Behindertenorganisationen in der Schweiz und vertritt die Interessen von Menschen mit Behinderungen. Die Abteilung Gleichstellung von Inclusion Handicap hat die Aufgabe, die Umsetzung sowie Weiterentwicklung des Behindertengleichstellungsrechts zu fördern und so die autonome Lebensführung von Menschen mit Behinderungen in allen Aspekten des täglichen Lebens zu unterstützen.

Die Bundesverfassung verbietet in Art. 8 Abs. 2 Diskriminierungen wegen einer körperlichen, geistigen oder psychischen Behinderung. Art. 8 Abs. 4 BV verpflichtet den Gesetzgeber, Massnahmen zur Beseitigung der Benachteiligungen von Menschen mit Behinderungen zu ergreifen. Demnach müssen die in Erarbeitung stehenden oder einer Revision unterliegenden Gesetze sowie Verordnungen immer auch unter dem Aspekt der Gleichstellung von Menschen mit Behinderungen überprüft werden. Führen sie zu einer direkten oder indirekten Diskriminierung, sind sie mit Art. 8 Abs. 2 BV nicht vereinbar. Den Auftrag von Art. 8 Abs. 4 BV hat der Bundesgesetzgeber bis jetzt hauptsächlich durch den Erlass des Behindertengleichstellungsgesetzes vom 13. Dezember 2002 (Behindertengleichstellungsgesetz, BehiG; SR 151.3) wahrgenommen, aber auch durch die Verankerung von behindertengleichstellungsrechtlicher Vorschriften in der Spezialgesetzgebung.

Zudem verpflichtet die UNO-Konvention über die Rechte von Menschen mit Behinderungen (UNO-BRK; SR 0.109) die Schweiz seit Mai 2014 zur Berücksichtigung derer Anliegen, insbesondere auch im Gesetzgebungsverfahren (Art. 4 Abs. 1 lit. a+b UNO-BRK).

Bei der Ausarbeitung von Rechtsvorschriften, die Menschen mit Behinderungen betreffen, hat der Staat Behindertenorganisationen aktiv miteinzubeziehen (Art. 4 Abs. 3 BRK).

Relevant im Zusammenhang mit dem Vorentwurf des E-ID-Gesetzes ist insbesondere Art. 9 der UNO-BRK[1] als allgemeine Klausel zur Gewährleistung der Zugänglichkeit. Der hindernisfreie Zugang zu Dienstleistungen gehört zu den wesentlichen Voraussetzungen einer selbstbestimmten Teilhabe am gesellschaftlichen Leben und ist für die Inklusion von zentraler Bedeutung. Nach Art. 9 UNO-BRK[2] müssen auch bei der Entwicklung von Informations- und Kommunikationstechnologien und –systemen, einschliesslich des Internets, die Bedürfnisse von Menschen mit Behinderungen berücksichtigt werden. Die Schweiz ist somit verpflichtet, zur Sicherstellung des Zugangs von Menschen mit Behinderungen zu Dienstleistungen des Internets die nötigen Massnahmen zu ergreifen. Dabei hat sie nach Art. 9 Abs, 2 lit. b UNO-BRK insbesondere auch sicherzustellen, dass private Rechtsträger, die öffentlich-zugängliche Dienste anbieten, alle Aspekte der Zugänglichkeit für Menschen mit Behinderungen berücksichtigen. Im vorliegenden Zusammenhang von Bedeutung ist auch Art. 5 Abs. 2 UNO-BRK, welches ein Verbot der Diskriminierung wegen einer Behinderung beinhaltet. Schliesslich hat sich die Schweiz als Folge von Art. 4 Abs. 1 lit. e UNO-BRK ausdrücklich dazu verpflichtet, alle geeigneten Massnahmen zur Beseitigung der Diskriminierung aufgrund von Behinderung durch private Unternehmen zu ergreifen.

Um Benachteiligungen von Menschen mit Behinderungen zu vermeiden, welche die Dienstleistungen gemäss dem Vorentwurf zum E-ID-Gesetz – die Erstellung und die Bewirtschaftung einer E-ID – in Anspruch nehmen, müssen diese Dienstleistungen demzufolge nach dem *design for all* ausgestaltet sein (Art. 2 Abs. 5 UNO-BRK).

Bis heute sind die Grundlagen des Behindertengleichstellungsrechts auch im Dienstleistungsbereich und insbesondere im Bereich der e-accessibility in der Praxis wenig bekannt. Sogar in der Bundesverwaltung sind sich viele Behörden ihrer Verpflichtungen noch zu wenig bewusst. Eine klare Verankerung und Konkretisierung der behindertengleichstellungsrechtlichen Anforderungen in der jeweils relevanten Spezialgesetzgebung kann dies ändern und zur konsequenten Umsetzung der Rechte von Menschen mit Behinderungen beitragen.

Eine Umsetzung der Verpflichtungen aus der UNO-BRK hat im vorliegenden Vorentwurf zum E-ID-Gesetz offensichtlich nicht stattgefunden. Um sicherzustellen, dass Menschen mit Behinderungen aus den Möglichkeiten gesellschaftlicher Teilhabe, welche durch die Verwendung einer E-ID eröffnet werden, nicht ausgeschlossen werden, schlägt Inclusion

---

[1] Aus der Lehre zur Tragweite von Art. 9 UNO-BRK siehe TRENK-HINTERBERGER, Zugänglichkeit, Art. 9, in: Kreutz Marcus/Lachwitz Klaus/Trenk-Hinterberger Peter (Hrsg.), Die UNO-Behindertenrechtskonvention in der Praxis, Köln 2013, S. 130ff sowie WELTI, Zugänglichkeit, Art. 9, in: Welke Antje (Hrsg.), UN-Behindertenrechtskonvention mit rechtlichen Erläuterungen, Ettenheim 2012, S. 127ff.

[2] Vgl. insbesondere Art. 9 Abs. 1 lit. b und Abs. 2 lit. a,b,f und g UNO-BRK.

Handicap vor, die Anforderungen an die hindernisfreie Ausgestaltung von E-ID-Systemen im Rahmen verschiedener Bestimmungen des E-ID-Gesetzes zu verankern. Wir beschränken uns dabei auf punktuelle, allgemeine Anregungen und bitten Sie, zwecks Überprüfung der Vereinbarkeit des Gesetzesentwurfs mit der UNO-BRK sowie der Formulierung von konkreten Gesetzesbestimmungen mit dem Eidgenössischen Büro für die Gleichstellung von Menschen mit Behinderungen (EBGB) Kontakt aufzunehmen.

Art. 3 Abs. 1: Persönliche Voraussetzungen

Gemäss dem E-ID-Gesetz besteht für die IdP keine Pflicht, ein Vertragsverhältnis mit den Antragstellenden einzugehen, selbst wenn jemand die in Art. 3 aufgeführten Voraussetzungen für eine E-ID erfüllt. Es darf jedoch einer Person mit Behinderung nicht das Erstellen einer E-ID und das Eingehen des damit verbundenen Vertrags verweigert werden, 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, als zweites Beispiel, mit der Begründung, dass der IdP nicht über ein barrierefrei zugängliches Gebäude verfügt und somit die Person mit Behinderung nicht zur persönlichen Vorsprache empfangen werden kann. Zudem hat der Akt der Antragsstellung bei allen Sicherheitsstufen für alle Personen barrierefrei möglich zu sein[3].

Art. 4 Abs. 2: Anerkennung von IdP

Gemäss Art. 4 Abs. 1 brauchen IdP, die eine E-ID ausstellen wollen, eine Anerkennung der Anerkennungsstelle. In Abs. 2 werden sodann die Voraussetzungen aufgeführt, welche notwendig sind, damit ein IdP anerkannt wird. An dieser Stelle ist nach der Auffassung von Inclusion Handicap 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.

Dazu müssen von den IdP die nötigen technischen Voraussetzungen geschaffen werden, sodass die Online-Registrierung der Sicherheitsstufe «niedrig» barrierefrei für alle Benutzenden zugänglich ist. Bei den Sicherheitsstufen «substanziell» und «hoch» müssen die technischen Voraussetzungen geschaffen werden, damit die Videoidentifikation für alle Benutzenden zugänglich ist und/oder, dass eine persönliche Vorsprache barrierefrei (zu denken ist insbesondere an die Beseitigung von Barrieren baulicher Art oder von Barrieren im Bereich der Kommunikation) möglich ist.

[3] Nähere Erläuterungen siehe sogleich unter «Art. 4 Abs. 2: Anerkennung von IdP».

Art. 12 Abs. 3

Art. 12 Abs. 3 benennt die alternativen Voraussetzungen, unter welchen die Anerkennungsstelle den IdP die Anerkennung zur Ausstellung und Bewirtschaftung von E-ID entziehen kann. Unseres Erachtens ist die Bestimmung dadurch zu ergänzen, dass auch ein Verstoss gegen Art. 8 Abs. 2 BV sowie der UNO-BRK zum Entzug der Anerkennung führen kann.

Art. 17 Abs. 1 lit. f: Pflichten der IdP

Lit. f verpflichtet die IdP von der Inhaberin oder dem Inhaber der E-ID das ausdrückliche Einverständnis zur Erstübermittlung von Personenidentifizierungsdaten an Betreiberinnen von E-ID-verwendenden Diensten einzuholen.

Im erläuternden Bericht zum Vorentwurf wird als Praxisbeispiel aufgeführt, dass der/die InhaberIn der E-ID dazu vom IdP eine Meldung mit der Frage auf das Smartphone erhält, ob er/sie seine/ihre Daten dem E-ID-verwendenden Dienst übermitteln will. Die Bestätigung erfolgt wiederum direkt auf das Smartphone der/des E-ID-Inhabers/in. Auch hier muss sichergestellt werden, 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 können.

Art. 17 Abs. 2: Pflichten der IdP

Gemäss Art. 17 Abs. 2 des Vorentwurfs haben die IdP einen Kundendienst einzurichten, der es erlaubt, Meldungen über Störungen oder über den Verlust einer E-ID entgegenzunehmen und zu bearbeiten. Der erläuternde Bericht zum Vorentwurf hält dazu ausdrücklich fest, dass es dem Markt überlassen werden soll, ob eine Hotline eingerichtet wird oder ob die Meldungen per E-Mail oder über anderen Kanäle kommuniziert werden. Auch hier sind die technischen Voraussetzungen zu schaffen, dass Menschen mit Behinderungen den Kundendienst in gleicher Weise benützen können, wie Menschen ohne Behinderungen. Dabei erachten wir es als sinnvoll, mehrere verschiedene barrierefreie Kanäle zur Verfügung zu stellen.

Art. 24 Haftung

Die Haftung für die InhaberInnen einer E-ID richtet sich nach dem Obligationenrecht (OR; SR 220). Gemäss dem erläuternden Bericht ist von Fall zu Fall abzuklären, ob es sich dabei um eine vertragliche oder deliktische Haftung handelt. Wird vertragliche Haftung angenommen, gilt gemäss Art. 97 OR die gesetzliche Vermutung des Verschuldens, sodass der Schuldner, in diesem Fall der/die E-ID-Besitzende den Exkulpationsbeweis erbringen muss. Umso wichtiger wird daher eine barrierefreie Nutzung der E-ID erachtet, da

für allfällige Fehler bei der Benutzung der E-ID, welche einen Schaden anrichten, die betroffenen E-ID-NutzerInnen einstehen müssen. Der Exkulpationsbeweis dürfte – wie generell im Cyberspace/im Internet - nicht einfach sein.

Wir danken Ihnen im Voraus für die Berücksichtigung unserer Vorschläge und stehen Ihnen für Fragen jederzeit sehr gerne zur Verfügung.

Mit freundlichen Grüssen

Julien Neruda	Caroline Hess-Klein, Dr. iur.
Geschäftsführer	Stv. Geschäftsführerin, Leiterin Abteilung Gleichstellung

KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST
CONFÉRENCE DES AUTORITÉS CANTONALES DE SURVEILLANCE DE L'ÉTAT CIVIL
CONFERENZA DELLE AUTORITÀ CANTONALI DI VIGILANZA SULLO STATO CIVILE

Eidgenössisches Justiz- und
Polizeidepartement
Bundesamt für Justiz

Per Mail an:
copiur@bj.admin.ch

Münsingen, 10. Mai 2017

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz); Vernehmlassungsverfahren
Stellungnahme Konferenz der Kantonalen Aufsichtsbehörden im Zivilstandsdienst (KAZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Brief vom 23. Februar 2017 laden Sie in der eingangs erwähnten Angelegenheit zur Vernehmlassung ein. Wir wurden als betroffene Konferenz wiederholt nicht direkt bedient und figurierten nicht unter den Vernehmlassungsadressaten. Wir bitten Sie, uns künftig im Rahmen von Vernehmlassungen in Personenstandsangelegenheiten, Datenbekanntgabe und -bewirtschaftung, Registerfragen und dgl. wiederum direkt anzuschreiben, resp. uns in den entsprechenden Verzeichnissen aufzunehmen.

Gerne nehmen wir zum E-ID-Gesetz nachfolgend Stellung.

Zu Art. 3 Abs. 1 lit. b: Der Vorentwurf sieht vor, dass Ausländerinnen und Ausländern die zum Zeitpunkt der Ausstellung über einen gültigen Ausländerausweis gemäss Bundesgesetz vom 16. Dezember 2005 über die Ausländerinnen und Ausländer verfügen, eine E-ID auszustellen ist. Der erläuternde Bericht differenziert, dass derzeit darauf verzichtet werden soll, Personen mit N-, F- und S-Ausweis eine E-ID auszustellen. Die Begründung im erläuternden Bericht, wonach viele Asylsuchende im Asylverfahren keine Identitätsdokumente einreichen, was eine sichere Identifizierung verunmöglicht, können wir aus Sicht der das Zivilstandswesen vollziehenden Kantone vorbehaltlos bestätigen. Da eine Identifizierung immer ein Zusammenspiel zwischen registrierten Personendaten resp. Personenstandsdokumenten mit der dazugehörenden Person, inkl. deren biometrischen Merkmalen darstellt, ist unseres Erachtens die Eintrittsschwelle für eine E-ID bei Ausländerinnen und Ausländern angemessen hoch zu gestalten. Wir beantragen, den Wortlaut von Art. 3 Abs. 1 lit. b so zu ergänzen, dass die E-ID *für Ausländerinnen und Ausländer die zum Zeitpunkt der Ausstellung über einen gültigen biometrischen Ausländerausweis verfügen* ausgestellt wird. Mindestens müsste für Asylsuchende die E-ID auf Stufe Gesetz verunmöglicht werden, da die Personenangaben in

KAZ-GESCHÄFTSSTELLE
Sonnhaldeweg 3
3110 Münsingen
Tel. 079 785 88 45
E-Mail: info@kaz-zivilstandswesen.ch

den Ausweisen N, F und S oftmals selbstdeklaratorischen Charakter haben und zu ein und derselben Person oftmals Mehrfacheinträge in ZEMIS bestehen (sog. Alias).

Zu Art. 7 Abs. 1 lit. b und c: Der Vorentwurf sieht vor, dass der amtliche Name als eines der Merkmale der Personenidentifizierungsdaten zugeordnet wird. Der amtliche Name ist kein definierter Begriff und wird nirgends als solcher vermerkt. Dies gilt auch für den Vornamen. In verschiedenen amtlichen Dokumenten resp. Registern, sind Namen nicht immer identisch (Möglichkeit von Erweiterungen in den schweizerischen Ausweispapieren bspw. durch Ledignamen, Abweichung Vornamensschreibweise, etc.). Wir beantragen, Art. 7 Abs. 1 lit. b und c wie folgt anzupassen:
b. Name gemäss Eintragung Informatisiertes Standesregister Infostar
c. Vorname gemäss Eintragung Informatisiertes Standesregister Infostar

Da Infostar als Personenstandsregister mit erhöhter Beweiskraft das Masterregister hinsichtlich Personendaten darstellt, ergibt diese Präzisierung Logik.

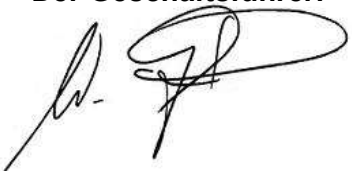
Wir danken Ihnen bestens für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

KONFERENZ DER KANTONALEN AUFSICHTSBEHÖRDEN IM ZIVILSTANDSDIENST

Namens des Vorstandes

Die Präsidentin: **Der Geschäftsführer:**



Esther Gassler, Regierungsrätin Walter Grossenbacher

Kopie an
- alle Kantone, z.H. der für den Zivilstandsdienst zuständigen Regierungsmitglieder und die kantonalen Aufsichtsbehörden

KAZ-GESCHÄFTSSTELLE
Sonnhaldeweg 3
3110 Münsingen
Tel. 079 785 88 45
E-Mail: info@kaz-zivilstandswesen.ch

Konsumfinanzierung Schweiz
Financement à la consommation Suisse
Finanziamento al consumo Svizzera
Swiss Consumer Finance

Per eMail: copiur@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Bern

Zürich, 29. Mai 2017

Stellungnahme zum Vorentwurf Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Damen und Herren

Wir beziehen uns auf die am 22. Februar 2017 eröffnete Vernehmlassung des Eidgenössischen Justiz- und Polizeidepartementes (EJPD) betreffend Vorentwurf zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Wir danken Ihnen und benützen die Gelegenheit zur Stellungnahme hiermit gerne. Der Verband Konsumfinanzierung Schweiz (KFS), vormals Verband Schweizerischer Kreditbanken und Finanzierungsinstitute (VSKF) genannt, vertritt die Konsumkreditbranche, mithin die Anbieterinnen von Bar- und Objektkrediten, Überziehungskrediten sowie Kredit- und Kundenkarten mit Kreditoption. Kernkompetenz unseres Verbandes ist das Konsumkreditgesetz (KKG).

Unsere Stellungnahme lässt sich wie folgt zusammenfassen:

1. Wir begrüssen die schnellstmögliche Einführung einer E-ID in der Schweiz, welche sich sowohl durch einen hohen Sicherheitsstandard als auch durch eine breite Akzeptanz (insb. bei Schweizer Behörden und Regulatoren, aber auch im Ausland) auszeichnet.
2. Die E-ID sollte so ausgestaltet sein, dass die in verschiedenen Gesetzen (namentlich im Geldwäschereigesetz) erforderlichen Identifikationen vollelektronisch und einfach wahrgenommen werden können.
3. Obwohl das System der elektronischen Signatur in Verbindung mit der E-ID grundsätzlich befürwortet wird, ist im Sinne der Digitalisierung dennoch zu prüfen, ob nicht in bestimmten Fällen bzw. Gesetzen (namentlich in den Art. 9, 11 und 12 KKG), ein Nachweis durch Text für einen gültigen Vertragsabschluss genügen würde.
4. Die E-ID ist so auszugestalten, dass der Inhaber sie zusammen mit weiteren persönlichen Daten speichern kann, wobei er je nach beabsichtigtem Geschäftsabschluss dem jeweiligen Vertragspartner einzelne Daten direkt zugänglich machen kann. So sollen insbesondere Daten für eine Kreditfähigkeitsprüfung gemäss Art. 28, 29, 30 und 31 KKG vom Inhaber der E-ID zusammen mit der E-ID in einem elektronischen Wallet gespeichert und von ihm bei Bedarf abgerufen werden können.

1. Einführung einer E-ID

Für den KFS steht die schnelle Einführung einer E-ID mit hohem Sicherheitsstandard im Vordergrund. Eine solche E-ID ist die Grundlage für die meisten digitalen Dienste und Anwendungen, sowohl in der Privatwirtschaft als auch im staatlichen Bereich. Seit dem ersten Anlauf 2004 ist viel Zeit vergangen und die Schweiz ist im internationalen Vergleich unterdurchschnittlich unterwegs (vgl. E-Gouvernement-Benchmark-Bericht der EU).

Die vorgeschlagene Kaskade von drei E-ID-Sicherheitsniveaus ermöglicht es unseres Erachtens, branchenspezifisch und je nach Anwendungsfall ein ausgewogenes Verhältnis zwischen Sicherheit und Benutzerfreundlichkeit zu finden.

2. Gesetzliche Anforderungen an Identifikationen

In diversen Gesetzen werden unterschiedliche Anforderungen an die Identifikation von natürlichen Personen gestellt. Im Bereich der Geldwäscherei- und Terrorismusbekämpfung hat die FINMA mit ihrem Rundschreiben 2016/07 zur Video- und Online-Identifizierung sehr detaillierte Vorgaben aufgelistet, denen Rechnung zu tragen ist. Die Anforderungen erscheinen nicht technologieneutral, sondern von den dazumal bekannten ersten technischen Möglichkeiten beeinflusst.

Die Verwendung der E-ID muss demgegenüber einfach und namentlich für die GwG-Zwecke ausreichend sein. Die Digitalisierung der Identität führt sonst nur zu weiterem Aufwand ohne entsprechenden Nutzen.

Anforderungen aus anderen Gesetzen, namentlich dem Datenschutzgesetz, ist ebenfalls Rechnung zu tragen.

3. Schriftlichkeit von Verträgen

Die Digitalisierung und zunehmende Nutzung mobiler und elektronischer Medien hat zu verändertem Verhalten der Marktteilnehmer geführt. Zunehmend wird auf eine Schriftlichkeit im Sinne der Herstellung eines Dokumentes mit eigenhändiger Unterschrift gemäss Art. 14 OR verzichtet. Auch wenn das System der elektronischen Signatur in Verbindung mit der E-ID grundsätzlich befürwortet wird, ist im Sinne der Digitalisierung deshalb dennoch zu prüfen, ob nicht in bestimmten Fällen bzw. Gesetzen (namentlich in den Art. 9, 11 und 12 KKG), ein Nachweis durch Text für einen gültigen Vertragsabschluss genügen würde. Es stellt sich mit anderen Worten die Frage, ob das Erfordernis der Schriftlichkeit im Einzelfall überhaupt noch gerechtfertigt ist.

So hielt die (nicht für mangelnden Formalismus bekannte) FINMA in ihrem Rundschreiben 2009/1 Eckwerte zur Vermögensverwaltung (dort in Rz. 8) für die Vertragsform Folgendes fest: „Der Vermögensverwaltungsvertrag wird schriftlich oder in anderer durch Text nachweisbarer Form abgeschlossen." Damit rückte sie vom Schriftformerfordernis im Sinne von Art. 14 OR ausdrücklich und bewusst ab. Und dies in einem sensiblen Bereich des Anlegerschutzes.

Nachdem Privatanleger wohl genau gleich schutzbedürftig sind wie Konsumkreditnehmer, steht nichts entgegen, die gleiche Regelung auch für Konsumkreditverträge einzuführen. Dies rechtfertigt sich umso mehr, als der Gesetzgeber gerade erst die Widerrufsfrist im KKG von 7 auf 14 Tage verlängert hat (vgl. Art. 16 Abs. 1 KKG, in Kraft seit 1.1.2016). Es besteht demnach für den Konsumenten eine sehr lange Überlegungsfrist, ob er den abgeschlossenen Vertrag gegebenenfalls doch noch widerrufen will oder nicht. Einen zusätzlichen Schutz vor Überrumpelung (in Form des Schriftformerfordernisses) braucht es deshalb nicht. Die Art. 9, 11 und 12 KKG können demnach dergestalt geändert werden, dass es ausreichend ist, wenn die Verträge sich durch Text nachweisen lassen. Zu ändern sind alle drei

Artikel des KKG, weil dort auch drei Vertragsarten, nämlich der Konsumkredit (Art. 9 KKG), der Leasingvertrag (Art. 11 KKG) und die Überziehungskredite sowie Kredit- und Kundenkarten mit Kreditoption (Art. 12 KKG) je separat geregelt werden. Der jeweilige Absatz 1 dieser drei Artikel ist jedoch bezüglich der Formvorschriften inhaltlich deckungsgleich, weshalb bei den nachstehenden Anträgen nur der Text von Art. 9 KKG aufgeführt wird.

Diese Änderung des KKG wurde bereits in Zusammenhang mit der Stellungnahme zur Vernehmlassung der Fintech-Vorlage vom 4. Mai 2017 beantragt und lautet wie folgt:

Änderung von Art. 9 Abs. 1 (analog auch Art. 11 Abs. 1 und 12 Abs. 1 KKG; Änderung kursiv und rot):

„Konsumkreditverträge sind schriftlich *oder in anderer durch Text nachweisbaren Form* abzuschliessen; die Konsumentin oder der Konsument erhält eine Kopie des schriftlich abgeschlossenen Vertrags *oder Zugang zum vollständigen Vertragstext*.

Anpassung von Art. 16 Abs. 2 KKG (Änderung kursiv und rot):

„Die Widerrufsfrist beginnt zu laufen, sobald die Konsumentin oder der Konsument nach den Artikeln 9 Absatz 1, 11 Absatz 1 oder 12 Absatz 1 eine Kopie des schriftlich abgeschlossenen Vertrags *oder den Zugang zum vollständigen Vertragstext* erhalten hat. Die Frist ist eingehalten, wenn die Konsumentin oder der Konsument die Widerrufserklärung am letzten Tag der Widerrufsfrist der Kreditgeberin oder der Post übergibt.

Anpassung von Art. 82 Abs. 1 SchKG (Änderungen kursiv und rot)

Beruht die Forderung auf einer durch öffentliche Urkunde festgestellten, einer *gemäss besonderer gesetzlicher Bestimmung durch Textnachweis begründeten oder* durch Unterschrift bekräftigten Schuldanerkennung, so kann der Gläubiger die provisorische Rechtsöffnung verlangen.

4. E-ID und Wallet für persönliche Daten

Für verschiedene Rechtsgeschäfte müssen Vertragsparteien, namentlich Konsumentinnen und Konsumenten im Rahmen der Kreditfähigkeitsprüfungen gemäss Art. 28 – 31 KKG, verschiedene persönliche Daten an den Anbieter übermitteln. Bei der Entwicklung einer E-ID sollte deshalb darauf geachtet werden, den Inhabern die Möglichkeit zu geben, in einer Art (elektronischem) Wallet zusammen mit der E-ID (freiwillig) weitere persönliche Daten abzuspeichern, die sie dann zielgerichtet jenen Anbietern (z.B. den Kreditgeberinnen bei einem Konsumkredit) zur Verfügung stellen können, die solche Daten benötigen.

Einerseits wäre so sichergestellt, dass die Konsumentinnen und Konsumenten selbst Daten übermitteln und dies nur an jene Anbieter, denen sie diese Daten auch wirklich zukommen lassen wollen, und andererseits könnte eine Abklärungs- oder Sorgfaltspflicht des Anbieters klarer definiert werden. So wäre es zum Beispiel möglich, dass für die Kreditfähigkeitsprüfung der Kreditgeberinnen die benötigten Daten genau definiert und vom Kunden zur Verfügung gestellt werden. Ebenso liessen sich jene Daten genau bezeichnen, die von den Kreditgeberinnen zu verifizieren sind. Man könnte so die in vielen Teilen unbefriedigende Prüfung eines das (erweiterte Existenzminimum) übersteigenden Freibetrages durch klare Vorgaben und vertrauenswürdige und sichere Datenquellen ersetzen. Dies führte zu einer heute nicht in allen Teilen gegebenen Rechtssicherheit bei der Vornahme der Kreditfähigkeitsprüfungen. Die Herstellung von Rechtssicherheit in diesem Bereich ist umso dringlicher, als Art. 32 KKG drakonische Sanktionen eines totalen Forderungsverlustes bei

schwerwiegenden und des Verlustes der Forderungen auf Zinsen und Kostenersatz für den Fall einer geringfügigen Verletzung der Vorschriften über die Kreditfähigkeitsprüfung vorsieht.

Die E-ID ist demnach technisch so auszugestalten, dass die geschilderten Bedürfnisse damit abgedeckt werden können.

Vielen Dank für Ihre Kenntnisnahme. Für Rückfragen stehen wir jederzeit gerne zur Verfügung.

sig. Dr. Markus Hess
Geschäftsführer

Parldigi

Frau Bundesrätin
Simonetta Sommaruga
Eidg. Justiz- und Polizeidepartement
3003 Bern

29. Mai 2017

Stellungnahme der Parlamentarischen Gruppe Digitale Nachhaltigkeit zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Namens der Parlamentarischen Gruppe Digitale Nachhaltigkeit Parldigi bedanken wir uns für die Möglichkeit, unsere Position zum Entwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) darzulegen und reichen Ihnen hiermit unsere Stellungnahme ein.

Die digitale Welt verlangt für eine Vielzahl von Dienstleistungen unsere Identifikation als Nutzer. Manchmal genügen dazu einige Angaben zur Person, z.B. eine gültige Email-Adresse oder bloss eine Kreditkartennummer. Manchmal sind aber Informationen nötig, die von einer staatlichen Stelle beglaubigt sein müssen, weil die Applikation besonders heikel ist. Beispiele sind das elektronische Patientendossier, das E-Voting oder ein Strafregisterauszug. Wie in der nicht-digitalen Welt benötigen wir dann einen amtlichen Ausweis, welcher unsere Identität staatlich nachweist.

In der nicht-digitalen Welt hat der Staat dazu bereits vor langer Zeit hoheitliche Institutionen und Verfahren eingerichtet, über welche wir einen solchen amtlichen Ausweis beziehen können. Die Glaubwürdigkeit der Schweizer Ausweispapiere, insbesondere des Schweizer Passes, ist legendär und Basis für zahllose Geschäftstransaktionen. Wir vertrauen dem Schweizer Pass, weil er vom Staat und nicht von einer privaten Unternehmung oder Organisation ausgestellt wird.

Glaubwürdigkeit und Vertrauen sind auch in der digitalen Welt elementar für den Aufbau erfolgreicher Geschäftsbeziehungen. Wir wissen, dass dieses Vertrauen bei digitale Dienstleistungen leider nicht immer gerechtfertigt ist.

Aus diesen grundsätzlichen Überlegungen empfehlen wir, den vom Bundesrat vorgelegten Entwurf und das darin abgebildete Konzept (namentlich das „Konzept 2016“ des fedpol „Staatlich anerkannte elektronische Identifizierungsmittel (E-ID)“) grundsätzlich zu überarbeiten und dabei die folgenden prinzipiellen Punkte zu berücksichtigen:

Parldigi

(i) der staatliche elektronische Identitätsnachweis (staatliche E-ID) soll eine hoheitliche Staatsaufgabe bleiben, welche nicht an mehrere konkurrierende nichtstaatliche Identitätsdienstleister abgegeben wird;

(ii) der Staat gibt die staatliche E-ID entweder alleine heraus oder beauftragt maximal einen Dritten, diese hoheitliche Aufgabe im Auftrag des Staates wahrzunehmen;

(iii) die Nutzung der staatlichen E-ID soll für bestimmte Anwendungen zwingend sein (z.B. in den hoheitlichen Anwendungsbereichen E-Government und E-Health).

Wir setzen uns dafür ein, dass der Vorentwurf des E-ID-Gesetzes in diesem Sinn überarbeitet und ein pragmatischer Weg für eine rasche Umsetzung gesucht wird. Die bereits seit längerer Zeit bestehenden Personenregister stellen aus unserer Sicht eine völlig ausreichende Basis für die Realisierung der staatlichen E-ID dar. Eine Erschliessung dieser Register für den staatlichen elektronischen Identitätsnachweis ist daher umgehend auf rechtlicher, organisatorischer und technischer Ebene zu prüfen.

Der staatliche elektronische Identitätsnachweis ist für die digitale Zukunft der Schweiz von zentraler Bedeutung. Die staatliche E-ID soll so rasch wie möglich auf Basis der bestehenden Personenregister mit minimalem Aufwand realisiert und für alle Einwohner und Bürger der Schweiz flächendeckend eingeführt werden.

Edith Graf-Litscher
Nationalrätin und Co-Präsidentin Parldigi

Kontaktadresse:

Dr. Matthias Stürmer,
Geschäftsleiter Parlamentarische Gruppe Digitale Nachhaltigkeit Parldigi
info@digitale-nachhaltigkeit.ch
www.digitale-nachhaltigkeit.ch

privatim
die schweizerischen datenschutzbeauftragten
les préposé(e)s suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Per E-Mail an: copiur@bj.admin.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
3003 Bern

Basel, 2. Mai 2017

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

Sehr geehrte Damen und Herren

Wir danken für die Einräumung der Gelegenheit zur Stellungnahme zum Entwurf eines Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Das E-ID-Gesetz regelt elektronische Identifizierungseinheiten, die als vertrauenswürdige Identifizierungs- oder Authentifizierungsmittel (analog des Einsatzes von Ausweispapieren in der physischen Welt) zur sicheren Abwicklung von Online-Geschäften beitragen sollen. Gerne äussern wir uns zum Gesetzesentwurf wie folgt.

Grundsätzlich

Wir enthalten uns zur Frage, ob die Ausstellung einer E-ID nicht gleich wie die Ausstellung amtlicher Ausweise in der analogen Welt eine staatliche Aufgabe ist, die auch durch staatliche Stellen zu erfüllen ist. Mehrere Anläufe, diese Aufgabe Privaten zu überlassen, sind erfolglos geblieben – es sei an Swisskey und die SuisseID erinnert.

Problematisch erscheint uns bei den vorgeschlagenen Regelungen ausserdem die Verhältnismässigkeit im Zusammenhang mit der Bekanntgabe von hinterlegten Personendaten (siehe sogleich unten).

Im Einzelnen

In Bezug auf den Einsatz der E-ID im Rahmen von staatlichen Dienstleistungen weisen wir darauf hin, dass nicht mehr Personendaten bearbeitet werden dürfen als dies in der

privatim
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 2015, CH-4010 Basel
Tel. +41 (61) 201 16 40, Fax +41 (61) 201 16 41
praesident@privatim.ch, www.privatim.ch

physischen Welt vorgesehen ist (Verhältnismässigkeitsprinzip). Wenn beispielsweise für die Einreichung einer Steuererklärung die Angabe des Namens und der Adresse sowie der Unterschrift der Dokumente erforderlich ist, dürfen nicht durch die Verwendung der E-ID dafür weitere Personendaten wie das Gesichtsbild gefordert bzw. bekannt gegeben werden. Dies ist insbesondere auch zu berücksichtigen, falls bestimmte staatliche Dienstleistungen zukünftig nur noch mittels Identifizierung bzw. Authentisierung durch eine E-ID genutzt werden können und somit für betroffene Personen ein faktischer Zwang entstünde, die zusätzlichen Personendaten bekanntzugeben.

Art. 7 E-ID-Gesetz hält die Personenidentifizierungsdaten fest, welche die Identitätsstelle einer E-ID zuordnet. Je nach Sicherheitsniveau ist die Anzahl zugeordneter Personenidentifizierungsdaten unterschiedlich hoch (Absätze 1 und 2). Zudem können die Personenidentifizierungsdaten durch die Identitätsstelle mit weiteren Informationen versehen werden (Abs. 3). Darüber hinaus kann der Identity Provider der E-ID noch weitere Daten zuordnen (Abs. 4). Der in dieser Bestimmung aufgeführte Datenkatalog erscheint lang und enthält auch sensible Personendaten wie biometrische Daten. Es ist nicht ersichtlich, wofür die Bearbeitung dieser grossen Anzahl von Personendaten geeignet oder erforderlich ist. Weil die Aufzählung ausserdem nicht abschliessend ist, da die Möglichkeit offen gelassen wird, noch weitere Personendaten zuzuordnen, ist diese Bestimmung nicht mit dem Verhältnismässigkeitsgrundsatz zu vereinbaren. Es werden damit Daten auf Vorrat gesammelt und miteinander verknüpft.

Die in Art. 7 E-ID-Gesetz aufgeführten Daten werden zudem an Betreiberinnen von E-ID-verwendenden Diensten übermittelt (Art. 17 Abs. 1 lit. f E-ID-Gesetz). Selbst wenn dafür das Einverständnis der betroffenen Person erforderlich ist, handelt es sich auch hier um eine unverhältnismässige Datenbekanntgabe. Betreiberinnen von E-ID-verwendenden Diensten erhalten dadurch eine grosse Anzahl von Personendaten, die sie bei der bisherigen Geschäftsabwicklung in der physischen Welt nicht erhalten hätten. Auch diesbezüglich ist somit nicht nachvollziehbar, wofür die Datenbekanntgabe geeignet und erforderlich und damit verhältnismässig ist. Es handelt sich im Ergebnis um bisher nicht zulässige Datenbekanntgaben an Private aus den staatlichen Personenregistern ISA, ZEMIS, Infostar und ZAS-UPI.

Antrag: Reduktion der Menge der einer E-ID zuzuordnenden Personendaten, allenfalls einschränkende Regelung der Verwendung bzw. Bekanntgabe der Daten

Der Vorentwurf E-ID-Gesetz sieht die Verwendung der Versichertennummer nach Art. 50c AHVG vor. Die AHV-Versichertennummer wird der E-ID für die Sicherheitsniveaus substanziell und hoch als Personenidentifizierungsdatum zugeordnet (Art. 7 Abs. 2 lit. a E-ID-Gesetz). Zudem soll die Identitätsstelle berechtigt werden, die AHV-Versichertennummer systematisch zur Identifizierung von Personen beim elektronischen Datenaustausch mit den Personenregistern (ISA, ZEMIS, Infostar und ZAS-UPI) zu verwenden (Art. 9 Abs. 1 E-ID-Gesetz). Weiter soll der Identity Provider berechtigt werden, die AHV-Versichertennummer zu führen und sie den zur systematischen Verwendung der AHV-Versichertennummer berechtigten Betreiberinnen von E-ID-verwendenden Diensten bekannt zu geben (Art. 9 Abs. 2 E-ID-Gesetz). Die AHV-Versichertennummer war ursprünglich eine Nummer für den Bereich der Sozialversicherungen. Obwohl die Nummer immer mehr in anderen staatlichen Bereichen verwendet wird, sollte sie nicht auch für Private zugänglich werden. Grundsätzlich soll die systematische Verwendung für Stellen ermöglicht werden, die mit Aufgaben der Sozialversicherung betraut sind. Eine systematische Verwendung in weiteren Bereichen auch ausserhalb des Sozialversicherungsrechts ist nur möglich, sofern ein

Gesetz dies vorsieht. Der vorliegende Gesetzesentwurf würde eine solche Grundlage schaffen. Aus datenschutzrechtlicher Sicht ist eine Ausweitung des Anwendungsbereichs der Versichertennummer dennoch problematisch: Die Einführung der AVH-Versichertennummer wollte primär die Koordination im Bereich der sozialen Sicherheit erleichtern; aus datenschutzrechtlicher Sicht widerspricht eine weitere Verwendung ohne jeglichen Bezug zum Sozialversicherungsrecht den ursprünglichen Absichten der Einführung der AHV-Versichertennummer. Die Datenschutzbeauftragten sprechen 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 erhöht 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 ist deshalb zu verzichten.

Antrag: Verzicht auf die Verwendung der AHV-Versichertennummer, allenfalls Ersatz durch einen bereichsspezifischen Identifikator.

Schliesslich enthält der Vorentwurf keine Regelung zum Ablauf, zur Erneuerung oder Ungültigkeit usw. einer E-ID. Auch das Vorgehen bezüglich Sperrung oder Widerruf einer E-ID müsste noch geregelt werden.

Antrag: Ergänzung des Gesetzes durch Regelungen zum Ablauf, zur Erneuerung oder Ungültigkeit usw., zur Sperrung oder zum Widerruf einer E-ID.

Schliesslich wird in Art. 11 das Erlöschen der Anerkennung einer IdP geregelt. Es erscheint uns ungenügend, dass der Anerkennungsstelle bei der Aufgabe der Geschäftstätigkeit nur Angaben über das geplante Vorgehen bezüglich der ausgestellten E-ID zu machen sind. Hier fehlen unseres Erachtens Vorgaben für dieses Vorgehen.

Antrag: Ergänzung des Gesetzes durch klare Regelungen, was im Falle der Geschäftsaufgabe einer IdP mit den Daten zu geschehen hat.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen. Für Rückfragen steht Ihnen als Ansprechperson gerne zur Verfügung:

Dr. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich, Beckenhofstrasse 23, 8090 Zürich, bruno.baeriswyl@dsb.zh.ch, Tel. 043 259 39 99.

Freundliche Grüsse

Beat Rudin
Präsident privatim

SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Bundesrain 20
3003 Berne

per Email versandt:
copiur@bj.admin.ch

RR/ARU

Bern, den 24. Mai 2017

SAV Stellungnahme zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Der Schweizerische Anwaltsverband (SAV) dankt Ihnen für die Gelegenheit zur obgenannten Vernehmlassung Stellung nehmen zu können.

Der SAV begrüsst, dass mit dem E-ID einerseits die Anpassung des schweizerischen Rechts an die eIDAS VO der EU vorgenommen und andererseits Voraussetzungen zur Vereinfachung des ERV in der Schweiz geschaffen werden. Zu den einzelnen Bestimmungen des Gesetzesentwurfes lassen wir uns wie folgt vernehmen:

Art. 1 und 2

Keine Bemerkungen.

Art. 3

In Art. 3 Abs. 1 sollte anstelle von «kann» das Verb «dürfen» gewählt werden. Da das Gesetz keinen Kontrahierungszwang der IdP vorsieht und Art. 3 Abs. 1 lit. a und b den Kreis derjenigen Personen bestimmt, denen der IdP eine E-ID ausstellen darf, sollte der Gesetzeswortlaut auch entsprechend gefasst werden.

Klärungsbedürftig ist unseres Erachtens die Frage, wie die Ausstellung von E-ID an nicht handlungsfähige Personen erfolgt. Insbesondere deshalb, weil in Art. 7 des VE nicht vorgesehen ist, die vertretungsberechtigte Person bzw. Personen in der E-ID zu erwähnen. Im erläuternden Bericht (Seite 20/49, unter Ziffer 1.8.3) wird die Ansicht vertreten, der Gebrauch der E-ID durch nicht handlungsfähige Personen habe unter Aufsicht der vertretungsberechtigten Person zu erfolgen. Nachdem davon auszugehen ist, dass die E-ID im elektronischen Rechtsverkehr Zertifikate gemäss ZertES zumindest teilweise (bis zu gewissen Transaktionsbeträgen) ersetzen wird, stellt sich die Frage, ob es genügt, wenn die vertretungsberechtigte Person beim Gebrauch der E-ID anwesend ist. Zudem erscheint das «Anwesendsein» insbesondere bei Jugendlichen ab einem gewissen Alter nicht opportun und teilweise auch nicht üblich.

Art. 4 Abs. 2 lit g und Art. 4 Abs. 4 lit. b

Unseres Erachtens sollte auf den zweiten Satzteil «…oder gleichwertige finanzielle Sicherheiten nachweisen» verzichtet werden. Die Regelung würde nur dann Sinn machen, wann das Vorhandensein der finanziellen Mittel (durch die Behörde) auch regelmässig geprüft würde und die Mittel dem Zugriff von Dritten entzogen wären.

Art. 6 Abs. 3

Der technische Ablauf sollte unseres Erachtens so gestaltet werden, dass eine Nachfrage der Identitätsstelle bei der antragstellenden Person nicht notwendig ist (vgl. erläuternden Bericht, Seite 25, oben).

Art. 7 Abs. 2 lit. d und e

Unseres Erachtens tragen die in Art. 7 Abs. 2 lit. d und e erwähnten Angaben nicht dazu bei, das Sicherheitsniveau zu erhöhen. Es ist deshalb darauf zu verzichten.

Art. 7 Abs. 3

Sinnvollerweise sollte eine Delegationsnorm zugunsten des Bundesrates geschaffen werden. Die

offene gesetzliche Norm lässt im Grundsatz alles zu.

Art. 8

Nachdem eine Person mehrere E-ID's haben kann und derzeit noch offen ist, ob die AHVN13 als Nummer verwendet werden kann, wird es zur Identifikation der Person nicht genügen, wenn die E-ID gemeldet wird. Vielmehr muss eine eineindeutige Zuordnung erfolgen können. Dies ist jedoch nur dann möglich, wenn auch eine eineindeutige Angabe erfolgt, sprich, dass zusätzlich die AHVN13 verwendet wird. Zudem wird die Identitätsstelle wohl eine Datenbank führen müssen, in welcher alle Personen mit den zugehörigen E-ID geführt werden.

Art. 10 Abs. 2

Unseres Erachtens ist der Handel mit Daten auf das Notwendige zu beschränken. Damit alle Personen gleich behandelt werden ist im vorliegenden Gesetz zu bestimmen, welche Daten gehandelt werden dürfen. Andernfalls werden die IdP in den Allgemeinen Geschäftsbedingungen, bestimmen welche Daten gehandelt werden. Diesen Geschäftsbedingungen können sich Nutzer erfahrungsgemäss «nicht entziehen».

Art. 11

Unseres Erachtens ist zu regeln, was im Falle des Konkurses mit den Daten geschieht und nicht wie es sich mit dem Schicksal der «E-ID-Systeme» verhält. Zudem genügt es nicht zu bestimmen, dass die E-ID Systeme nicht in die Konkursmass fallen. Vielmehr ist zu bestimmen, welche Stelle im Fall des Konkurses über das Schicksal der Daten verfügen kann bzw. an wen die Daten anheimfallen, wenn sie im Zuge der Konkursliquidation nicht verkauft werden können.

Art. 12 Abs. 3 lit. b

Hier dürfte es sich um einen Verschrieb handeln. Der Verweis bezieht sich auf Art. 4 Abs. 2.

Art. 12 Abs. 3 lit. d

Die Einschränkung auf Internetkriminalität ist unseres Erachtens nicht notwendig und zu eng gefasst. In Fällen von Art. 12 Abs. 3 lit. d dürfte in aller Regel die Vertrauenswürdigkeit nicht mehr gegeben sein.

Art 13

Da seitens der IdP kein Kontrahierungszwang besteht, sollte sich der Bund eine generelle Kompetenz vorbehalten, eigenständig tätig zu werden.

Art. 17 lit. g

Die Löschungsfrist lehnt wohl an die Bestimmungen des BüPF an. Ob diese Gleichschaltung in einer eigenen Norm sinnvoll ist, ist unseres Erachtens fraglich. Wenn eine «Gleichschaltung» mit dem BüPF erreicht werden soll, dann sollte wohl auf das BüPF verwiesen werden.

für den SAV

SAV Präsident

Sergio Giacomini

SAV Generalsekretär

René Rall

Association suisse des officiers de l'état civil
Associazione svizzera degli ufficiali dello stato civile
Schweizerischer Verband für Zivilstandswesen

Eidg. Justiz- und Polizeidepartement
Bundesamt für Justiz

Per Mail an:
copiur@bj.admin.ch

Zürich, 20. Mai 2017

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)
Stellungnahme des Schweizerischen Verbandes für Zivilstandswesen (SVZ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Zum im Titel genannten Vernehmlassungsverfahren wurde der Schweizerische Verband für Zivilstandswesen nicht eingeladen. Die Zivilstandsämter sind täglich und direkt mit der Abklärung der Identität von Personen beschäftigt. Aus diesem Grund nehmen wir zum E-ID-Gesetz gerne Stellung:

Der Schweizerische Verband für Zivilstandswesen schliesst sich vollumfänglich der Stellungnahme der Konferenz der kantonalen Aufsichtsbehörden im Zivilstandswesen vom 10. Mai 2017 an.

Wir danken Ihnen für die Berücksichtigung unserer Eingabe.

Freundliche Grüsse

Schweizerischer Verband für Zivilstandswesen

Roland Peterhans
Präsident

Geschäftsstelle Schweizerischer Verband für Zivilstandswesen
c/o bwd, Weiterbildung BV Bern, Papiermühlestrasse 65, 3014 Bern
Tel. 031 330 19 89, Fax 031 330 19 80, E-Mail: zivilstandswesen@bwdbern.ch

Frau Bundesrätin
Simonetta Sommaruga
Eidg. Justiz- und Polizeidepartement
3003 Bern
Per E-Mail:
copiur@bj.admin.ch

Bern, 29.05.2017

Stellungnahme: Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID Gesetz)

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

2013 wurde die Stiftung für Konsumentenschutz (SKS) im Rahmen einer informellen Konsultation und 2015 zum Konzepte für staatlich anerkannte eID-Systeme befragt. Wir erlauben uns daher, nun auch im Rahmen des Vernehmlassungsverfahrens zum Entwurf des eID-Gesetzes eine kurze Stellungnahme abzugeben. .

Die SKS begrüsst grundsätzlich die Schaffung eines Ausweises für die Online-Welt. Für den Konsumenten sowie auch für Unternehmen bietet der digitale Identitätsnachweis einen Zeit-, Kosten- und Sicherheitsgewinn. An oberster Stelle steht dabei der datenrechtliche Schutz der Privatpersonen, welche die E-ID nutzen. Glaubwürdigkeit und Vertrauen sind in der digitalen Welt elementar. Deshalb zielt der ausgearbeitete Entwurf in die falsche Richtung, denn gemäss diesem würde der Staat seine Rolle auf die Anerkennung und Überwachung der Marktteilnehmer beschränken. Dies führt früher oder später zu einer gefährlichen Wissens- und Kompetenzverschiebung weg vom Staat hin zu den Privaten. Wie bei amtlichen Ausweispapieren soll auch der elektronische Identitätsnachweis eine hoheitliche Aufgabe bleiben, welche der Staat selbst wahrnimmt.
Gemäss Gesetzesentwurf spielen Identitätsdienstleister eine Schlüsselrolle zwischen Staat und Bürger. Was bislang ausschliesslich in die Kompetenz der staatlichen Ausweis-/Passausgabestellen fällt, soll im Rahmen der E-ID von privaten, gewinnorientierten Unternehmen übernommen werden. Eine derartige Rollverschiebung würde Verwirrung und Unsicherheit stiften und die Akzeptanz stark senken. Ein Merkmal von sich konkurrierenden Produkten ist unter anderem, dass diese auch wieder vom Markt verschwinden können. Beim Anbieten eines Identitätsausweises (in welchem Bereich dieser auch immer zum Einsatz kommen mag) darf dies aber gerade nicht passieren. Nur der Staat geniesst hier die notwendige Glaubwürdigkeit und das Vertrauen und verfügt über die notwendige Beständigkeit.

Aus Sicht der SKS muss der ausgearbeitete Entwurf nochmals durchdacht und überarbeitet werden. Die Herausgabe einer EID darf keinesfalls dem freien Markt und somit dem Gutdünken einzelner Unternehmen überlassen werden. Auch zwecks Gewährleistung der datenschutzrechtlichen Sicherheitsstandards ist eine aktive Beteiligung des Staats am Geschehen unverzichtbar. Allenfalls besteht die Möglichkeit, dass der Staat einen Dritten beauftragt, diese hoheitliche Aufgabe im Namen des Staates wahrzunehmen.

Freundliche Grüsse

Sara Stalder, Geschäftsleiterin SKS

Verband Schweizerischer Einwohnerdienste (VSED)
Association suisse des services des habitants (ASSH)
Associazione svizzera dei servizi agli abitanti (ASSA)
Associaziun svizra dals servetschs als abitants (ASSA)

Per Mail

copiur@bj.admin.ch

Zürich/Wettingen, 22.05.2017

Vernehmlassung E-ID

Sehr geehrte Damen und Herren

Der Verband Schweizerischer Einwohnerdienste VSED hat über das Bundesportal von der Vernehmlassung zur E-ID erfahren. Nachdem unser Verband bereits bei der Konzeptstudie und danach bei der informellen Konsultation zur Mitwirkung eingeladen wurde, erstaunt es uns sehr diesmal nicht direkt zum Vernehmlassungsverfahren eingeladen worden zu sein.

Die Einwohnerdienste sind zwar zum heutigen Zeitpunkt nicht direkt involviert, können aber auf eine langjährige Erfahrung in der Datenbearbeitung zurückblicken.

I Grundsätzliches

Auf der einen Seite unterstützt der VSED Ablaufoptimierungen und medienbruchfreie Prozesse, welche durchaus dank einer E-ID ermöglicht werden würden. Auf der anderen Seite, wie bereits in unserer Stellungnahme zur Anhörung betont, zieht der VSED nach wie vor ganz klar eine staatliche E-ID dem nun vorgesehenen Modell vor.

Den digitalen Identitätsausweis in die Hände der Privatwirtschaft zu delegieren, kann nicht zielfördernd sein und wird voraussichtlich auch weiterhin in der Bevölkerung auf wenig Akzeptanz stossen, **weshalb wir hier auf die Relevanz hinweisen, dass ein zukünftiger privater IdP über einen sehr umfassenden Datenbestand einer Person verfügen wird.** Es handelt sich dabei um mehr - respektive je nach Quellregister - um andere zusätzliche Daten, als sie heute in den einzelnen Registern zur Verfügung stehen.

Da das E-ID-Verfahren insbesondere für den Laien technisch komplex ist, muss die Bevölkerung transparent über ihre Rechte informiert werden und sich darauf verlassen können, dass der Staat, wie dies im Gesetzestext und dem erläuternden Bericht auch zum Ausdruck kommt, ausreichend um die Sicherheit besorgt ist und Daten nicht missbräuchlich verwendet werden. Ebenfalls muss der E-ID-Inhaber Klarheit darüber haben, was mit seinen Daten genau passiert bzw. welche Daten weitergegeben werden. Ein E-ID Inhaber muss unbedingt die Möglichkeit

haben, Einfluss auf die Datenbekanntgabe respektive auf die Einschränkung der Datenbekanntgabe zu nehmen.

Da es sich nicht um eine staatliche E-ID handelt, muss zwingend gewährleistet sein, dass die Bevölkerung eine Wahlfreiheit hat und der Antrag für eine E-ID an keine Bedingungen geknüpft werden kann, die dem Interesse der Bevölkerung im Wesentlichen entgegensteht. Das heisst, dass weder ein E-ID-Anbieter eine Monopol-Stellung erhält, noch dass Absprachen zwischen den E-ID-Anbietern stattfinden.

II Zu den einzelnen Artikeln

Art. 6 Ausstellungsprozess

Abs. 1

Laut Erläuterungen wird eine E-ID in der Regel nach Vorsprache bei einem IdP ausgestellt. Die Registrierung beinhaltet je nach Sicherheitsniveau auch eine Identifizierung mittels elektronischer Medien. Aus Sicht des VSED ist in jedem Fall eine persönliche Vorsprache für die Beantragung einer E-ID zwingend. Mit den heutigen Mitteln erachten wir eine reine virtuelle Identifikation als relativ leicht manipulierbar für Personen mit dem nötigen technischen Wissen.

Ergänzung im Gesetz:

[1] Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP. ***Eine persönliche Vorsprache zur Identitätsüberprüfung ist unabdingbar.***

Abs. 3

Für den VSED ist in diesem Punkt unklar, ob der zukünftige Inhaber einer E-ID auch die durch die Identitätsstelle übermittelnden Daten an den IdP oder durch den IdP abzurufende Daten einschränken kann. Gemäss Wortlaut von Art. 6 verstehen wir, dass die Personenidentifizierungsdaten nach Art. 7 Abs. 1 und 2 abschliessend übermittelt werden, wenn eine E-ID bei einem IdP beantragt wird.

Aus Sicht des VSED muss zwingend gewährleistet sein, dass diese Merkmale je nach Anforderungsniveau der gewünschten E-ID durch den Inhaber ebenfalls eingeschränkt werden können. Es ist durchaus denkbar, dass ein zukünftiger Inhaber ausschliessliche eine E-ID mit tiefem Sicherheitsniveau verwendet und deshalb nur die Grunddaten: Name, Vorname, Geburtsdatum auf seiner E-ID benötigt. **Aus diesem Grund stellt sich uns hier die Frage, wofür der IdP in einem solchen Fall den gesamten Datenumfang von Art. 7 Abs. 2 benötigt?**

Art. 7 Personenidentifizierungsdaten

Abs. 1 und 2

Der VSED unterstützt, wie im erläuternden Bericht beschrieben, die Einschränkung von Personenidentifizierungsdaten durch den Inhaber bei einer konkreten Anwendung einer E-ID, die vom IdP an eine Betreiberin von E-ID verwendeten Diensten übermittelt werden.

Abs. 4

Inwiefern kann ein E-ID-Inhaber bezüglich diesen zusätzlichen vom IdP hinzuzufügenden Daten Einfluss nehmen? **Es muss auch hier unbedingt gewährleistet sein, dass ein E-ID-Inhaber diese einschränken kann bzw. seine Einwilligung erteilen muss.** Geht es hier

doch immerhin um die durch den IdP – zwar nicht mit dem Staat verifizierten - zusätzlich zugewiesenen Daten, wie z.B. E-Mail-Adresse, Mobile-Telefon, Adresse etc.

Wir weisen darauf hin, dass es Personen gibt, welche in den amtlichen Registern die Auskunft über Daten gegenüber Privaten haben sperren lassen. Äusserst heikel erachten wir deshalb, wenn Daten, wie die Adresse, Mobile-Nr. oder E-Mail-Adresse ohne Einwilligung der Person oder sogar in Unkenntnis des Inhabers hinzugefügt werden und diese Daten privaten Dritten bekannt gegeben würden. Oft sind Personen, die eine Adress- und Datensperre z.B. in den Einwohnerregistern beantragt haben an Leib und Leben bedroht.

Art. 8 Aktualisierung der Personenidentifizierungsdaten

Es muss auch hier sichergestellt sein, 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 (vgl. Einwand zu Art. 6 Abs. 3).

Art. 10 Datenbearbeitung und Datenweitergabe

Weshalb unterliegen die Daten nach Art. 7 Abs. 1 und 4 in diesem Zusammenhang nicht auch dem Handelsverbot? Nach Art. 7 Abs. 4 könnten hier eine Varietät an Daten hinzugefügt werden, die mit Name, Vorname und Geburtsdatum verknüpft werden.

Der Wortlaut im Bericht zu Art. 10 Absatz 3, Seite 27/28 ist in diesem Zusammenhang nicht präzis formuliert bzw. ist verwirrend. **Welche Daten dürfen nun gegen Entgelt weitergeben werden und welche nicht?**

Der E-ID Inhaber muss sich auf jeden Fall bewusst sein, welche Daten an Dritte weitergegeben werden und welche nicht.

Der VSED beantragt den Wortlaut des Gesetzes folgendermassen abzuändern:

Art. 10 Abs. 3

Weder (……) von E-ID-verwendenden Diensten dürfen die Personenidentifizierungsdaten gemäss Artikel 7 Abs. 2 oder die darauf basierenden Nutzungsprofile weitergeben. ***Für die Bekanntgabe der Daten nach Art. 7 Abs. 1 und 4 an Dritte ist das Einverständnis des E-ID Inhabers einzuholen.***

Gemäss Seite 10 und 12 (Grafik) des Konzeptes aus dem Jahre 2016 garantiert, wenn immer möglich der Staat für sichere und verlässliche Attributsquellen.

In diesem Zusammenhang möchten wir auf folgende Gegebenheiten aufmerksam machen.

Es ist in der Praxis durchaus möglich, dass sich ein Datenfeld bzw. ein Attribut im Nachhinein als falsch erweist, wenn z.B. eine Person ihre Meldepflicht über eine Änderung eines Attributes gegenüber der Quelldatenbank nicht erfüllt hat oder sich das Datum infolge eines in der Vergangenheit liegenden Ereignisses rückwirkend verändert.

Für die Prüfung und Berücksichtigung unserer Anliegen bedanken wir uns. Der Verband der Schweizerischen Einwohnerdienste ist gespannt über die Ausgestaltung der Verordnung wünscht Ihnen für den weiteren Verlauf des Verfahrens viel Erfolg.

Freundliche Grüsse

Verband Schweizerischer Einwohnerdienste

Carmela Schürmann, Präsidentin

Walter Allemann, Sekretär

Kopie:
Schweizerischer Gemeindeverband, Bern
Schweizerischer Städteverband, Bern
Eidg. Datenschutzbeauftragter, Bern

Präsidium: Carmela Schürmann, stv. Leiterin Personenmeldeamt, Bevölkerungsamt Stadt Zürich, Stadthausquai 17, Stadthaus, Postfach, 8022 Zürich, Tel. 044/ 412 32 09 / Fax 044/ 412 36 74 / carmela.schuermann@zuerich.ch

Sekretariat: Walter Allemann, Leiter Einwohnerdienste, Rathaus, Alb.Zwyssigstr. 76, 5430 Wettingen Tel. 056/ 437 77 41 / Fax. 056/ 437 77 98 / walter.allemann@wettingen.ch

VZGV
Ressort Vernehmlassungen
c/o Gemeinde Dürnten
Brigit Frick
Rütistrasse 1
8635 Dürnten
Telefon 055 251 57 18
Telefax 055 251 57 01
www.vzgv.ch
brigit.frick@duernten.ch

Federas, Stiftung Chance, Institut für Verwaltungs-Management und die Interessengemeinschaft ICT der Zürcher Gemeinden sind Partner-Organisationen des VZGV.

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Herr Urs Paul Holenstein
Leiter Fachbereich Rechtsinformatik
Bundesrain 20
3003 Bern

Dürnten, 3. Mai 2017

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

Sehr geehrte Damen und Herren
Sehr geehrter Herr Holenstein

Gemäss Medienmitteilung vom 22. Februar 2017 erhält der Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute VZGV die Gelegenheit, sich zum geplanten Neuerlass des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) zu äussern. Hierfür danken wir Ihnen und nehmen dazu gerne wie folgt Stellung:

1. Generelle Würdigung

Geschäftsprozesse werden immer häufiger digital abgewickelt, was eine grundlegende Sicherheit im Hinblick auf die Identität des elektronischen Gegenübers voraussetzt. Der Bundesrat will deshalb rechtliche und organisatorische Rahmenbedingungen für die Anerkennung von elektronischen Identifizierungsmitteln und deren Anbieter schaffen. Mit weitherum akzeptierten und einsetzbaren elektronischen Identifizierungsmitteln (E-ID) könnten Geschäfts- und Verwaltungsprozesse im Internet effizienter gestaltet und abgewickelt werden. Diese technologische Entwicklung erfordert eine entsprechende gesetzliche Regelung, weshalb der vorliegende Gesetzesentwurf grundsätzlich unterstützt wird.

Die nachfolgende Stellungnahme bezieht sich vor allem auf die organisatorischen und technischen Rahmenbedingungen, nicht jedoch auf die politischen Aspekte.

2. Vernehmlassung im Einzelnen

Die in Kapitel 2.2 (Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete) des Erläuternden Berichtes zum Vorentwurf aufgelisteten Vorteile sind aus Sicht des VZGV stimmig.

Art. 6 Abs. 5
Der Zweck der Protokollierung muss aufgeführt werden.

Art. 7 Abs. 2
Das Argument der abschliessenden Aufzählung der Personenidentifizierungsdaten ist nicht nachvollziehbar, es können zukünftig durchaus weitere Identifizierungsdaten in den Bundessystemen aufgenommen werden. Eine Beschränkung bzw. abschliessende Aufzählung ist daher nicht notwendig.

Art. 12 Abs. 2 und 3
Für die Behebung eines Mangels sind kurze Fristen vorzusehen. Ein allfälliger Entzug der Anerkennung muss – insbesondere in Fällen von Art. 12 Abs. 2 lit. d – sehr kurzfristig erfolgen, was in den nachgelagerten Verordnungen bzw. Ausführungsbestimmungen zu regeln ist. Ein Zuwarten, bis ein Verfahren abgeschlossen oder eine rechtskräftige Verurteilung erfolgt ist, dauert je nach Sicherheitsstufe möglicherweise zu lange.

Art. 14 Abs. 2
Die notwendigen Massnahmen sind abhängig von der Sicherheitsstufe nach Art. 5 Abs. 1. Demzufolge ist eine Präzisierung erforderlich.

Im Hinblick auf die später zu erarbeitenden Verordnungen ist Folgendes anzumerken:

Die Definition der Anforderungen betreffend Standards, Schnittstellen, technische Anforderungen usw. in den nachgelagerten Verordnungen hat zur Folge, dass neben dem Bund auch die Kantone und insbesondere die Gemeinden von den Regelungen betroffen sein werden. Die Erarbeitung der Verordnungen und die Konkretisierung ihrer Inhalte müssen demzufolge auf die Bedürfnisse und den Wissensstand der verschiedenen Ebenen Rücksicht nehmen, was bei derart komplexen Vorhaben wie der E-ID ein besonderes Augenmerk erfordert.

Der VZGV begrüsst die angedachte Erweiterung des Kreises der Berechtigten zur Verwendung der Versichertennummer.

Wir danken Ihnen für die Möglichkeit zur Vernehmlassung und bitten Sie, unsere Bemerkungen und Anregungen aufzunehmen und im Rahmen der weiteren Bearbeitung der Vorlage zu berücksichtigen.

Freundliche Grüsse

VZGV

Thomas-Peter Binder
Präsident

Brigit Frick
Ressort Vernehmlassungen

Eidg. Justiz- und
Polizeidepartement EJPD
3003 Bern

2. Juni 2017

Referenz: Thomas Mahrer

Stellungnahme Coop zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit der Stellungnahme zum neuen Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Die Coop-Gruppe, ihre Divisionen und Tochtergesellschaften verzeichnen durchschnittlich über eine Million Kundenkontakte pro Tag, mit zunehmender Häufigkeit nicht mehr nur im stationären Handel, sondern auch online.

Daher begrüsst Coop die Schaffung einer Rechtsgrundlage für den elektronischen Identitätsnachweis auf verschiedenen Sicherheitsniveaus. Dies bringt sowohl den Konsumentinnen und Konsumenten als auch dem Handel zusätzliche Sicherheit und vereinfacht die Interaktion. Zum Vorentwurf des E-ID-Gesetzes bringt Coop folgende Punkte ein:

1. International kompatibles System sicherstellen – kein "Swiss Finish"

Im erläuternden Bericht wird an verschiedenen Stellen erwähnt, dass sich die Vorlage an internationalen Standards orientiert, insbesondere betreffend Einteilung der verschiedenen Sicherheitsniveaus und der damit verbundenen technischen Anforderungen. Coop begrüsst diese Absicht und betont die Wichtigkeit einer konsequenten, vollständigen Angleichung der gesetzlichen und technischen Anforderungen an die EU. Standardisierung und Interoperabilität eines E-ID-Systems dürfen nicht an der Grenze aufhören, da dieses sonst für Schweizer Online-Anbieter zum Wettbewerbsnachteil werden kann. Das E-ID-Gesetz ist daher so auszurichten, dass bei einem künftigen bilateralen Abkommen zwischen der Schweiz und der EU die technischen und organisatorischen Voraussetzungen für eine gegenseitige Anerkennung bereits bestehen.

Auf einen "Swiss Finish" ist daher unbedingt und zwar in jeder Form zu verzichten.

Coop Genossenschaft
Wirtschaftspolitik
Hauptsitz

Thiersteinerallee 14
Postfach 2550
4002 Basel
Schweiz

Tel. +41 61 336 72 52
Mobile +41 79 255 51 35
Fax +41 61 335 80 31
CHE-116.311.185 MWST

Thomas.Mahrer@coop.ch
www.coop.ch
Stellungnahme Coop E-ID-Gesetz

2. Privatwirtschaftliche Identity Provider (IdP) vorsehen

Die angestrebte Aufgabenteilung zwischen Staat und Markt beurteilt Coop ebenfalls positiv. Privatwirtschaftliche Identity Provider (IdP) sind besser in der Lage, der Nachfrage entsprechende Systeme anzubieten und agil auf (technische) Veränderungen zu reagieren. Die staatliche Rolle als Anerkennungsstelle für die IdP sowie als Kontrollinstanz für die vom IdP erhobenen Daten erscheint ebenfalls zweckmässig. Allerdings ist darauf zu achten, dass die Anforderungen für die Anerkennung der IdP nicht zu unnötig hohen Markteintrittshürden führen, welche neue Anbieter faktisch ausschliessen und so das Aufkommen neuer Konzepte verhindern.

3. Flexibilität und Einfachheit gewährleisten

Die neue Gesetzesgrundlage darf keine komplizierten Pflichten für Betreiberinnen von E-ID-verwendenden Diensten vorsehen oder in irgendeiner Weise regulierend in das Vertragsverhältnis zwischen Anbietern von E-ID-Systemen und Betreiberinnen von E-ID-verwendenden Diensten eingreifen. Coop begrüsst in diesem Zusammenhang die schlanke Formulierung des Gesetzesentwurfs und verlangt auch eine entsprechend schlanke Umsetzung auf Verordnungsebene. Wie für die Konsumentinnen und Konsumenten sind auch für die Betreiberinnen die Einfachheit und Flexibilität eines E-ID-Systems entscheidende Voraussetzungen für dessen Nutzung.

4. Obligationenrecht ebenfalls anpassen

Ein E-ID-System muss nicht nur die sichere Identifikation des Gegenübers ermöglichen, sondern den Konsumenten und dem Handel auch die Möglichkeit bieten, sämtliche Verträge online abzuschliessen. Insbesondere der eCommerce kann durch eine ergänzende Revision des Obligationenrechts zusätzlich unterstützt werden, indem die elektronische Übermittlung, die eine dauerhafte Aufzeichnung einer Vereinbarung ermöglicht, mit der heute geforderten Schriftlichkeit gleichgesetzt wird. Dies wäre mindestens für jene Rechtsgeschäfte sinnvoll, für welche in der Praxis häufig dispositiv "Schriftlichkeit" vorgesehen wird, welche jedoch nicht von Gesetzes wegen zwingend der handschriftlichen Unterzeichnung bedürfen.

Coop fordert, dass die entsprechenden Änderungen im Anhang "Änderung weiterer Erlasse" des E-ID-Gesetzes berücksichtigt wird.

5. Gesetzesgrundlage offenlassen für zukünftige Entwicklungen

Insbesondere auf tiefem Sicherheitsniveau sollen zukünftig die Hürden für neue Geschäftsmodelle und Markteintritte tief bleiben. Beispiele hierfür sind die Anbindung von B2C-Lösungen an digitale Zahlungsmittel oder die Übertragung auf bestehende und neue C2C-Geschäftsmodelle (z.B. Plattformen für Gratisinserate). Der Vorentwurf zum E-ID-Gesetz wählt diesbezüglich einen guten, technologieneutralen Regulierungsansatz, muss jedoch auch auf Verordnungsebene und im Vollzug innovationsfreundlich konkretisiert und umgesetzt werden.

Wir danken Ihnen für die Berücksichtigung unserer Argumente.

Freundliche Grüsse

Coop

Reto Conrad
Mitglied der Geschäftsleitung

Thomas Mahrer
Mitglied des Managements

Post CH AG
Corporate Center
Wankdorfallee 4
3030 Bern

Telefon +41 58 386 63 16
Fax +41 58 667 33 73
www.post.ch

C, Wankdorfallee 4, 3030 Bern

Als PDF und Word per E-Mail (copiur@bj.admin.ch)
Eidg. Justiz- und Polizeidepartement EJPD
Frau Simonetta Sommaruga, Bundesrätin

Datum 29. Mai 2017
Ihre Nachricht 23. Februar 2017
Kontaktperson Christoph Stalder
E-Mail christoph.stalder@post.ch
Direktwahl +41 (0)58 386 63 16

Stellungnahme der Schweizerischen Post zum E-ID-Gesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der Vernehmlassung zum neuen E-ID-Gesetz Stellung zu nehmen.

1. Vorbemerkungen

Die Digitalisierung verändert sowohl den Post- wie auch den Finanzmarkt fundamental und führt zu zunehmend individualisierten Bedürfnissen von Kundinnen und Kunden. Dies gilt auch für den an und für sich „physischen Logistikmarkt", welcher durch den zunehmend internationalen Wettbewerb geprägt ist. Gemäss den Strategischen Zielen des Bundesrates für die Schweizerische Post 2017-2020 hat die Post u.a. moderne Kommunikations- und Logistikbedürfnisse abzudecken durch die Entwicklung zeitgemässer Angebote insbesondere im Bereich des Informations- und Datenverkehrs. Entsprechend diesem Auftrag sowie den Bedürfnissen unserer Kunden versteht die Schweizerische Post die digitale Transformation als Teil ihrer Strategie. Unsere Strategie korrespondiert mit der vom Bundesrat verabschiedeten Strategie „Digitale Schweiz". Gemäss dieser Strategie soll sich die Wirtschaft im digitalen Raum möglichst frei entfalten können.

Digitale Identitäten sind ein zentrale Voraussetzung für die digitale Transformation. Der Schweiz fehlt heute eine allgemein akzeptierte und vielfach genutzte digitale Standard-Identität, über die Unternehmen ihre Kunden erkennen und einfach in ihre digitalen Prozesse einbinden können.

Der vorliegende Gesetzesentwurf bietet die Chance, dass sich in der Schweiz auf der Basis hoheitlicher Daten und staatlicher Anerkennungsprozesse einerseits und innovativer Lösungen für digitale Identitäten bestehender Anbieter anderseits ein digitales Pendant zur Identitätskarte etablieren kann.

2. Ausgangslage für die Schweizerische Post

Der Postkonzern hat mit einem Ökosystem für digitale Identitäten in den nachfolgend beschrieben Rollen umfassende Erfahrungen sammeln können.

Die Post hat in der **Rolle als Online-Dienst** (sog. Relaying Party) Bedarf nach Dienstleistungen zur verlässlichen digitalen Identifikation ihrer eigenen Kunden, z.B. für das sichere Login auf ihren Webseiten und Apps. Besonders hohe Anforderungen diesbezüglich beachtet die PostFinance z. B. für Online-Kontoeröffnungen und für das Online-Banking.

Die Post erbringt in der **Rolle als Anbieterin von Online-Dienst-Lösungen** zahlreiche digitale Dienstleistungen für Behörden- und Geschäftskunden, bei denen eine qualitativ hochstehende Identifikation der Endkunden als Grundanforderung teilweise regulatorisch gefordert oder dann von den Kunden ausdrücklich gewünscht wird (z.B. E-Health, E-Voting, elektronische Zustellplattform Incamail, E-Post-Office, Lösungen für qualifizierte elektronische Signaturen usw.).

Im Rahmen des Projekts «SwissID» bündelt die Post ihre Kompetenzen für digitale Identitäten in der SwissSign AG – mit dem Ziel, diese digitale Identität für alle Anwender der Schweiz aufzubauen. An der SwissSign AG beteiligt sind die Post und die SBB. Die SwissSign evaluiert die Positionierung ihrer digitalen Identität als E-ID und dementsprechend eine **Rolle als Identity Provider** (IdP). In der Post stehen ferner Dienstleistungen wie die Gelbe Identifikation oder Video-Identifikation (ID-Check Video) in einem thematischen Zusammenhang zur IdP-Rolle.

Die Post hat im Rahmen der vorliegenden Stellungnahme ihre von unterschiedlichen Rollen geprägten Interessen konsolidiert und mit ihren Partnern und Verbänden abgestimmt.

3. Grundsätzliches zum Entwurf

Die Erfolgsfaktoren für eine vom Anwender akzeptierte digitale Identität sind die Vertrauenswürdigkeit des Systems, die vollumfängliche Einhaltung des Datenschutzes sowie die Einsetzbarkeit der digitalen Identität in allen Aspekten des digitalen Lebens.

Den Ansatz durch **Kombination hoheitlicher Daten und staatlicher Anerkennungsprozesse** einerseits und **innovativer Identitätslösungen privater Anbieter** anderseits für die Öffentlichkeit Mehrwerte zu schaffen, beurteilen wir als vorteilhaft und als geeignete Basis für eine weite Verbreitung und Akzeptanz digitaler Identitäten, selbst wenn andere Ansätze auch für die Post denkbar sind. **Die im Vorentwurf definierte Aufgabenteilung zwischen Staat und Markt, wonach der Staat die Personenidentifizierungsdaten herausgibt und die vom Staat anerkannten IdP diese nutzbar machen, wird damit ausdrücklich begrüsst**. Die Harmonisierung unterschiedlicher Anerkennungssysteme ist für die Post als Anbieterin von Vertrauensdiensten ein wichtiges Anliegen, das im E-ID-Gesetz und vor allem auch darüber hinaus vom Gesetzgeber konsequent verfolgt werden sollte.

Für den Erfolg des im Vorentwurf gewählten Ansatzes möchten wir die nachfolgenden Punkte zu bedenken geben. Wo der Vorentwurf diesen unseres Erachtens noch nicht angemessen Rechnung trägt, macht diese Stellungnahme im Anhang konkrete Anpassungsvorschläge.

a. **Bürgerinnen und Bürger stehen im Zentrum:** Diese wollen mit einer einzigen Identität kommerzielle und behördliche digitale Prozesse nutzen.
b. **Beantragung der E-ID:** Pro Jahr werden 500’000 Pässe und 750’000 Identitätskarten erstellt resp. erneuert. Die Beantragung und Ausstellung der E-ID muss im Rahmen der staatlichen Ausweis-Ausstellungsprozesse einfach möglich sein. Zudem soll die Beantragung direkt bei einem IdP möglich sein.

c. **Beitrag des Staates als Vertrauensbasis:** Die Verwendung der Identitätsdaten aus den hoheitlich geführten Registern vermittelt der staatlichen Identitätsstelle garantiert eine sehr hohe Datenqualität und begünstigt die Akzeptanz der E-ID. Mit den staatlichen Anerkennungsprozessen wird sichergestellt, dass nur geeignete und vertrauenswürdige Anbieter von Identitätsdienstleistungen Zugang zu den Registerdaten erhalten. Durch die Einbindung der E-ID Ausstellung in die staatlichen Ausweis-Ausstellungsprozesse wird das Vertrauen zudem gestärkt. Die zentrale Vertrauensfunktion des Staates bei der E-ID ist unseres Erachtens deshalb im Gesetz klarer zu definieren und ihm die Rolle der „Herausgabe der elektronischen Identifizierungseinheit" zuzuweisen.

d. **Private E-ID Aussteller als vertrauenswürdige Partner:** Die Ausstellung der E-ID durch verschiedene vom Staat anerkannte Anbieter von Identitätsdienstleistungen, die mit einander im Wettbewerb stehen, fördert die Entwicklung innovativer anwendungsfreundlicher Lösungen. Die Bürgerinnen und Bürger können den Anbieter ihres Vertrauens aussuchen. Aus dem Einsatz der einzelnen E-ID fallen nicht an einer einzigen Stelle Nutzungsdaten an, was zusätzlich vertrauensfördernd wirkt.

e. **Keine Gebührenfinanzierung:** Mit einer staatlich anerkannten E-ID können Bund, Kantone und Gemeinden bei ihren E-Government-Prozessen profitieren und Kosten einsparen. Gebühren für Erstbestätigung und Aktualisierung verteuern die Gestehungskosten der IdP. Sie haben erhebliche negative Auswirkungen auf deren Business-Case. Die IdP sind durch die Kosten der Umsetzung der gesetzlichen Vorgaben bereits stark belastet. Der Aufbau und Betrieb der staatlichen Identitätsstelle soll deshalb durch den Bund finanziert werden und auf die Transaktionsgebühr ist zu verzichten. Ansonsten werden die Digitalisierungsgewinne an breiter Front durch die Einführung eines Gebührensystems für verhältnismässig kleine zentralen Aufwände der Identitätsstelle wieder gefährdet.

f. **Aktualisierung der Personenidentifizierungsdaten:** Die Qualität der E-ID hängt stark von der Aktualität der Personenidentifizierungsdaten und von einer bedarfsgerechten Aktualisierung ab. Die geplanten Gebühren erhöhen jedoch die Hürde für Aktualisierungen und sind damit ungünstig für eine den Publikumserwartungen angemessene Dienstleistungsqualität. Auf die Gebühren ist deshalb zu verzichten. Die regelmässige Aktualisierung von stabilen Daten erscheint zudem nicht als zweckmässig. Das Aktualisierungsziel kann genauso gut mit einer bedarfsgerechten Aktualisierung auf der Basis von erkannten Risiken erreicht werden, d.h. jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID. Gesetzestechnisch scheint es uns ausreichend, im Gesetz eine bedarfsgerechte Aktualisierung vorzuschreiben und die Detailregelung den Ausführungsbestimmungen (Verordnung, TAV) zu überlassen.

g. **Universelle Akzeptanz bei allen Behörden in der Schweiz:** Für E-ID-Inhaber und die Betreiber von E-ID-verwendenden Diensten („Betreiber", „Dienste") nimmt der Nutzen einer E-ID mit der zunehmenden Anzahl von anderen Inhabern und Betreibern bzw. Diensten (sog. Netzwerkeffekt) zu. Die Öffentlichkeit erwartet universelle Einsatzmöglichkeiten auf allen Ebenen des Gemeinwesens, insbesondere für E-Government, E-Health und E-Voting und zwar unabhängig davon, ob Bundesrecht, kantonales oder kommunales Recht vollzogen wird. Das E-ID Gesetz sollte deshalb eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz im Behördenumfeld. Falls auf eine zentrale Akzeptanznorm im E-ID-Gesetz zu Gunsten von punktuellen Akzeptanznormen, verstreut über die ganze Rechtsordnung verzichtet werden sollte, ist ein besonderes Augenmerk auf die Lückenlosigkeit zu legen. Namentlich sollte unseres Erachtens die E-ID bei den folgenden Erlassen als Referenz für elektronische Identitäten und deren Sicherheitsniveaus dienen: EPDG, ZertES, VEleS, FMG, div. Finanzmarktregulierungen, VeÜ-ZSSV, VeÜ-VwV.

h. **Keine Spezial-E-ID:** Ausserhalb des E-ID Gesetzes haben sich die Anwendungsgesetze auf die Bezeichnung der geforderten Sicherheitsniveaus zu beschränken. Auf zusätzliche Anforderungen z.B. für E-Government, E-Voting, E-Health, E-Banking und E-Commerce ist unter allen Umständen zu verzichten.

i. **Einführung bei Kantonen und Gemeinden:** Wichtige elektronische Dienste, die die elektronische Identität nutzen werden, sind die unzähligen virtuellen Schalter der Kantone und der Gemeinden. Um eine rasche und breite Ausbreitung in den Kantonen zu fördern, muss die universelle Akzeptanz gesetzlich verankert werden. Zu prüfen sind ferner ein nationales Einführungsprojekt verbunden mit einer Anschubfinanzierung .
j. **Interoperabilität der IdP:** Im Zusammenhang mit der geforderten Interoperabilität der E-ID-Systeme unterschiedlicher IdP ist unbedingt die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer Roaming-Gebühr zu regeln. Andernfalls droht eine Diskriminierung von IdP mit grossen E-ID-Stamm. Zur Interoperabilität namentlich betreffend technische Spezifikationen und die finanzielle Abgeltung soll der Bund realisierbare Regeln zusammen mit den Betroffenen in den Ausführungsbestimmungen festlegen.
k. **Internationale Interoperabilität:** Im vorliegenden Entwurf ist die internationale Interoperabilität und gegenseitige staatliche Anerkennung kein Thema. Diese Lücke sollte geschlossen werden. Die Regelung in Art. 20 ZertES kann als Vorbild dienen.
l. **Harmonisierung Anerkennungssysteme:** Die anerkannten Anbieter von Identitätsdienstleistungen sind sogenannte Trust Service Provider („TSP") im Sinne der eIDAS-Verordnung. In der Schweizer Rechtsordnung bestehen für verschiedene TSP unterschiedliche Anerkennungssysteme (z.B. für qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, E-Health, E-Voting usw.). Ohne harmonisierte Anerkennungssysteme drohen Ineffizienzen und Widersprüche. Eine Harmonisierung der Anerkennungssysteme und der entsprechenden Anerkennungsvoraussetzungen über alle TSP-Angebote hinweg ist aus unserer Sicht deshalb angezeigt. Dabei ist darauf zu achten, dass einer internationalen gegenseitigen Anerkennung (z.B. eIDAS) nichts im Wege steht.

Wir bedanken uns für Ihre Kenntnisnahme und wohlwollende Prüfung der Eingabe. Sehr gerne unterstützen wir Sie im Rahmen des weiteren Gesetzgebungsprozesses und bieten eine aktive Mitarbeit beispielsweise in einer vom Bund einzusetzenden Expertenkommission ausdrücklich an.

Freundliche Grüsse

Post CH AG
Corporate Center

Markus Schumacher
Leiter

Katrin Nussbaumer
Leiterin Regulation

Beilage: Anhang Stellungnahme im Einzelnen

Anhang

Zur Stellungnahme der Schweizerischen Post zum E-ID-Gesetz vom 29. Mai 2017

Bezogen auf unseren gesetzlichen Auftrag sowie unsere Tätigkeiten möchten wir zu den folgenden Artikeln aus Sicht der Schweizerischen Post **im Einzelnen** wie folgt Stellung beziehen.

Art. 1 VE E-ID-Gesetz: Gegenstand und Zweck

- *Abs. 1*

Die Reihenfolge a., c., b., d. wäre sinnvoller, um inhaltliche Themen näher zusammen zu rücken

- *Abs. 1 lit. a.*

Die Verwendung der E-ID zu regeln, wird begrüsst. Das Gesetz sollte in einer zentralen Akzeptanznorm die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennen. Siehe zu Art. Stellungnahme, Ziffer 3.

- *Abs. 1 lit. e. (neu)*

Nebst der Rolle der IdP (lit. b), der Inhaberinnen und Inhaber der E-ID (lit. c) und der Betreiberinnen von E-ID-verwendenden Diensten (lit. d) ist zusätzlich die Rolle des Bundes als Herausgeber der elektronischen Identifizierungseinheiten zu beschreiben und der Begriff „herausgeben" im E-ID Gesetz entsprechend zu verwenden:

> „e. die Rechte und Pflichten des Bundes als Herausgeber der elektronischen Identifizierungseinheiten sowie als Träger der Identitäts- und Anerkennungsstelle."

- *Abs. 2 Ziff. lit. a.*

Damit B2B, B2C,G2B und G2C ermöglich wird, schlagen wir folgende Änderung vor:

> „den sicheren elektronischen Geschäftsverkehr unter Privaten, unter Behörden und zwischen Privaten und Behörden zu fördern; und"

- *Abs. 2 Ziff. lit. b.*

Wir sind der Ansicht, dass der Begriff Interoperabilität sich auf eine Internationale Interoperabilität beziehen soll (Bsp. STORK). Siehe Stellungnahme zu Art. 18.

Art. 2 VE E-ID-Gesetz: Begriffe

Der Begriff „Identitätsstelle" sollte bereits bei den Legaldefinitionen aufgenommen werden unter klarer Bezeichnung Hinweis auf deren Rolle als Herausgeber der elektronischen Identifizierungseinheiten.

> „b. (neu) Identitätsstelle: Schweizerischen Stelle für elektronische Identität mit der Rolle als Herausgeber der elektronischen Identifizierungseinheiten;"

Art. 3 VE E-ID-Gesetz: Persönliche Voraussetzungen

- *Abs. 1*

Nicht geregelt ist, ob ein Anspruch auf eine E-ID besteht (vgl. Art. 1 Abs. 1 Ausweisgesetz). Gegen einen „Kontrahierungszwang" sprechen die geplante Pluralität von IdP und die beim IdP in jedem Fall (auch ohne Gebühren) anfallenden Kosten. Für einen „Kontrahierungszwang" spricht die zunehmende Bedeutung zu elektronischen Diensten und die Verhinderung der digital divide. Im Falle eines Kontrahierungszwanges im Sinne eines Service Public muss eine angemessene Abgeltung der dadurch entstehenden Kosten durch die öffentliche Hand vorgesehen werden.

- *Abs. 2*

Im Interesse eines möglichst niederschwelligen und diskriminierungsfreien Zuganges zur E-ID und den über dies zugänglichen elektronischen Behördenleistungen sollte der Bundesrat die Möglichkeit erhalten, in Abs. 1 nicht genannte Kategorien von in- und ausländischen Ausweisen zu bestimmen, die zur Ausstellung einer E-ID berechtigen.

Art. 4 VE E-ID-Gesetz: Anerkennung von IdP

Die Anerkennungsvoraussetzungen für IdP, für anerkannten Zertifizierungsdienstanbieter (ZertES), für anerkannte Zustellplattformen und für zertifizierte Gemeinschaften (EPDG) weichen jeweils voneinander ab. Die Gemeinsamkeiten der genannten Stellen rechtfertigen eine Harmonisierung der materiellen und formellen Anerkennungsvoraussetzungen; zusätzliche Voraussetzungen je Trust Service bleibt Platz, dort wo zwingend sachlich erforderlich. Das europäische eIDAS System spricht generell von Trust Service Providern und harmonisiert die Anforderungen an diese. Bezüglich den Anforderungen an die Anerkennung ist eine Synchronisierung über alle TSP-Angebote (z.B. Qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, usw.) auch deshalb sicherzustellen, damit einer internationale gegenseitigen Anerkennung (insbesondere im eIDAS Raum) nichts im Wege steht.

- *Abs. 3*

Es ist unklar, ob und wie die Pflicht zur 3-jährlichen Erneuerung die Onlinedienste beeinflusst. Was geschieht namentlich, wenn die Anerkennung des IdP nicht erneuert wird? Was geschieht dann mit den E-ID Daten der Kunden? Müssen sich die Kunden alle neu identifizieren?

Art. 5 VE E-ID-Gesetz: Sicherheitsniveaus

- *Abs. 1*

Es ist sinnvoll die Namensgebung der eIDAS Verordnung zu verwenden, obwohl diese eher nicht ohne Weiteres verständlich ist. Für den Erfolg dieses Gesetzes ist es zentral, dass diese Sicherheitsniveaus klar definiert werden und in den darauf referenzierenden Gesetzen genutzt werden.

- *Abs. 2*

In den Artikeln 6 ff. wird detailliert aufgezeigt, wie sich die verschiedenen Sicherheitsniveaus unterscheiden. Der Abs. 2 bringt keinen Mehrwert. Wir empfehlen daher diesen Absatz zu streichen.

Art. 6 VE E-ID-Gesetz: Ausstellungsprozess

Dieser Text erscheint uns als unklar und nicht verständlich. Des Weiteren sind wir der Ansicht, dass man im Gesetz nicht den Prozess mit seinen Schritten definieren soll, sondern die zentralen Anforderungen an diesen. Dabei soll auch die Möglichkeit gegeben werden den Entwicklungen und Erfahrungen diesbezüglich Rechnung zu tragen.

Wenn man aber zum Schluss kommt, dass der Prozess unbedingt beschrieben werden muss, schlagen wir folgende Änderungen vor:

„1 Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP oder bei einer Ausweise gemäss Art. 3 ausstellenden Behörde.
2 Der IdP oder die Ausweise gemäss Art. 3 ausstellende Behörde überprüft die persönlichen Voraussetzungen der Person, die einen Antrag auf Ausstellung einer E-ID stellt.
3 Der IdP beantragt bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) als Herausgeber der elektronischen Identifizierungseinheiten mit dem Einverständnis der antragstellenden Person die Übermittlung der Personenidentifizierungsdaten nach Artikel 7 Absätze 1 und 2.
4 Der IdP ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person.
5 Die Identitätsstelle protokolliert die Datenübermittlungen."

Art. 7 VE E-ID-Gesetz: Personenidentifizierungsdaten

- *Abs. 2*

Der Heimartort kann z.B. für Auslandschweizer sehr bedeutsame sein, z.B. für Abstimmungen und Wahlen. Er sollte deshalb aufgeführt werden.

- *Abs. 2 lit. a. Versichertennummer*

Die Zuordnung der AHVN13 wird zur Kenntnis genommen. Zur Verwendung der Nummer siehe Stellungnahme zu Art. 9.

Art. 8 VE E-ID-Gesetz: Aktualisierung der Personenidentifizierungsdaten

- *Abs. 1*

Die regelmässige Aktualisierung von stabilen Daten erscheint nicht als zweckmässig. Das Aktualisierungsziel kann genauso gut mit einer bedarfsgerechten Aktualisierung auf der Basis von erkannten Risiken erreicht werden, d.h. jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID. Wir würden eine Formulierung bevorzugen, in der die Gültigkeits-und Nutzungsdauer der Personenidentifizierungsdaten im Fokus stehen, so das Abfragen nur notwendig werden, wenn die E-ID auch genutzt wird.

Gesetzestechnisch genügte es, die Aktualisierungsfrequenz in den Ausführungsbestimmungen (Verordnung, technischen und administrativen Vorschriften) zu regeln.

„**Art. 8** ~~Aktualisierung~~ Abfrage der Personenidentifizierungsdaten

1 Zum Zeitpunkt der Nutzung der E-ID fragt der IdP ~~Der IdP aktualisiert die von ihm geführten Personenidentifizierungsdaten durch eine automatisierte Abfrage anhand der E-ID-Registriernummer~~ bei der Identitätsstelle die von ihre geführten Personenidentifizierungsdaten ab. ~~mindestens wie folgt:~~
~~a. für E-ID des Sicherheitsniveaus niedrig: jährlich;~~
~~b. für E-ID des Sicherheitsniveaus substanziell: quartalsweise;~~
~~c. für E-ID des Sicherheitsniveaus hoch: wöchentlich.~~
2 Er ist verantwortlich, dass von ihm ausgestellte E-ID umgehend gesperrt oder widerrufen werden, wenn die E-ID-Registrierungsnummer nicht mehr verwendet werden darf. (Anm. Übersetzung: Er sperrt oder widerruft …)"

Art. 9 VE E-ID-Gesetz: Systematische Verwendung der Versichertennummer zum Datenaustausch

In der Gesamtrechtsordnung ist ein konsistenter Umgang mit der AHVN13 erwünscht. Das ATSG erlaubt die Verwendung nur sehr restriktiv. Insbesondere das EPDG hat die Verwendung von Versichertennummer verboten, aber eine E-ID ist definiert. Daher gilt es hier darauf zu achten, dass keine Inkompatibilität entsteht, die dann die Nutzung der E-ID für Patientendossiers erschwert.

Art. 10 VE E-ID-Gesetz: Datenbearbeitung und Datenweitergabe

Die Restriktionen gemäss Abs. 1, 2 und 3 widersprechen sich teilweise. Unklar ist insbesondere, 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.

Bei der DSG Revision sind zahlreiche Fragen offen und mit einer vom VE in wesentlichen Punkten abweichende Schlussfassung muss gerechnet werden. Dem Ergebnis der Revision des DSG ist bei der Schlussfassung des Art. 10 angemessen Rechnung zu tragen.

Art. 11 VE E-ID-Gesetz: Erlöschen der Anerkennung

Da der Betrieb eines IdP privatrechtlich organisiert wird, ist es sinnvoll das Thema Geschäftsaufgabe zu klären. Dabei wichtig erscheint uns auch die gewollten Auswirkungen auf die eID Inhaber und Relaying-Party zu betrachten inkl. deren Pflichten und Rechte. So stellen sich dabei folgende Fragen: Was geschieht mit den E-ID Daten der Kunden, die im System der Relaying Party verwendet werden? Müssen sich alle Kunden neu identifizieren?

Angezeigt wäre daher eine gesetzliche Regelung, welche IdP verpflichtet, Inhaberinnen und Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc" (gegen entsprechende Entschädigung durch den Bund) zu übernehmen. Will der Gesetzgeber nicht so weit gehen, ist auf Gesetzesebene mindestens sicherzustellen, dass von der Geschäftsaufgabe eines IdP betroffene Inhaberinnen und Inhaber einer E-ID von anderen IdP eine E-ID ausgestellt erhalten, ohne den gesamten Ausstellungsprozess gemäss Art. 6 VE E-ID-Gesetz erneut durchlaufen zu müssen.

Art. 16 VE E-ID-Gesetz: Behörden als Betreiberinnen von E-ID-verwendenden Diensten

Für E-ID-Inhaber und Relaying Parties nimmt der Nutzen einer E-ID zu mit der zunehmenden Anzahl von anderen Inhabern und Relaying Parties/Anwendungsfällen zu (Netzwerkeffekt). Beim Einsatz der E-ID im Behördenumfeld setzt dies die flächendeckende Harmonisierung der betreffenden Gesetze voraus. Das Publikum erwartet universelle Einsatzmöglichkeiten insbesondere für E-Government, E-Health und E-Voting. Das E-ID Gesetz sollte eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz.

Art. 16 wird im Grundsatz begrüsst. Zur besseren Positionierung als universelle Akzeptanznorm schlagen wir folgende Änderung vor:

> „Jede E-ID, die das geforderte Sicherheitsniveau erfüllt, ist für sämtliche elektronischen Identifizierungen im Rahmen der Kommunikation mit Behörden des Bundes, der Kantone und der Gemeinden sowie mit Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht der Verwaltung angehören, und mit Verwaltungsaufgaben betraut sind, akzeptiert."

Art. 17 VE E-ID-Gesetz: Pflichten

- *Abs. 1 lit. e*

Das Wort „periodisch" soll weggelassen oder durch „ordnungsgemäss" ersetzt werden. Siehe Stellungnahme zu Art. 8 VE E-ID-Gesetz.

- *Abs. 1 lit. g*

Die Anforderung beeinflusst die vom IdP eingesetzten Verrechnungsmodelle und ist mit den zivilrechtlichen Verjährungsfristen nicht abgestimmt. Es stellt sich ferner die Frage, wie nach dem Löschen der Daten über die Anwendung eine E-ID ein Missbrauch nachgewiesen werden kann.

Art. 18 VE E-ID-Gesetz: Interoperabilität

Als Voraussetzung für eine funktionierende Interoperabilität müssen neben den technischen Fragen sowohl die Haftungsfrage als auch die Finanzierung geklärt sein. Die Gebühren für Aktualisierungen bei den Identitätsstellen können ein Fehlanreiz sein, bei der Promotion der E-ID Systeme der Anwendung (Einnahmen) vor der Ausstellung (Kosten) Vorrang zu geben und über die Interoperabilität von IdP Anbietern mit einer grosser Basis ausgestellter E-ID zu profitieren. Jedenfalls ist die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer Roaming Gebühr unbedingt zu regeln. Andernfalls droht eine Diskriminierung von IdP mit grossen E-ID Stamm. Zur Interoperabilität namentlich betreffend technische Spezifikationen und die finanzielle Abgeltung soll der Bund mit den potentiellen IdP und anderen Stakeholdern möglichst früh den Dialog suchen. Realisierbare Regeln für Interoperabilität sind dann in den Ausführungsbestimmungen fest zu legen.

*Des Weiteren wäre es sinnvoll die **internationale** Interoperabilität ebenfalls zu beachten und z.B. den Aufbau und Betrieb von STORK Servern durch den Bund vorzuschreiben.*

Art. 19 VE E-ID-Gesetz: Organisation

Die Art. 19 und 21 bezeichnen zwei unterschiedliche Departement (EDF, EJPD). Es fehlen Regeln zur Koordination zwischen Identitätsstelle und Anerkennungsstelle.

Art. 21 VE E-ID-Gesetz: Zuständigkeit

Im allgemeinen siehe Stellungnahme zu Art. 19 VE E-ID-Gesetz.

- *Abs. 1*

Abs. 1 sollte zu einer Delegationsnorm umgestaltet werden und der Bundesrat ermächtigt werden, die Zuständigkeiten betreffend die Anerkennungsstelle zu bestimmen. Dies vereinfacht die Zuständigkeiten und Aufsichten für die verschiedenen Trust Service Provider zu harmonisieren. Die bisher unterschiedlichen Zuständigkeiten für die verschiedenen Trust Service Provider (ZertES: SAS, SECO; Zustellplattform: BJ, EJPD; Patientendossier: BAG) sind ineffizient und stehen dem Erfolg der einzelnen Services im Weg. Insbesondere auch im Zusammenhang mit den Identitäten für das Patientendossier sind zwei Zuständigkeiten/Anerkennungen unnötig kompliziert, kostspielig und ohne Mehrwert. Im EPDG wird die Anerkennung der Identität für die Nutzung des Patientendossiers vom BAG (EDI) wahrgenommen. Eine gemäss E-ID anerkannte Identität muss ohne zusätzliche Aufwände für Anbieter vom BAG anerkannt werden.

Art. 23 VE E-ID-Gesetz:

Der Aufbau und Betrieb der staatlichen Identitätsstelle soll durch den Bund finanziert werden. Auf die Gebühren für die Dienstleistungen der Identitätsstelle ist zu verzichten. Die Daten der Identitätsstelle sollen den IdP kostenlos zur Verfügung stehen.

Art. 24 VE E-ID-Gesetz:

Die Vorschriften zur Haftung geben wieder, was ohnehin gilt. Das Haftungsregime für die verschiedenen TSP sollte harmonisiert werden. Dabei ist zu beachten, dass nicht Haftungsvorschriften zu einem Standortnachteil für Schweizer Akteure führt.

Art. 25 VE E-ID-Gesetz: Änderung anderer Erlasse

Neben einer universellen Akzeptanznorm ist es sinnvoll, im Minimum für die folgenden Gesetze die E-ID ausdrücklich als Referenz für elektronische Identitäten und deren Sicherheitsniveaus zu verankern: EPDG, ZertES, VEleS, FMG, div. Finanzmarktregulierungen, VeÜ-ZSSV, VeÜ-VwV usw..

Anhang Änderung anderer Erlasse, Ziffer 3.

Bundesgesetz vom 20. Dezember 194614 über die Alters- und Hinterlassenenversicherung:

Um die Bekanntgabe der AHVN13 zu ermöglichen, genügte eine auf dieses Datum beschränkte Norm. Der neue Artikel 50a AHVG schränkt die Daten lediglich über das unscharfe und schwer zu handhabende Kriterium des „überwiegenden Privatinteresses" ein.

Anhang Änderung anderer Erlasse, Ziffer 4.

Bundesgesetz vom 18. März 2016 über die elektronische Signatur

Sinnvollerweise wird das Sicherheitsniveau bezeichnet. Das Niveau sollte so gewählt werden, dass mit einer zu niedrigen EID (UserName/Password) kein qualifiziertes Zertifikat ausgestellt werden kann.

SBB CFF FFS

Konzernleitung · Hilfikerstrasse 1 · 3000 Bern 65

Eidgenössisches Justiz- und
Polizeidepartement
Bundeshaus West
3003 Bern

Per E-Mail an: copiur@bj.admin.ch

Bern, 24. Mai 2017

Vernehmlassung zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) – Stellungnahme der SBB

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit, im Rahmen der Vernehmlassung zum Vorentwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung nehmen zu können.

1. Vorbemerkungen

Die SBB und die Schweizerische Post bieten über ihre gemeinsame Tochtergesellschaft SwissSign AG interessierten Unternehmen und Behörden unter dem Namen SwissID eine schweizweite einheitliche digitale Identität an, welche das Abwickeln von Online-Geschäften einfacher und sicherer macht. Anwender können mit der SwissID künftig über ein sicheres Login auf verschiedene Online-Dienste zugreifen, anstatt eine Vielzahl von Benutzernamen und Passwörtern zu verwenden und sich dabei unnötigen Sicherheitsrisiken auszusetzen. Eine einheitliche Identität ist ein zentraler Meilenstein für die weitere Digitalisierung in der Schweiz, deren Nutzen Gesellschaft, Wirtschaft und Behörden gleichermassen zugutekommt.

Die SwissSign AG evaluiert die Positionierung ihrer digitalen Identität als E-ID und entsprechend eine Rolle als Identity Provider (IdP) im Sinne des Vorentwurfs zum E-ID-Gesetz. Ausserdem prüft die SBB, zukünftig als Betreiberin von E-ID-verwendenden Diensten aufzutreten.

2. Kernanliegen zum Gesetz

- **Die SBB begrüsst die Schaffung eines E-ID-Gesetzes**: Die Etablierung von digitalen Identitäten setzt klare rechtliche und organisatorische Rahmenbedingungen für die Anerkennung von elektronischen Identifizierungsmitteln voraus. Die Erfolgsfaktoren für eine vom Anwender akzeptierte digitale Identität sind die Vertrauenswürdigkeit des Systems, die vollumfängliche Einhaltung des Datenschutzes sowie die Einsetzbarkeit der digitalen Identität in allen Aspekten des digitalen Lebens.

- **Es bedarf einer umfassenden Anerkennung der E-ID im Behördenkontext**: Statt punktueller Akzeptanznormen in verschiedenen Gesetzen ist eine zentrale Akzeptanznorm im E-ID-Gesetz zu schaffen, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange anerkennt. Es ist zu prüfen, ob für die rasche und breite Einführung der E-ID in den Kantonen und Gemeinden ein nationales Einführungsprojekt und eine Anschubfinanzierung notwendig ist.

- **Die SBB erachtet eine Aufgabenteilung zwischen Staat und Markt als richtig**: Das Konzept, wonach der Staat die Personenidentifizierungsdaten herausgibt und die vom Staat anerkannten IdP (Markt) diese nutzbar machen, hat gegenüber einer staatlich ausgestellten E-ID klare Vorteile: Potentielle Inhaber einer E-ID müssen einen konkreten Nutzen in der Anwendung der E-ID sowohl im kommerziellen Bereich als auch im Behördenkontext sehen. *Eine Verbreitung der E-ID wird nur erreicht durch eine Kombination einer staatlich herausgegebenen* elektronischen Identifizierungseinheit mit kommerziellen Identifizierungsmitteln, wie beispielsweise dem SwissPass. Mit diesem Ansatz entstehen zudem innovative und anwenderfreundliche Lösungen, welche den Grundstein für die Verbreitung der E-ID in Bevölkerung, Wirtschaft und Verwaltung legen. Schliesslich kann der Markt rascher und flexibler auf technologische Entwicklungen und sich ändernde Kundenbedürfnisse reagieren als der Staat.

- **Die Rollen sind klar zu definieren**: Gemäss dem Vorentwurf besteht die Rolle des Staates darin, die elektronische Identifizierungseinheit (verstanden als Einheit von staatlichen Personenidentifizierungsdaten) herauszugeben. Demgegenüber hat der private IdP die Aufgabe, die elektronische Identifizierungseinheit mit Zustimmung der Inhaber nutzbar zu machen, d.h. sie mit der digitalen Identität des Nutzers zu verknüpfen und den Betreiberinnen von E-ID-verwendenden Diensten zur Verfügung zu stellen (vgl. Anhang 1: Grafik Begriffe). In diesem Sinne ist der IdP Aussteller der E-ID. Um Unklarheiten zu vermeiden, sollte der Gesetzgeber sowohl die Rolle des Staates und der IdP als auch die Begriffe „Herausgabe der elektronischen Identifizierungseinheit" und „Ausstellung der E-ID" klar definieren.

- **Der Anwendernutzen muss im Zentrum stehen und bestehende Prozesse sind zu nutzen**: Die Akzeptanz der digitalen Identität und deren Verbreitung hängt massgeblich davon ab, ob die Ausstellung anwenderfreundlich ausgestaltet und mit geringem Aufwand erhältlich ist. Nebst der Ausstellung der E-ID durch IdP (Art. 6) sind deshalb auch die bestehenden staatlichen Prozesse zur Beantragung von physischen Ausweisen zu nutzen: Bei jährlich rund 500'000 bzw. 750'000 ausgestellten Pässen und Identitätskarten[1] sowie Ausländerausweisen drängt es sich zur Vermeidung von Doppelspurigkeiten auf, die bei der Ausstellung der physischen Ausweise erfolgte Identitätsprüfung auch für einen leichten Zugang zur E-ID zu nutzen.

  Die staatlichen Prozesse sind so zu ergänzen, dass die einen Ausweis gemäss Art. 3 Antrag stellende Person in den kantonalen Passstellen und regionalen Erfassungszentren gleichzeitig und zusätzlich zur Identitätskarte oder dem Pass die Erstellung der E-ID beantragen kann. Beantragt sie diese, stellt ihr die Behörde einen Nachweis der Identifizierung gemäss Art. 6 Abs. 2 aus (Onboarding-Dokument). Diese Bestätigung erlaubt es dem IdP, ohne zusätzliche Überprüfung der persönlichen Voraussetzungen bei der Identitätsstelle die Übermittlung der Personenidentifizierungsdaten zu beantragen und diese Daten der E-ID und die E-ID dem Antragsteller zuzuordnen (vgl. Anhang 2: Prozess Ausweisausstellung). Die vorgeschlagene Lösung hat den Vorteil, dass die Behörden lediglich ihre Prozesse minimal ergänzen müssen sowie die IdP und die Antragsteller auf einen aufwändigen Identifizierungsschritt verzichten können, der keinen zusätzlichen Nutzen bringt. Abgesehen davon, dass die Gesamtsystemkosten der E-ID sinken, dürfte die Bereitschaft der Nutzer höher sein, im Rahmen des ordentlichen Ausweisantragsverfahren auch eine E-ID zu beantragen, als wenn sie dazu eine zusätzliche Identifizierung vornehmen lassen müssen. 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 Datenabfrage soll zum Zeitpunkt der Nutzung der E-ID erfolgen**: Die vorgesehene periodische Aktualisierung der Personenidentifizierungsdaten lehnen wir ab, weil bei den in Art. 8 enthaltenen Aktualisierungsvorgaben bis zu einem Jahr alte Daten verwendet würden. Stattdessen ist eine Regelung vorzusehen, wonach die IdP die Daten bei der Identifizierungsstelle ausschliesslich zum Zeitpunkt der Nutzung der E-ID abfragen. Mit dieser Lösung können sich nicht nur Inhaber der E-ID und Betreiberinnen von E-ID-verwendenden Diensten stets auf aktuelle Personenidentifizierungsdaten verlassen, sondern es werden auch unnötige Datenabfragen vermieden.

- **Auf eine Gebühr für die Datenübermittlung ist zu verzichten**: Die in Art. 23 Abs. 1 vorgesehene Gebühr für die Datenübermittlung zwischen der Identitätsstelle und dem IdP lehnen wir ab. Die Bereitstellung aktueller Personenidentifizierungsdaten ist eine staatliche Aufgabe, die aus den allgemeinen Steuereinahmen zu finanzieren und nicht vom IdP zu tra-

[1] Quelle: https://www.schweizerpass.admin.ch/pass/de/home/aktuell/news/2011/ref_2011-12-16.html.

gen ist. Wir beantragen deshalb, dass der Bund den Aufbau und Betrieb der Identitätsstelle finanziert und die Daten den IdP kostenlos zur Verfügung stellt. Dies auch deshalb, weil der Bund indirekt von der Verbreitung und Verwendung der E-ID profitiert und am Digitalisierungsgewinn partizipiert. Wird dem Antrag auf Gebührenverzicht nicht stattgegeben, ist zumindest eine Gleichbehandlung zwischen privatwirtschaftlichen IdP und solchen der öffentlichen Hand sicherzustellen.

- **Klare Regeln zur nationalen und internationalen Interoperabilität sind nötig**: Schliesslich vermissen wir im Gesetzesentwurf klare Regeln zur Interoperabilität. Einerseits fehlt die internationale Interoperabilität von staatlich anerkannten ausländischen digitalen Identitäten. Zur Schliessung dieser Lücke sollte die Regelung in Art. 20 des Bundesgesetzes über die elektronische Signatur, ZertES, als Vorbild dienen. Andererseits müssen bei der Interoperabilität zwischen den inländischen IdP neben den technischen Fragen auch die Haftungsfragen geklärt werden. Um eine Diskriminierung von IdP mit einem grossen E-ID-Stamm zu verhindern, ist in den Ausführungsbestimmungen ausserdem die finanzielle Abgeltung (Roaming Gebühr) zwischen den Beteiligten zu regeln. Der Bund soll zur Klärung dieser offenen Fragen möglichst rasch den Dialog mit potentiellen IdP und anderen Stakeholdern suchen.

Wir bitten Sie, unsere Kommentare und Anträge (vgl. Anhang 3: Änderungsanträge) zum Vorentwurf im Rahmen der Vernehmlassung zu berücksichtigen. Gerne bieten wir unsere konstruktive Mitarbeit in einer allfälligen Expertenkommission an.

Freundliche Grüsse

Peter Kummer

Mitglied Konzernleitung SBB AG
Leiter Informatik und Chief Information Officer

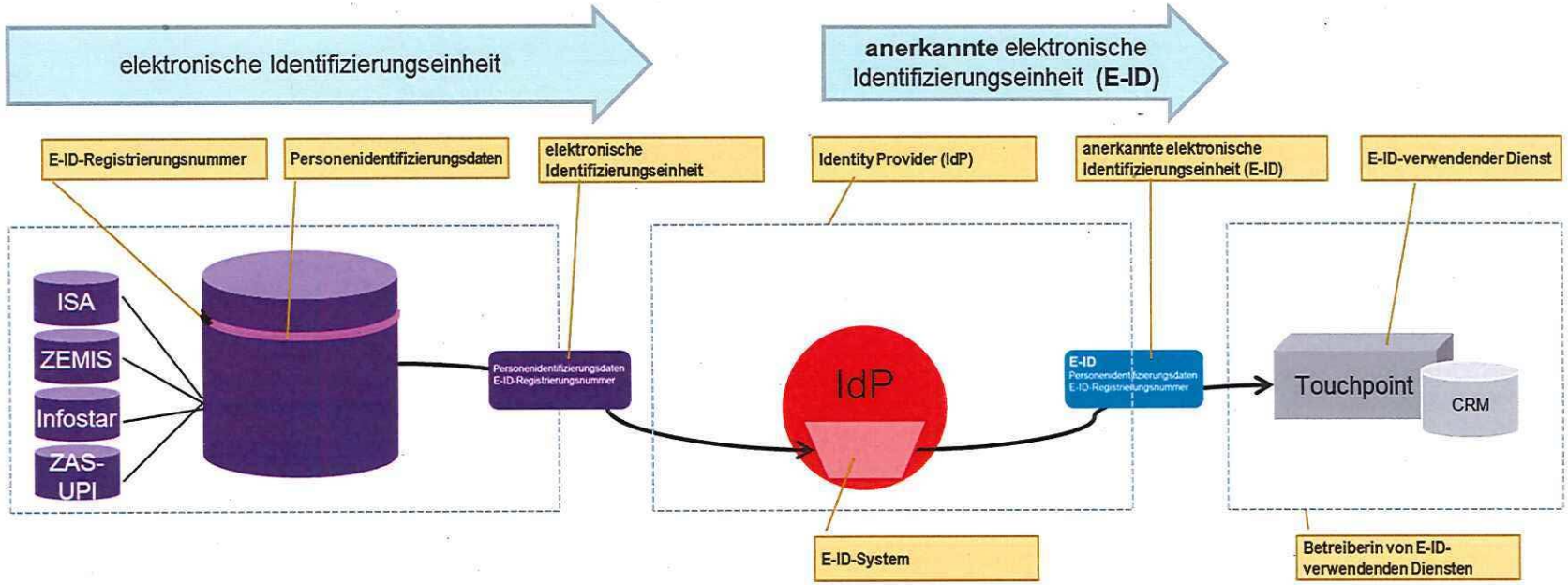
Dr. Kathrin Amacker

Mitglied Konzernleitung SBB AG
Leiterin Kommunikation

Anhang:
-Anhang 1: Grafik Begriffe
-Anhang 2: Grafik Prozess Ausweisausstellung
-Anhang 3: Änderungsanträge

SBB CFF FFS

Anhang 1: Grafik Begriffe



Herausgeber (Identitätsstelle)
- «Herausgeber der elektronischen Identifizierungseinheit»

Anerkannter Aussteller (IdP)
- «Aussteller der anerkannten elektronischen Identifizierungseinheit (E-ID)»
- «Aussteller der E-ID»
- Staatlich selektierter und überwachter IdP

Onlinedienstanbieter (Betreiberin von E-ID verwendender Dienst)

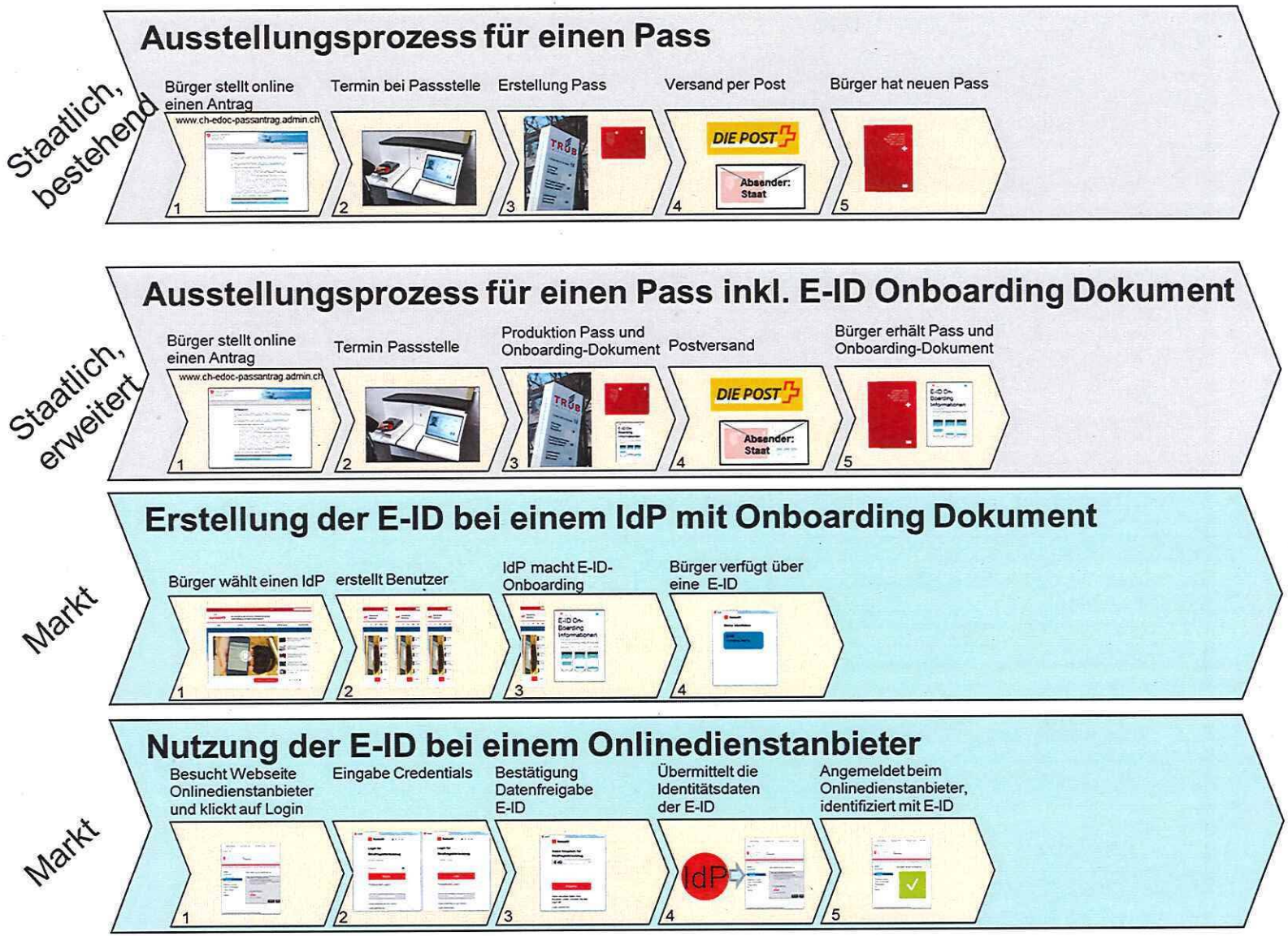
Staat

Markt

Staat

Markt

Anhang 2: Prozess Ausweisausstellung



Anhang 3: Änderungsanträge

Art. 1 Gegenstand und Zweck	
• Abs. 1 lit. e (neu)	Nebst der Rolle der IdP (lit. b), der Inhaber der E-ID (lit. c) und der Betreiberinnen von E-ID-verwendenden Diensten (lit. d) ist 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."*
• Abs. 2 lit. a	Damit B2B, B2C,G2B und G2C ermöglicht wird, schlagen wir die folgende Ergänzung vor: *„den sicheren elektronischen Geschäftsverkehr unter Privaten, unter Behörden und zwischen Privaten und Behörden zu fördern; und"*
• Abs. 2 lit. b	Wir sind der Ansicht, dass sich der Begriff Interoperabilität auf eine Internationale Interoperabilität beziehen soll (Bsp. STORK). Siehe unsere Ausführungen zu Art. 18.
• Abs. 2 lit. c (neu)	Als weiterer Zweck des Gesetzes ist die Aufgabenteilung zwischen Behörden und IdP zu nennen: *„die Aufgabeteilung zwischen Behörden und IdP klar zu regeln."*
Art. 2 Begriffe	
Anhang 1 unserer Stellungnahme bildet den Prozess der staatlichen Herausgabe einer elektronischen Identifizierungseinheit sowie der Ausstellung einer anerkannten elektronischen Identifizierungseinheit (E-ID) durch den IdP ab. Wir regen an, die Begriffe in Art. 2 in der Reihenfolge der Prozessschritte zu definieren. Ausserdem sind gewisse Definitionen zum besseren Verständnis zu ergänzen. Schliesslich sollte auch der Begriff „Identitätsstelle" definiert werden: • Personenidentifizierungsdaten: staatlich geführter Datensatz, der es ermöglicht, die Identität einer Person festzustellen; • E-ID-Registrierungsnummer: einer Person eindeutig zugeordnete Identifikationsnummer; • elektronische Identifizierungseinheit: eine elektronische Einheit, bestehend aus E-ID-Registriernummer und den Personenidentifizierungsdaten, die zur Identifizierung und Authentifizierung einer natürlichen Person verwendet wird; • Identitätsstelle: Herausgeber der elektronischen Identifizierungseinheiten;	

- Identity Provider (IdP): nach diesem Gesetz anerkannter Anbieter von Identitätsdienstleistungen;
- E-ID-System: elektronisches System für die Ausstellung, Verwaltung und Anwendung von E-ID als Bestandteil des IdPs;
- anerkannte elektronische Identifizierungseinheit (E-ID): eine elektronische Identifizierungseinheit, die von einem IdP nach den Vorgaben dieses Gesetzes ausgestellt wird;
- Betreiberin von E-ID-verwendenden Diensten: natürliche oder juristische Person, die für ihre Tätigkeit Online-Dienste betreibt, die Vertrauen in die Identität der sie nutzenden Person und in deren Authentizität voraussetzen;
- E-ID-verwendender Dienst: eine Informatikanwendung, die ein E-ID-System nutzt.
- Identifizierung: Prozess der Nutzung von Personenidentifizierungsdaten, die eine Person eindeutig repräsentieren;
- Authentifizierung: Prozess der Überprüfung einer behaupteten Identität;

Art. 3 Persönliche Voraussetzungen

• Abs. 1	*Der Vorentwurf sieht keinen Kontrahierungszwang für IdP vor. Falls dieser im Rahmen der Vernehmlassung gefordert werden sollte, muss eine angemessene Abgeltung der dadurch entstehenden Kosten durch die öffentliche Hand vorgesehen werden.*
• Abs. 2	Um einen möglichst niederschwelligen und diskriminierungsfreien Zugang zur E-ID und den über diese zugänglichen elektronischen Behördenleistungen zu gewähren, ist der Anwenderkreis möglichst breit zu fassen. Zu denken ist beispielsweise an ausländische Eigentümer von Grundstücken in der Schweiz, die eine elektronischen Identität zum Ausfüllen der Steuerklärung verwenden oder Touristen, die ihre elektronische Identität im Bereich E-Health oder für touristische Zwecke einsetzen möchten.

Art. 4 Anerkennung von IdP

Die Anerkennungsvoraussetzungen für IdP, für anerkannte Zertifizierungsdienstanbieter (ZertES), für anerkannte Zustellplattformen und für zertifizierte Gemeinschaften (EPDG) weichen jeweils voneinander ab. Die Gemeinsamkeiten der genannten Stellen rechtfertigen eine Harmonisierung der materiellen und formellen Anerkennungsvoraussetzungen. Wo dies sachlich erforderlich ist, bleibt für zusätzliche Voraussetzungen je Trust Service Platz. Das europäische eIDAS System spricht generell von Trust Service Providern und harmonisiert die Anforderungen an diese. Bezüglich den Anforderungen an die Anerkennung ist eine Synchronisierung über alle Trust Service Provider- (TSP) Angebote (z.B. Qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, usw.) auch deshalb sicherzustellen, damit einer internationalen gegenseitigen Anerkennung (insbesondere im eIDAS Raum) nichts im Wege steht. Aktuell bestehen für verschiedene TSP unterschiedliche Anerkennungssysteme (z.B. für qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, E-Health, E-Voting usw.). Dies ist ineffizient und kann zu Widersprüchen

führen. Eine Harmonisierung der Anerkennungssysteme und der entsprechenden Anerkennungsvoraussetzungen über alle TSP-Angebote hinweg tut Not. Wichtig erscheint uns dabei, dass einer internationalen gegenseitigen Anerkennung (z.B. eIDAS) nichts im Wege steht.	
• Abs. 3	Es ist unklar, ob und wie die Pflicht zur dreijährlichen Erneuerung der Anerkennung die Onlinedienste beeinflusst. Namentlich zu regeln ist, was bei einer Nichterneuerung mit den im System der Betreiberin von E-ID-verwendenden Diensten enthaltenen Daten geschieht und ob sich alle Kunden neu identifizieren lassen müssen.
Art. 5 Sicherheitsniveaus	
• Abs. 1	Obwohl die Namensgebung der eIDAS Verordnung nicht ohne weiteres verständlich ist, ist es sinnvoll, die Namensgebung der eIDAS Verordnung zu verwenden. Für den Erfolg des E-ID-Gesetzes ist es zentral, dass die Sicherheitsniveaus klar definiert und in den darauf referenzierenden Gesetzen genutzt werden.
• Abs. 2	In den Art. 6 ff. wird detailliert aufgezeigt, wie sich die verschiedenen Sicherheitsniveaus unterscheiden. Abs. 2 bringt keinen Mehrwert, weshalb wir anregen, diesen Absatz zu streichen.
Art. 6 Ausstellungsprozess	
Um den Entwicklungen und Erfahrungen Rechnung tragen zu können, sollte der Gesetzgeber den Ausstellungsprozess nicht auf Gesetzesstufe detaillieren, sondern lediglich die zentralen Anforderungen an diesen nennen. Falls der Prozess trotzdem beschrieben werden soll, schlagen wir zur Vereinfachung die folgenden Änderungen für Abs. 1 bis 4 vor:	
• Abs. 1	*Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP oder bei einer Ausweise gemäss Art. 3 ausstellenden Behörde.*
• Abs. 2	*Der IdP oder die Ausweise gemäss Art. 3 ausstellende Behörde überprüft die persönlichen Voraussetzungen der Person, die einen Antrag auf Ausstellung einer E-ID stellt.*
• Abs. 3	*Der IdP beantragt bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) mit dem Einverständnis der antragstellenden Person die Übermittlung der Personenidentifizierungsdaten nach Art. 7 Abs. 1 und 2.*

• Abs. 4	*Der IdP ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person.*
Art. 7 Personenidentifizierungsdaten	
• Abs. 2	Der Heimartort kann beispielsweise für Auslandschweizer bei Abstimmungen und Wahlen sehr bedeutsam sein und sollte deshalb in der Liste der zusätzlichen Personenidentifizierungsdaten ebenfalls aufgeführt werden.
• Abs. 2 lit. a.	Die Zuordnung der AHVN13 nehmen wir zur Kenntnis. Zur Verwendung der Versichertennummer siehe unsere Ausführungen zu Art. 9.
Art. 8 Aktualisierung der Personenidentifizierungsdaten	
Die regelmässige Aktualisierung von stabilen Daten erscheint unzweckmässig. Das Aktualisierungsziel kann ebenso gut mit einer bedarfsgerechten Aktualisierung auf der Basis von erkannten Risiken erreicht werden, d.h. jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID. Bevorzugt wird eine Formulierung, bei der die Gültigkeits-und Nutzungsdauer der Personenidentifizierungsdaten im Fokus steht, so dass Abfragen nur notwendig werden, wenn die E-ID tatsächlich genutzt wird. Davon abgesehen, dass die Aktualisierungsfrequenz in den Ausführungsbestimmungen geregelt werden könnte, regen wir an, die Überschrift sowie Abs. 1 wie folgt zu ändern:	
• Titel	*~~Aktualisierung~~ Abfrage der Personenidentifizierungsdaten*
• Abs. 1	*Zum Zeitpunkt der Nutzung der E-ID fragt der IdP ~~Der IdP aktualisiert die von ihm geführten Personenidentifizierungsdaten durch eine automatisierte Abfrage anhand der E-ID-Registriernummer~~ bei der Identitätsstelle die von ihr geführten Personenidentifizierungsdaten ab. ~~mindestens wie folgt:~~* *~~a. für E-ID des Sicherheitsniveaus niedrig:jährlich;~~* *~~b. für E-ID des Sicherheitsniveaus substanziell: quartalsweise;~~* *~~c. für E-ID des Sicherheitsniveaus hoch: wöchentlich.~~*
Art. 9 Systematische Verwendung der Versichertennummer zum Datenaustausch	
In der Gesamtrechtsordnung ist ein konsistenter Umgang mit der AHVN13 erwünscht. Das ATSG erlaubt die Verwendung der Versichertennummer nur sehr restriktiv. Insbesondere das EPDG hat deren Verwendung verboten, aber eine E-ID ist definiert. Es gilt hier darauf zu achten, dass keine Inkompatibilität ent-	

steht, die die Nutzung der E-ID für Patientendossiers nicht erlaubt.
Art. 10 Datenbearbeitung und Datenweitergabe
Die Restriktionen gemäss Abs. 1, 2 und 3 widersprechen sich teilweise. Unklar ist insbesondere, 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 Absätze 1, 2 und 3 sollten besser aufeinander *abgestimmt und präzisiert werden.* Bei der Revision des DSG sind zahlreiche Fragen offen. Es muss mit einer vom Vorentwurf in wesentlichen Punkten abweichenden Schlussfassung gerechnet werden. Dem Ergebnis der Revision des DSG ist bei der Schlussfassung von Art. 10 angemessen Rechnung zu tragen.
Art. 11 Erlöschen der Anerkennung
Da der Betrieb eines IdP privatrechtlich organisiert wird, ist es sinnvoll, das Thema Geschäftsaufgabe zu klären. Wichtig erscheint uns, auch die gewollten Auswirkungen auf die Inhaber der E-ID und Betreiberinnen von E-ID-verwendenden Diensten zu betrachten, inkl. deren Rechte und Pflichten. Namentlich ist zu regeln, was mit den im System der Betreiberin verwendeten Daten geschieht und ob sich alle Kunden neu identifizieren lassen müssen. Angezeigt wäre eine gesetzliche Regelung, welche IdP verpflichtet, Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc" (gegen entsprechende Entschädigung durch den Bund) zu übernehmen. Will der Gesetzgeber nicht so weit gehen, ist auf Gesetzesebene mindestens sicherzustellen, dass von der Geschäftsaufgabe eines IdP betroffene Inhaber einer E-ID von anderen IdP eine E-ID ausgestellt erhalten, ohne den gesamten Ausstellungsprozess gemäss Art. 6 erneut durchlaufen zu müssen.
Art. 13 Subsidiäres E-ID-System des Bundes
Da im Vorentwurf der Begriff „Herausgabe" im Zusammenhang mit elektronischen Identifizierungseinheiten und „Ausstellung" mit E-ID verwendet wird, sollte Art. 13 Abs. 1 wie folgt lauten:

Abs. 1	*„Falls kein IdP für die Ausstellung von E-ID der Sicherheitsniveaus substanziell oder hoch anerkannt ist, kann der Bundesrat eine Verwaltungseinheit bezeichnen, die für die Bedürfnisse von Behörden ein E-ID-System betreibt und E-ID ~~herausgibt~~ausstellt."*

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

Für E-ID-Inhaber und Betreiberinnen von E-ID-verwendenden Diensten nimmt der Nutzen einer E-ID mit der zunehmenden Anzahl von anderen Inhabern und Betreiberinnen/Anwendungsfällen zu (Netzwerkeffekt). Beim Einsatz der E-ID im Behördenumfeld setzt dies die flächendeckende Harmonisierung der betreffenden Gesetze voraus. Das Publikum erwartet universelle Einsatzmöglichkeiten, insbesondere für E-Commerce, E-Government, E-Health und E-Voting. Das E-ID Gesetz sollte eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz.

Art. 16 wird im Grundsatz begrüsst. Allerdings regen wir an, eine zentrale Akzeptanznorm zu schaffen, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange anerkennt.

• Art. 16	*Jede E-ID, die das geforderte Sicherheitsniveau erfüllt, ist für sämtliche elektronischen Identifizierungen im Rahmen der Kommunikation mit Behörden des Bundes, der Kantone und der Gemeinden sowie mit Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht der Verwaltung angehören und mit Verwaltungsaufgaben betraut sind, akzeptiert.*

Art. 17 Pflichten

• Abs. 1 lit. e	Das Wort „periodisch" soll weggelassen oder durch „ordnungsgemäss" ersetzt werden (siehe oben die Ausführungen zu Art. 8).
• Abs. 1 lit. g	Diese Anforderung beeinflusst die vom IdP eingesetzten Verrechnungsmodelle und ist mit den zivilrechtlichen Verjährungsfristen nicht abgestimmt. Es stellt sich ferner die Frage, wie nach dem Löschen der Daten über die Anwendung eine E-ID ein Missbrauch nachgewiesen werden kann.

Art. 18 Interoperabilität

Eine funktionierende Interoperabilität setzt voraus, dass neben den technischen Fragen auch die Haftungsfrage und Finanzierungsfragen geklärt sind. Die in Art. 23 vorgesehenen Gebühren für die Aktualisierungen bei den Identitätsstellen (Art. 8) können insofern ein Fehlanreiz sein, als IdP bei der Promotion der E-ID Systeme der Anwendung (Einnahmen) vor der Ausstellung (Kosten) Vorrang zu geben und über die Interoperabilität von IdP Anbietern mit einer grosser Basis ausgestellter E-ID zu profitieren. Jedenfalls ist die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer Roaming Gebühr unbedingt zu regeln.

Andernfalls droht eine Diskriminierung von IdP, die über einen grossen E-ID Stamm verfügen. Des Weiteren wäre es sinnvoll, die internationale Interoperabilität ebenfalls zu beachten und z.B. den Aufbau und *Betrieb von STORK Servern durch den Bund vorzuschreiben.*	
Art. 19 Organisation	
Da in Art. 19 und Art. 21 zwei unterschiedliche Departemente (EDF und EJPD) bezeichnet werden, regen wir an, Regeln zur Koordination zwischen der Identitätsstelle und der Anerkennungsstelle zu schaffen.	
Art. 21 Zuständigkeit	
Im Allgemeinen siehe unsere Ausführungen zu Art. 19.	
• Abs. 1	Abs. 1 sollte zu einer Delegationsnorm umgestaltet und der Bundesrat ermächtigt werden, die Zuständigkeiten betreffend die Anerkennungsstelle zu bestimmen. Dies vereinfacht die Zuständigkeiten und Aufsichten für die verschiedenen Trust Service Provider zu harmonisieren. Die bisher unterschiedlichen Zuständigkeiten für die verschiedenen Trust Service Provider (ZertES: SAS, SECO; Zustellplattform: BJ, EJPD; Patientendossier: BAG) sind ineffizient und stehen dem Erfolg der einzelnen Services im Weg. Insbesondere auch im Zusammenhang mit den Identitäten für das Patientendossier sind zwei Zuständigkeiten/Anerkennungen unnötig kompliziert, kostspielig und ohne Mehrwert. Im EPDG wird die Anerkennung der Identität für die Nutzung des Patientendossiers vom BAG (EDI) wahrgenommen. Eine gemäss E-ID anerkannte Identität muss ohne zusätzliche Aufwände für Anbieter vom BAG anerkannt werden.
Art. 23 Gebühren	
Der Aufbau und Betrieb der staatlichen Identitätsstelle soll durch den Bund finanziert werden. Auf die Gebühren für die Dienstleistungen der Identitätsstelle ist zu verzichten. Die Daten der Identitätsstelle sollen den IdP kostenlos zur Verfügung stehen (vgl. dazu die Ausführungen in unserer Stellungnahme).	
Art. 25 Änderung anderer Erlasse	
Neben einer universellen Akzeptanznorm ist es sinnvoll, im Minimum für die folgenden Gesetze die E-ID ausdrücklich als Referenz für elektronische Identitäten und deren Sicherheitsniveaus zu verankern (EPDG, ZertES, VEleS , diverse Finanzmarktregulierungen, VeÜ-ZSSV VeÜ-VwV, VeÜ-ZSSV, usw.).	

Anhang Änderung anderer Erlasse
3. Bundesgesetz vom 20. Dezember 194614 über die Alters- und Hinterlassenenversicherung
Um die Bekanntgabe der AHVN13 zu ermöglichen, genügt eine auf dieses Datum beschränkte Norm. Der neue Artikel 50a AHVG schränkt die Daten lediglich über das unscharfe und schwer zu handhabende Kriterium des „überwiegenden Privatinteresses" ein.
4. Bundesgesetz vom 18. März 2016 über die elektronische Signatur
Sinnvollerweise wird das Sicherheitsniveau bezeichnet. Das Niveau sollte so gewählt werden, dass mit einer zu niedrigen E-ID (UserName/Password) kein qualifiziertes Zertifikat ausgestellt werden kann.

swisscom

Swisscom (Schweiz) AG, Konzernrechtsdienst, 3050 Bern

Per E-Mail an:
copiur@bj.admin.ch

Zu Handen:
Frau Bundesrätin Sommaruga
Eidgenössisches Justiz- und
Polizeidepartement EJPD

Datum	24. Mai 2017	**Seite**
Ihr Kontakt	Stéphane Vaucher / 058 221 03 95 / stephane.vaucher@swisscom.com	1 von 5
Thema	**Stellungnahme zum Vorentwurf des E-ID-Gesetzes**	

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Vielen Dank für die Einladung vom 23. März 2017 und die Möglichkeit, im Vernehmlassungsverfahren zum Entwurf des Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) Stellung zu nehmen.

Auch für Swisscom ist die digitale Identität ein wichtiges, ungelöstes Thema ist. Nach wie vor ist es ein dringendes Anliegen, eine elektronische Identifizierungseinheit mit breiter Akzeptanz einsetzen zu können. Swisscom ist überzeugt, dass der Erfolg der E-ID in der Schweiz von drei Faktoren abhängt:

- das Erlangen der E-ID muss so einfach wie möglich sein,
- die Verwendung der E-ID muss bei wenigen, jedoch weit verbreiteten Services zwingend sein und
- die Umsetzung muss schnell erfolgen.

1. Grundsätzliches

Unabhängig vom E-ID-Gesetz arbeiten verschiedene Branchen an Lösungen rund um die digitale Identität. Es wird das Ziel verfolgt, ein elektronisches Identifizierungsmittel zu schaffen, mit dem die Identität einer natürlichen Person in digitalisierten Prozessen ausgewiesen und geprüft werden kann – ähnlich wie dies mit dem klassischen Vorweisen des herkömmlichen Identitätsdokuments bei physischer Präsenz gemacht wird. Es zeichnet sich ab, dass die Lösungen der Privatwirtschaft nicht Jahre auf die Schaffung einer staatlichen E-ID werden warten können. Auch deshalb erachtet es Swisscom als wichtig, diese beiden Sphären – Staat und Markt – bei der E-ID zusammen zu halten und künftig näher zusammen zu bringen.

Swisscom (Schweiz) AG
Konzernrechtsdienst
Postfach, 3050 Bern

Standortadresse
Alte Tiefenaustrasse 6
3048 Worblaufen

Swisscom unterstützt deshalb nach wie vor das im Vorentwurf gewählte Modell mit der Aufgabenteilung zwischen Staat und Markt. Hierbei sieht Swisscom die folgenden Punkte als entscheidend für den Erfolg der E-ID gemäss dem Grundmodell des Vorentwurfs:

- Erstens muss sichergestellt sein, dass die E-ID bei deren Inhaberin oder dessen Inhaber und den E-ID-verwendenden Diensten grosse Akzeptanz findet. Hierfür ist eine grosse Verbreitung auch durch den Bund sicherzustellen. Weiter müssen Einfachheit, Vertrauen, Sicherheit, Datenschutz und ein finanziell interessantes Angebot garantiert sein.
- Soll dem Markt eine wichtige Rolle zur Gestaltung der Umsetzung der E-ID zukommen, muss zweitens den Anbietern aus der Wirtschaft (insbesondere den IdP) ermöglicht werden, interessante Anwendungen anzubieten.

Swisscom ist der Ansicht, dass beide Punkte bei Umsetzung der E-ID gemäss aktuellem Vorentwurf nur teilweise gewährleistet wären (vgl. hierzu die Ziffern 2 und 3 nachfolgend). Allerdings ist Swisscom nicht der Ansicht, dass die Schwachstellen des aktuellen Vorentwurfs nur dann beseitigt werden können, wenn auf ein anderes Modell (z.B. mit direkter Herausgabe der elektronischen Identifizierungseinheiten durch den Bund) ausgewichen würde.

Zum Vorentwurf abweichende Grundmodelle, wie sie in den informellen Konsultationen zur Rede standen und kürzlich von verschiedenen Verbänden wieder thematisiert wurden, enthalten sicherlich auch interessante Punkte. Auch diese Modelle könnten grundsätzlich erfolgreich sein, da hauptsächlich die konkrete Umsetzung des jeweiligen Modells entscheidend ist für dessen Erfolg. Allerdings hätte der Wechsel des Grundmodells mit hoher Wahrscheinlichkeit auch eine wesentliche Verzögerung zur Folge – eine rasche Einführung der staatlich anerkannten E-ID könnte dadurch erheblich erschwert werden.

Eine weitere Verzögerung der Einführung einer staatlichen E-ID vergrössert die Wahrscheinlichkeit, dass die vom Markt lancierten digitalen Identifizierungsmittel sich später nicht mehr mit der staatlichen E-ID verbinden lassen. Würden die digitalen Identifizierungsmittel des Markts breite Akzeptanz finden, bevor die staatlich anerkannte E-ID lanciert wird, bestünde für die E-ID eine zusätzliche Hürde: Elektronische Identifizierungsmittel der Privatwirtschaft und des Bundes würden sich konkurrenzieren. In dieser Situation wäre der Mehrwert der staatlich anerkannten E-ID im Bereich des eCommerce nicht mehr klar, da die Bedürfnisse bereits abgedeckt sein könnten durch die Lösung des Markts. Andererseits könnten die digitalen Identifizierungsmittel der Privatwirtschaft mangels staatlicher Anerkennung nicht (ohne Weiteres) für Anwendungen im staatlichen Umfeld ("eGov") verwendet werden und auch die Kompatibilität mit internationalen Standards (insbesondere mit der eIDAS-Verordnung) wäre nicht sichergestellt.

Swisscom befürwortet deshalb die Weiterverfolgung des Modells mit der Aufgabenteilung zwischen Staat und Markt.

2. Risiken und Verbesserungsvorschläge aus Sicht Swisscom

Das Modell des Vorentwurfs enthält Risiken, die dazu führen könnten, dass sich die staatlich anerkannte E-ID nicht etabliert. Das Risiko, dass sich kein IdP staatlich anerkennen lässt, wurde bereits im Konzept 2016 benannt (Konzept 2016, S. 61, Risiko "NUL"). Dieses Risiko ist nicht von der Hand zu weisen, insbesondere wenn der Mehrwert der staatlich anerkannten E-ID im Vergleich zu nicht staatlich anerkannten digitalen Identitätseinheiten für Inhaberinnen und Inhaber einer E-ID, IdP, und E-ID-verwendende Dienste nicht erkennbar ist. Um diesem Risiko entgegen zu wirken, sollten aus Sicht Swisscom die folgenden Punkte berücksichtigt werden:

a) Förderung der Verbreitung bereits bei der gemäss Art. 3 VE Ausweise ausstellenden Behörde

Das Modell des Vorentwurfs macht es nötig, dass die Personen gemäss Art. 3 VE bei einem anerkannten IdP vorstellig werden, um eine E-ID zu erhalten. Dieser Schritt zur Identifizierung durch den IdP ist eine grosse Hürde und stellt die grösste Gefahr dar, dass die Personen gemäss Art. 3 VE gar nicht erst versuchen werden, sich um eine E-ID zu bemühen. Der Prozess der persönlichen Vorsprache bei den Behörden zur Ausstellung der Ausweise gemäss Art. 3 VE sollte deshalb konkrete Schritte zur Förderung der E-ID enthalten. Es sollte dort eine konkrete Verknüpfung zur E-ID gemacht werden. Den Personen gemäss Art. 3 VE muss klar sein, dass es eine E-ID gibt und wie diese beschafft werden kann, bevor sie mit einem IdP Kontakt haben.

Es braucht deshalb aktive Information an die Personen gemäss Art. 3 VE, z.B. durch Abgabe eines vorausgefüllten (elektronischen) Formulars für das Einverständnis in die Übermittlung der Daten gemäss Art. 6 VE. Den Personen gemäss Art. 3 VE muss klar sein, welcher Schritt konkret nach Verlassen der gemäss Art. 3 VE Ausweise ausstellenden Behörde unternommen werden muss, um eine E-ID zu erhalten und sie müssen wissen, wozu die E-ID im privaten und staatlichen Umfeld verwendet werden kann und welches die Vorteile der E-ID sind. Sicherlich muss vermieden werden, dass eine antragstellende Person sich selbst Informationen beschaffen muss, um die Funktionsweise der E-ID zu verstehen. Aus Sicht Swisscom ist weiter zur Förderung der Verbreitung der E-ID in Art. 6 VE die alternative Möglichkeit aufzunehmen, dass der Antrag zur Ausstellung einer E-ID auch bei einer Ausweise gemäss Art. 3 VE ausstellenden Behörde gestellt werden kann, verbunden mit der Pflicht der Behörde, die persönlichen Voraussetzungen der antragstellenden Person zu prüfen.

Zur Verwirklichung der Strategie „Digitale Schweiz" sieht Swisscom in diesem Punkt eine aktive Aufgabe und Verantwortung beim Bund. Dieser Punkt müsste im Vorentwurf klar aufgenommen und nicht erst auf Verordnungsstufe geregelt werden.

b) Sicherstellen und Förderung der Verbreitung einer einheitlichen Lösung

Einerseits sollte der Bund 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 vorschreiben. Solange die E-ID im digitalen Kanal nur als Option im Raum steht (vgl. Erläuternder Bericht, Ziffer 2.1.1 S. 37), werden die Unsicherheiten rund um das E-ID-Ökosystem vergrössert. Dies wiederum trägt erheblich zur Steigerung des Risikos bei, dass potentielle IdP den Nutzen einer Anerkennung nach dem E-ID-Gesetz nicht sehen. Art. 16 VE sollte entsprechend angepasst werden.

Andererseits müsste auch sichergestellt sein, dass der Bund am Tag des Inkrafttretens des E-ID-Gesetzes an ein anerkanntes E-ID-System eines IdP angeschlossen ist. Ist im Zeitpunkt des Inkrafttretens des E-ID-Gesetzes kein IdP anerkannt worden, müsste der Bundesrat eine Verwaltungseinheit bezeichnen, die für die Bedürfnisse von Behörden ein E-ID-System betreibt und die E-ID herausgibt. Soll die Verbreitung einer einheitlichen Lösung gefördert werden, sollte also aus Sicht Swisscom 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. Die zwingende Ausgestaltung des Art. 13 VE würde dadurch wesentlichen Bedenken der Befürworter des Modells, in welchem der Staat das elektronische Identifizierungsmittel direkt selbst herausgibt, Rechnung tragen. Falls der Markt die staatlich anerkannte E-ID nicht von Anfang an fördert, dann muss 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.

c) Entscheidende Punkte nicht erst in der Verordnung regeln

Der Gesetzesentwurf regelt die Eckpunkte der E-ID und verweist an zahlreichen Stellen auf die Möglichkeit oder die Pflicht des Bundesrates, auf Verordnungsstufe Ausführungsbestimmungen zu erlassen.

Grundsätzlich ist daran natürlich nichts auszusetzen. Bevor die Details zur Regelung der Interoperabilität (Art. 18 VE) und der Gebühren (Art. 23 VE) jedoch nicht hinreichend konkret sind, können potentielle IdP ihre Geschäftsmodelle nur ungenügend ausarbeiten. Dadurch wird auch die Planung von potentiellen E-ID-verwendenden Diensten verzögert. Dies birgt das Risiko, dass zwischen Inkrafttreten des Gesetzes und der Anerkennung von IdP unnötig viel Zeit verstreichen könnte, oder dass sich schlimmstenfalls herausstellt, dass die potentiellen IdP keine rentablen Geschäftsmodelle sehen. Deshalb ist es aus Sicht Swisscom wichtig, frühzeitig Klarheit zu schaffen in Punkten, die finanzielle Entscheide der IdP massgeblich beeinflussen werden.

d) Identitäts-Broker

Die Handhabung der Interoperabilität könnte besonders anspruchsvoll werden, insbesondere auch weil IdP gemäss Art. 7 Abs. 4 VE die Möglichkeit haben, der E-ID weitere Daten zuzuordnen. Der Identitäts-Broker könnte als Bindeglied zwischen den IdP und den E-ID-verwendenden Diensten wirken und dadurch erheblich zur Verbreitung der E-ID beitragen. Im erläuternden Bericht wird zu Art. 18 VE auch festgehalten, dass solche Modelle zur Diskussion gestellt werden sollen. Swisscom ist der Ansicht, dass es sich hierbei um einen wichtigen Punkt handelt, und dass dieser konkreter und frühzeitig angegangen werden muss.

e) ID-Prozess (Art. 5 und Art. 6 VE)

Die Erfahrungen, insbesondere im Bereich der elektronischen Signaturen gemäss ZertES, zeigen, dass die persönliche Vorsprache für den Identifikationsprozess von Konsumenten als sehr hohe Hürde wahrgenommen wird und abschreckend wirkt. Deshalb sollte bereits im Gesetz festgehalten werden, dass Verfahren, die eine gleichwertige Sicherheit zum persönlichen Erscheinen bieten, von IdP verwendet werden können. Als konkretes Beispiel sollte auch das Verfahren mittels audiovisueller Kommunikation in Echtzeit (Videoidentifikation) als Ersatz für das persönliche Erscheinen im Gesetz aufgenommen werden. Hierfür könnte das E-ID-Gesetz die Regelung des Art. 7 Abs. 1 und 2 der Verordnung über die elektronische Signatur (VZertES; SR 943.032) übernehmen.

Damit bereits bezwungene Hürden nicht mehrmals überwunden werden müssen, erscheint es Swisscom zudem als sehr wichtig, dass eine bereits erfolgte Identifikation, die als gleichwertig anzusehen ist, nicht ein zweites Mal durchgeführt werden muss. Im Vorentwurf wird dies im Bereich der elektronischen Signatur konkretisiert mit einer Änderung des ZertES (Anhang Änderung anderer Erlasse; Ziff. 4 ZertES). Analog sollten bereits erfolgte, gleichwertige Identifikationen, z.B. diejenige nach den Regeln des ZertES, auch im Anwendungsbereich des E-ID-Gesetzes verwendet werden können. Für die potentielle Inhaberin einer E-ID bzw. den potentiellen Inhaber einer E-ID stellt dies eine entscheidende Erleichterung des Prozesses dar.

3. Einzelpunkte aus dem Vorentwurf

a) Zu Art. 8 (Aktualisierung der Personenidentifizierungsdaten) und Art. 14 (Pflichten)

Die Pflichten der IdP im Zusammenhang mit der Sperrung oder dem Widerruf von E-ID sind bereits auf Gesetzesstufe, z.B. in Art. 8 VE, klarer zu regeln. Gleichzeitig ist 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.

b) Zu Art. 10 (Datenschutz)

Soweit es um Themen geht, die bereits von den Bestimmungen des Datenschutzgesetzes abgedeckt sind, ist Swisscom der Ansicht, dass auf datenschutzrechtliche Bestimmungen im E-ID-Gesetz zu verzichten ist.

Im Vorentwurf besteht noch Abstimmungsbedarf zwischen Art. 10 und Art. 7 VE. Allgemein wird auch den Bestimmungen des künftigen Datenschutzgesetzes Rechnung zu tragen sein. Zudem sollten unabhängig

vom Sicherheitsniveau mit Einwilligung der betroffenen Person Daten verwendet werden können. Der Absatz 3 sollte deshalb dahingehend geändert werden, dass die Daten nur dann Dritten nicht bekannt gegeben werden dürfen, wenn hierfür keine Zustimmung der Inhaberin oder des Inhabers der E-ID vorliegt.

c) Zu Art. 17 (Pflichten)

Art. 17 Bst. g VE (Löschung Daten nach sechs Monaten) sollte gestrichen werden. Einerseits bestehen teilweise Bestimmungen, die eine längere Aufbewahrung nötig machen und andererseits regelt das Datenschutzgesetz bereits, wann Daten zu löschen sind.

d) Zum Anhang Änderung anderer Erlasse; Ziff. 4 ZertES

Swisscom 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.

e) Allgemein zum Anhang Änderung anderer Erlasse

Die Gesetzgebung des Bundes sieht an verschiedenen Stellen Prozesse vor, in denen die Identität einer natürlichen Person durch persönliches Erscheinen mit Vorweisen eines Ausweisdokuments geprüft werden muss. Wo immer möglich sollten diese Prozesse mit einer digitalisierten Variante mit Einsatz der E-ID ergänzt werden (so wie es der VE bereits im ZertES vorsieht). Swisscom denkt hier beispielsweise an den Prozess zur Erfassung von Personendaten beim Verkauf von SIM-Karten (Art. 19a VÜPF; SR 780.11). Für Inhaberinnen und Inhaber einer E-ID wären solche Erleichterungen der Prozesse bei Beibehaltung der Sicherheit ein wirklicher Gewinn, der die E-ID attraktiv machen würde.

Zusammengefasst begrüsst Swisscom den Vorentwurf grundsätzlich, sieht aber gleichzeitig Verbesserungsbedarf in wichtigen Punkten. Für eine konstruktive Verbesserung des Vorentwurfs schlägt Swisscom deshalb vor, dass eine Expertengruppe eingesetzt werden sollte – basierend auf der Grundidee des Vorentwurfs mit Vertretern des Staats und des Markts. Swisscom würde sich gerne aktiv in dieser Expertengruppe einbringen.

Gerne stehen wir Ihnen zur Erläuterung unserer Sichtweise zur Verfügung. Für die Prüfung unserer Anliegen danken wir Ihnen im Voraus bestens.

Freundliche Grüsse

Swisscom (Schweiz) AG

Patrick Dehmer

General Counsel

Stéphane Vaucher

Senior Counsel

SwissSign

SwissSign AG
Sägereistrasse 25
8152 Glattbrugg
www.swisssign.com

Reinhard Dietrich, COO
reinhard.dietrich@swisssign.com

Per E-Mail (copiur@bj.admin.ch)
Eidg. Justiz- und Polizeidepartement EJPD
Frau Simonetta Sommaruga, Bundesrätin

29. Mai 2017

Stellungnahme der SwissSign AG zum E-ID-Gesetz

Sehr geehrte Frau Bundesrätin Sommaruga
Sehr geehrte Damen und Herren

Wir danken Ihnen bestens für die Gelegenheit, im Rahmen der Vernehmlassung zum neuen E-ID-Gesetz Stellung nehmen zu können.

1. Vorbemerkungen

Die Digitalisierung verändert die Wirtschaft und die Gesellschaft fundamental und führt zunehmend zu individualisierten Bedürfnissen von Kundinnen und Kunden. Dies bedingt zudem Agilität für sämtliche Marktteilnehmer, welche vor allem durch den zunehmend internationalen Wettbewerb beeinflusst wird. Als Joint-Venture der Post und SBB haben wir stets die Kundinnen / Kunden wie auch die Marktteilnehmer im Fokus und bieten Lösungen/Produkte, welche den entsprechenden Kundengruppen den gewünschten Nutzen in der digitalen Welt bringen. Unsere Strategie korrespondiert mit der vom Bundesrat verabschiedeten Strategie „Digitale Schweiz“; gemäss welcher sich die Wirtschaft im digitalen Raum möglichst frei entfalten können soll. Digitale Identitäten sind eine zentrale Voraussetzung für die digitale Transformation. Eine einheitliche Identität ist ein zentraler Meilenstein für die weitere Digitalisierung in der Schweiz, deren Nutzen Gesellschaft, Wirtschaft und Behörden gleichermassen zugute kommt. Der Schweiz fehlt heute noch diese allgemein akzeptierte und vielfach genutzte digitale Standard-Identität, über die Unternehmen ihre Kundinnen und Kunden erkennen und einfach in ihre digitalen Prozesse einbinden können. Ausserdem fehlt den Kundinnen/Kunden eine solche Standard-Identität, um sich einfach in der digitalen Welt auszuweisen zu können.

Der vorliegende Gesetzesentwurf bietet die Chance, dass sich in der Schweiz auf der Basis hoheitlicher Daten und staatlicher Anerkennungsprozesse einerseits und innovativer Lösungen für digitale Identitäten bestehender Anbieter anderseits ein digitales Pendant zur Identitätskarte etablieren kann.

2. Ausgangslage für die SwissSign AG

Marktteilnehmer in der **Rolle als Online-Dienst Anbieter** haben Bedarf nach Dienstleistungen zur verlässlichen digitalen Identifikation ihrer eigenen Kunden, z.B. für das sichere Login auf ihre Webseiten und Apps. Besonders hohe Anforderungen diesbezüglich sind beispielsweise in der Bankenwelt zu beachten (Online-Kontoeröffnungen, Online-Banking).

Die SwissSign AG erbringt heute schon in der **Rolle als Anbieterin von Online-Dienst Lösungen** zahlreiche digitale Dienstleistungen für Behörden- und Geschäftskunden, bei denen eine qualitativ hochstehende Identifikation der Endkunden eine Grundanforderung darstellt, teilweise regulatorisch gefordert oder von den Kunden ausdrücklich gewünscht wird (z.B. Lösungen für qualifizierte elektronische Signaturen).

Im Rahmen des Projekts «SwissID» bündeln die Post und die SBB ihre Kompetenzen für digitale Identitäten in ihrem Joint-Venture SwissSign AG – mit dem Ziel, **die digitale Identität** für alle Anwender der Schweiz aufzubauen. Das Joint-Venture wurde anfangs Mai 2017 gegründet, welches auf der bestehenden SwissSign AG aufbaut und die für Identitäten und Zertifikate relevanten Services einbringt.

Die SwissSign evaluiert die Positionierung ihrer digitalen Identität als E-ID und nimmt dementsprechend die **Rolle als Identity Provider** (IdP) ein.

Die SwissSign AG hat über die letzten Jahre mit einem kontinuierlich weiterentwickelten und optimierten Ökosystem für digitale Identitäten umfassende Erfahrungen gesammelt:

- seit mehr als 7 Jahren hat SwissSign AG Erfahrungen in der **Entwicklung**, im **Betrieb** und **Support** eines IdP im Sinne dieses Gesetzes (Stichwort „SuisseID“);
- SwissSign AG hat enormes Know-How in der Beratung und Unterstützung von Marktteilnehmern, sogenannten Relaying Parties, d.h. als Betreiberin von (potentiell) E-ID-verwendenden Diensten;
- Mitarbeitende der SwissSign AG wie auch Mitarbeitende der Aktionärinnen nutzen bereits die bestehende SuisseID täglich für ihre Arbeit.

In der vorliegenden Stellungnahme hat die SwissSign AG ihre von unterschiedlichen Rollen geprägten Interessen konsolidiert und mit ihren Aktionärinnen, Partnern und Verbänden abgestimmt.

3. Grundsätzliche Anliegen zum Entwurf des E-ID Gesetzes

Den Ansatz durch Kombination hoheitlicher Daten und staatlicher Anerkennungsprozesse einerseits und innovativer Identitätslösungen von privaten Anbietern anderseits für die Öffentlichkeit Mehrwerte zu schaffen, beurteilen wir als vorteilhaft und als geeignete Basis für eine weite Verbreitung und Akzeptanz digitaler Identitäten und somit als grossen Beitrag zur Digitalisierung der Schweiz. Die im Vorentwurf definierte **Aufgabenteilung zwischen Staat und Markt**, wonach private digitale Identitäten dank hoheitlicher Daten und kraft staatlicher Anerkennung zur E-ID werden, wird ausdrücklich begrüsst. Die Harmonisierung unterschiedlicher Anerkennungssysteme ist für SwissSign AG u.a. als Anbieterin von Vertrauensdiensten ein wichtiges Anliegen, das im E-ID Gesetz und vor allem auch darüber hinaus vom Gesetzgeber konsequent verfolgt werden sollte.

Für den Erfolg des im Vorentwurf gewählten Ansatzes und auch mit Blick auf alternative Lösungsansätze möchten wir die nachfolgenden Punkte als Anregung zur Umsetzung eingeben. Wo der Vorentwurf diesen noch nicht angemessen Rechnung trägt, macht diese Stellungnahme im Anhang konkrete Anpassungsvorschläge.

- **Der Kunde/Benutzer resp. Bürger steht im Zentrum:** Dieser will mit einer einzigen Identität kommerzielle sowie behördliche digitale Anwendungen / Prozesse nutzen.

- **Ausstellung der E-ID:** Pro Jahr werden 500'000 Pässe und 750'000 Identitätskarten erstellt resp. erneuert. **Die staatlichen Ausweis-Ausstellungsprozesse** sind der ideale und unverzichtbare Ort, um den Bürgerinnen und Bürgern im Rahmen der Ausweiserstellung und -erneuerung die Ausstellung einer ID einfach zu ermöglichen. Die Ausstellung einer E-ID muss daneben auch direkt bei einem IdP möglich sein.

- **Beitrag des Staates als Vertrauensbasis:** Die Verwendung der Identitätsdaten aus den hoheitlich geführten Registern vermittelt der staatlichen Identitätsstelle garantiert eine sehr hohe Datenqualität und begünstigt die Akzeptanz der E-ID. Mit den staatlichen Anerkennungsprozessen wird sichergestellt, dass nur geeignete und vertrauenswürdige Anbieter von Identitätsdienstleistungen Zugang zu den Registerdaten erhalten. Durch die Einbindung der E-ID Ausstellung in die staatlichen Ausweis-Ausstellungsprozesse wird das Vertrauen zudem gestärkt.

- **Beitrag des Marktes als Vertrauensbasis:** Die Ausstellung der E-ID durch private Anbieter von Identitätsdienstleistungen fördert die Entwicklung innovativer anwendungsfreundlicher Lösungen im Rahmen des Wettbewerbs. Die Bürgerinnen und Bürger können den Anbieter ihres Vertrauens aussuchen. Aus dem Einsatz der einzelnen E-ID fallen nicht an einer einzigen Stelle Nutzungsdaten an, was zusätzlich vertrauensbildend wirkt.

- **Keine Gebührenfinanzierung:** Mit einer staatlich anerkannten E-ID können Bund, Kantone und Gemeinden bei ihren e-Government-Prozessen profitieren und Kosten einsparen. Gebühren für Erstbestätigung und Aktualisierung verteuern die Gestehungskosten der IdP. Sie haben erhebliche negative Auswirkungen auf deren Business-Case. Die IdPs sind durch die Kosten der Umsetzung der gesetzlichen Vorgaben bereits stark belastet. Der Aufbau und Betrieb der staatlichen Identitätsstelle soll durch den Bund vollständig finanziert werden und auf die Transaktionsgebühr ist vollständig zu verzichten. Die Digitalisierungsgewinne an breiter Front dürfen nicht durch die Einführung eines Gebührensystems für verhältnismässig kleine zentrale Aufwände der Identitätsstelle gefährdet werden.

- **Universelle Akzeptanz bei allen Behörden in der Schweiz:** Für E-ID-Inhaber und die Betreiber von E-ID-verwendenden Diensten („Betreiber", „Dienste") nimmt der Nutzen einer E-ID mit der zunehmenden Anzahl von anderen Inhabern und Betreibern bzw. Diensten (sog. Netzwerkeffekt) zu. Die Öffentlichkeit erwartet universelle Einsatzmöglichkeiten auf allen Ebenen des Gemeinwesens, insbesondere für e-Government, e-Health oder e-Voting, unabhängig davon, ob Bundesrecht, kantonales oder kommunales Recht vollzogen wird. Das E-ID Gesetz sollte eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz im Behördenumfeld.

  Beim Verzicht auf eine zentrale Akzeptanznorm im E-ID Gesetz – entgegen unserer Empfehlung – zu Gunsten von punktuellen Akzeptanznormen verstreut über die ganze Rechtsordnung, ist ein besonderes Augenmerk auf die Lückenlosigkeit zu legen. Namentlich muss die E-ID bei den folgenden Erlassen als Referenz für elektronische Identitäten und deren Sicherheitsniveaus dienen: EPDG, ZertES, VEIeS, FMG, div. Finanzmarktregulierungen, VeÜ-ZSSV, VeÜ-VwV usw.

- **Keine Spezial-E-ID:** Ausserhalb des E-ID Gesetzes haben sich die Anwendungsgesetze auf die Bezeichnung der geforderten Sicherheitsniveaus zu beschränken. Auf zusätzliche Anforderungen z.B. für e-Government, e-Voting, e-Health, e-Banking und e-Commerce ist unter allen Umständen zu verzichten.

- **Einführung bei Kantonen und Gemeinden:** Wichtige elektronische Dienste, die die elektronische Identität nutzen werden, sind die unzähligen virtuellen Schalter der Kantone und der Gemeinden. Um eine Ausbreitung in den Kantonen sicherzustellen, muss die universelle Akzeptanz gesetzlich verankert werden. Zudem sollte eine Anschubfinanzierung für die rasche und breite Einführung der E-ID bei Kantonen und Gemeinden vorgesehen werden.

- **Aktualisierung der Personenidentifizierungsdaten:** Die Qualität der E-ID hängt in der Wahrnehmung der Öffentlichkeit stark von der Aktualität der Personenidentifizierungsdaten und von einer bedarfsgerechten Aktualisierung ab. Die geplanten Gebühren reduzieren die Aktualisierung auf ein notwendiges Minimum und sind damit ungünstig – sogar schädlich – für eine den Publikumserwartungen angemessene Dienstleistungsqualität. Auf die Gebühren ist deshalb unbedingt zu verzichten. Die regelmässige Aktualisierung von stabilen Daten erscheint zudem nicht als zweckmässig. Das Aktualisierungsziel kann mit einer bedarfsgerechten Aktualisierung auf der Basis von erkannten Risiken erreicht werden, d.h. jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID. Regulatorisch genügt es, im Gesetz eine bedarfsgerechte Aktualisierung vorzuschreiben und die Detailregelung den Ausführungsbestimmungen (Verordnung, TAV) zu überlassen.

- **Nationale und internationale Interoperabilität:** Interoperabilität der IdP: Im Zusammenhang mit der geforderten Interoperabilität der E-ID-Systeme unterschiedlicher IdP ist unbedingt die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer „Roaming Gebühr“ zu regeln. Andernfalls droht eine Diskriminierung von IdPs mit grossem E-ID Stamm. Bei der Interoperabilität zwischen IdPs müssen neben den technischen Fragen auch die Haftungsfragen geklärt werden.
  Internationale Interoperabilität: Im vorliegenden Entwurf ist die internationale Interoperabilität und gegenseitige staatliche Anerkennung kein Thema. Diese Lücke sollte unbedingt geschlossen werden. Die Regelung in Art. 20 ZertES kann als Vorbild dienen.

- **Harmonisierung Anerkennungssysteme:** Die anerkannten Anbieter von Identitätsdienstleistungen sind sogenannte Trust Service Provider („TSP“) im Sinne der eIDAS-Verordnung. In der Schweizer Rechtsordnung bestehen für verschiedene TSP unterschiedliche Anerkennungssysteme (z.B. für qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP, e-Health, e-Voting usw.). Ohne harmonisierte Anerkennungssysteme drohen Ineffizienzen und Widersprüche. Eine Harmonisierung der Anerkennungssysteme und der entsprechenden Anerkennungsvoraussetzungen über alle TSP-Angebote hinweg ist notwendig. Dabei ist darauf zu achten, dass einer internationalen gegenseitigen Anerkennung (z.B. eIDAS) nichts im Wege steht.

SwissSign

Wir bitten Sie, im Hinblick auf allfällige Rückfragen sich an die Unterzeichneten zu wenden. Sehr gerne unterstützen wir Sie im Rahmen des weiteren Gesetzgebungsprozesses und bieten eine aktive Mitarbeit ausdrücklich an.

Wir bedanken uns für Ihre Kenntnisnahme und wohlwollende Prüfung der Eingabe.

Freundliche Grüsse
SwissSign AG

Markus Naef
CEO

Marcus Griesser
Verwaltungsrat

Beilage: Anhang Stellungnahme im Einzelnen

SwissSign

Anhang

Zur Stellungnahme der SwissSign AG zum E-ID-Gesetz vom 29. Mai 2017

Bezogen auf unseren gesetzlichen Auftrag sowie unsere Tätigkeiten möchten wir zu den folgenden Artikeln aus Sicht der SwissSign AG im Einzelnen wie folgt Stellung beziehen.

Art. 1 VE E-ID-Gesetz: Gegenstand und Zweck

- *Abs. 1*
  Die Reihenfolge a., c., b., d. wäre sinnvoller, um inhaltliche Themen näher zusammen zu rücken

- *Abs. 1 lit. a)*
  Die Verwendung der E-ID zu regeln, wird begrüsst. Das Gesetz sollte in einer zentralen Akzeptanznorm die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennen. Siehe Stellungnahme, Kapitel 3.

- *Abs. 2 lit. a)*
  Damit B2B, B2C,G2B und G2C ermöglich wird, schlagen wir folgende Änderung vor:
  „den sicheren elektronischen Geschäftsverkehr unter Privaten, unter Behörden und zwischen Privaten und Behörden zu fördern; und“

- *Abs. 2 lit. b)*
  Wir sind der Ansicht, dass der Begriff Interoperabilität sich auf eine Internationale Interoperabilität beziehen soll (Bsp. STORK). Siehe Stellungnahme zu Art. 18.

Art. 2 VE E-ID-Gesetz: Begriffe

Der Begriff „Identitätsstelle“ sollte bereits bei den Legaldefinitionen aufgenommen werden.

Art. 3 VE E-ID-Gesetz: Persönliche Voraussetzungen

- *Abs. 1*
  Nicht geregelt ist, ob ein Anspruch auf eine E-ID besteht (vgl. Art. 1 Abs. 1 Ausweisgesetz). Gegen einen „Kontrahierungszwang“ sprechen die geplante Pluralität von IdP und die beim IdP in jedem Fall (auch ohne Gebühren) anfallenden Kosten. Für einen „Kontrahierungszwang“ spricht die zunehmende Bedeutung von elektronischen Diensten und die Verhinderung der digital divide. Im Falle eines Kontrahierungszwanges im Sinne eines Service Public muss eine angemessene Abgeltung der dadurch entstehenden Kosten durch die öffentliche Hand vorgesehen werden.

- *Abs. 2*
  Im Interesse eines möglichst niederschwelligen und diskriminierungsfreien Zuganges zur E-ID und den überdies zugänglichen elektronischen Behördenleistungen sollte der Bundesrat die Möglichkeit erhalten, in Abs. 1 nicht genannte Kategorien von in- und ausländischen Ausweisen zu bestimmen, die zur Ausstellung einer E-ID berechtigen.

SwissSign

Art. 4 VE E-ID-Gesetz: Anerkennung von IdP

Die Anerkennungsvoraussetzungen für IdP, für anerkannte Zertifizierungsdienstanbieter (ZertES), für anerkannte Zustellplattformen und für zertifizierte Gemeinschaften (EPDG) weichen jeweils voneinander ab. Die Gemeinsamkeiten der genannten Stellen rechtfertigen eine Harmonisierung der materiellen und formellen Anerkennungsvoraussetzungen; für zusätzliche Voraussetzungen je Trust Service bleibt Platz, dort wo dies zwingend sachlich erforderlich ist. Das europäische eIDAS System spricht generell von Trust Service Providern und harmonisiert die Anforderungen an diese. Bezüglich den Anforderungen an die Anerkennung ist eine Synchronisierung über alle TSP-Angebote (z.B. Qualifizierte Zertifikate, Siegel, anerkannte Zustellplattformen, IdP usw.) auch deshalb sicherzustellen, damit einer internationalen gegenseitigen Anerkennung (insbesondere im eIDAS Raum) nichts im Wege steht.

- *Abs. 2 lit. f)*
  Der Vorentwurf sieht vor, dass die IdP die E-ID-Systemdaten in der Schweiz und nach schweizerischem Recht halten und bearbeiten müssen. Diese absolute Anforderung wird u.E. den heutigen Realitäten nicht mehr gerecht. Der Gesetzgeber sollte hier – ohne bei den Sicherheitsanforderungen Abstriche zu machen – mehr Flexibilität zeigen und auch eine Datenhaltung ausserhalb der Schweiz zulassen, sofern die Daten bezüglich Datensicherheit und Datenschutz adäquat nach schweizerischem Recht bearbeitet und gehalten werden.

- *Abs. 3*
  Es ist unklar, ob und wie die Pflicht zur 3-jährlichen Erneuerung die Onlinedienste beeinflusst. Was geschieht namentlich, wenn die Anerkennung des IdP nicht erneuert wird? Was geschieht dann mit den E-ID Daten der Kunden? Müssen sich die Kunden alle neu identifizieren?

Art. 5 VE E-ID-Gesetz: Sicherheitsniveaus

- *Abs. 1*
  Es ist sinnvoll die Namensgebung der eIDAS Verordnung zu verwenden, obwohl diese eher nicht ohne Weiteres verständlich ist. Für den Erfolg dieses Gesetzes ist es zentral, dass diese Sicherheitsniveaus klar definiert werden und in den darauf referenzierenden Gesetzen genutzt werden.

- *Abs. 2*
  In den Artikeln 6 ff. wird detailliert aufgezeigt, wie sich die verschiedenen Sicherheitsniveaus unterscheiden. Der Abs. 2 bringt keinen Mehrwert. Wir empfehlen daher diesen Absatz zu streichen.

Art. 6 VE E-ID-Gesetz: Ausstellungsprozess

Dieser Text erscheint uns als unklar und nicht verständlich. Des Weiteren sind wir der Ansicht, dass man im Gesetz nicht den Prozess mit seinen Schritten definieren soll, sondern die zentralen Anforderungen an diesen. Dabei soll auch die Möglichkeit gegeben werden, den Entwicklungen und Erfahrungen diesbezüglich Rechnung zu tragen.

Wenn man aber zum Schluss kommt, dass der Prozess unbedingt beschrieben werden muss, schlagen wir folgende Änderungen vor:

[1] Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP oder bei einer Ausweise gemäss Art. 3 ausstellenden Behörde.

[2] Der IdP oder die Ausweise gemäss Art. 3 ausstellende Behörde überprüft die persönlichen Voraussetzungen der Person, die einen Antrag auf Ausstellung einer E-ID stellt.

[3] Der IdP beantragt bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) mit dem Einverständnis der antragstellenden Person die Übermittlung der Personenidentifizierungsdaten nach Artikel 7 Absätze 1 und 2.

[4] Der IdP ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person.

[5] Die Identitätsstelle protokolliert die Datenübermittlungen.

Art. 7 VE E-ID-Gesetz: Personenidentifizierungsdaten

- *Abs. 2*
  Der Heimatort kann z.B. für Auslandschweizer sehr bedeutsam sein, z.B. für Abstimmungen und Wahlen. Er sollte deshalb aufgeführt werden.

- *Abs. 2 lit. a. Versichertennummer*
  Die Zuordnung der AHVN13 wird zur Kenntnis genommen. Zur Verwendung der Nummer siehe Stellungnahme zu Art. 9.

Art. 8 VE E-ID-Gesetz: Aktualisierung der Personenidentifizierungsdaten

- *Abs. 1*
  Die regelmässige Aktualisierung von stabilen Daten erscheint nicht als zweckmässig. Das Aktualisierungsziel kann genauso gut mit einer bedarfsgerechten Aktualisierung auf der Basis von erkannten Risiken erreicht werden, d.h. jeweils im Zusammenhang mit dem konkreten Einsatz der E-ID. Wir würden eine Formulierung bevorzugen, in der die Gültigkeits- und Nutzungsdauer der Personenidentifizierungsdaten im Fokus stehen, so das Abfragen nur notwendig werden, wenn die E-ID auch genutzt wird.

  Gesetzestechnisch genügte es, die Aktualisierungsfrequenz in den Ausführungsbestimmungen (Verordnung, technische und administrative Vorschriften) zu regeln.

  Art. 8 Abfrage der Personenidentifizierungsdaten

  [1] Zum Zeitpunkt der Nutzung der E-ID fragt der IdP bei der Identitätsstelle die von ihr geführten Personenidentifizierungsdaten ab.

  [2] Er ist verantwortlich, dass von ihm ausgestellte E-IDs umgehend gesperrt oder widerrufen werden, wenn die E-ID-Registrierungsnummer nicht mehr verwendet werden darf. (Anm. Übersetzung: Er sperrt oder widerruft ...)

Art. 9 VE E-ID-Gesetz: **Systematische Verwendung der Versichertennummer zum Datenaustausch**

In der Gesamtrechtsordnung ist ein konsistenter Umgang mit der AHVN13 erwünscht. Das ATSG erlaubt die Verwendung nur sehr restriktiv. Insbesondere das EPDG hat die Verwendung von Versichertennummer verboten, aber eine E-ID ist definiert. Daher gilt es hier darauf zu achten, dass keine Inkompatibilität entsteht, die dann die Nutzung der E-ID für Patientendossiers nicht erlaubt.

Art. 10 VE E-ID-Gesetz: **Datenbearbeitung und Datenweitergabe**

Die Restriktionen gemäss Abs. 1, 2 und 3 widersprechen sich teilweise. Unklar ist insbesondere, 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.

Bei der DSG Revision sind zahlreiche Fragen offen und mit einer vom VE in wesentlichen Punkten abweichende Schlussfassung muss gerechnet werden. Dem Ergebnis der Revision des DSG ist bei der Schlussfassung des Art. 10 angemessen Rechnung zu tragen.

Art. 11 VE E-ID-Gesetz: **Erlöschen der Anerkennung**

Da der Betrieb eines IdP privatrechtlich organisiert wird, ist es sinnvoll das Thema Geschäftsaufgabe zu klären. Dabei wichtig erscheint uns auch die gewollten Auswirkungen auf die eID Inhaber und Relaying-Party zu betrachten inkl. deren Pflichten und Rechte. So stellt sich dabei folgende Fragen: Was geschieht mit den E-ID Daten der Kunden, die im System der Relaying Party verwendet werden? Müssen sich alle Kunden neu identifizieren?

Angezeigt wäre daher eine gesetzliche Regelung, welche IdP verpflichtet, Inhaberinnen und Inhaber einer E-ID eines nicht mehr bestehenden IdP „en bloc“ (gegen entsprechende Entschädigung durch den Bund) zu übernehmen. Will der Gesetzgeber nicht so weit gehen, ist auf Gesetzesebene mindestens sicherzustellen, dass von der Geschäftsaufgabe eines IdP betroffene Inhaberinnen und Inhaber einer E-ID von anderen IdP eine E-ID ausgestellt erhalten, ohne den gesamten Ausstellungsprozess gemäss Art. 6 VE E-ID-Gesetz erneut durchlaufen zu müssen.

Art. 16 VE E-ID-Gesetz: **Behörden als Betreiberinnen von E-ID-verwendenden Diensten**

Für E-ID-Inhaber und Relaying Parties nimmt der Nutzen einer E-ID mit der zunehmenden Anzahl von anderen Inhabern und Relaying Parties/Anwendungsfällen zu (Netzwerkeffekt). Beim Einsatz der E-ID im Behördenumfeld setzt dies die flächendeckende Harmonisierung der betreffenden Gesetze voraus. Das Publikum erwartet universelle Einsatzmöglichkeiten insbesondere für e-Government, e-Health und e-Voting. Das E-ID Gesetz sollte eine zentrale Akzeptanznorm beinhalten, welche die E-ID in der gesamten Rechtsordnung und für alle Behördenbelange als akzeptiert anerkennt. Die unterschiedlichen Sicherheitsniveaus bieten die nötige Flexibilität für eine universelle Akzeptanz.

Art. 16 wird im Grundsatz begrüsst. Zur besseren Positionierung als universelle Akzeptanznorm schlagen wir folgende Änderung vor:

Jede E-ID, die das geforderte Sicherheitsniveau erfüllt, ist für sämtliche elektronischen Identifizierungen im Rahmen der Kommunikation mit Behörden des Bundes, der Kantone und der Gemeinden sowie mit Organisationen und Personen des öffentlichen oder privaten Rechts, die nicht der Verwaltung angehören, und mit Verwaltungsaufgaben betraut sind, akzeptiert.

Art. 17 VE E-ID-Gesetz: Pflichten

- *Abs. 1 lit. e*
  Das Wort „periodisch“ soll weggelassen oder durch „ordnungsgemäss“ ersetzt werden. Siehe Stellungnahme zu Art. 8 VE E-ID-Gesetz.

- *Abs. 1 lit. g*
  Die Anforderung beeinflusst die vom IdP eingesetzten Verrechnungsmodelle und ist mit den zivilrechtlichen Verjährungsfristen nicht abgestimmt. Es stellt sich ferner die Frage, wie nach dem Löschen der Daten über die Anwendung eine E-ID ein Missbrauch nachgewiesen werden kann.

Art. 18 VE E-ID-Gesetz: Interoperabilität

Als Voraussetzung für eine funktionierende Interoperabilität müssen neben den technischen Fragen sowohl die Haftungsfrage als auch die Finanzierung geklärt sein. Die Gebühren für Aktualisierungen bei den Identitätsstellen können ein Fehlanreiz sein, bei der Promotion der E-ID Systeme der Anwendung (Einnahmen) vor der Ausstellung (Kosten) Vorrang zu geben und über die Interoperabilität von IdP Anbietern mit einer grosser Basis ausgestellter E-ID zu profitieren. Jedenfalls ist die finanzielle Abgeltung zwischen den Beteiligten im Sinne einer „Roaming / Terminierungs-Gebühr“ unbedingt zu regeln. Andernfalls droht eine Diskriminierung von IdP mit einem grossen E-ID Stamm.

Des Weiteren wäre es sinnvoll, die internationale Interoperabilität ebenfalls zu beachten und z.B. den Aufbau und Betrieb von STORK Servern durch den Bund vorzuschreiben.

Art. 19 VE E-ID-Gesetz: Organisation

Die Art. 19 und 21 bezeichnen zwei unterschiedliche Departemente (EDF, EJPD). Es fehlen Regeln zur Koordination zwischen Identitätsstelle und Anerkennungsstelle.

Art. 21 VE E-ID-Gesetz: Zuständigkeit

Im allgemeinen siehe Stellungnahme zu Art. 19 VE E-ID-Gesetz.

- *Abs. 1*
  Abs. 1 sollte zu einer Delegationsnorm umgestaltet und der Bundesrat ermächtigt werden, die Zuständigkeiten betreffend die Anerkennungsstelle zu bestimmen. Dies vereinfacht die Zuständigkeiten und Aufsichten für die verschiedenen Trust Service Provider zu harmonisieren. Die bisher unterschiedlichen Zuständigkeiten für die verschiedenen Trust Service Provider (ZertES: SAS, SECO; Zustellplattform: BJ, EJPD; Patientendossier: BAG) sind ineffizient und stehen dem Erfolg der einzelnen Services im Weg. Insbesondere auch im Zusammenhang mit den Identitäten für das Patientendossier sind zwei Zuständigkeiten/Anerkennungen unnötig kompliziert, kostspielig und ohne Mehrwert. Im EPDG wird die Anerkennung der Identität für die Nutzung des Patientendossiers vom BAG (EDI) wahrgenommen. Eine gemäss E-ID anerkannte Identität muss ohne zusätzlichen Aufwände für Anbieter vom BAG anerkannt werden.

Art. 23 VE E-ID-Gesetz:

Der Aufbau und Betrieb der staatlichen Identitätsstelle soll durch den Bund finanziert werden. Auf die Gebühren für die Dienstleistungen der Identitätsstelle ist zu verzichten. Die Daten der Identitätsstelle sollen den IdP kostenlos zur Verfügung stehen.

Art. 24 VE E-ID-Gesetz:

Die Vorschriften zur Haftung geben wieder, was ohnehin gilt. Das Haftungsregime für die verschiedenen TSP sollte harmonisiert werden. Dabei ist zu beachten, dass Haftungsvorschriften nicht zu einem Standortnachteil für Schweizer Akteure führt.

Art. 25 VE E-ID-Gesetz: Änderung anderer Erlasse

Neben einer universellen Akzeptanznorm ist es sinnvoll, im Minimum für die folgenden Gesetze die E-ID ausdrücklich als Referenz für elektronische Identitäten und deren Sicherheitsniveaus zu verankern: EPDG, ZertES, VEIeS, FMG, div. Finanzmarktregulierungen, VeÜ-ZSSV, VeÜ-VwV usw..

Anhang Änderung anderer Erlasse, Ziffer 3.

Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung:

Um die Bekanntgabe der AHVN13 zu ermöglichen, genügte eine auf dieses Datum beschränkte Norm. Der neue Artikel 50a AHVG schränkt die Daten lediglich über das unscharfe und schwer zu handhabende Kriterium des „überwiegenden Privatinteresses“ ein.

Anhang Änderung anderer Erlasse, Ziffer 4.

Bundesgesetz vom 18. März 2016 über die elektronische Signatur

Sinnvollerweise wird das Sicherheitsniveau bezeichnet. Das Niveau sollte so gewählt werden, dass mit einer zu niedrigen E-ID (UserName/Password) kein qualifiziertes Zertifikat ausgestellt werden kann.

UBS

Vernehmlassung zum Vorentwurf eines Bundesgesetzes über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

A. Allgemeine Bemerkungen

Wir gehen davon aus, dass anerkannte elektronische Identifizierungseinheiten (E-IDs) im Geschäfts- und Behördenverkehr in Zukunft – wenn richtig ausgestaltet - eine entscheidende Rolle spielen werden. Für den Wirtschaftsstandort Schweiz ist es von grosser Bedeutung, dass die gesetzlichen und tatsächlichen Grundlagen für ein System so ausgestaltet werden, dass E-IDs bei Benutzern und Betreibern gleichermassen auf hohe Akzeptanz stossen und damit weit verbreitet angewendet werden. Gleichzeitig muss den hohen Ansprüchen an Datensicherheit und –schutz in der Schweiz Rechnung getragen werden. werden kann.

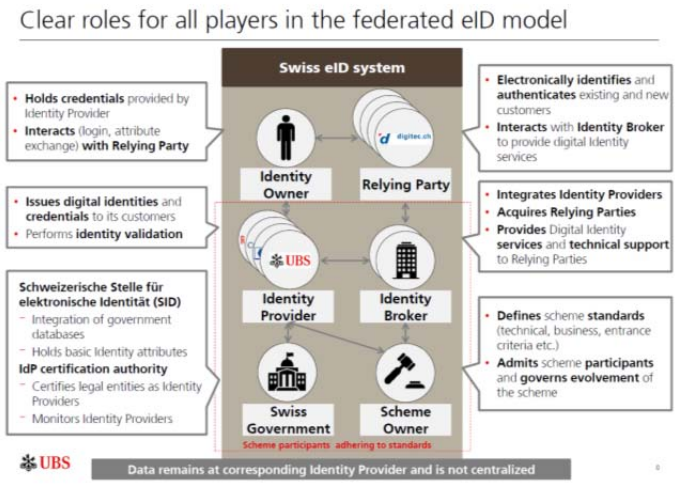
Die Gesetzgebung sollte sich unseres Erachtens an folgenden Grundsätzen orientieren:

- **Maximale Verbreitung durch Dezentralisierung:** Eine weite Verbreitung der E-ID in der Schweiz erfordert es, dass möglichst viele potentielle Benützer angesprochen werden können. Dies funktioniert am effizientesten mit einem dezentralen System, wie es im Vernehmlassungsentwurf vorgeschlagen wird. Mit der dezentralen Lösung gelingt es am besten (aufgrund der bestehenden Kundenbasis potentieller Anbieter), eine möglichst grosse Anzahl Nutzer zu erreichen. Grosse Unternehmungen haben einen entsprechend bedeutenden Kundenstamm, den sie für die Zwecke der E-ID ansprechen können. Oft wurde sogar schon eine Identifikation vorgenommen, die der E-ID zugrunde gelegt werden kann (z.B. bei Banken, Telekommunikationsunternehmen etc.). Damit wird die Hürde für Benutzer, eine E-ID anzulegen, noch einmal gesenkt, weil sie ohne Aufwand bezogen werden kann. Schliesslich ist auch davon auszugehen, dass private E-ID Anbieter aufgrund bereits bestehender Verbindungen besser geeignet sind, ein Netzwerk mit E-ID anwendenden Dienstleistern aufzubauen, als im Fall eines staatlichen Monopols.

  Eine rein staatliche bzw. auf einem Monopol beruhende Lösung erachten wir hingegen nicht für geeignet, die Regulierungsziele zu erreichen und lehnen solche Konzepte ab.

  Es muss aber sichergestellt sein, dass zumindest sämtliche staatlichen Stellen die E-ID für den Behördenverkehr akzeptieren. Dies sollte als Auftrag für Kantone und Gemeinden im Gesetz festgehalten werden.

- **Interoperabilität:** In einem System mit mehreren E-ID Anbieter gibt ist eine Koordination besonders wichtig. Dienstleistungsanbieter, welche die E-ID benützen wollen, sollen dies möglichst ohne Aufwand tun können, und die Benutzer sollen mit ihrer E-ID nicht von irgendwelchen Dienstleistungen ausgeschlossen werden, sondern diese flächendeckend und umfassen anwenden können. Da sich im Modell gemäss Vernehmlassungsentwurf potentiell mehrere IdP und Dienstleister gegenüberstehen werden, könnte sich damit ein komplexes Anbindungsnetzwerk bilden, das in der Praxis nur schwer zu handhaben wäre. Um einen reibungslosen und für alle Beteiligten möglichst einfach umzusetzender Betrieb gewährleistet werden kann, schlagen wir ein Broker Konzept vor, das im Übrigen auch in der eIDAS vorgesehen ist und im Wesentlichen nach folgendem Schema funktioniert:



Ohnehin zentral ist, dass die IdP einem gemeinsamen Standard folgen, so dass diese "austauschbar" sind und sich gegenseitig akzeptieren. Es soll einem E-ID benutzenden Dienst nicht darauf ankommen, mit welcher IdP sich seine Kunden identifizieren.

- **Vertrauen und Sicherheit:** Dem Datenschutz und der Datensicherheit gebührt erhöhte Aufmerksamkeit. Mängel in dieser Beziehung würden die Akzeptanz der E-ID in der Schweiz nachhaltig stören. Eine dezentrale Lösung bietet für den Benutzer auch diesbezüglich die grössten Vorteile. Sie erlaubt es ihm, je nach konkreter Dienstleistung den für ihn geeignetsten E-ID Anbieter zu nutzten. Die mit der Nutzung der E-ID anfallenden Randdaten müssen dann nicht zentral einem einzigen Anbieter anvertraut werden. Vielmehr erlaubt die dezentrale Lösung dem Benutzer, seine Daten auf verschiedene E-ID Anbieter zu verteilen.

  Ebenfalls im Sinne der Datensicherheit und dem Vertrauen in das System sollte es möglich sein, dass eine Person verschiedene E-ID mit je unterschiedlichen Registrierungsnummern unterhalten kann. Damit kann der Nutzer entscheiden, welche Daten er welcher E-ID zuordnen will. Würden sämtliche E-ID einer Person unter derselben Nummer beim Staat zentralisiert, wäre dieser in der Lage, umfassende Persönlichkeitsprofile zu erstellen. Dies ist aus Sicht des Datenschutzes, aber auch der Datensicherheit problematisch. Würde bei einer einzigen eindeutigen E-ID Nummer, diese "gehackt", wäre der Schaden maximal und das Vertrauen in das System ruiniert. Vor diesem Hintergrund müssen die Nutzer die Möglichkeit haben, ihre Informationen auf verschiedene Anbieter zu verteilen, ohne dass eine logische Verknüpfung der Daten besteht.

Auch in tatsächlicher Hinsicht ist zu verhindern, dass der Staat bzw. staatliche oder staatsnahe Betriebe aufgrund ihrer Stellung faktische Monopole schaffen, welche einerseits die Entwicklung privater IdP beschränken und möglichen Nutzern die Wahlmöglichkeit nehmen.

Vor diesem Hintergrund unterstützen wir die Initiative des Bundes und den Vernehmlassungsentwurf im Wesentlichen, schlagen aber im Sinne der auch vom Bund verfolgten Regulierungsziele folgende Anpassungen vor.

UBS

B. Zu den einzelnen Bestimmungen

Art. 1

Formulierungsvorschlag

Art. 1 Gegenstand und Zweck

[1] Dieses Gesetz regelt:

a. Inhalt, Ausstellung, Verwendung, Sperrung und Widerruf von anerkannten elektronischen Identifizierungseinheiten (E-ID);
b. die Anerkennung der Anbieter von Identitätsdienstleistungen und ihrer E-ID-Systeme sowie die Aufsicht über diese Anbieter und Systeme;
c. die Rechte und Pflichten der Inhaberinnen und Inhaber einer E-ID;
d. die Rechte und Pflichten der Betreiberinnen von E-ID-verwendenden Diensten.

[2] Es hat zum Zweck:

a. den sicheren elektronischen Geschäftsverkehr unter Privaten und mit Behörden zu fördern; und
b. eine weite Verbreitung, die Standardisierung und die Interoperabilität der E-ID sicherzustellen.

[3] Es orientiert sich dabei an internationalen Standards.

Begründung

Mit Blick auf die bisherigen Erfahrungen mit ähnlichen Instrumenten (z.B. elektronische Signatur), sollte auch eine möglichst umfassende Verbreitung der anerkannten E-ID als Ziel in die Gesetzgebung aufgenommen werden. Es muss darum gehen, ein Instrument zur Verfügung zu stellen, dass von der Bevölkerung angenommen und rege genutzt wird. Dies bedingt einerseits eine einfache, aber dennoch sichere Handhabung der E-ID und anderseits ein möglichst weites Anwendungsfeld derselben, sowohl im öffentlichen als auch im privaten Sektor. Das erweiterte Ziel sollte insbesondere auch den Verordnungsgeber bei der Ausarbeitung der Verordnung leiten.

Schliesslich sollen internationale Standards beachtet werden, damit die Interoperabilität auch mit ausländischen Lösungen (insbesondere mit jener der EU) möglichst gut sichergestellt werden kann. Es sind daher solche Standards, wo möglich und sinnvoll, auch im schweizerischen Recht abzubilden.

Art. 2

Formulierungsvorschlag

Art. 2 Begriffe

In diesem Gesetz bedeuten:

a. elektronische Identifizierungseinheit: eine elektronische Einheit, die zur Identifizierung und Authentifizierung einer natürlichen Person verwendet wird;
b. anerkannte elektronische Identifizierungseinheit (E-ID): eine elektronische Identifizierungseinheit, die von einem IdP nach den Vorgaben dieses Gesetzes ausgestellt wird;
c. Identity Provider (IdP): nach diesem Gesetz anerkannter Anbieter von Identitätsdienstleistungen;
d. Identifizierung: Prozess der Nutzung von Personenidentifizierungsdaten, die eine Person eindeutig repräsentieren;
e. Authentifizierung: Prozess der Überprüfung einer behaupteten Identität;
f. Personenidentifizierungsdaten: staatlich geführter Datensatz, der es ermöglicht, die Identität einer Person festzustellen;
g. E-ID-Registrierungsnummer: einer Person eindeutig zugeordnete Identifikationsnummer;
h. E-ID-System: elektronisches System für die Ausstellung, Verwaltung und Anwendung von E-ID;
i. Betreiberin von E-ID-verwendenden Diensten: natürliche oder juristische Person, die für ihre Tätigkeit Online-Dienste betreibt, die Vertrauen in die Identität der sie nutzenden Person und in deren Authentizität voraussetzen;
j. E-ID-verwendender Dienst: eine Informatikanwendung, die ein E-ID-System nutzt.

UBS

k. Attribute: Andere als die von der Identitätsstelle zur Verfügung gestellten Merkmale, die einer Person zugeordnet werden können.
l. Broker: Eine Person, welche die Verbindung zwischen den E-ID verwendenden Diensten und den verschiedenen IdP herstellt.

Begründung

Gesetzesentwurf und Erläuterungsbericht gehen davon aus, dass neben den von der Identitätsstelle zum Abgleich der Daten zur Verfügung gestellten Identitätsmerkmalen auch noch weitere Attribute mit der E-ID verbunden werden können. Dies ist unseres Erachtens sinnvoll und könnte einen wichtigen Beitrag zur Verbreitung der E-ID beitragen. Um dies noch klarer zum Ausdruck zu bringen, schlagen wir vor den Begriff "Attribute" entsprechend zu definieren.

Zwischen IdP und den E-ID verwendenden Diensten braucht es eine Vermittlerstelle, welche die entsprechenden Zugänge organisiert. Ohne einen sog. Broker müsste jeder E-ID verwendender Dienst mit jedem IdP eine Vereinbarung schliessen und sodann die technische Anbindung erstellen. Der Broker soll hier als Vermittlerstelle dienen, welche es erlauben würde, dass die E-ID verwendenden Dienste lediglich die Verbindung zum Broker unterhalten und letzterer dann dafür sorgt, dass die Weiterverbindung zum IdP hergestellt wird. Der Broker dient damit als Relaisstation zwischen IdP und dem E-ID verwendenden Dienst. Damit würde es den E-ID verwendenden Diensten erheblich erleichtert, die E-ID für Ihre Dienste einzuführen, da sie nur einen Ansprechpartner haben (den Broker) und nicht viele verschiedene (IdP). Die Möglichkeit, einen Broker einzusetzen, ist unseres Erachtens ein entscheidender Faktor für die Frage, ob sich die E-ID in der Praxis durchsetzen wird. Der Broker muss nicht staatlich betrieben werden, das kann auf privater Ebene geschehen. Zudem ist die Zwischenschaltung des Broker auch nicht zwingend, die Anbindung der E-ID verwendenden Diensten an die IdP kann auch unmittelbar erfolgen. Mit dem Broker System würden wir eine auch in der eIDAS vorgesehene Rechtsfigur übernehmen, was zusätzlich für eine Verankerung des Brokers im schweizerischen Gesetz spricht.

Art 3

Formulierungsvorschlag

Art. 3 Persönliche Voraussetzungen

[1] IdP können folgenden Personen eine E-ID ausstellen:

a. Schweizerinnen und Schweizer, die zum Zeitpunkt der Ausstellung über einen gültigen Schweizer Ausweis gemäss Bundesgesetz vom 22. Juni 2001[3] über die Ausweise für Schweizer Staatsangehörige verfügen;
b. Ausländerinnen und Ausländer die zum Zeitpunkt der Ausstellung über einen gültigen Ausländerausweis gemäss Bundesgesetz vom 16. Dezember 2005[4] über die Ausländerinnen und Ausländer verfügen.

[2] Der Bundesrat kann Kategorien von Ausländerausweisen bestimmen, die nicht zur Ausstellung einer E-ID berechtigen. Er kann für die betroffenen Personen alternative Verfahren zur elektronischen Identifizierung und Authentifizierung vorsehen.

[3] Der Bundesrat regelt die Voraussetzungen zum Bezug, den Ausstellungsprozess sowie die Sperrung, Entsperrung und den Widerruf einer E-ID.

Begründung

Der Vollständigkeit halber sollte der Bundesrat nicht nur die Sperrung der E-ID, sondern auch die Voraussetzungen einer darauffolgenden Entsperrung regeln, da sich auch dabei Fragen stellen, die vom Bundesrat adressiert werden sollten (z.B. Zeitpunkt und Voraussetzungen der Entsperrung).

Artikel 4

Formulierungsvorschlag

UBS

[1] IdP, die E-ID ausstellen wollen, brauchen eine Anerkennung der Anerkennungsstelle (Art. 21).

[2] IdP werden anerkannt, wenn sie:

a. ihren Sitz in der Schweiz haben;
b. über eine UID-Nummer gemäss Bundesgesetz vom 18. Juni 2010[5] über die Unternehmens-Identifikationsnummer (UIDG) verfügen;
c. nachweisen, dass die für die E-ID-Systeme verantwortlichen Personen kein Risiko für die Sicherheit darstellen;
d. Personen mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen beschäftigen;
e. Gewähr bieten, dass die von ihnen betriebenen E-ID-Systeme die für das jeweilige Sicherheitsniveau vorgesehenen Sicherheitsanforderungen erfüllen;
f. die E-ID-System-Daten auf dem ~~in der~~ für die Schweiz ~~geltenden~~ vorgeschriebenen Niveau an Datenschutz und Datensicherheit ~~nach schweizerischem Recht~~ halten und bearbeiten;
g. eine ausreichende Versicherung zur Deckung der Haftpflicht nach Artikel 24 oder gleichwertige finanzielle Sicherheiten nachweisen;
h. die Einhaltung des anwendbaren Rechts, namentlich dieses Gesetzes und seiner Ausführungsbestimmungen, gewährleisten.

[3] Die Anerkennung muss spätestens nach drei Jahren erneuert werden. Eine Wiederholung der Anerkennung gemäss Absatz 2 ist nicht notwendig, wenn innerhalb der dreijährigen Frist eine Anerkennung bereits nach einem anderen Gesetz erteilt worden ist, die gleichwertig ist.

[4] Der Bundesrat erlässt nähere Vorschriften zu den Voraussetzungen der Anerkennung, insbesondere zu:

a. den fachlichen und sicherheitsbezogenen Anforderungen und ihrer Überprüfung;
b. der notwendigen Versicherungsdeckung beziehungsweise zu den gleichwertigen finanziellen Sicherheiten;
c. den anwendbaren Standards und technischen Protokollen für die E-ID-Systeme sowie zu deren regelmässiger Überprüfung.

Begründung

In Abs. 2 lit. f sieht der Vorentwurf vor, dass die E-ID System Daten in der Schweiz und nach schweizerischem Recht gehalten und bearbeitet werden müssen. Diese so absolut formulierte Voraussetzung wird unseres Erachtens der Realität, worin z.B. Cloud Lösungen eine immer grössere Rolle spielen, nicht mehr gerecht. Hier sollte grössere Flexibilität herrschen, 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 bringt. Nur so kann auch die grenzüberschreitende Interoperabilität genutzt werden. Das Gesetzt sollte daher lediglich voraussetzen, dass das vom schweizerischen Recht vorgegebene Niveau an Datensicherheit und Datenschutz einzuhalten ist.

Ein regelmäßiges Anerkennungsverfahren für IdP erscheint grundsätzlich sinnvoll. Jedoch ist zu beachten, dass Banken z.B. als "Signature Generation Service Provider" bereits jährliche Audits und Anerkennungen (e-Signatur) zu durchlaufen haben und mit der Anerkennung für e-ID's eine dritte hinzu käme, welche den gleichen Bereich abdeckt. Man würde permanent und von unterschiedlichen Parteien auditiert. Bis die verschiedenen Anerkennungsverfahren harmonisiert sind, muss ein Anerkennungsverfahren jeweils auch für den anderen Bereich gelten, sofern eine gewisse Gleichwertigkeit vorliegt.

Artikel 5

Formulierungsvorschlag

Art. 5 Sicherheitsniveaus

[1] IdP können E-ID-Systeme mit unterschiedlichen, aufeinander aufbauenden Sicherheitsniveaus betreiben und entsprechend E-ID ausstellen, die folgendes Mass an Vertrauen vermitteln:

a. niedrig: Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;

UBS

b. substanziell: substanzielle Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung;
c. hoch: Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung.

[2] Die verschiedenen Sicherheitsniveaus unterscheiden sich durch:

a. den Ausstellungsprozess, insbesondere in Bezug auf die Identifizierung und Authentifizierung der Inhaberin oder des Inhabers bei der Registrierung;
b. den Betrieb, insbesondere die Aktualisierung der Personenidentifizierungsdaten;
c. die Anwendung, insbesondere in Bezug auf die Identifizierung und Authentifizierung; und
d. weitere technische oder organisatorische Sicherheitsmassnahmen nach dem jeweiligen Stand der Technik.

[3] Eine für ein bestimmtes Sicherheitsniveau ausgestellte E-ID kann auch auf einem tieferen Sicherheitsniveau eingesetzt werden.

[4] Der Bundesrat regelt die verschiedenen Sicherheitsniveaus, insbesondere die angemessenen Mindestanforderungen an die Identifizierung und Authentifizierung.

Begründung

In Bezug auf Abs. 4 soll der Bundesrat in der Verordnung dem Ziel der weiten Verbreitung der E-ID Rechnung tragen. Dies bedeutet, dass Identifizierung und Authentifizierung zwar sicher, aber auch zweckmässig ausgestaltet sein müssen. Die Erfahrungen zeigen, dass beispielsweise das Erfordernis der persönlichen Vorsprache von den Nutzern in der Regel als zu grosse Hürde angesehen wird. Eine Videoidentifikation sollte genügen, wie dies im Begleitbericht bereits vorgesehen ist.

Artikel 6

Formulierungsvorschlag

Art. 6 Ausstellungsprozess

[1] Wer eine E-ID will, beantragt deren Ausstellung bei einem IdP.

[2] Der IdP überprüft die persönlichen Voraussetzungen.

[3] Er beantragt bei der Schweizerischen Stelle für elektronische Identität (Identitätsstelle) mit dem Einverständnis der antragstellenden Person die Übermittlung der Personenidentifizierungsdaten nach Artikel 7 Absätze 1 und 2.

[3bis] Er kann Signaturmittel und Identifizierungseinheit zentral führen.

[3ter] Er identifiziert und authentifiziert die antragstellende Person. Dies kann auf persönliche Vorsprache hin, mittels Videoidentifikation oder durch vergleichbare technische Identifikationsmittel erfolgen. Eine bereits erfolgte Identifikation, die mit den Anforderungen dieses Gesetzes gleichwertig ist, muss nicht wiederholt werden.

[4] Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person. Eine Person kann mehrere E-ID besitzen.

[5] Die Identitätsstelle protokolliert die Datenübermittlungen.

Begründung

Nach dem Antrag für eine E-ID muss der IdP die Identität und die Authentizität des Antragstellers überprüfen, bevor er ihm eine E-ID zuweist. Dieser Schritt wird zwar im Gesetz vorausgesetzt, müsste aber explizit aufgeführt sein. Zusätzlich sollte im Gesetz klargestellt werden, dass neben der persönlichen Vorsprache eine Videoidentifikation oder eine Identifikation über vergleichbare technische Identifikationsmittel erfolgen kann. Mit dem Einschub "vergleichbare technische Identifikationsmittel" soll sichergestellt werden, dass dem technischen

Fortschritt Rechnung getragen wird, sofern mit einer neuen Technologie eine vergleichbare Sicherheit bzw. Zuverlässigkeit erreicht werden kann.

Bereits identifizierte Personen sollen nicht noch einmal identifiziert werden müssen, sofern die Identifikation für die Erstellung einer eID bereits ausreichend gewesen wäre. Eine erneute Identifikation brächte lediglich mehr Aufwand ohne zusätzlichen Nutzen, da die Identität bereits vorliegt.

Letztlich muss schon im Gesetz klargestellt werden, dass eine Person auch mehrere eID besitzen kann. Der Erläuterungsbericht verweist bereits auf diese Möglichkeit. Dem Bedürfnis z.B. verschiedene ID's auf verschiedenen Sichterheitsniveaus einsetzen zu können, sollte bereits auf Gesetzes Ebene Rechnung getragen werden.

Der Erläuterungsbericht (S. 34) geht davon aus, dass die E-ID mit einem Gerät verknüpft bzw. diese darauf angebracht wird. Zudem wird auf technische Standards im Rahmen von eIDAS verwiesen. Dort enthalten ist jedoch auch ein Standard (CEN 419.241). Das würde es ermöglichen, Zertifikate für e-Signaturen zentral zu verwalten und bei Bedarf abzurufen. Der Träger der eID würde von der Last entbunden, ein entsprechendes Gerät (bsp. SuisseID) mitzuführen, könnte es jedoch mit den entsprechenden Zugangsmitteln (Zwei-Faktor) einholen. Dies würde mit den Anforderungen zur E-Signatur korrelieren.

Artikel 7

Formulierungsvorschlag

Art. 7

[1] Die Identitätsstelle ordnet einer E-ID die folgenden Personenidentifizierungsdaten zu:

a. E-ID-Registrierungsnummer;
b. amtlicher Name;
c. Vornamen;
d. Geburtsdatum.

[2] Für die Sicherheitsniveaus substanziell und hoch kann sie der E-ID zusätzlich insbesondere folgende Personenidentifizierungsdaten zuordnen:

a. Versichertennummer nach Artikel 50c des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (Versichertennummer);
b. Geschlecht;
c. Geburtsort;
d. Zivilstand;
e. Staatsangehörigkeit und gegebenenfalls Aufenthaltsstatus;
f. Gesichtsbild;
g. Nummer und Art des von der Schweiz ausgestellten Identitäts- oder Ausländerausweises;
h. Unterschriftsbild.

[3] Sie kann die Personenidentifizierungsdaten mit zusätzlichen Informationen versehen, insbesondere betreffend den Zeitpunkt der letzten Aktualisierung der Daten in den Informationssystemen nach Artikel 20.

[4] Der IdP kann einer E-ID weitere Daten (Attribute) zuordnen. Diese können vom IdP den entsprechenden Sicherheitsniveaus zugeteilt werden.

Begründung

In Art. 7 Abs. 4 soll die mit der von uns vorgeschlagenen Terminologie Konsistenz hergestellt werden.

Art. 7 Abs. 2 nennt die Personenidentifizierungsdaten, welche für die Sicherheitsniveaus „substantiell“ und „hoch“ verwendet werden können. Diese Aufzählung ist abschliessend. Vor dem Hintergrund der ausdrücklich angestrebten Technologieneutralität sowie möglicher technologischer Entwicklungen (z.B. Verwendung von Stimmklangmuster oder biometrische Daten wie Iris-Scan, Fingerabdrücke) erscheint es uns sachgemäss, die

Aufzählung in Art. 7 Abs. 2 VE-E-IDG nicht abschliessend zu formulieren oder die Aufzählung auf Verordnungsstufe aufzunehmen.

Wir schlagen vor, dass die Attribute, die wir bei Art. 2 definiert haben und die Merkmale darstellen, die nicht von der Identitätsstelle stammen, je nach vertraglicher Abmachung zwischen IdP und Nutzer auf sämtlichen Sicherheitsniveaus eingesetzt werden können und dürfen. Da es sich hierbei um Daten handelt, die üblicherweise nicht von einer staatlichen Stelle stammen, sollte es den beteiligten Personen, insbesondere dem IdP überlassen bleiben, unter welchem Sicherheitsniveau die entsprechenden Attribute verfügbar gemacht werden.

Artikel 8

Formulierungsvorschlag

Art. 8 Aktualisierung der Personenidentifizierungsdaten

[1] Der IdP aktualisiert die von ihm geführten Personenidentifizierungsdaten durch eine automatisierte Abfrage anhand der E-ID-Registrierungsnummer bei der Identitätsstelle mindestens wie folgt:

a. für E-ID des Sicherheitsniveaus niedrig: jährlich;
b. für E-ID des Sicherheitsniveaus substanziell: quartalsweise;
c. für E-ID des Sicherheitsniveaus hoch: wöchentlich.

[2] Er ~~ist verantwortlich, dass von ihm ausgestellte E-ID umgehend ge~~sperrt oder widerruf~~ten werden, wenn~~ die von ihm ausgestellte E-ID, wenn ihm mitgeteilt wird, dass die E-ID-Registrierungsnummer nicht mehr verwendet werden darf. Im Zweifel kann er die E-ID sperren.

Begründung

In Abs. 2 wird der IdP verpflichtet, eine E-ID umgehend zu sperren oder zu widerrufen, wenn sie nicht mehr verwendet werden darf. Dabei stellt sich die Frage, woran die Sperrung anknüpft. Im Normalfall wird der IdP nicht von sich aus feststellen können, ob und wann die entsprechenden Voraussetzungen erfüllt sind. Er muss sich auf die Interventionen Dritter verlassen. Dies sollte in Absatz 2 besser zum Ausdruck kommen. Sodann kann die Beurteilung, ob die Voraussetzungen für die Sperrung gegeben sind oder nicht, mitunter sehr heikel bzw. unklar sein. In solchen Fälle sollte das Gesetz dem IdP erlauben, im Zweifel und in guten Treuen eine Sperre vorzunehmen, ohne dafür haftbar gemacht zu werden.

Artikel 10

Formulierungsvorschlag

Art. 10 Datenbearbeitung und Datenweitergabe

[1] IdP dürfen von der Identitätsstelle übermittelte Personenidentifizierungsdaten nur bearbeiten, um nach diesem Gesetz Identifizierungen und Authentifizierungen durchzuführen.

[2] Sie dürfen Betreiberinnen von E-ID-verwendenden Diensten nur die Personenidentifizierungsdaten weitergeben, die dem geforderten Sicherheitsniveau entsprechen und von der Inhaberin oder dem Inhaber der E-ID freigegeben sind.

[3] Darüber hinaus dürfen weder anerkannte IdP noch Betreiberinnen von E-ID-verwendenden Diensten ~~dürfen~~ die Personenidentifizierungsdaten gemäss Artikel 7 Absatz 2 oder die darauf basierenden Nutzungsprofile ohne die Zustimmung des E-ID Inhabers Dritten bekannt geben.

[4] Im Übrigen gilt die Datenschutzgesetzgebung.

Begründung

Abs. 3 statuiert das Verbot der Bekanntgabe von Personenidentifizierungsdaten an Dritte. Die Weitergabe an E-ID verwendende Dienste kann damit nicht gemeint sein. Auch die Weitergabe der Daten unter den IdP kann nicht

unter das Verbot fallen. Um dies klarzustellen, schlagen wir vor, Absatz 3 geringfügig zu ergänzen. Mit Zustimmung des Inhabers sollte eine Weitergabe ebenfalls möglich sein, was im Gesetzestext klargestellt werden sollte.

Artikel 14

Formulierungsvorschlag

Art. 14 Pflichten

[1] Eine E-ID ist persönlich und darf Dritten nicht zum Gebrauch überlassen werden.

[2] Die Inhaberin oder der Inhaber einer E-ID hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit die E-ID nicht missbräuchlich verwendet werden kann.

[2bis] Die Inhaberin oder der Inhaber meldet dem IdP Missbräuche.

[3] Der Bundesrat bestimmt die im Zusammenhang mit der E-ID einzuhaltenden Sorgfaltspflichten.

Begründung

Meist wird der Inhaber selbst feststellen, wenn mit seiner E-ID Missbrauch betrieben wird. In solchen Situationen ist ihm zuzumuten, dem IdP eine Meldung zu erstatten, damit dieser möglichst umgehend die notwendigen Massnahmen (Sperrung, Widerruf) einleiten kann.

Art. 15:

Formulierungsvorschlag

Art. 15: Vereinbarung mit IdP

Wer einen E-ID-verwendenden Dienst betreiben will, braucht eine Vereinbarung mit einem IdP oder einem Broker. Die Vereinbarung regelt insbesondere: (…)

Begründung

Wird im Gesetzestext der Begriff des Brokers definiert, so sollte Art. 15 dahingehend angepasst werden, als dass die Betreiberinnen von E-ID-verwendenden Diensten die entsprechende Vereinbarung entweder mit jedem IdP einzeln oder mit dem Broker pauschal abschliessen können.

Art. 16:

Formulierungsvorschlag

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

~~Wenn eine~~ Behörden in Vollzug von Bundesrecht ~~eine elektronische Identifizierung vorsieht, muss sie~~ akzeptieren jede E-ID nach diesem Gesetz ~~akzeptieren~~, die das geforderte Sicherheitsniveau erfüllt.

Kantone und Gemeinden sorgen dafür, dass eine E-ID nach diesem Gesetz auch im Vollzug von kantonalem oder kommunalem Recht akzeptiert werden.

Begründung

Um das Ziel einer weiten Verbreitung der E-ID zu erreichen, sollte diese im Behördenverkehr umfassend anerkannt werden. Dies wäre auch auf kantonaler bzw. kommunaler Ebene wünschenswert. Im Vollzug von Bundesrecht müssen kantonale und kommunale Behörden auch nach der im Vernehmlassungsentwurf vorgesehenen Bestimmung die E-ID anerkennen. Die technischen Voraussetzungen müssen also ohnehin geschaffen werden.

Entsprechend sollte Art. 16 noch umfassender formuliert sein und einen Auftrag an die Gemeinden und Kantone auf Gesetzesstufe enthalten.

Artikel 17

Formulierungsvorschlag

Art. 17 Pflichten

[1] Der IdP hat folgende Pflichten:

a. Er sorgt für das korrekte Funktionieren und den sicheren Betrieb des E-ID-Systems.
b. Er ordnet die Personenidentifizierungsdaten der E-ID zu und die E-ID der natürlichen Person.
c. Er gestaltet das E-ID-System so aus, dass die Gültigkeit aller E-ID, die es ausstellt, von der Identitätsstelle mit einem gebräuchlichen Verfahren jederzeit zuverlässig und kostenlos überprüft werden kann.
d. Er hält die Sicherheitsanforderungen nach Artikel 4 Absatz 1 Buchstabe e ein.
e. Er aktualisiert die Personenidentifizierungsdaten bei der Identitätsstelle periodisch.
f. Er holt von der Inhaberin oder dem Inhabers der E-ID das ausdrückliche Einverständnis ein zur Erstübermittlung von Personenidentifizierungsdaten an Betreiberinnen von E-ID-verwendenden Diensten.
g. Beim Teilen von Attributen ist das ausdrückliche Einverständnis bei jeder Übermittlung an Betreiberinnen von E-ID verwendenden Diensten notwendig.
~~h. Er löscht die Daten über die Anwendung einer E-ID nach sechs Monaten.~~

[2] Er ~~sorgt für einen Kundendienst, der es erlaubt~~ organisiert sich so, dass Meldungen über Störungen oder Verlust einer E-ID entgegengenommen und bearbeitet werden können ~~entgegenzunehmen und zu bearbeiten~~. Er meldet Fehler in den Personenidentifizierungsdaten der Identitätsstelle.

[3] Besteht die Gefahr, dass eine Drittperson Zugang zu einer E-ID haben könnte, oder wird der Verlust oder der Verdacht auf Missbrauch gemeldet, so ist der IdP verpflichtet, die E-ID unverzüglich zu sperren.

[4] Er muss sich vergewissern, dass die Person, welche die Sperrung beantragt, dazu berechtigt ist. Er informiert die Inhaberin oder den Inhaber der E-ID unverzüglich über die Sperrung.

Begründung

Abs. 1 lit c verlangt vom IdP, dass er das E-ID System so ausgestaltet, dass es jederzeit zuverlässig und kostenlos überprüft werden kann. Dies ist zu präzisieren, denn diese Pflicht kann nur gegenüber der Identitätsstelle gelten. Gegenüber Dritten, insbesondere gegenüber E-ID betreibenden Diensten, kann diese Pflicht nicht uneingeschränkt gelten.

Für die Löschung der Daten gelten bereits die Grundsätze des Datenschutzes (Datensparsamkeit). Zudem kann es regulatorische Anforderungen geben, welche eine längere Aufbewahrung erfordern, auch im Interesse des Kunden. Wir schlagen daher vor, lit. g zu streichen und für die E-ID keine Speziallösung vorzusehen.

Stattdessen schlagen wir für das Teilen von Attributen, die ja über die Personenidentifizierungsdaten hinausgehen, vor, bei jedem Ereignis das ausdrückliche Einverständnis des E-ID Inhabers vorzuschreiben. Da es sich bei diesen Attributen um sensible Daten handeln kann, erscheint dies als Standard sachgerecht.

Bezüglich Abs. 2 ist wichtig, dass Meldungen über Störungen oder den Verlust gemeldet und bearbeitet werden können. Wie dies organisiert ist, soll dem IdP überlassen bleiben. Es würde zu weit führen, wenn jeder IdP über einen voll ausgebauten Kundendienst verfügen müsste. Solange die Meldemöglichkeit gewahrt ist, sollte der IdP selber entscheiden können, wie weit er einen Kundendienst führen und ausbauen möchte.

Artikel 18

Formulierungsvorschlag

UBS

Art. 18 Interoperabilität

[1] IdP und Broker sorgen dafür ~~akzeptieren~~, dass ihre E-ID-Systeme gegenseitig akzeptiert werden und stellen sicher, dass die E-ID-Systeme interoperabel sind.

[2] Der Bundesrat bestimmt die technischen Standards und definiert die Schnittstellen. Er orientiert sich dabei an internationalen Standards.

Begründung

Mit der Einführung des Brokers wäre die Interoperabilität grundsätzlich sichergestellt. Das ist genau seine Funktion und die IdP, die einem Broker angeschlossen sind, müssen selber nicht mehr für Operabilität sorgen. Wenn der IdP ein Broker Netzwerk benützt, muss es an Letzterem liegen, die Interoperabilität sicherzustellen. Das stellt eine seiner Kernaufgaben dar, die zur Verbreitung der E-ID führen soll. Dieses System erleichtert insbesondere den Markteintritt von IdP, weil diese mit dem Anschluss an einen Broker gewährleistet haben, dass sie mit den bestehenden E-ID Systemen kompatibel sind. Entsprechend ist Art. 18 Abs. 1 um den Begriff des Brokers zu erweitern.

Damit eine Interoperabilität ggf. auch mit ausländischen Systemen hergestellt werden kann, ist es notwendig, dass die Standards und Schnittstellen entsprechend dem im Ausland Üblichen ausgestaltet werden. Dies soll in der Delegationsnorm zum Ausdruck gebracht werden.

Beat Lehman
lic.iur. Fürsprech
Acting Counsel Alcan Holdings Switzerland
Postfach 3244
5001 Aarau

Mobil-Tf +41 (0)79 500 82 32
e-mail b.lehmann-aarau@bluewin.ch

Aarau, 29.Mai 2017

Per E-Mail an das
Bundesamt für Justiz
z.H. Herrn Urs Paul Holenstein
Bundesrain 20
3003 Bern

Stellungnahme

zum Entwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID Gesetz)

Sehr geehrte Damen und Herren

Der Unterzeichnende war während mehr als zehn Jahren als Rechtskonsulent der IBM (Schweiz) und anschliessend im Konzernstab einer international ausgerichteten Schweizer Unternehmensgruppe (Alusuisse-Lonza - Alcan - Rio Tinto), heute nach deren Restrukturierung auch über das Erreichen der Altersgrenze hinaus tätig. Aufgrund dieser Erfahrungen wurde ich vom Bundesrat zur Mitwirkung in der Arbeitsgruppe für die Schaffung des Bundesgesetzes über den Datenschutz sowie 1975 und 1999 zur Mitarbeit an der Neufassung der handelsrechtlichen Buchführungs- und Aufbewahrungsvorschriften berufen. Darüber war und ist der Unterzeichnende Mitglied im Vorstand bzw. in der juristischen Kommission oder im Beirat von Berufs- und Wirtschaftsverbänden (u.a. swissmem, Swico, Verein Unternehmensdatenschutz (VDU), Information Security Society Switzerland (ISSS), sowie der Schweizer Informatikgesellschaft (s-i). Aus diesem Grunde bin ich am Verhältnis von Informatik, Wirtschaft und Recht und dessen Weiterentwicklung seit vielen Jahren persönlich interessiert und erlaube mir, als Ergänzung meiner Mitwirkung in Arbeitsgruppen von Fachorganisationen die nachstehende persönliche Stellungnahme abzugeben. Dabei habe ich mich vor allem mit den wirtschaftspolitischen Aspekten des Gesetzgebungsprojektes im Rahmen der europäischen Harmonisierung der Vorschriften über elektronische Identifizierung und Vertrauensdienste gemäss der Verordnung Nr. 9210/2014 des europäischen Parlaments und des Rats vom 24. Juli. 2014 ("eIDAS-Vo") befasst http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=DE

1. Regelungsbedarf

1.1 /1 Im Bereich **E-Commerce** ("B2C") kann darauf hingewiesen werden, dass wirtschaftlich tätige Unternehmen und (internationale) Handelsfirmen (der Alusuisse Konzern schon in den frühen 90er Jahren) wie auch Privatpersonen als Besteller von Güter und Dienstleistungen Wege zur elektronischen Abwicklung von Transaktionen ohne Anpassung der geltenden Gesetze entwickelt haben ha-

ben: Kommunikation durch ausgewählte (den in- bzw. ausländischen Unternehmens- oder Handelsregistern eingetragene) Vertreter, bzw. Eröffnung einer Vertragsbeziehung über eine elektronische Plattform durch Hinterlegung von persönlichen Angaben und einem Passwort (heute bestehend aus einer Kombination von Zahlen, Buchstaben und Sonderzeichen und Beantwortung von Identifizierungsfragen) über eine (gesicherte) E-Mail Verbindung und Bezahlung der bestellten bzw. gelieferten Güter und Dienstleistungen durch die Belastung der persönlichen oder Firmen-Kreditkarte bzw. über eine Bezahlplattform wie PayPal.

/2 Demgemäss besteht heute eine weite Verbreitung von meist durch Passwort/PIN abgesicherten analogen und/oder maschinell lesbaren elektronischen Ausweisen wie SuisseID, Apple ID oder Google Accounts sowie eine grosse Zahl von Kunden- oder Kreditkarten, SwissPass Versichertenkarte nach VVK - SR 832.105, Parkhaus- oder Bibliotheks-Benützungskarte, Ski- und Regionalpässe, usw., welche den Marktteilnehmern den Zugang zu Gütern und Dienstleistungen sowie eine Bezahlungsmöglichkeit eröffnen bzw. die erfolgte Bezahlung nachweisen. Man kann diese Entwicklung aus der Sicht der Rationalisierung der Verkehrsbeziehungen als unkontrollierten "Wildwuchs" mit einer Vielzahl von Missbrauchsmöglichkeiten bedauern – sie ist aber eine feste Tatsache des heutigen Wirtschaftslebens.

/3 In diesem Zusammenhang kann darauf hingewiesen werden, dass die Vielfalt der gegenwärtigen Identifzierungsmittel der **Gewährleistung des Datenschutzes** förderlich ist, weil sie die Zusammenführung von Daten über ausgeführte online-Transaktionen zu eigentlichen **Persönlichkeitsprofilen** (Art. 3 Bst. d DSG, bzw. Erwägungen 24 und 30, Art. 4 Ziff. 4 sowie Art. 22 der Verordnung (EU) 2016/679 - "Datenschutz-Grundverordnung" – DSGVO) beschränkt, erschwert oder gar verhindert. Darüber hinaus spielt bei verschiedenen dieser Karten, Ausweise und Pässe die überprüfbare Identität des Inhabers gar keine Rolle.

1.2 /1 Im Bereich **E-Government** ("C2G") besteht in der Schweiz seit mehreren Jahren ein **vielfältiges frei zugängliches und rege benütztes elektronisches Informationsangebot** auf Stufe Gemeinde, Kanton und Bund. Zusätzlich verfügen unsere Bürger vielerorts über die elektronische Unterstützung für die Einreichung der **Steuererklärung** sowie von Gesuchen, Anträgen und Begehren die in einem "hybriden Verfahren" durch online verfügbare Formulare am elektronischen Arbeitsplatz ausgefüllt, eigenhändig unterzeichnet und per Post, allenfalls auch eingescannt und elektronisch eingereicht werden können.

/2 Nach hier vertretener Auffassung ist der Einsatz der Informatik primär im **Massengeschäft**, d.h. der Bearbeitung einer grossen Zahl gleichartig strukturierter Vorgänge gerechtfertigt. Dabei steht vor allem die Einreichung der **Belege für die MWST-Abrechnung** im Vordergrund steht, wo bisher nur zögerliche Schritte zum Übergang auf die elektronische Abwicklung unternommen wurden.

/3 Hingegen handelt es sich bei der elektronischen Abwicklung relativ seltener oder sogar einmaliger Ereignisse wie die Anmeldung eines Neugeborenen (in der Praxis ohnehin in der Regel durch die Geburtsklinik) oder eines Todesfalles, die Anmeldung für eine Kinderkrippe, der Wohnungsumzug, der Wechsel des Zivilstandes u.ä. nach der Präsentation von "E Government im Alltag" https://www.egovernment.ch/de/ kaum um Anwendungen, welche im Lauf unseres Lebens zu wirklich realen Einsparungen führen dürfte (So hat der Unterzeichnende bisher einmal geheiratet, ist zweimal umgezogen und ist Vater von zwei erwachsenen Söhnen).

1.3 /1 Aufgrund der vorstehenden Überlegungen entspricht die Schaffung einer national und international gültigen elektronischen Identität nach hier vertretener Auffassung nicht unbedingt einem aktuellen dringenden Bedürfnis unserer Mitbürger als potentielle Anwender. Die Herausgabe digitaler Identifizierungsmittel dürfte aus diesem Grunde jedenfalls in näherer Zukunft nur ein beschränktes wirtschaftliches für Potential für die Anbieter dieser Mittel aufweisen. Die in der Motion 17.083 https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173083 enthaltenen spekulativen Annahmen über die durch die Einführung der elektronischen Identität in der wirtschaftlich und elektronisch hoch entwickelten und der Innovation verpflichten Schweiz zu der vergleichsweise winzigen Volkswirtschaft des mit EU Subventionen geförderten Schwellenlandes Estland erzielbaren Einsparungen von 2% unseres BIP von CHF 650.9 Mia/2016 dürften somit kaum realisierbar sein.
https://de.statista.com/statistik/daten/studie/14415/umfrage/bruttoinlandsprodukt-in-der-schweiz/

/2 Gemäss Angabe von Prof. Dr. A. Dietrich, HSLU, machen zur Zeit in der Schweiz **nur 33'500 Personen** d.h. ein sehr kleiner Teil der Gesamtbevölkerung - nicht einmal die "*digital natives*" - von den vorhandenen Möglichkeiten der digitalen Identifizierung und Authentifizierung Gebrauch https://blog.hslu.ch/retailbanking/2017/04/18/elektronische-id-grosse-chance-fuer-die-schweizer-banken/

/3 Auch **in unseren Nachbarländern ist die Akzeptanz elektronischer Ausweise sehr beschränkt** http://www.zdnet.de/88237100/online-funktion-des-neuen-personalausweises-wird-kaum-genutzt/ http://www.abendzeitung-muenchen.de/inhalt.ein-chip-als-flop-neuer-personalausweis-der-ungeliebte-ausweis.40c4a8b4-02c2-423e-95e3-bbbe4a158022.html http://www.zeit.de/digital/datenschutz/2017-04/elektronischer-personalausweis-eid-gesetz-biometrie-datenbank https://www.welt.de/wirtschaft/article142233969/Deutschland-verschlaeft-die-Ausweis-Revolution.html http://www.tagesanzeiger.ch/schweiz/standard/Eine-staatliche-digitale-Identitaet-fuer-alle/story/2792524 https://www.welt.de/wirtschaft/article13463921/Elektronischer-Ausweis-wird-zum-Totalausfall.html 7 https://www.heise.de/newsticker/meldung/Oesterreich-setzt-nach-Scheitern-der-Buergerkarte-auf-die-Handysignatur-2644097.html http://derstandard.at/2627319/Wie-wir-lernen-sollen-die-Buergerkarte-zu-lieben

/4 Diesen Realien ist Rechnung zu tragen. Ungeachtet dieser Vorbehalte sehen wir aus der Sicht der Wirtschaft einen **echten Bedarf für eine international, insbesondere im europäischen Wirtschaftsraum (EWR) von Privaten und Behörden anerkannte, harmonisierte und gültige elektronische Identifizierung und Authentifizierung** von natürliche Personen, vor allem aber auch von **geschäftlich international tätigen Unternehmen**.

2. Verhältnis E-ID Gesetz zur eIDAS Verordnung

2.1 /1 Mit der Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rats vom 23. Juli 2014 ("eIDAS-Vo") http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32014R0910 soll eine **einheitliche Grundlage für eine in sämtlichen EU Mitgliedländern anerkannte elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt** geschaffen werden (Erwägung 2 eIDAS-Vo).

/2 Demgemäss enthält die eIDAS-Vo (Erwägung 6) ein **integriertes Gesamtpaket von Harmonisierungsvorschriften** für

(1) die elektronische Identifizierung und Authentifizierung von natürlichen und juristischen Personen, die im europäischen Wirtschaftsraum (EWR) niedergelassen sind

(2) die Erstellung maschinell lesbarer Dokumente

(3) elektronische Signaturen und Siegel

(4) die Authentifizierung von Webseiten sowie

(5) elektronische Zustelldienste für interoperable elektronische Behördendienste.

2.2 /1 Im Unterschied zur eIDAS-Vo beschränkt sich das **E-ID-Gesetz** (”E-ID-G”) gemäss Vorentwurf vom 23. Februar 2017 https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/e-id/vorentw-d.pdf auf

- die digitale Identifizierung und Authentifizierung
- von natürlichen Personen
- Schweizer Staatsangehöriger mit gültigem Ausweis oder zugelassene Inhaber eines Ausländerausweises

/2 Dagegen wird die Regelung der elektronische Unterschrift und des elektronischen Siegels sowie aller weiteren Mittel zur Identifizierung und Authentifzierung der an der digitalen Wirtschaft beteiligten natürlichen oder juristischen, inländischen oder ausländischen Personen (wie Ferienreisende; Grenzgänger) nicht erfasst bzw. weiterhin der Regelung in der bestehenden Signaturgesetzgebung (ZertES und VZertES) überlassen.

3. Harmonisierung von E-ID-G und eIDAS-Vo

3.1 Nach hier vertretener Auffassung wäre im Sinne der Herstellung von Konformität der schweizerischen Lösung mit dem harmonisierten europäischen Recht und deren Nutzung im Verkehr mit Privaten und Behörden im Europäischen Binnenmarkt ein Vorgehen vorzuziehen gewesen, durch welches die Voraussetzungen für die Anerkennung der elektronischen Identität **und Authentifizierung in die kürzlich aktualisierte Gesetzgebung über die elektronische Signatur** (ZertES / VZertES) https://www.admin.ch/opc/de/classified-compilation/20011277/ **integriert** worden wäre. Dies hätte namentlich eine gewisse Vereinheitlichung der organisatorischen und technischen Massnahmen für die Herausgabe der Identifizierungsmittel sowie der Zertifikate für die elektronische Signatur und elektronischen Siegel ermöglicht.

3.2 Immerhin ist davon auszugehen, dass die Inhaber einer digitalen Identität nach E-ID-G die Voraussetzungen für den Erwerb eines geregelten Zertifikats nach ZertES erfüllen und von der persönlichen Vorlage von Pass oder Identitätskarte gemäss Art. 9 Abs. 1 ZertES entbunden werden sollen. Eine entsprechende Freistellung sollte u.E. noch in Art. 5 Abs. 1 VZertE vorgesehen werden.

3.3 Darüber hinaus sollte bei der organisatorisch-technischen Umsetzung des E-ID Gesetzes gemäss dessen 7. Abschnitt zur Vermeidung von Doppelspurigkeiten und nicht gerechtfertigtem bürokratischen Aufwand angestrebt werden, die Aufgabe und Tätigkeit der Anerkennungsstellen gemäss E-ID Gesetz und ZertES zu vereinigen und auf jeden Fall aufeinander abzustimmen.

4. Private oder staatliche Vertrauensdiensteanbieter (VDA)

4.1 Das E-ID-G beruht - wohl aus Gründen der damit verbundenen Kosten und Risiken sowie der Haftung nach Verantwortlichkeitsgesetz - auf der Bereitstellung von Identifizierungsmitteln durch **pri-**

vatrechtlich organisierte VDA, bzw. ”Identity Provider“ (IdP) nach dem Wortlaut von Art. 2 Bst. c E-ID-G. Diese Regelungen sind mit der eIDAS-Vo gemäss deren Erwägungen 12, 13 und 13 verträglich, weil die **eIDAS-Vo privatrechtliche Lösungen ebenfalls zulässt**.

4.2 Dennoch muss an dieser Stelle festgehalten werden, dass **ein vom Staat herausgegebenes digitales Identifizierungsmittel wohl ein grösseres Vertrauen der Anwender** erzeugen würde; dies vor allem im der Inhaber einer schweizerischen E-ID im Verkehr mit ausländischen Behörden und Geschäftspartnern im EWR.

4.3 Es wird daher postuliert, die subsidiäre Rolle des Bundes bei der Ausstellung von E-ID der Sicherheitsniveaus ”substanziell“ und/oder ”hoch” zu verstärken und zu konkretisieren, indem das subsidiäre Bundes-System zur Verfügung stehen muss, wenn in dem gemäss Art. 26 Abs. 2 E-ID G vom Bundesrat festgelegten Zeitpunkt für das Inkrafttreten des E-ID Gesetzes, bzw. nach Ablauf einer Übergangsperiode von 3-6 Monaten, kein privater IdP für die Ausstellung von E-ID für diese Sicherheitsniveaus anerkannt worden ist.

5. Identifizierung und Authentifizierung natürlicher und juristischer Personen

5.1 /1 Im Unterschied zur eIDAS-Vo, welche in den Erwägungen 58-60 und 65 sowie in Art. 1 (a), Art. 3 durchgehend, Art. 7 (d), Art. 8 (3) (a) und (c) sowie Art 12 (4) (d) die **digitale Identifizierung und Authentifizierung juristischer Personen jeder Art und Form** (bzw. die Identifizierung einer natürlichen Person, welche eine juristische Person für den Erwerb eines elektronischen Siegels berechtigterweise vertreten kann) **ausdrücklich zulässt**, beschränkt das E-ID Gesetz die Identifizierung und Authentifizierung wie die eIDAS-Vo (Erwägung 16) auf **natürliche Personen.**

/2 Gemäss Erwägung 68 der eIDAS-Vo in Übereinstimmung mit Art. 54 des konsolidierten Vertrages über die Arbeitsweise der Europäischen Union (AEUV) vom 26. 10.2012 http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex:12012E/TXT steht es den Teilnehmern am europäische Binnenmarkt frei, die Rechtsform zu wählen, die sie für die Ausübung ihrer Tätigkeit für geeignet halten. Folglich gelten gemäss eIDAS-VO als ”juristische Personen“ ”sämtliche Einrichtungen, die nach dem Recht eines Mitgliedstaats gegründet wurden oder diesem Recht unterstehen, unabhängig von ihrer Rechtsform”.

5.2 /1 Nach hier vertretener Auffassung ist die **Verfügbarkeit einer elektronischen Identität vor allem für Unternehmen wichtig, welche im EWR Geschäfte abwickeln und mit europäischen Behörden verkehren** müssen. Für diesen definierten Kreis von Nutzern der elektronischen Identität bringt der vorliegende Entwurf des E-ID Gesetzes leider keine Erleichterung.

/2 Die gemäss den Bestimmungen des UIDG https://www.admin.ch/opc/de/classified-compilation/20082601/index.html im UID Register eingetragenen Unternehmen bleiben somit auf den Erwerb einer geregelten elektronischen Signatur nach Art. 2 Bst. c ZertES bzw. eines geregelten elektronischen Siegels nach Art. 2 Bst. d ZertES angewiesen, um sich im Verkehr mit ausländischen Lieferanten, Kunden, Geschäftspartnern oder Behörden vertrauenswürdig ausweisen zu können.

/3 Immerhin ist in den Schlussbestimmungen des E-ID Gesetzes die Möglichkeit geschaffen, dass die durch den Eintrag im Handelsregister ausgewiesenen Vertreter einer UID Einheit sich beim Erwerb einer geregelten elektronischen Signatur bzw. eines geregelten elektronischen Sigels gegenüber

einer anerkannten Anbieterin von Zertifizierungsdienstes gemäss Art. 9 Abs. 1bis ZertES in Zukunft mit dem Identitätsnachweis nach dem E-ID Gesetz legitimieren können.

/4 Auf diesem Umweg sollte es es für die im Handelsregister eingetragenen UID Einheiten – und darunter fallen auch wirtschaftlich tätige Unternehmen - u.E. möglich werden, auf dem Umweg über den Erwerb einer E-ID durch die einzeln oder kollektiv (Art. 460 Abs. 2 OR) zur Vertretung eines im UID-Register eingetragenen Unternehmens ermächtigten Personen im Online-Verfahren, ohne persönliche Vorsprache bei der Ausgabestelle, die Ausstellung einer geregelten elektronischen Signatur bzw. eines geregelten elektronischen Siegels zu erwirken.

5.3 Darüber hinaus sollte nach hier vertretener Auffassung die in den Schussbestimmungen des E-ID Gesetzes enthaltene Möglichkeit der online-Ausstellung geregelter Zertifikate gemäss Art. 9 Abs. 1bis ZertES die Erstellung von **Fernsignaturen** im Sinne von Erwägung 52 eIDAS-VO für geregelte elektronische Signaturen und geregelte elektronische Siegel ermöglichen. In diesem Sinne sollte das E-ID Gesetz u.E. noch präzisiert und konkretisiert werden.

6. Teilnahme am europäischen elektronischen Binnenmarkt

6.1 Ungeachtet der vorstehend umschriebenen Vorbehalte und Einschränkungen sollte nach hier vertretener Meinung durch das E-ID Gesetz die Grundlage dafür geschaffen werden, dass in der Schweiz niedergelassene Personen und Unternehmen in gleicher Art und Weise am europäischen elektronischen Binnenmarkt teilnehmen können wie ihre Kunden, Geschäftspartner und Mitbewerber im EWR (eIDAS-Vo Erwägung 9 und 12).

6.2 Zu diesem Zweck sollte die Möglichkeit geschaffen werden, dass die in der Schweiz erworbenen Identifizierungsmittel gemäss Erwägung 13 und 14 eIDAS-Vo **der EU Kommission notifiziert**, dadurch im EWR amtlich anerkannt und bei grenzüberschreitenden Transaktionen mit Kunden, Geschäftspartnern und Mitbewerber sowie ausländischen Behörden im EWR verwendet werden können.

6.3 Umgekehrt sollten ausländische (natürliche und juristische) Personen als Inhaberinnen einer gemäss den Anforderungen der eIDAS-Vo von einem ausländischen Staat, insbesondere einem EU Mitgliedland ausgestellten und anerkannten Identifzierungsmittel ohne weiteren Nachweis der Identität und Authentifizierung zu Transaktionen mit schweizerischen Kunden, Lieferanten oder Geschäftspartnern bzw. mit schweizerischen Behörden zugelassen werden.

6.4 Demgemäss wird vorgeschlagen, dass der Bundesrat im E-ID-G analog zu Art. 20 ZertES ermächtigt wird, **internationale Abkomme**n **betreffend die gegenseitige Anerkennung** der in den Staaten der Vertragsparteien herausgegebenen und anerkannten elektronischen Identifizierungsmittel abzuschliessen.

6.5 In einem solchen Abkommen könnte auch festgelegt werden, dass eine den Anforderungen der eIDAS-Vo entsprechende **qualifizierte elektronische Signatur** einer natürlichen oder juristischen Person im EWR gemäss Erwägung 60 eIDAS-Vo in der Schweiz gegenüber Privaten und Behörden die **gleiche Rechtswirkung wie eine handschriftliche Unterschrift** haben soll.

7. Bedeutung des Datenschutzes im E-ID Gesetz

7.1 Der Gewährleistung des Datenschutzes kommt bei der Verwendung elektronischer Identifizierungseinheiten nach Massgabe der eIDAS-Vo und des E-ID-G besondere Bedeutung zu, weil dadurch sämtliche elektronische Transaktionen auf einen eindeutig bestimmten identifizierten und authentifizierten Urheber zurückgeführt werden können. In diese Zusammenhang haben b e i d e in Art. 1 DSG erwähnten Aspekte des Datenschutzes eine erhebliche Bedeutung:

A. Schutz der Persönlichkeit und der **Privatsphäre** (Art. 13 BV; Art. 28 ZGB: "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", umschrieben vom deutschen Bundesverfassungsgericht im Entscheid vom 27. Februar 20098 1 BvR 370/07 und 1 BvR 595/07 im Zusammenhang mit der umstrittenen "Online-Durchsuchung" http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html;jsessionid=D9883915902F181CD936648A5BAC101E.2_cid393

B. Gewährleistung der persönlichen Freiheit (Art. 10 Abs. 2 BV) im Sinne des Grundrechts auf "**informationelle Selbstbestimmung**" nach ständiger Praxis des Bundesgerichts (BGE 120 II 118 Erw. 3a; 122 II 153; 124 I 176; 128 II 259; 138 II 346 in der Nachfolge des Entscheids des deutschen Bundesverfassungsgerichts BVerfGE 65 Nr. 1 S. 41 E. 1a https://www.emr-sb.de/datenschutz-urteile-nachrichtenleser/items/bverfge-65-1-volkszaehlung.html

7.2 /1 Datenschutz im Bereich der elektronischen Identifizierung von (natürlichen oder juristischen) Personen bedeutet zunächst gemäss eIDAS-Vo Erwägung 11 dass zur Identifizierung und Authentifizierung für Online-Dienste **n u r solche Daten verarbeitet werden die dem Zweck der Gewährung des Zugangs zu Online-Diensten entsprechen, dafür erforderlich sind und nicht darüber hinausgehen**.

/2 Diesbezüglich bestehen gegenüber der Art. 7 Abs. 2 Bst. a sowie Art. 9-10 E-ID-G zugelassene **Verwendung der u n v e r ä n d e r t e n Versichertennummer** nach 50c AHVG ("AHV- oder Sozialversicherungsnummer") als Bestandteil der Personenidentifizierungsdaten **aus datenschutzrechtlicher Sicht erhebliche Bedenken**.

/3 Die Proliferation der Verwendung der Sozialversicherungsnummer schafft die Möglichkeit der Zusammenführung sämtlicher online Transaktionen des Inhabers einer E-ID in der Informationsgesellschaft und daher zur Möglichkeit der Entstehung von **Persönlichkeitsprofilen** im Sine von Art. 3 Bst. d DSG bzw. zum "**Profiling**" gemäss den Erwägungen 24, 60, 71, 72 und Art. 4 (4) und Art. 22 der Verordnung (EU) 201/679 Datenschutz-Grundverordnung (DSGVO) http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE sowie Art. 3 Bst. f, 4 Abs. 6, 23 Abs. 2 Bst. d, und Art. 27 des Vorentwurfs zu einer Totalrevision des schweizerischen Datenschutzgesetzes https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Entwurf-DSB_de.pdf.

/4 Denn wenn Art. 36 Abs. 4 Bst. c DSG für die Verwendung von Mitteln zur Identifikation von Personen eine besondere Rechtsgrundlage fordert, sollte damit nicht im Sinne von Art. 50d und 50e AHVG zum Ausdruck gebracht werden, dass für die Verwendung der Versichertennummer einfach ein Bundesgesetz als Rechtsgrundlage genüge, sondern dass dies nur gilt, wenn der Verwendungszweck diese Verwendung erfordert und rechtfertigt. Mit anderen Worten, die Verwendung der AHV-

Nummer soll auf das absolut Notwendige beschränkt werden. So die Botschaft 88.032 zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988 S. 487:
https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10050713 "Die AHV-Nummer wird heute in derart vielen Bereichen eingesetzt, dass, würden die entsprechenden Informationen verknüpft, umfassende Persönlichkeitsbilder entstünden."

/5 Dieses Risiko für den Datenschutz in dem unter vorstehender Ziff. 7.1 dargestellten umfassenden Begriff als Grundrecht wäre insbesondere dann gegeben, wenn in der durch das E-ID Gesetz geschaffenen Grundlage der künftigen Informationsgesellschaft sämtlichen online-Transaktionen der InhaberInnen einer E-ID mit den Sicherheitsniveaus "substanziell" oder "hoch"die Versichertennummer nach Art. 50c AHVG zugeordnet werden kann. Darüber hinaus wir ddem IdP in Art. 9 Abs. 2 E-ID-G das Recht eingeräumt, die Versichertennummer allen zur systematischen Verwendung der Sozialversicherungsnummer berechtigten Dritten bekannt zu geben.

/6 Dies würde durch die Möglichkeit der Verknüpfung der elektronischen Handlungen der InhaberInnen einer E-ID in der digitalen Welt mit den überaus zahlreichen zugelassenen Anwendungsfällen der Sozialversicherungsnummer [Es gab deren gemäss Bericht des EDÖB im Jahre 2015 schon **14'000** (sic!) https://biblio.parlament.ch/e-docs/384220.pdf] die **Erstellung eines umfassenden Persönlichkeitsbildes in einem bisher nirgends realisierten Umfang erlauben** und darüber hinaus ein **breites Feld von Möglichkeiten zum Missbrauch** durch Einflussnahme und Einwirkungen auf die betreffende InhaberInnen einer E-ID in der realen und/oder virtuellen Welt schaffen.

/7 Der EdÖB hat daher vorgeschlagenen, dass in jenen Situationen, wo mit Hilfe und auf der Grundlage der AHV-Versichertennummer die eindeutige Identifizierung einer natürlichen Person geschaffen werden soll, mit Hilfe der heute zur Verfügung stehenden kryptographischen Transformationen eine von der AHV-Nummer abgeleitete **sektorielle Identifikationsnummer** wie in Österreich erzeugt wird. https://www.edoeb.admin.ch/dokumentation/00153/00341/00343/index.html?lang=de

/8 Aufgrund der vorstehenden Überlegungen wird daher beantragt in Anlehnung an die Formulierung von Art. 26 des aktuellen Entwurfs zu einem Informationssicherheitsgesetz des Bundes (ISG) https://www.newsd.admin.ch/newsd/message/attachments/47359.pdf die datenschutzkonforme Lösung vorzusehen, dass die Versichertennummer nach 50c AHVG im Identitätsverwaltungssystem nur vorübergehend verwendet werden kann, um **eine den Inhaber einer E-ID eindeutig identifizierende aber nicht rückrechenbare Personennummer** zu erzeugen. Anschliessend müsste die Versicherungsnummer gelöscht werden. Art. 9 E-ID-G müsste entsprechend angepasst werden.

7.3 /1 Ähnliche Bedenken ergeben sich aus der mit Art. 7 Abs. 2 Bst. f E-ID Gesetz geschaffenen Recht der IdP das "**Gesichtsbild**" der InhaberInnen einer E-ID in den Bestand der Personenidentifizierungsdaten aufzunehmen.

/2 Die Erfassung des Gesichtsbildes bzw. **weiterer biometrischer Merkmale** in den von den IdP für natürliche Personen ausgestellten E-ID's der Sicherheitsniveaus "substanziell" oder "hoch" schafft zweifellos einen zusätzlichen Schutz gegen deren Unterschiebung, Fälschung und Imitation, greift jedoch in die grundrechtlich geschützte Privatsphäre und das informationelle Selbstbestimmungsrecht der betroffenen Personen als InhaberInnen der E-ID ein.

/3 Denn mit der automatisierten Gesichtserkennung durch Abgleich des mit elektronischen Verfahren erfassten und analysierten Gesichtsbildes mit Fotos, die von Überwachungskameras oder Zutrittskontrollsystemen aufgenommen wurden oder in sozialen Netzwerken wie Facebook gespeichert sind können Personen identifiziert und deren Verhalten analysiert und ausgewertet werden http://www.zeit.de/digital/datenschutz/2016-05/findface-gesichtserkennung-republica-adam-harvey http://www.faz.net/aktuell/technik-motor/computer-internet/gesichtserkennung-bei-facebook-gesucht-erkannt-verlinkt-1657009.html

/4 **Gesichtsbilder und andere biometrische Merkmale** einer natürlichen Person wie z.B. Fingerabdruck, Irismuster, Handgeometrie gehören - wenn sie mit besonderen technischen Verfahren erfasst und analysiert werden - gemäss den Erwägungen 51 und Art. 4 Ziff. 14 DSGVO http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE sowie Art. 3 Bst. c Ziff. 3 des Vorentwurfs zu einer Totalrevision des Datenschutzgesetzes vom 21. Dezember 2016 https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des- Datenschutzgesetzes_Entwurf-DSB_de.pdf zu den "**besonders schützenswerten Personendaten**".

/5 Der EDÖB hat daher klare rechtliche Grenzen für das **elektronische Personentracking** durch Nutzung des Gesichtsbildes und biometrischer Daten natürlicher Personen aufgezeigt https://www.edoeb.admin.ch/datenschutz/00625/01170/index.html?lang=de Ihre Bearbeitung ist gemäss Art. 9 Abs. 1 DSGVO **grundsätzlich untersagt** und darf gemäss Art. 9 Abs. 2 DSGVO nur in bestimmten **Ausnahmesituationen** vorgenommen werden bzw. bedarf gestützt auf Art. 9 Abs. 2 Bst. a DSGVO und ensprechend Art. 4 Abs. 6 Satz 2 VE Total Rev DSG bzw. der **ausdrücklichen informierten Einwilligung** der betroffenen Personen.

/6 Die Aufnahme des Gesichtsbildes und weiterer biometrischer Merkmale wie z.B. Fingerabdruck, Irismuster, Handgeometrie in die Personenidentifizierungsdaten gemäss Art. 7 Abs. 2 EID Gesetz ist somit nach hier vertretener Auffassung grundsätzlich zulässig und im Sinn der Sicherung qualifizierter Identifizierungsmittel gegen die Risiken von Verfälschung oder Imitation erwünscht, vorausgesetzt dass **der IdP dafür vorgängig die ausdrückliche und in Textform nachzuweisende Einwilligung der betroffenen Person eingeholt hat**. Dies wäre in Ergänzung von Art. 7 Abs. 2 E-ID G festzuhalten. Art. 9 E-ID Gesetz wäre entsprechend datenschutzgerecht anzupassen.

7.3 Im Weiteren wird auch unter dem Aspekt des Datenschutzes und der Befürchtungen gegenüber der Herstellung von Persönlichkeitsbildern durch "**Profiling**" gemäss den Erwägungen 60, 71, 72 sowie den Art. 4 (4) und Art. 22 der Europäischen Datenschutzgrundverordnung (DSGVO) http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE sowie Art. 3 Bst. f, 4 Abs. 6, 23 Abs. 2 Bst. d, und Art. 27 des Vorentwurfs zu einer des Totalrevision DSG https://www.admin.ch/ch/d/gg/pc/documents/2826/Totalrevision-des-Datenschutzgesetzes_Entwurf-DSB_de.pdf beantragt, dass im E-ID Gesetz ausdrücklich erklärt wird, dass **eine Person mehrere E-ID** mit möglicherweise unterschiedlichen Sicherheitsniveaus erwerben kann. Dies wird zwar durch die vorliegende Fassung des Gesetzesentwurfs nicht ausgeschlossen, aber auch nicht ausdrücklich zugelassen. Die vorgeschlagene Ergänzung würde der Präzisierung und Konkretisierung des Gesetzes dienen.

7.4 Dem Persönlichkeits- und Datenschutz dient im Weiteren in Analogie zu Art. 7 Abs. 2 Bst. d ZertES die Zulassung von **Pseudonymen** für natürliche Personen in den ausgegebenen E-ID's. Dies müsste

im E-ID-G klar gesagt werden. Selbstverständlich setzt dies die Identifikation der hinter dem Pseudonym stehenden natürlichen Person voraus (vgl. eIDAS-Vo Erwägung 33).

8. Langzeitsicherung und Haftung der IdP

8.1 Gemäss Art. 17 Abs. 1 Bst. c E-ID Gesetz hat der IdP das E-ID-System so auszugestalten, dass die **Gültigkeit aller E-ID, die es ausstellt, mit einem gebräuchlichen Verfahren jederzeit zuverlässig und kostenlos überprüft** werden kann. Gemäss Erwägung 61 eIDAS Vo soll durch die Langzeitbewahrung von Informationen gewährleistet werden, dass die Gültigkeit der mit Hilfe der Identifizierungsmittel (in der Schweiz: E-ID) erzeugten elektronischen Signaturen und elektronischen Siegel über lange Zeiträume nachgewiesen werden kann, so dass diese ungeachtet künftiger technologischer Veränderungen noch validiert werden können.

8.2 Die nachträgliche Überprüfbarkeit der Identifizierung und Authentifizierung der durch eine E-ID ausgewiesenen Beteiligten an einer elektronischen Transaktion stellt an die IdP besonders hohe organisatorische und technische Herausforderungen. Denn es geht hier nicht nur um die Gewährleistung der Nachprüfbarkeit der Abwicklung eines Austauschgeschäfts, sondern um den **gerichtsfesten Nachweis der Gültigkeit und Rechtskonformität von Dauerschulverhältnissen**, die sich über viele Jahrzehnte erstrecken können, wie z.B. die Gründung einer Gesellschaft, Statutenänderungen; Eröffnung eines während Jahrzehnten genutzten Bankkontos; Nachweis des Jahre zurück liegenden Inhalts einer Webseite mit den damals geltenden AGB eines Anbieters im E Commerce; Darlehens-, Arbeits-, Agentur-, Miet-, Sukzessivlieferungs-, Lizenz- oder Versicherungsverträge; Erbverträge; Erwerb, Belastung und Nutzung von Immobilien, Ausstellung von Bewilligungen und Konzessionen.

8.3 Wie diese höhst anspruchsvolle Aufgabe gelöst werden kann sollte sich aus den gemäss Art. 4 Bst. c E-ID-G vom Bundesrat zu erlassenden **näheren Vorschriften** über die für die E-ID Systeme anwendbaren **(technischen) Standards** (z.B. Verwendung des Dokumentenstandards PDF-A? bzw. Bedingugnen für die Datenmigration im Sinne von Art. 10 GeBüV) ergeben.

8.4 Nicht klar geregelt ist im E-ID Gesetz die **Folge von Konkurs oder Geschäftsaufgabe eines IdP** wenn das betreffende E-ID-System nicht im Sinn von Art. 11 Abs. 3 E-ID Gesetz von einem anderen IdP übernommen wird (vgl. Erwägung 4 eiDAS Vo). Für diesen Fall wäre 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 soll.

8.5 Für den **Schaden** welcher den InhaberInnen einer E-ID und den an einer online Transaktion Beteiligten selche auf die Gültigkeit einer Identifizierung und Authentifizierung einer E-ID vertrauen aufgrund der Nichterfüllung der Pflicht zum dauernden Nachweis der Gültigkeit ausgestellter E-ID entstehen kann, haften die Inhaberinnen der E-ID sowie die IdP nach Obligationenrecht (Art. 24 Abs. 1 E-ID Gesetz sowie Erwägung 27, 18, 35 und 37 sowie Art. 11 und 13 eIDAS Vo), somit nach hier vertretener Auffassung nach 97 ff OR (Vertragshaftung) bzw. nach Art. 41 ff OR (Deliktshaftung).

8.6 Nicht geregelt ist in diesem Zusammenhang, ob und unter welchen Voraussetzungen die InhaberInnen der E-ID bzw. der IdP die **Nutzung der von ihnen angebotenen Dienste unter bestimmten Bedingungen beschränken und damit eine Haftung für Schäden aus einer darüber hinausge-**

henden Nutzung ausschliessen (Art. 100 OR- können. Dabei sollten nach Erwägung 35 sowie Art. 13 Abs. 2 eIDAS Verordnung die InhaberInnen der E-ID bzw. die vertrauenden Dritten über eine solche Nutzungs- und Haftungsbeschränkung erkennbar unterrichtet werden.

9. Weitere Massnahmen in Anlehnung an die eIDAS-Vo

9.1 Im Hinblick auf die Herstellung der Konformität der in der Schweiz ausgegebenen E-ID mit den Anforderungen an die Identifizierungsmittel und die organisatorischen und technischen Massnahmen für deren Ausgabe wäre zu prüfen, ob in Anlehnung zu Erwägung 43-44 und Art. 17 Abs. 4 Art. 18 und Art. 20 eIDAS-Vo zur Förderung des Vertrauens in die aufgrund des E-ID G ausgestellten E-ID in unserem Land ebenfalls **Konformitätsbewertungen** durchgeführt und eine **Konformitätsbewertungsstelle** für E-ID-Systeme und E-ID in Anlehnung an die Regeln des Bundesgesetzes über technische Handelshemmnisse (THG) eingerichtet werden soll.

9.2 Zur **Förderung des Vertrauens** der Anwender wäre darüber hinaus zu prüfen, ob im E-ID Gesetz, bzw. in einer Ergänzung des ZertES, im Sinne der 47 und Art. 23 eIDAS-Vo ein **Vertrauenssiegel** für anerkannte qualifizierte IdP und die Anbieterinnen von Zertifizierungsdiensten nach Art. 3 ZertES eingeführt werden könnte.

Ich bin Ihnen aus der Sicht der künftigen Anwender unserer produzierenden Wirtschaft zu Dank verpflichtet, wenn Sie die aus der Sicht eines Wirtschaftsjuristen und Datenschützers der ersten Stunde entwickelten vorstehenden Überlegungen und Formulierungsvorschläge bei der Erarbeitung der anspruchsvollen Gesetzgebung über die elektronische Identifizierung und Authentifizierung in möglichst grosser Übereinstimmung mit dem durch die eIDAS Verordnung harmonisierten europäischen Recht und in Abstimmung auf die inhaltlich verwandten Anforderungen der Gesetzgebung über die elektronische Signatur und die Ausgabe elektronischer Siegel berücksichtigen.

Mit vorzüglicher Hochachtung

Beat Lehmann

Cham, 29-Mai-17 / bo

An: copiur@bj.admin.ch

Sehr geehrte Damen und Herren

Bitte finden Sie die Anmerkungen Vernehmlassung zu Bundesgesetz über anerkannte elektronische Identifizierungseinheiten E-ID-Gesetz

Art. 2 Abs. a
Ergänzung Juristischen Person
und Authentifizierung einer natürlichen und oder juristischen Person verwendet wird;
Es gibt natürliche Personen, die auch eine Einzelfirma haben.

Art. 2 Abs. d.
Änderung Personeneinheit (sich wiederholende Begriffe „Person" sinngemäss)
eine Personeinheit (juristische und oder natürliche Person) eindeutig repräsentieren;

Art. 3 Abs. 1 d
Ergänzung juristische Personen sinngemäss welche im Schweiz. Handelsregister eingetragen sind oder eine Geschäftstätigkeit nachweisen.
(Anmerkung: Es sollte die Identifikation einer Firma auch für Rechtsschriften nachgewiesen werden können. Weiteres Beispiel eine Anwaltskanzlei XY-Partner nicht im HR eingetragen und Anwalt 1, Anwalt 2, Anwalt n dieser Kanzlei, welche einer Kanzlei partnerschaftlich angehört, aber auf eigene Rechnung handelt.)

Art. 4
Abs. 2 a ihren Sitz in der Schweiz haben; Ergänzung Schweiz. Botschaft und Konsulat im Ausland

Erklärung: Als Auslandschweizer kann ich im Ausland eine ID bekommen, aber keinen E-ID. Weiteres Beispiel Ich will als Schweizer im Ausland ein E-mail z. B. an eine Schweizer Behörde schreiben und kann mein E-mail nicht identifizieren. Sinngemäss Ähnliches gilt, wenn ich im Ausland in einer Tochterfirma, Niederlassung eines Schweizer Unternehmens arbeite.

Röhrliberg 8, CH-6330 Cham, Tel. 041 534 29 18 - E-mail: datazug@ittema.ch

Art. 4 Abs. 2 g
Diesen Artikel 4 Abs. 2 g und Art. 24 streichen, weil er unpraktikabel ist.
Es handelt sich nicht um ID-Karten oder Schweiz. Passbücher, sondern es handelt sich bei der E-ID lediglich um einen Code! Es ist bekannt, dass der Amerikanische Geheimdienst NSA oder CIA alles Elektronische lesen können. Sie können es lesen, ohne dass der Betreffende etwas davon merkt. Das Bundesamt für Justiz will Trojaner Vieren zur angeblichen Verbrecherbekämpfung verwenden. Ein Richter segnet dies ab und ein Polizist hackt bei einem IdP und klaut eine falsche Identität, um seine wahre Indentität, als Ermittler zu verschleiern und wenn alles raus kommt soll die Haftpflichtversicherung des Idtentity Service Provider dafür gerade stehen. Und wenn sie dies nicht macht, soll der IdP sein Leben lang dafür gerade stehen. Dieser Killerartikel ermöglicht es nur den grossen IdP (Swisscom, Post, SBB usw.) E-ID anzubieten. Falls es irgendwo keine absolute Sicherheit gibt ist es in der E-ID. Kleinere Unternehmen können es sich, wegen der zu zahlenden horrend hohen Versicherungsprämie gar nicht leisten diesen IdP Service anzubieten.

Damit man mich besser versteht folgende Erklärung:

Das Problem ist der hohe Preis, weshalb sich die E-ID nicht durch setzte.

Wir (mit steigender Anzahl) Informatikprofessoren und Studenten verschiedener Unis, Fachhochschulen und ETH planen einen ID-Schlüssel zu entwickeln, welcher günstig z. B. Fr. 5.00 evt. Kostenlos ist, damit er von möglichst vielen benutzt wird. Als Beispiel besteht der ID-Schlüssel aus noch zu bestimmenden Teilen der AHV-Nr., Nummer des Passes oder ID, dem Geburtsdatum, der Personennummer des Steueramtes, der Strassennummer und einem Algorhythums, der daraus einen Code generiert. Ich gehe z. B. zur Einwohnerkontrolle, um mich ins Einwohnerregster anzumelden oder eine neue ID zu beantragen oder einer Polizeistelle, Handelsregisteramt oder Strassenverkehrsamt. Die Sachbearbeiterin überprüft meine Identität und gibt mir auf Wunsch einen Code, welcher den ID-Schlüssel beim ersten Login generiert. Das ist ein Arbeitsaufwand von ca. 5 Minuten. Da braucht es keine grosse teure Bürokratie und all die Vorschriften betreffend. Die Dienstleistung eines IdP sollte nicht in erster Linie z. B. der Post oder SBB helfen das Weiterbestehen im Markt zu sichern, sondern ein kostengünstiges zu vernachlässigendes Nebengeschäft sein.

Art. 4 Abs. 4
Diesen Artikel streichen. Das ist keine Passdruckerei, sondern eine Ausgabestelle für einen Code! Das ergibt eine überflüssige, nicht praktikable, nicht kontrollierbare Gesetzesflut und Papiertieger. Ein eventuelles Problem löst man nicht mit Gesetzen, sondern mit technischen Sicherheiten. Falls ein Gefahrenpotential besteht, löst man es mit technischer Innovation und nicht mit Vorschriften. Bei der E-ID geht es nicht

darum ein Büchlein herzustellen und aufzubewahren, sondern um einen Code auszuhändigen, nachdem die begehrende Person identifiziert wurde. Das ist wie in Deutschland, da hatte das Projekt auch Schiffbruch erlitten, weil man erdrückend zu viel Gewicht auf das Juristische und zu wenig Gewicht auf das Technische legte. Es lässt vermuten, dass die Gesetzesartikel von reinen Juristen mit Null Verständnis in Informatik formuliert wurden.

Art. 5 streichen
Art. 5 macht für Juristen Sinn, aber löst das technische Problem oder Gefahr nicht. Stellen Sie sich das in der Praxis vor. Ihre ID-Karte hat den höchsten Status an Vertrauen. Was bringt das für einen Nutzen, wenn Sie nur einen niedrigen Status haben? Zum Vergleich, einen niedrigen Vertrauensstatus heisst Ihre ID-Karte ist nur an ungeraden Tagen gültig. Entsprechend Art. 5 müssten Sie zum Geldabheben am Bankschalter bei der Bank 2 oder 3 ID gleichzeitig vorweisen, je nach dem wie viel Geld Sie abheben möchten. Es gibt keinen Grund verschiedene Sicherheitsniveaus zu haben. Ein Ausweis ist gültig oder ungültig – nicht teilgültig.

Art. 6 Ergänzung
Man sollte Art. 6 noch so formulieren, dass man auch eine E-ID für juristische Personen beantragen kann.

Art. 7 Ergänzung
Art. 7 sollte von Beginn weg die höchste Stufe entsprechend Abs. 3 gewählt werden. Weiter Ähnliches auch für juristische Personen z. B. sinngemäss Ar. 7 Abs. 1 b HR-Name, Art. 7 Abs. 1 d sinngemäss Grundungsdatum, sinngemäss Art. 7 Abs. 2 a Firmenregisternummer, sinngemäss Art. 7 Abs. 2 c Gründungsort usw.

Art. 8 Abs. 2 nicht praktikabel
Man sollte die Hinterlegung der E-ID so organisieren, wie das zentrale Einwohnerregister des Bundes. Es ist nicht praktikabel, wenn z. B. eine Behörde, ein Richter im Kanton Jura die E-ID für ungültig erklärt, dass die Ausgabestelle z. B. in Samnaun der ausgegebenen E-ID hinter her rennt und dafür verantwortlich zeichnet, dass in Chiasso die E-ID am Zoll nicht missbraucht wird. Es handelt sich dabei um einen Code. Meines Wissens ist der Bund für den Passport zuständig und nicht die Wohngemeinde.

Art. 9 sinngemäss für juristische Personen

Art. 15 streichen
Art. 15 ist unpraktikabel
Man stelle sich das in der Praxis vor. Ein E-ID-verwendenden Dienst kann jeder Onlineshop sein. Jetzt muss ich von meinem Kunden wissen wer der jeweilige IdP des jeweiligen E-ID Inhabers ist, der bei mir einkaufen will, damit ich vorgängig eine Vereinbarung treffen kann. Das ist nicht praktikabel. Wenn ich mit der Gemeinde X per E-mail kommuniziere und ich zur Sicherheit der Gemeinde noch meinen E-ID schlüssel gebe, dann muss ich das mit der Vereinbarung noch organisieren. Unpraktikabel.

Art. 17 Abs. 1 b Ergänzung juristischen
Natürlichen oder juristischen Person.

Art. 23 Gebühren
Ergänzung Abs. 1
Die Identitätsstelle und die Anerkennungsstelle können auf Gebühren verzichten. Falls Gebühren erhoben werden dienen sie zur Deckung des Aufwandes. Einsparungen des Aufwandes durch technische Weiterentwicklungen bewirken eine Gebührensenkung.

Weiteres Faktum, die Behörden (Bund, Kantone, Gemeinden) werden wegen der e ID vermehrt per E-mail kommunizieren und ersparen sich gesamthaft Kosten für Briefpapier, Kuvert, Porto in Millionenhöhe. Diese Minderausgaben sind ein Gewinn zur Finanzierung der durch die e ID anfallenden Anwendungskosten.

Abs. 2 streichen
Begründung:
1. Die hohen Gebühren verhinderten bis heute den Markterfolg der e ID.
2. Das Erheben und Eintreiben der Gebühr (Rechnung versenden, mahnen, Bareinzahlungsspesen am Postschalter, Kontoführungsspesen usw.) kostet mehr, als die verursachten Kosten für die Übermittlung von Personenidentifizierungsdaten. Das erschwert eine möglichst tiefe Gebühr.

Art. 24 Haftung streichen
Diesen Artikel streichen, weil er nicht praktikabel ist. Weltweit haftet kein Softwarehersteller für eine Software.

Freundlichste Grüsse

beat Oldani

Röhrliberg 8, CH-6330 Cham, Tel. 041 534 29 18 - E-mail: datazug@ittema.ch

Berner Fachhochschule
Rektorat

Prof. Dr. Herbert Binggeli
Rektor

Falkenplatz 24
3012 Bern

Telefon +41 31 848 33 01
Telefax +41 31 848 33 03

office@bfh.ch
www.bfh.ch

BFH | Falkenplatz 24 | 3012 Bern

Per Email an
copiur@bj.admin.ch

29. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin Simonetta Sommaruga
Sehr geehrte Damen und Herren

Grundsätzlich ist das staatliche Engagement für eine EU-notifizierbare E-ID sehr zu begrüssen. Wenn es in den nächsten Jahren nicht gelingt ein international interoperables eID-Ökosystem, so wie es im eID-Ökosystem Modell des SECO beschrieben ist, erfolgreich zu etablieren, wird die Schweiz dadurch wirtschaftliche Nachteile erleiden und der Wirtschaftsstandort im Kontext Digitalisierung geschwächt. Die internationale Erfahrung zeigt, dass ein systemischer Ansatz notwendig ist für den Erfolg und dass Anwendungsmöglichkeiten einer E-ID eine entscheidende Rolle spielen.

Die nachfolgende Stellungnahme wurde von Mitarbeitenden des Zentrums Digital Society der Berner Fachhochschule (BFH) erarbeitet. Die diskutierten Punkte betreffen nicht ausschliesslich das E-ID-Gesetz, sondern beziehen sich ebenso auf das dem Gesetz zu Grunde liegende Konzept und den erläuternden Bericht.

Wir erachten den Gesetzesvorschlag wie auch das Konzept für wenig tauglich, um der Schweiz die seit mindestens 2012 versprochene und noch seit weit längerem geforderte, staatliche E-ID zu realisieren. Die deutlichste Ablehnung müssen wir hierbei gegenüber dem E-ID Privatisierungsgedanken äussern. Der hoheitliche Identitätsnachweis ist eine nicht delegierbare Aufgabe des Staates. Privatwirtschaftliche Akteure können und sollen nachgelagerte Mehrwertdienste zur E-ID oder aufbauend auf der E-ID anbieten, aber nicht für die sichere, langfristige und kostendeckende Verfügbarkeit des staatlich anerkannten, elektronischen Identitätsnachweises der Schweiz verantwortlich sein. Da sich diese Kritik gegen den innersten Kern des Gesetzesvorschlags richtet, verzichten wir in der Folge auf die Ausarbeitung detaillierter Änderungsvorschläge im Gesetzestext.

Wir sehen es als notwendig an, dass der Staat eine hoheitliche E-ID anbietet und sich dazu verpflichtet, eine breite Nutzung im E-Government zu ermöglichen. Die Schweiz muss vermeiden, Hindernisse für eine zukünftige, internationale Nutzung aufzubauen. Darüber hinaus sind alle notwendigen Massnahmen für den Erfolg der Schweizer E-ID zu planen, vorzubereiten und umzusetzen. Dazu gehört auch, dass der Staat primär die Kosten für seine E-ID trägt. Nur so kann die Schweizer E-ID für alle sie einsetzenden Personen und Organisationen einen echten Mehrwert generieren; nur so wird die E-ID grosse Verbreitung und häufige Nutzung erfahren.

1. Identitätsnachweis ist hoheitliche Aufgabe des Staates

Der aktuelle Entwurf für ein Bundesgesetz über anerkannte elektronische Identifikationsmittel (E-ID-Gesetz) sieht vor, dass der Bund die staatliche, elektronische Identität an private Unternehmen und Organisationen abgibt, die vorgängig für diese Aufgabenerfüllung zertifiziert werden müssen. Die BFH ist der Ansicht, dass der Schweizer Bundesstaat seine hoheitlichen Aufgaben bezüglich der nationalen, elektronischen Identität in derselben Form wahrzunehmen hat, wie er es bei den existierenden, analogen Ausweisen Pass und Identitätskarte tut. Eine Teilprivatisierung würde zu einem elektronischen Identitätsnachweis zweiter Klasse führen. Der elektronische Identitätsnachweis dient der Etablierung und Vermittlung von Vertrauen in digitalen Prozessen, die zwischen natürlichen und juristischen Personen sowie Behörden ausgeführt werden. Vertrauen in den elektronischen Identitätsnachweis erfordert langfristige, stabile Verfügbarkeit der Schweizer E-ID. Dies kann aus Sicht der BFH nur durch einen staatlichen Akteur gewährleistet werden. Das Anbieten der E-ID durch privatwirtschaftliche Dienstleister wird inhärent mit komplementären, kommerziellen Produkte oder Dienstleistungen von Ersteren erfolgen, da ansonsten nicht von einer wirtschaftlichen Tragbarkeit auszugehen ist. Eine solche Privatisierung und Kommerzialisierung einer hoheitlichen Aufgabe wie dem Identitätsnachweis ist unvertretbar. Des Weiteren bringt die Auslagerung der Leistungserbringung an Unternehmen und nicht-hoheitliche Organisationen Risiken durch Konkurse, Konzernaufspaltungen, Fusionen und ausländische Übernahmen mit sich, die allesamt im Kontext Identitätsnachweis als höchst kritisch zu erachten sind. Privatwirtschaftlichen Akteuren kann daher nicht derselbe Grad an Vertrauen entgegengebracht werden wie dem Bund, was aber gerade der entscheidende Faktor im Kontext E-ID ist. Daran ändert auch eine Zertifizierung wie im Gesetzesentwurf vorgesehen wenig. Dies bedeutet aber dennoch nicht, dass der Bund intern die Implementierung der E-ID in Hardware und Software selbst zu realisieren hat. Analog zu Identitätskarte und Pass kann die Eidgenossenschaft private Anbieter mit der Erbringung dieser Teilleistungen beauftragen und so für eine rasche, grossflächige Verbreitung der E-ID in der Schweiz sorgen.

Der Gesetzesvorschlag sieht vor, dass Identitätsinformationen von Personen nur dann elektronisch an Behörden übermittelt werden können, wenn diese Daten vorher einer privaten E-ID-Anbieterin zugänglich gemacht wurden. Dass eine Interaktion von Bürgerinnen und Bürgern und staatlichen Stellen nur unter Einbindung von privaten Unternehmen oder Organisationen als Informationsvermittler möglich ist, ist untragbar. Der verpflichtende Umweg über ein privates Unternehmen und der damit einhergehende Datenfluss ist aus Sicht des Datenschutzes und des Schutzes der Privatsphäre der E-ID nutzenden Person nicht vertretbar.

Fazit 1: Der anerkannte Identitätsnachweis ist eine hoheitliche Kernaufgabe des Staates. Diese darf auch in elektronischer Form nicht an private Anbieter ausgelagert werden, sondern ist hoheitlich durch Schweizer Behörden zu erbringen.

Fazit 1.1: Der elektronische Identitätsnachweis von Personen mit Schweizer E-ID gegenüber staatlichen Stellen hat direkt zu erfolgen, ohne dass die Personendaten einen Umweg über private Informationsvermittler machen.

2. Förderung der Digitalisierung statt Vollkostendeckung

Das Hauptziel einer E-ID-Gesetzgebung muss eine rasche, möglichst starke Verbreitung der E-ID sowie deren regelmässige Nutzung sein. Eine Vollkostendeckung ist ebenso wenig das Ziel von Einführung und Betrieb der E-ID wie bei der Zurverfügungstellung von analogen Ausweispapieren. Sollte sich die E-ID erfolgreich verbreiten und bei vielen Behördengängen zum Einsatz kommen, kann mit Effizienz-Einsparungen in der gesamten Volkswirtschaft

gerechnet werden. Daher wäre es denkbar, hochgradig automatisierte und auf den Einsatz der E-ID ausgelegte E-Government-Dienstleistungen entsprechend der tieferen Verfahrenskosten zu vergünstigten Preisen anzubieten, um die Attraktivität der E-ID weiter zu steigern und deren Effizienz aufzuzeigen.

Um eine möglichst rasche und hohe Verbreitung der E-ID-Nutzung zu erreichen, sollte von einer Pay-Per-Use-Lösung abgesehen und analog zu Pass und Identitätskarte auf eine einmalige, moderate Bezugsgebühr gesetzt werden. Die Argumentation der Kostendeckung bzw. Kostenneutralität leuchtet nicht ein. Die Schweiz hat ein zentrales Interesse daran, die fortschreitende Digitalisierung zu unterstützen und für mehr Sicherheit und Vertrauen in online Transaktionen zu sorgen. Die E-ID ist daher im Sinne einer Basisinfrastruktur über die zu erwartenden, höheren Steuereinnahmen aus der florierenden, digitalen Wirtschaft zu finanzieren.

Um einer möglichst grossen Verbreitung der E-ID nicht im Wege zu stehen, ist der finanzielle und organisatorische Aufwand für Relying Parties möglichst gering zu halten. Um die häufige Benutzung der E-ID, die ja genau angestrebt wird, nicht zu bestrafen, ist ein volumenabhängiges Kostenmodell klar abzulehnen. Darüber hinaus ist aber auch zu beachten, dass die Initialaufwände für Relying Parties hoch sind, sowohl was die Kosten als auch was den Know-how Bedarf betrifft. Referenzimplementierungen, analog wie sie in der EU existieren, können hier substanzielle Hilfe bieten. Darüber hinaus können aber Beratungsdienste die Implementierung signifikant vereinfachen. Beratungsdienste können durch die Privatwirtschaft angeboten werden, Referenzimplementierungen können als Open Source Software entwickelt und bereitgestellt werden.

Fazit 2: Das vorrangige Ziel ist der verbreitete Einsatz der E-ID, der damit verbundene Effektivitäts- und Effizienzzuwachs und die resultierende Stärkung der digitalen Wirtschaft. Eine Vollkostendeckung anzustreben oder die häufige Benutzung durch ein Pay-per-Use-Modell zu bestrafen, ist kontraproduktiv.

Fazit 2.1: Es ist mit frei verfügbaren Open Source Referenzimplementierungen dazu Sorge zu tragen, dass Kosten und Know-how Bedarf für Relying Parties möglichst gering sind und diese dadurch die weite Verbreitung und häufige Verwendung der E-ID unterstützen.

3. eIDAS Notifizierbarkeit und Interoperabilität der E-ID

Die E-ID muss in der EU notifizierbar sein, da eine Insellösung inmitten Europas keine Zukunft hat. Regelungen zur ausschliesslichen Datenablage in der Schweiz sind entsprechend anzupassen.

Die Verwendung von Begriffen und Definitionen im E-ID Gesetz (und nachgelagerten Verordnungen, TAV etc.), die nicht mit bestehenden Standards konform sind, ist weder für die Notifizierbarkeit noch für die Interoperabilität im allgemeinen gut. Wo immer möglich sind die Definitionen und Begrifflichkeiten aus dem eIDAS-Kontext eins zu eins zu übernehmen. Wo diese nach eingehender Prüfung für den nationalen Kontext als ungeeignet oder unvollständig befunden werden, ist auf die Schweizer E-Government Standards des Vereins eCH zurückzugreifen. eCH-Standards sind subsidiär, richten sich aber nach internationalen Normen (ETSI, ISO, etc.) und definieren üblicherweise ein deutsches und französisches Glossar. Wenn eCH-Standards ggf. Fehler enthalten, können diese mittels RfC für alle effizient behoben werden. Auf Eigenkreationen von Begriffen und Definitionen, wie sie im E-ID Konzept und Gesetz vorkommen, ist grundsätzlich zu verzichten.

Fazit 3: Die Schweizer E-ID ist auf internationale Interoperabilität und eIDAS-Notifizerbarkeit hin zu definieren und zu entwickeln, um damit eine breite Verwendung bei digitalen Prozessen im In- und Ausland zu erreichen.

Fazit 3.1: Begriffsdefinitionen und -verwendungen sind nationalen und internationalen Standards anzupassen - mit erster Priorität für eIDAS Begrifflichkeiten und zweiter Priorität eCH-Standards - und Eigenkreationen zu vermeiden.

4. Schweizer Qualität erfordert E-ID mit Sicherheitsniveau «hoch»

Der vorliegende Gesetzesentwurf schlägt die Implementierung der E-ID in drei Qualitätsniveaus vor. Es ist korrekt, dass verschiedene elektronische Identitäten, insbesondere auch nationale E-ID aus unterschiedlichen Ländern, über unterschiedliche Qualitätsniveaus verfügen, weshalb dies im Kontext etwa von eIDAS berücksichtigt werden muss. Die Schweiz benötigt aber nicht drei sondern nur eine staatlich anerkannte Schweizer E-ID. Daher sind die vorgeschlagenen, rechtlichen Definitionen und darauf aufbauende Realisierungen verschiedener Sicherheitsniveaus für die E-ID unnötig bzw. ungeeignet. Die Schweizer E-ID ist auf einem sehr hohen Qualitätsniveau zu implementieren, was gemäss Gesetzesvorschlag dem Sicherheitsniveau «hoch» entspricht. Entsprechend technisch umgesetzt, ist eine E-ID mit Sicherheitsniveau hoch danach gleichfalls für Authentifizierungen auf substantiellem oder niedrigem Niveau verwendbar. Relevant ist dabei die Definition unterschiedlicher Anforderungen an E-ID verwendende Dienste (Relying Parties) bezüglich Attributverfügbarkeit, Datenschutzanforderungen, Haftung etc. bei unterschiedlichen Authentifizierungsniveaus (vgl.eCH-0170[1]).

Fazit 4: Die Schweizer E-ID ist mit Sicherheitsniveau «hoch» zu realisieren.

Fazit 4.1: Für E-ID verwendende Dienste sind je nach angestrebtem Authentifizierungsniveau unterschiedliche, rechtliche Anforderungen zu definieren.

5. E-ID bei Online-Diensten des Schweizer Gemeinwesens

Erfahrungen aus dem Ausland wie auch mit der SuisseID haben in der Vergangenheit klar gezeigt, dass eine (nationale) E-ID nur dann dauerhaft erfolgreich ist, wenn für ihre Nutzung ein entsprechendes Portfolio an Online-Diensten bereitsteht. Aus Sicht der BFH ist es daher hoch relevant, dass die Schweizer E-ID von allen E-Government-Angeboten des Bundes, aber auch der Schweizer Kantone und Gemeinden, als Identifizierungsmittel akzeptiert wird. Der Einsatz in anderen E-Domänen ist zudem zu prüfen und zu unterstützen, etwa im Bereich E-Health im Kontext elektronisches Patientendossier. Prinzipiell ist anzustreben, dass alle subventionierten bzw. staatlich finanzierten Online-Dienste, die E-ID akzeptieren müssen. Dazu kann eine angemessene Übergangsfrist von maximal 10 Jahren gewährt werden. Nur so können dezentrale, staatliche Parallellösungen vermieden und ein hoher Grad an Verbreitung und Verwendung der E-ID erreicht werden. Entsprechende Gesetzesanpassungen und technische Erweiterungen bestehender Online-Dienste sind vor der Einführung der E-ID durchzuführen.

Fazit 5: Die Schweizer E-ID ist von allen Gemeinwesen der Schweiz im elektronischen Verkehr als offizieller Identitätsnachweis zu akzeptieren.

---

[1] Verein eCH (Hrsg.) (2014): Standard eCH-0170: eID Qualitätsmodell. Zürich. URL: https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170

6. Nationale Zusammenarbeit im internationalen E-ID-Ökosystem

Die Weiterverwertung der E-ID-Funktionalitäten und -Daten für privatwirtschaftliche Zwecke ist, anders als die privatwirtschaftliche Erbringung des hoheitlichen Identitätsnachweises, klar zu unterstützen. Die Implementierung und Markteinführung von nicht-notifizierbaren, elektronischen Identitäten mit variablen Sicherheitsniveaus, ist den privaten Anbietern zu überlassen. Hier sehen wir die Aufgabenteilung zwischen Markt und Staat. Wichtig dabei ist, dass die Schweizer E-ID für private Identifikationslösungen, seien dies organisationsinterne oder auf dem Markt zu platzierende, die rechtlichen und technischen Möglichkeiten liefert, damit bestätigte Personenidentifizierungsdaten weiterverwendet werden können. Dies ist für die Bildung und Nutzung von abgeleiteten, elektronischen Identitäten ausschlaggebend und führt zu mehr Sicherheit in der digitalen Wirtschaft. Es erlaubt ausserdem, dass der Markt für elektronische Identitäten innerhalb der Schweiz frei spielen und sich die Anbieter auch international gut positionieren können.

Um eine Einbindung von Zusatzattributen von privater Seite zu ermöglichen und so die Einsatzmöglichkeiten der E-ID qualitativ zu erweitern, muss es privaten Anbietern möglich sein, zusätzliche Attribute mit einer E-ID zu verknüpfen. Für den Wahrheitsgehalt dieser zusätzlich verknüpften Attribute bürgt ausschliesslich der Attribute-Verwalter und nicht der Bund als Aussteller der E-ID. Das strategische Schweizer E-Government Projekt «Identitätsverbund Schweiz»[2] eignet sich hierbei ideal als Enabler komplementärer Leistungen wie zusätzlichen Attributbestätigungen. Diese können etwa für Zeichnungsberechtigungen, Stellvertretung etc. benutzt werden. Das steigert den Mehrwert der E-ID, ohne dem Bund zusätzliche Verantwortungen oder Kosten zu verursachen. Ein höherer Mehrwert wird positiv zum Erfolg der Schweizer E-ID beitragen.

Operativ wird auf europäischer Ebene die internationale Interoperabilität von elektronischen Identitäten durch das Netzwerk der eIDAS-Knoten bereitgestellt. Lösungen zur Verknüpfung von staatlichen mit privatwirtschaftlichen E-ID- und Attributs-Zertifikaten werden derzeit auf internationaler Ebene diskutiert. Für E-ID-Broker von hoher Relevanz wäre, wenn es dazu eine Referenzimplementierung gäbe. Das Projekt IDV-Schweiz könnte für die Schweiz den eIDAS Knoten implementieren und gleichzeitig Broker-Dienste gemäss eCH-Standards (z.B. eCH-0167[3], eCH-0170) anbieten. Eine derartige Umsetzung erlaubt, elektronische Identitäten ihrem Qualitäts- resp. Sicherheitsniveau entsprechend differenziert zu beurteilen, egal ob nationale oder privatwirtschaftliche E-ID.

Fazit 6: Die Schweizer E-ID ist abseits des hoheitlichen Identitätsnachweises rechtlich und technisch so zu gestalten, dass sie privatwirtschaftliche Weiterverwertungen aktiv unterstützt.

Fazit 6.1: Private Unternehmen aus dem In- und Ausland dürfen die Schweizer E-ID mit weiteren Attributen verknüpfen und so für flexible Einsatzmöglichkeiten, grossen Mehrwert und starke Verbreitung der Schweizer E-ID sorgen.

Fazit 6.2: Für den Identitätsverbund-Schweiz ist eine aktive Rolle im E-ID-Ökosystem innerhalb der Schweiz wie auch zwischen der Schweiz und dem Ausland zu definieren.

---

[2] https://www.idv-fsi.ch/

[3] Verein eCH (Hrsg.) (2014): Standard eCH-0167: SuisseTrustIAM Rahmenkonzept. Zürich. URL: https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0167

7. Datenschutz und Datenweitergabe

Die vorgeschlagene Regelung zur Datenverwertung birgt das Risiko, dass ein neu als IdP agierendes Unternehmen seine bis dahin rechtskonform bearbeiteten und verwerteten Personendaten nicht mehr verwerten darf, sofern diese mit Artikel 7 übereinstimmen. Eine Abgrenzung des bestehenden vom neuen, über den E-ID-Einsatz generierten Datenbestand findet nicht statt. Es gibt zudem keinen Anlass, von den bestehenden Regelungen des Datenschutzes abzurücken, zumal die Daten dieselben verbleiben, ob die Übermittlung nun über elektronisches Login oder andere Wege erfolgt. Nutzungsprofile jeglicher Art sind persönliche Daten und dürfen grundsätzlich nicht ohne Freigabe des Benutzers weitergeben werden. Eine Ausnahme bildet diesbezüglich der Fall, in welchem das europäische Datenschutzgesetz schärfer Regelungen vorsieht als das Schweizerische. Um Kompatibilität mit Europa zu gewährleisten, sind die schweizerischen Regelungen in diesem Fall an die europäischen Regelungen anzugleichen.

Fazit 7: Die bestehenden Datenschutzregulierungen der EU und der Schweiz (wo strikter) reichen aus, um die staatliche Vergabe einer nationalen E-ID wirksam zu regeln.

Fazit 7.1: Die Schweizer Datenschutzgesetze sind den Entwicklungen aus der EU anzugleichen.

8. Bezug der E-ID analog zu Identitätskarte und Reisepass

Mit Wegfallen der E-ID-Implementierung über private, zertifizierte IdP ist ein Abweichen von den etablierten und funktionierenden Abläufen für die Ausstellung und Abgabe staatlicher Ausweise bei der E-ID nicht länger erforderlich bzw. nachvollziehbar. Bezug und Ausgabe der E-ID ist somit analog zu Reisepass und Identitätskarte über die kantonalen Passbüros und regionalen Erfassungsstellen zu realisieren. Ideal und aus unserer Sicht einzig realistisch ist dabei, dass Erstbestellung und Datenerhebung in einem einzigen Prozess geschehen und die E-ID zusammen mit Identitätskarte und Pass in Kombipaketen bezogen werden kann.

Da bei der E-ID von einer kürzeren Gültigkeitsdauer auszugehen ist als bei Pass und Identitätskarte, ist ein alternativer Prozess für die Erneuerung der E-ID innerhalb des Zeitraums von 10 Jahren (Gültigkeit Pass und Identitätskarte) zu definieren.

Fazit 8: Ausstellungs- und Abgabeverfahren des elektronischen Identifizierungsmittels sind nach denjenigen der staatlichen Ausweise (Identitätskarte und Pass) auszurichten.

9. Vertrauen durch hohe Verfügbarkeit des Gesamtsystems

Bei analogen Ausweispapieren wie dem Reisepass oder der Identitätskarte kann von einer Verfügbarkeit von praktisch 100% (von verlorenen und beschädigten Karten abgesehen) ausgegangen werden. Um das Vertrauen in elektronische Identitätsnachweise nicht zu gefährden, müssen auch diese, bzw. die damit verbundenen Dienste, eine Verfügbarkeit von praktisch 100% gewährleisten. Bei der entsprechenden Anforderungsdefinition kann gegebenenfalls auf jene der biometrischen Pässe zurückgegriffen werden.

Hierbei muss ausserdem darauf hingewiesen werden, dass ohne Implementierung eines E-ID-Dienstes mit eigener Datenhaltung betreffend Personenidentifizierungsdaten, eine Authentifizierungslösung mit brauchbarer Leistungsfähigkeit nicht zu realisieren sein wird. Die vorgeschlagene Umsetzung mittels undefinierter Schnittstellen zu bestehenden Registern (Infostar, ZEMIS, EWR etc.) sehen wir nicht als praktikabel an.

Fazit 9: Die Authentifizierung über die Schweizer E-ID hat eine sehr hohe Systemverfügbarkeit und Leistungsfähigkeit zu gewährleisten.

10. Gültigkeit von Personenidentifizierungsdaten und E-ID

Die Geltungsdauer der Personenidentifizierungsdaten der E-ID ist analog zu Pass und Identitätskarte zu definieren. Es liegen keine zwingenden Gründe vor, wie etwa sich rasch ändernde Grundinformationen, die für eine davon abweichende Regelung sprechen. Da mit dem Wegfallen privater IdPs die Daten ausschliesslich über Systeme der öffentlichen Hand bezogen werden, fällt auch die wöchentliche Überprüfung der Daten (bei Sicherheitsniveau «hoch») weg.

Sofern die E-ID auf Zertifikaten implementiert wird, sollte die Gültigkeitsdauer einer E-ID sich an den im ZertES (2017) spezifizierten, geregelten Zertifikaten orientieren. Hier muss zwischen E-ID und ZertES-Umsetzung eine regulatorische Angleichung erzielt werden. Wichtig ist, dass die Zertifikate der E-ID während der Gültigkeitsdauer der Personenidentifizierungsdaten mit einem vereinfachten Prozess z.B. über einen Onlinedienst erneuert und die Gültigkeit der E-ID so verlängert werden kann. Vorstellbar wäre etwa eine Gültigkeit des E-ID-Zertifikats von 2 Jahren, mit der Möglichkeit dieses maximal 4 Mal zu verlängern, womit nach jeweils 10 Jahren Pass, Identitätskarte und E-ID inklusive der Personenidentifizierungsdaten zu erneuern sind.

Fazit 10: Die Gültigkeit der Personenidentifizierungsdaten orientiert sich an jener von Pass und Identitätskarte. Die Gültigkeit der E-ID Zertifikate orientiert sich an den geregelten Zertifikaten gemäss ZertES. Die Verlängerung der E-ID Zertifikate innerhalb des Gültigkeitszeitraums der Personenidentifizierungsdaten ist mittels vereinfachtem Prozess umzusetzen.

Freundliche Grüsse

Berner Fachhochschule

Prof. Dr. Herbert Binggeli
Rektor

Stellungnahme zum E-ID-Gesetz

Version 1.0
16. Mai 2017

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. Zweck einer Vernehmlassung zu einem Gesetzesentwurf ist es, aus Sicht der Rückmeldenden auf Unstimmigkeiten hinzuweisen, und nicht, zu erwähnen, was alles gut bewerkstelligt worden ist. Dies mag für die Verfasser eines Gesetzesentwurfes sehr unbefriedigend sein.

1.2. Ich begrüsse es, dass dem Parlament ein Gesetzesentwurf zu diesem Thema vorgelegt werden soll.

I.2 Grundsätzliche, aber offen gebliebene Fragen

1.3. Beim Durchlesen des Gesetzesentwurfs haben sich unter anderem folgende Fragen gestellt:

- Was ist eine E-ID- konkret, stellt sie eine Urkunde dar?
- Wie fälschungssicher und wie leicht ist sie auf Dritte (missbräuchlich) übertragbar? Dies ist in Zusammenhang mit dem Diebstahl der Mittel für die Authentisierung von Bedeutung. Mittel für die Authentisierung sind z.B. Chip Card und dazugehöriges Passwort, Login Name und Passwort.
- Wie steht der Gesetzesentwurf in Relation zu bestehenden Bundesgesetzen wie zum ZertES und zum elektronischen Patientendossier (EPDG)? Ist z.B. eine nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten auch (automatisch) ein IdP?
- Weshalb wurden die Bestimmungen zum Thema E-ID anders als bei der Verordnung der EU nicht mit denen zu den elektronischen Zertifikaten zusammengezogen und in einem Erlass festgehalten?
- Wie gestaltet sich die Anerkennung ausländischer E-ID-Aussteller?
- Welche Archivierungszeit bei welchen Geschäftsprozessen gilt es zu beachten?
- Weswegen wurden andere Begriffe in diesem Entwurf verwendet als bei der erwähnten Bestimmung der EU, und warum wurde hier auf die in den eCH Standards verwendeten Begriffe abgestützt?

I.3 Begriffliches

1.4. Bei diesem Entwurf wie bereits auch beim ZertES (Art. 2 Bst. b Ziff. 2) wird der Begriff Identifizieren verwendet, welcher sich mit dem nicht deckt, 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 ohne nennenswerten Aufwand übertragbar. Weitere Ausführungen dazu, siehe Kapitel IV „Anhang Identifizieren und Authentisieren“ dieses Dokuments.

1.5. Folglich sollten die Begriffe „Authentisieren“ (in der EU Verordnung wohl als elektronisches identifizieren bezeichnet) und „Identifizieren“, sowie ihre rechtliche Wirkung auseinandergehalten werden; wie bei Eigentum und Besitz, oder Fahrer und Halter eines Fahrzeugs. Ansonsten werden bei der Allgemeinheit mit den im Entwurf verwendeten Begriffen Assoziationen geweckt, welche mit dem Sachverhalt nicht übereinstimmen. 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 darüber im vollen Bewusstsein der Sachlage entscheiden, wie z.B. bei Art. 6 Abs. 1 OBG.

1.6. In diesem Kontext wichtig ist die Frage nach der Verlässlichkeit der in der E-ID gemachten Angaben. D.h. man sollte auch das Recht besitzen, sich nicht auf die in der E-ID gemachten Angaben verlassen zu müssen und sie hinterfragen zu dürfen.

I.4 Erwartungen

1.7. Im Bericht S. 3 letzter Absatz, ist von „sicher und bequem“ zu lesen. Aus Erfahrung bedeutet dies, dass die Realisierung einer solchen IT-Lösung teuer wird. Denn Sicherheit und Bequemlichkeit sind meist entgegengesetzte (komplementäre) Eigenschaften. Beide gleichzeitig bei gleicher Funktionalität zu realisieren, verursacht bekanntlich Kosten.

I.5 Zum Bericht des Vorentwurfs

1.8. Im Bericht S. 5 Mitte, wird im Zusammenhang mit E-ID das „Vote électronique“ als Beispiel herbeigezogen. Beim elektronischen Abstimmen soll jedoch wegen der Wahrung des Stimmgeheimnisses eine Zuordnung des abgegebenen elektronischen Abstimmungs- oder Wahlzettels zum Wähler oder Abstimmenden am PC möglichst unterbunden werden. Also soll die Anonymität geschützt werden. Mit der Anonymität werden jedoch zur Authentisierung entgegengesetzte Ziele verfolgt.

1.9. Im Bericht S. 6:

> Der Einsatz der E-ID verlangt mindestens eine Zwei-Faktor-Authentifizierung, wobei ein Faktor biometrisch sein muss («inhärenter Faktor» gemäss eIDAS Durchführungsrechtsakte). Die Handhabung einer solchen E-ID ist vergleichbar mit einem Smartphone mit Fingerabdruck-, Gesichts- oder Stimmenerkennung. Die biometrische Authentifizierung bewirkt eine noch engere Bindung zwischen der E-ID und deren Inhaberin oder Inhaber. Bei Verlust des Authentifizierungsmittels der E-ID schützt die biometrische Authentifizierung die Inhaberin oder den Inhaber vor der Tätigung missbräuchlicher Transaktionen in deren Namen. Mit Blick auf den Identitätsmissbrauch müssen Inhaberinnen und Inhaber auch vor Cyberangriffen geschützt werden können.

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 und Gewähren des Zugangs zu den darauf abgespeicherten Daten ist dies erfüllt, oder bei physischen Zutrittssystemen. 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.

1.10. Folglich sollten die beim IdP vorhandenen biometrischen Informationen wie Foto, Unterschriftsbild, Passfoto und Daten zur Stimmerkennung nicht an einen möglichen E-ID-Dienst weitergeleitet werden dürfen, sonders besonders geschützt werden. Eine entsprechende Bestimmung ist im Gesetzestext aufzunehmen. Weiter ergibt sich die sicherheitstechnische Frage:

Wie können biometrische Authentifizierungsmethoden vor missbräuchlichen, übers Internet vorgenommenen Transaktionen wirksam schützen?

1.11. Dem Bericht nachgereicht werden sollte, welche technische Ausprägungen eine E-ID haben kann, wie die Authentisierung bei den einzelnen Sicherheitsstufen abläuft und dargelegt werden, wie biometrische Angaben mit grosser Sicherheit vor Authentisierungsmissbrauch bei übers Internet vorgenommenen Anmeldungen schützen. Ansons-

ten kann zu den Bestimmungen im Gesetzesentwurf nicht mit angemessener Kenntnis Stellung genommen werden.

II Zu den einzelnen Artikeln im Entwurf

II.1 Art. 2

2.1 **Bst. a)** 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. Weiter gibt es Anwendungen wie beim elektronischen Patientendossier, wo man Gewissheit 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 sollte sich beim Inhaber oder beim IdP auch „ausweisen“ können.

2.2 **Bst. b)** Was ist eine E-ID genau?

2.3 Siehe Bemerkungen zu den Begriffen Authentisierung und zur Identifikation in den Kapiteln I.3 und IV.

II.2 Art. 3

2.4 **Abs. 1)** Verbesserungsvorschlag: „Natürliche Personen können eine E-ID bei einem IdP beantragen“ oder „IdP können natürlichen Personen ausschliesslich auf deren Antrag eine E-ID ausstellen“. Der IdP sollte nicht von sich aus eine E-ID ausstellen dürfen.

2.5 Im Bericht zum Entwurf wird ein Kontrahierungszwang des IdP abgelehnt. Hier ein Beispiel 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 ein IdP B sich weigert, E-ID-Einheiten auszustellen, damit die Kunden des IdP weiterhin auf ihre Patientendaten zugreifen können? Medizinische Fachkräfte stünden im Umgang mit dem Patientendossier vor ähnlichen Problemen.

2.6 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 zu haben, würde ihn von der Geschäftswelt und von seinem sozialen Umfeld isolieren.

2.7 Folgende Frage stellt sich:

- Welche Maturität, Geisteszustand, Selbständigkeit oder Alter sollte eine natürlichen Person haben, bevor sie eine E-ID beziehen kann. Kann z.B. auch ein Minderjähriger oder Geisteskranker eine E-ID beziehen?

2.8 Weiter sollte die Anerkennung ausländischer E-IDs geregelt werden. 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.3 Art. 4

2.9 **Abs. 4)** „Insbesondere“ im Sinne der wirtschaftlichen und rechtlichen Sicherheit streichen. Die hier vorgenommene Aufzählung sollte abschliessend sein. Aus liberaler Sicht haben die Kompetenzen der Verwaltung bestimmt und nicht ausufernd zu sein.

II.4 Art. 5

2.10 Es gilt zu unterscheiden:

1. Sorgfalt bei der Identifikation, beim korrekten Erfassen der Personenangaben im Zusammenhang mit einer E-ID-Einheit (siehe auch Haftung)
2. Sicherheit der Anwendung (Authentisierungsprozess) und der E-ID selber

2.11 Bei Fall 1 im Sinne der allgemeinen Akzeptanz sollten keine unterschiedlichen Sicherheitsniveaus eingeführt und akzeptiert werden.

2.12 Fragen:

- Wurde bei der Einführung der verschiedenen Sicherheitsniveaus berücksichtigt, dass ein hohes Mass an Verlässlichkeit als ein wirtschaftlicher Standortvorteil betrachtet werden kann? Z.B. die Einführung der Verbindlichkeit der Grundbucheintragungen zu Beginn des letzten Jahrhunderts.
- Sollte das eGovernment Umfeld infolge der damit verbundenen Staatshaftung nicht ein hohes Sicherheitsniveau fordern und fördern? Das Vertrauen auf die behördlichen Angaben stellt m.E. ebenfalls einen Standortvorteil dar.
- Fragen zur Haftung siehe Fragen zu Artikel 24, Kapitel II.15.

- Wie sind die unterschiedlichen Niveaus anhand der Anwendung oder der E-ID-Einheit durch den nicht fachunkundigen Anwender unterscheidbar?
- Wurde eine Risikoanalyse im Vorfeld zum Gesetzesentwurf für die jeweiligen Sicherheitsstufen und involvierten Parteien durchgeführt? Falls ja, wurde dabei berücksichtigt, dass das Stehlen von Identitätsangaben bereits heute beträchtlich ist und wohl noch zunehmen wird, insbesondere je einfacher und verbreiteter die E-ID sein wird? Siehe auch Swisscom Security Report 2017.

II.5 Art. 6

2.13 Formelles. Ist Artikel 6 nicht bei Artikel 3 passender?

Im Bericht zu Art. 6 Abs. 4) Auch auf die Gefahr hin, sich zu wiederholen: Die Zuordnung der EI-D zur SIM-Karte ermöglicht letztlich nicht eine zweifelsfreie Zuordnung zur natürlichen Person. Der Eigentümer des Handys, der Besitzer des Handys und derjenige, welcher mit dem Handy telefoniert, müssen nicht identisch sein. Dies gilt es bei (straf)rechtlich relevanten Vorfällen zu beachten.

II.6 Art. 7

Abs. 1) Sollte es nicht IdP anstatt Identitätsstelle heissen?

2.14 Frage:

- Ist eine Risikoabschätzung betreffend Missbrauch angefertigt worden, falls digitalisierte Unterschriftsbilder, Passfotos oder digitalisierte Fingerabdrücke zuhauf im Internet verfügbar sind oder zentral illegal beschafft werden können und damit z.B. Gutachten gefälscht oder unrechtmässig Dienstleistungen bezogen werden können?
- Sollte Art. 25 EPDV nicht mit Art. 7 der Vorlage abgeglichen sein?

II.7 Art. 8

2.15 Fragen:

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

II.8 Art. 9

2.16 Formelles: Der Begriff Sozialversichertennummer oder AHV-Nr. im Gesetzestext verwenden.

> Anmerkung: Eine AHV-Nr identifiziert eine natürliche Person nicht. Ansonsten könnte man durch Vorzeigen der AHV-Nr den Zoll passieren. Die AHV-Nr. ist lediglich ein Datenbankschlüsselattribut oder eine Registernummer. Das Wort Identifikator assoziiert aber, dass damit eine Person identifiziert werden kann.

II.9 Art. 10

2.17 Abs. 3) Die E-ID-Daten wie ein elektronisches Zertifikat können kopiert werden. (Beim Zertifikat ist dies irrelevant in Bezug zur IT-Sicherheit.) Von wem (Inhaber der E-ID, Betreiber von E-ID verwendeten Diensten oder Hacker) lässt sich vielfach nicht zurückverfolgen, da sie nach meinem aktuellen Verständnis meist und wie angedacht mehreren Parteien zugänglich sein wird. Somit ist vermutlich die darauf beruhende Sicherheit nicht umfassend, einfach und bequem.

II.10 Art. 11

2.18 Frage: Was geschieht mit der Registriernummer?

II.11 Art. 12

2.19 Fragen:

- Ich erachte eine Trennung zwischen Vollzugs- (Anerkennungsstelle) und Aufsichtsbehörde als sinnvoll, siehe z.B. den Konsumgütermarkt, Holliger-Hagmann, Produktsicherheitsgesetz, S.23 ff und das ZertES. Eine Beschreibung der Aufgaben, Rechte und Pflichten der Aufsichtsbehörde sollte folglich separat aufgeführt werden.
- Hat der dafür verantwortliche Bereich im EFD ausreichend fachkundiges, d.h. juristisch versiertes Personal, um Verfügungen zu erlassen und eingegangene Beschwerden abzuhandeln?
- Welche Rechtsmittel bei Erlass einer Verfügung über den Entzug der Anerkennung bestehen, und wie sind die damit verbundenen Fristen ausgestaltet? Besteht z.B. ein Rechtsmittel mit aufschiebender Wirkung gegen diese Verfügung?

II.12 Art. 14

2.20 **Abs. 1)** Das Nichtaushändigen der E-ID an Dritte ist kaum realisierbar, denn die Informationen müssen nach bisherigem Verständnis dem Betreiber der E-ID-Diensten zugänglich gemacht werden. Folglich stellt sich die Frage: Was ist unter Dritten zu verstehen? Je nach Ausgestaltung der E-ID kann kaum wirksam verhindert werden, dass unrechtmässig Daten einer E-ID kopiert werden. Hier stellt sich auch die Frage nach dem Missbrauchspotential, wenn mit niedrigen Sicherheitsstufen operiert wird.

II.13 Art. 15

2.21 Fragen:

- Wer kontrolliert, dass die Vereinbarungen eingehalten werden und was sind die Kriterien der Vereinbarung?
- 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.

2.22 **Zum ersten Absatz)** Wird nicht eine Vereinbarung mit allen IdP benötigt, oder werden die Daten unter den IdP abgeglichen? Werden die Daten abgeglichen und bei verschiedenen Dienstleitern gespeichert, so stellt dies nicht ein erhöhtes Risiko dar. Diese Anmerkung gilt auch für Art. 18.

II.14 Art. 21

2.23 Im Sinne der Rechtssicherheit und der Ökonomie mit digitalen IDs (inklusive Zertifikaten) wäre eine Aufsichtsbehörde und ein Abgleich der Bestimmung mit dem ZertES betreffend Anerkennungsstelle wünschenswert? Z.B. wenn eine nach ZertES anerkannte Anbieterin von Zertifizierungsdiensten zugleich IdP ist. Dann gäbe es nämlich gemäss diesem Entwurf zwei verschiedene Aufsichts- und Anerkennungsstellen (EFD und die Akkreditierungsstelle, Anerkennungsstelle nach ZertES) für ähnliche Tätigkeiten.

II.15 Art. 24

2.24 **Abs. 1)** Im Sinne der Rechtssicherheit sollte die Haftung der jeweiligen Partei klarer geregelt werden; wie Z.B. in der EU-Verordnung. Folgende Fragen ergeben sich aus den Haftungsbestimmungen im Entwurf.

- Wird folgender Fall durch den allgemeinen Teil des OR abgedeckt? A hat den von B an C *absichtlich* und *unrechtmässig* begangenen Schaden zu begleichen. Der Schaden entstand dadurch, dass B den C aufgrund einer Sorgfaltspflichtverletzung von A zu täuschen vermochte. Die Frage basiert auf folgenden Überlegungen:

  > Nach Art. 17 ZertES haftet die Anbieterin von Zertifizierungsdienste, hier A, für Schäden an Dritten, hier C, die sich auf ein gültiges geregeltes Zertifikat verlassen haben, …
  >
  > Richtet sich die Haftung jedoch nach dem allgemeinen Teil des OR, dann stellt sich die Frage, ob das absichtliche Zufügen eines Schadens des B an C ein Grobverschulden darstellt und somit ein Unterbruch des Kausalzusammenhangs und einen Haftungsausschluss betreffend die von A begangene Sorgfaltspflichtverletzung darstellt. Zum Grobverschulden, 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) oder nach den Vorgaben eines konzessionierten Gewerbes (Art. 100 Abs. 2 und Art. 101 Abs. 3 OR)? Welche Haftung darf der IdP aus Vertrag also wegbedingen?
- Ist es sinnvoll, die Haftungsbestimmungen (Umfang der Gefahrtragung und unbegrenzte Höhe des Schadenersatzes) für die verschiedenen Sicherheitsstufen gleich auszugestalten?
- Wie haftet der IdP, wenn er zugleich ein nach ZertES anerkannter Aussteller von Zertifikaten ist?

III Angaben

III.1 Hinweise

Holliger	Eugénie Holliger-Hagmann, Produktesicherheitsgesetz PrSG, Schulthess Verlag 2010
Keller I	Alfred Keller, Haftpflicht im Privatrecht, Stämpfli Verlag AG, Bern 1993
Swisscom	Swisscom, Security Report 2017

III.2 Abkürzungsliste und Gesetzestexte

Abs.	Absatz
Bst.	Buchstabe
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
EU-Verordnung	Verordnung (EU) Nr. 910/2014 Des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
OBG	Ordnungsbussengesetz vom 24. Juni 1970, SR 741.03
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches vom 30. März 1911, SR 220
Rz	Randziffer
S.	Seite
u.a.	unter anderem
usw.	und so weiter
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

IV Anhang Identifizieren und Authentisieren

4.1 Über Begriffe lässt sich lange und eingehend diskutieren. Diese Abhandlung will hierzu keinen weiteren Beitrag leisten, sondern in Bezug zur Haftung und Digitalisierung gewisse allgemeine vorhandene Irrtümer beseitigen. Dazu soll das Ausstellen eines elektronischen Zertifikats nach ZertES (Bundesgesetz über die elektronische Signatur) für eine natürliche Person dienen.

IV.1 Prinzip des elektronischen Zertifikats

4.2 Das Prinzip der Ausstellung der elektronischen Zertifikate und ihrer Anwendungen beruhen grundsätzlich auf einem mathematischen Verfahren. Das Verfahren hat die Eigenschaft, dass zwei unterschiedliche Schlüssel erzeugt und verwendet werden. **Doch aus der Kenntnis eines Schlüssels lassen sich keine Rückschlüsse auf den anderen Schlüssel desselben Schlüsselpaars ziehen,** siehe folgende Abbildung Punkt 1)**.** Dies, obwohl sie mathematisch eindeutig miteinander verbunden sind oder zugeordnet werden können. Weil keine Rückschlüsse möglich sind, kann ein Schlüssel des Paars veröffentlicht und der andere privat (geheim) gehalten werden. Sinnigerweise bezeichnet man den veröffentlichten Schlüssel als öffentlichen Schlüssel, den anderen als privaten.

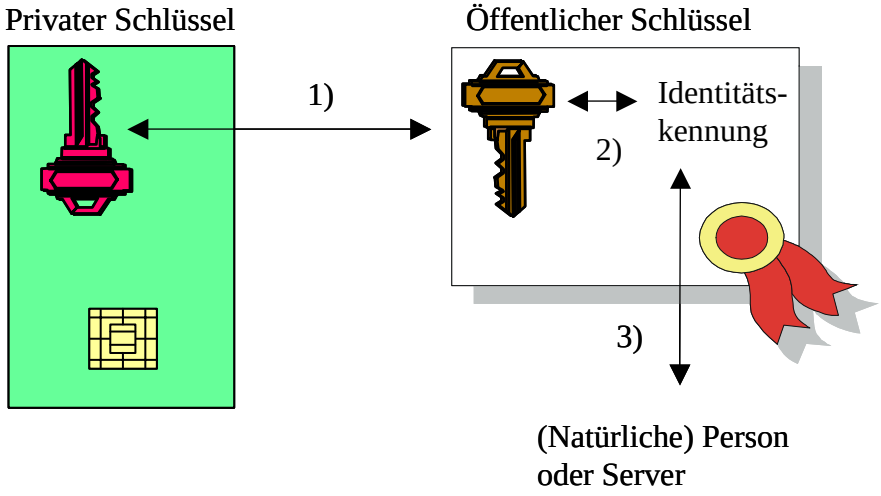


Abb. 1 Skizze der Funktionsweise rund um die elektronischen Zertifikate

4.3 Die Anmeldung übers Netz funktioniert prinzipiell nun so, dass man die andere Partei übers Datennetz davon überzeugt, dass man den anderen, dazu passenden privaten Schlüssel kennt, ohne dabei den privaten preiszugeben. Eine natürliche Person A generiert nun ein Schlüsselpaar nach diesem Verfahren. Publiziert A den öffentlichen

Schlüssel nun in seinem Namen, so kann sich eine andere Person B über das Datennetz davon „vergewissern“, dass Person A die entsprechenden Daten gesandt hat. Person A kann nämlich mittels eines mathematischen Prozesses Person B davon überzeugen, dass er Kenntnis vom dazu gehörigen privaten Schlüssel hat. Den Vorgang des Überzeugens wollen wir als „authentisieren“ bezeichnen.

4.4 Nun kann jeder behaupten, er sei z.B. der Verwaltungsratspräsident des Unternehmens XY mit dem entsprechenden öffentlichen Schlüssel. Deswegen sind digitale Zertifikate unerlässlich, welche die Zugehörigkeit von öffentlichem Schlüssel und gewissen Personenattribute wie Name, Adresse usw. beglaubigen 2). Anhand dieser Attribute im Zertifikat kann ein Rückschluss auf die natürliche Person oder Server gemacht werden 3). Dies nach erfolgter erfolgreicher Authentisierung.

4.5 Bevor der Aussteller des elektronischen Zertifikats die Personenattribute akzeptiert, sollte er sich davon vergewissern, dass die Person wirklich diejenige ist, welche sie vorgibt zu sein. Der Aussteller muss die Person also zuerst identifizieren 3). Erst dann sollte er dessen Attribute erfassen und Teile davon ins Zertifikat aufnehmen 2).

4.6 Wenn der private Schlüssel bekannt wird, so kann sich ein anderer als die betreffende Person A übers Datennetz bei Person B ausgeben. Deswegen werden die privaten Schlüssel in sicheren Einheiten wie einer Crypto Card (eine mögliche Ausprägung der sicheren Signaturerstellungseinheit) aufbewahrt.

IV.2 Unterscheidung zwischen Authentisieren und Identifizieren

4.7 Das Identifizieren beruht auf der physischen Prüfung anhand biometrischer Angaben wie Passfoto, Unterschrift. Das Authentisieren dagegen auf dem Überzeugungsprozess, dass die Person A am fernen Ende des Datennetzes den privaten Schlüssel kennt, welcher zum öffentlichen Schlüssel im Zertifikat passt.

4.8 Die Mittel zum Authentisieren lassen sich jedoch übertragen. Person A kann ihre sichere Signaturerstellungseinheit auf eine andere Person C übertragen, ohne dass Person B davon Kenntnis erhält. Person B wird also meinen, dass sich Person A, wie im Zertifikat angegeben, angemeldet hat und nicht Person C. Merkmale oder Attribute (genetischer Abdruck, Iris Scan), anhand welcher eine Identifikation vorgenommen werden, sind (bisher) jedoch nicht übertragbar.

IV.3 Zweifel und Verlässlichkeit (Haftung)

4.9 Person B muss sich, um etwelche Dispositionen nach der Authentisierung vorzunehmen, auf Folgendes verlassen (vertrauen) können:

1. Die Angaben im Zertifikat stimmen. D.h. der Aussteller des Zertifikats hat die Identifizierung und das Erfassen der Personenattribute sorgfältig vorgenommen.
2. Person A ist sorgsam mit seiner Signaturerstellungseinheit umgegangen, d.h. sie hat seinen privaten Schlüssel nicht einem Dritten zugänglich gemacht oder ihm übertragen.
3. Sicherheit des Verfahrens bei der Zuordnung vom öffentlichen Schlüssel im Zertifikat zum zugehörigen privaten (Authentisierungsverfahren).

4.10 Im Fall der Fälle 1 und 2, d.h. zur Risikominimierung bei durch Person B vorgenommen Dispositionen nach einer Authentisierung, sind entsprechende Haftungsbestimmungen im ZertES (Art. 17) und im OR (Art. 59a) eingebaut worden.

Nach dem Authentisieren besteht ein berechtigter Zweifel, ob sich wirklich diejenige Person, deren Angaben im Zertifikat enthalten sind, angemeldet oder ein Dokument signiert hat. Folglich besteht das Risiko, dass eine Person infolge einer inkorrekten Authentisierung geschädigt wird. Z.B. wenn sie nicht bezahlte Ware ausliefert. Dieses „Authentisierung“-Risiko kann durch entsprechende Haftungsregelung minimiert werden. Z.B. haftet der Inhaber des privaten Schlüssels für Schäden, wenn sich Dritte sich auf eine qualifizierte Signatur verlassen (Art. 59a Abs. 1 OR). Ausser er kann glaubhaft darlegen, dass er die entsprechenden, in Art. 13 VZertES geforderten Sicherheitsvorkehrungen betreffend Umgang mit dem privaten Schlüssel beachtet hat (Art. 59 a Abs. 2 und 3 OR).

Authentisieren bedeutet letztlich eine Zuordnung der Verantwortlichkeit der Vorgänge im Datennetz auf eine bestimmte Person. Doch bleibt ungewiss, wer sich angemeldet hat; dies in Analogie zum Fahrer und Halter eines Fahrzeugs.

Die Haftungsregelungen (wer, für welche Risiken in welchem Umfang einzustehen hat) sollten auch von der Sicherheit der bei der Zuordnung (Item 3) verwendeten Verfahren abhängen.

DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Frau Bundesrätin
Simonetta Sommaruga
Eidg. Justiz- und Polizeidepartement
3003 Bern

26. Mai 2017

Stellungnahme zum Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin Sommaruga, sehr geehrte Damen und Herren

Am 23. Februar 2017 haben Sie das Vernehmlassungsverfahren zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) eröffnet.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur sowie weitreichende Transparenz und Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft auf dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Vorentwurf wie folgt Stellung.

Vorbemerkung

Eine Vielzahl von Anwendungen im Internet setzen eine Identifikation der BenutzerInnen voraus. Meist ist eine E-Mail-Adresse ausreichend. Oft wäre nicht mal diese – um z.B. im Online-Shop ein Buch zu bestellen – tatsächlich nötig.

In anderen Bereichen ist eine Ausweispflicht, die auf einer staatlichen Beglaubigung beruht, und/oder eine (elektronische) Unterschrift zwingend vorgeschrieben; sei dies bei der Eröffnung eines Bankkontos, dem Abschluss eines Miet- oder Mobilfunkvertrags. Zudem mangelt es an eigentlich überfälligen E-Government-Angeboten (wie z.B. für Umzugsmeldungen, der Bestellung eines Strafregisterauszugs, Beantragung einer Handelsregisteränderung, im Bereich E-Health, für Schul-/Universitätsanmeldungen, Initiativen und Petitionen etc.), weil eine einheitliche, rechtlich bindende Identifizierungsmöglichkeit im Internet zur Zeit fehlt.

Im vorliegenden Vernehmlassungsentwurf für ein Bundesgesetz über anerkannte elektronische Identifikationsmittel (E-ID-Gesetz) schlägt der Bundesrat vor, die staatliche elektronische Identifikation an private Unternehmen und Organisationen auszulagern, welche für diese Aufgabe zertifiziert werden. Zudem möchte er eine E-ID über einen Anwendungsbereich schaffen, der vom Online-Shop über den Zugang zu Transportangeboten, bis zu Rechtsgeschäften und E-Government reicht – und dies gleich EU-weit. Mit diesen beiden Stossrichtungen drohen sich die Fehler aus dem Bundesgesetz über die elektronische Signatur (ZertES) zu wiederholen.

Wir lehnen die Vorlage ab, weil die Ausgabe von Identifikationsdokumenten eine wichtige Staatsaufgabe ist. Identifikationspapiere und elektronische Entsprechungen sind ein Bedürfnis der Bürgerinnen und Bürger in der heutigen Zeit. Die Gesetzesvorlage ersetzt den politischen Prozess, welcher die verschiedenen Interessen der Bürgerinnen und Bürger abzubilden vermag, durch eine blosse Überprüfung der Rechtskonformität der von der Wirtschaft – nach ihren Interessen – ausgestalteten Lösungen.

Überlegungen

[1] Der Identitätsnachweis und die Ausgabe von entsprechenden Ausweisen ist eine zentrale Staatsaufgabe. Dies gilt auch für digitale Ausweise. Es steht dem Bund frei, diese hoheitliche Aufgabe an eine externe Stelle zu vergeben, so wie auch Banknoten von einer externen Firma hergestellt werden. Wird jedoch die Initiative und die Ausgestaltung der E-ID Privaten überlassen, werden deren kommerziellen Überlegungen anstatt die Interessen der BürgerInnen und Bürger beim Aufbau dieses neuen Systems im Vordergrund stehen.

[2] Damit Private ihre Dienste auf dem staatlichen digitalen Identitätsnachweis aufbauen können, müssen die verwendeten Verfahren auf offenen Standards sowie die auf Benutzerseite verwendeten Software und Treiber auf quelloffener Software basieren.

[3] Wie es die Vorstösse von Post und SBB mit der SwissID sowie Swisscom, UBS und Crédit Suisse zeigen, benötigt die Privatwirtschaft kein dezidiertes E-ID-Gesetz als Grundlage für ihre E-Commerce-Anwendungen. Mit der Einführung eines solchen Gesetzes würden selbst für einfache, rechtlich weniger relevante Identifikationen sensible Daten erhoben – und nun auch automatisch und firmenübergreifend ausgetauscht. Dies verschafft den Anbieterinnen die Möglichkeit detaillierte Persönlichkeitsprofile über die NutzerInnen anzulegen. Ein griffiges Datenschutzrecht sowie die Möglichkeit, solche Angebote auch ohne SwissID wahrnehmen zu können, sind deshalb nötig. Es ist darüber hinaus nicht schlüssig, warum bestehende Lösungen

bei Online-Diensten durch die vergleichsweise komplexe Nutzung der E-ID ersetzt werden soll.

[4] Die Personen, welche eine E-ID benutzen, müssen die Kontrolle darüber behalten, welche Informationen zu welchem Zeitpunkt an eine identifizierende Stelle gesendet werden. So kann es allenfalls nur nötig sein, ein Alter über 16 Jahr zu bestätigen. Eine weiterführende Identifikation widerspricht dem Grundprinzip der Datensparsamkeit («Privacy by Default» und «Privacy by Design»).

[5] Für den Vorgang der Bestätigung von Identifikationsmerkmalen im Sinne des E-ID-Gesetzes braucht es nur eine beglaubigte Bestätigung, wie weiter unten beschrieben. Hierzu wird weder eine zusätzliche, eindeutige E-ID-Nummer noch ein neues, zentrales E-ID-Register benötigt.

[6] Nicht nur das Vertrauen in die Ausgabestelle ist von grosser Bedeutung, auch die Verhinderung von Identitätsdiebstahl muss verlässlich sichergestellt sein. Wie es das Bundesgesetz über die elektronische Signatur (ZertES) vorsieht, ist dazu eine Hardware-Lösung (Smartcard) zu verwenden. Hierzu drängt sich die bereits vorhandene Identitätskarte gerade zu auf, um darauf auf Wunsch der betroffenen Person ein entsprechendes Schlüsselpaar mit Zertifikat abzulegen.

[7] Im Unterschied zu Art. 8 Abs. 2 ZertES soll das Zertifikat das Schlüsselmaterial auch für die Verwendung zur Verschlüsselung freigeben. Damit würde das Grundproblem des vertraulichen und sicheren Schlüsselaustauschs bei der Kommunikationsverschlüsselung gelöst.

[8] Auf die Verwendung von biometrischen Merkmale, wie es der Vorentwurf zum E-ID-Gesetz – notabene auf als unsicher zu betrachtenden End-Benutzer-Geräten – vorsieht, muss hingegen verzichtet werden. Anders als beim Einsatz von oben beschriebenen Smartcards können biometrische Merkmale bei Fälschung oder Entwendung naturgemäss nicht zurückgezogen und ersetzt werden. Solch sensible Daten dürfen insbesondere auch nicht durch Dritte in zentralen Datenbanken bearbeitet werden (dürfen).

[9] Wie der Bundesrat im erläuternden Bericht zu Recht schreibt, stellt der Bund in der physischen Welt bereits heute konventionelle Identifizierungsmittel aus, nämlich Schweizer Pass, Identitätskarte und Ausländerausweis. Ergänzend dazu soll die Identität einer natürlichen Person nun auch elektronisch nachgewiesen werden

können. Als Gesetzesgrundlage ist kein neues E-ID-Gesetz nötig – es kann das bestehende Ausweisgesetz herangezogen werden:

> *Art. 2 Abs. 2quater AuG: Der Ausweis kann zudem elektronische Identitäten für Authentisierungs-, Signatur- und Verschlüsselungsfunktionen enthalten.*

Schlussfolgerung

Die Digitale Gesellschaft erachtet die Richtung, welche der Vorentwurf vorgibt, als grundlegend falsch. Aus den dargelegten Gründen lehnen wir den Vorschlag in der vorliegenden Form vollumfänglich ab. Es scheint, als ob der Blick auf das Wesentliche verloren gegangen ist.

Die Digitalisierung schreitet voran, und auch wir sehen den Bedarf einer benutzbaren und vertrauenswürdige elektronische Identität (wie auch Unterschrift). Dies ist vom Bund in seiner staatshoheitlichen Aufgabe an die Hand zu nehmen. Das Ausweisgesetz kann hierzu als Grundlage dienen. Eine E-ID muss jedoch den Bürgerinnen und Bürger dienen. Das Recht auf Privatsphäre – gerade im Internet - muss gestärkt und darf nicht weiter ausgehöhlt werden.

Wir bedanken uns für die Berücksichtigung unserer Anmerkungen und Vorschläge.

Mit freundlichen Grüssen

Erik Schönenberger
Geschäftsleiter

Per E-Mail an:
copiur@bj.admin.ch

Uster, den 26. Mai 2017

Stellungnahme zur Vernehmlassung „Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)“

Sehr geehrte Damen und Herren

A. Allgemeine Einschätzung

Die Stossrichtung der Vorlage ist grundsätzlich zu Begrüssen. Die Digitalisierung der Welt schreitet stetig fort und das Bedürfnis an verlässlicher digitaler Identifikation im Internet nimmt dementsprechend zu.

B. Ausstellungsverfahren: Privatwirtschaft unvorteilhaft

Das Ausstellungsverfahren verläuft gemäss Art. 6 des Vorentwurfs (VE) über einen anerkannten Identity Provider (IdP gem. Art. 2 VE). Der Bund soll nur subsidiär tätig werden (Art. 13 VE). Dies verläuft parallel zum ZertES (S. 4 des Berichts), wobei aber IdP keine elektronischen Signaturen im Sinne des ZertES anbieten müssen (ebendort). Dieses Vorgehen scheint für alle Beteiligten nachteilig.

I. Datenschutz der Inhaber

Die Inhaber der E-ID müssen ihre *Daten Privaten offenbaren*. Zwar gilt gemäss S. 28 des Berichts das DSG nach den strengeren Vorgaben für Bundesorgane (Art. 10 Abs. 4 VE i.V.m. Art. 16 ff. DSG), aber dies erschliesst sich m.E. nicht aus dem Gesetzestext. Ferner erhöht sich durch die Weitergabe von Informationen unweigerlich auch das Missbrauchspotential für die betreffenden Daten, indem nun mehr Personen diese Daten abrufen können, resp. mehr Computer – die kompromittiert werden können – die Daten verwahren. Dagegen wäre bei einer staatlich geführten Lösung der Staat bereits ohnehin im Besitz der fraglichen Daten.

Als Beispiel sei Google Inc. herausgegriffen, deren Google ID auf S. 2 und 10 des Berichts angesprochen wird. Google ist notorisch dafür bekannt, mit Personendaten verantwortungslos

umzugehen, insbesondere auch im kritischen Bereich der Schüler und Studenten,[1] und wurde in der Schweiz und der EU wegen Verletzung von Datenschutzrecht verurteilt.[2]

In der Praxis werden Bürgerinnen und Bürger nicht bloss einmal, sondern *mehrfach eine Validierung durchführen müssen*, gerade weil keine staatliche Lösung existiert und verschiedene Anbieter einander nicht vertrauen werden (bspw. wird sich Apple wohl weigern, andere Methoden als die Apple ID zur Identifikation von Personen anzuerkennen). Art. 18 Abs. 1 VE verpflichtet zwar die IdP, untereinander interoperabel auszugestalten und einander anzuerkennen, aber indes wird dies höchstens dazu führen, dass keiner der grossen Anbieter auf dem bestehenden Markt (wie auf S. 2 des Berichts beispielhaft aufgezählt) gewillt sein wird, IdP im Sinne des Gesetzes zu werden.

II. Kosten der Inhaber höher

Darüber hinaus müssen die Inhaber der E-ID müssen *mehr bezahlen* als bei einer staatlichen Lösung – die IdP werden kaum karitative Einrichtungen sein, sondern profitorientiert agieren (so denn auch S. 13 des Berichts). So werden die Gebühren des Bundes (Art. 23 VE) logischerweise auf den Kunden abgewälzt und zusätzlich ein Profit geschlagen. Der Markt wird dies nicht abfedern. Dagegen würde ein auf staatlicher Basis geführtes System durch das Kostendeckungs- und das Äquivalenzprinzip ein für den Inhaber vorteilhafteres Resultat erfolgen.

III. Haftung der IdP problematisch

Des Weiteren müssen die Inhaber der E-ID mit *unvorteilhaften Haftungsklauseln* der IdP zufriedenstellen (Art. 24 Abs. 1 VE). Gemäss Art. 41 Abs. 1 OR ist ein Verschulden erforderlich. Die Beweislast wird im Haftungsprozess gemäss Art. 8 ZGB somit beim Kläger liegen. In einer Zeit, in der allgemeine Geschäftsbedingungen a priori konsumentenfeindlich formuliert werden und die Anzahl der Anbieter naturgemäss klein sein wird, ist dies weitaus nachteiliger als eine Staatshaftung bei einer staatlichen Lösung.

S. 34 des Berichts behauptet: „Mit der E-ID allein können keine Rechtsgeschäfte abgeschlossen werden; […]“ In Anbetracht der heutigen Online-Shops würden E-ID die Identifikation des Gegenüber

---

[1] ALIM FRIDA/CARDOZO NATE/GEBHART GENNIE/GULLO KAREN/KALIA AMUL, Spying on Students: School-Issued Devices and Student Privacy, abrufbar unter <https://www.eff.org/files/2017/04/13/student-privacy-report.pdf>, besucht am 24. April 2017, S. 25.

[2] BGE 138 II 346; Urteil des EuGH vom 13. Mai 2014 C-131/12 *Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*.

übernehmen (bei mittleren Unternehmen – kleinere werden sich wohl kaum die anfallenden Gebühren leisten können) und sich ansonsten nichts ändern. Die Aussage, dass *kein Geschäftsverkehr bloss aufgrund der E-ID stattfinden wird, ist als illusorisch*. Warten auf einen Vertrag mit der EU betreffend Haftung ist eine mittelfristige Nicht-Lösung des Problems – die Verhandlungen über jegliche Themen stehen seit jeher still mangels des institutionellen Rahmenabkommens, auf das die EU insistiert.

IV. Henne-Ei-Problem der E-ID ungelöst

Zuletzt haben die Inhaber der E-ID ein sehr *hohes Interesse an einer einheitlichen Lösung*, die ihnen das Fortkommen im Alltag in einem Akt ermöglicht: Ausweis/Identitätskarte, elektronische Signatur und E-ID. Selbst unter Beibehaltung des aktuellen ZertES wäre es möglich, dies umzusetzen durch Opt-Out und Nachfrage bei der Vergabe des Ausweises, welcher Aussteller für die elektronische Signatur gewünscht ist mit anschliessender Weiterleitung an den ZertES-Zertifizierungsdienst.

Das ZertES-Konzept hat sich gerade nicht bewährt, wie dies der Bericht auf S. 11 behauptet. Es ist noch immer üblich im B2B-Verkehr, keine elektronische Signatur zu verwenden. Bei Konsumenten hat sich das ZertES überhaupt nicht durchgesetzt. *Dies droht, sich mit der E-ID zu wiederholen*. Damit die E-ID tatsächlich auch Verwendung findet, muss entweder ein dichtes Angebot von Geschäften, die mit der E-ID operieren, existieren oder eine breite Basis an E-IDs die Geschäfte anspornen, die E-ID zu akzeptieren, vorhanden sein.

Indem die E-ID mit der regulären Identitätskarte ausgegeben würde, wie dies ursprünglich vorgeschlagen war (S. 2 des Berichts), könnte die Umsetzung massiv beschleunigt werden.

V. Doppelter Aufwand der IdP und des Staates betr. elektronischer Signatur

Die IdP werden wohl ohnehin in ihrem Interesse Zertifizierungsdienste im Sinne des ZertES anbieten wollen, müssen sich aber nun für die im Kern gleiche Tätigkeit *doppelt anerkennen* lassen. Sodann muss der Staat auch doppelt Aufsicht dafür ausüben.

VI. Mehrfachbelastung des Staates

Der Staat hat nun *Kontroll- und Verwaltungsaufwand für ein neues System*, das in das existierende Ausweisvergabesystem integriert werden könnte. S. 2 des Berichts spricht von „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." In der Tat sind insb. Support und Softwareentwicklung teuer. Hier wäre aber ein Einfallstor für Private. Auslagerung von IKT-Support und -Entwicklung an Private ist dem Schweizer Recht nicht fremd.

Das Verhältnismässigkeitsprinzip (Art. 36 Abs. 3 BV) verbietet, aus Datenschutzgesichtspunkten heikle (Eingriff in den Schutz der Privatsphäre, Art. 13 Abs. 2 BV) und für den Geschäftsverkehr kritische Prozesse wie Identitätsverifikation in die Hände von Privaten zu geben, wenn eine mildere Massnahme besteht. Ebendies ist der Fall mit einer partiellen Auslagerung der kostenintensiven Faktoren.

VII. Sicherheitsverlust mit zunehmender Zahl an IdP

Die eidgenössischen Ausweispapiere sind mit mehreren Elementen gegen Fälschung gesichert. Einige davon werden zweifelsohne geheim sein und nur wenigen Personen offenbart. Je mehr IdP sich anerkennen lassen, desto höher ist die Wahrscheinlichkeit, dass diese geheimen Elemente ausser Kontrolle geraten und die *Schweizer Ausweise mittel-/langfristig kompromittiert werden*.

C. Kosten für Sperrung der E-ID durch den Inhaber

Im Vorentwurf wird das Verfahren der Sperrung einer *abhandengekommenen oder missbrauchten E-ID* den Privaten überlassen (Art. 17 Abs. 2 VE). Dabei wäre es möglich, dem Kunden Kosten dafür zu überbinden. Dies ist problematisch, denn der Missbrauchsfall ist keine blosse Möglichkeit, sondern wird mit Sicherheit eintreten, ggf. aus Gründen, die nicht im Machtbereich des Inhabers liegen[3]. Dadurch werden Konsumenten in ein Dilemma versetzt, in welchem sie zwischen potentiellem Missbrauch und Kostenfaktor abwägen müssen.

D. Rechte und Pflichten der Privaten im Gesetz unvollständig

Art. 14 VE ist sehr offen und gibt dem Bundesrat die Kompetenz, welche Sorgfaltspflichten Inhaber einer E-ID treffen. Dies steht in direktem Gegensatz zu Art. 164 Abs. 1 lit. c BV. Eine genauere Umschreibung ist unerlässlich.

Mit freundlichen Grüssen

Fabio E. R. Scotoni, BLaw
Student Rechtswissenschaften (MLaw) an der Universität Zürich

---

[3] Als Beispiel sei hier StartCom Ltd. genannt, die nach der Heartbleed-Lücke potentiell und tatsächlich kompromittierte SSL/TLS-Zertifikate nicht kostenfrei zurückziehen wollte (STARTCOM LTD., Twitter-Nachricht vom 8. April 2014, abrufbar unter <https://twitter.com/startssl/status/453494182544670721>, besucht am 24. April 2017).

grundrechte.ch
droitsfondamentaux.ch
dirittifondamentali.ch

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

26. Mai 2017

An die Vorsteherin des EJPD

Frau Bundesrätin Simonetta Sommaruga

3003 BERN

copiur@bj.admin.ch

Bundesgesetz über anerkannte elektronische Identifizierungseinheiten, E-ID-Gesetz

Vernehmlassungsfrist 29. Mai 2017

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Gerne nehmen wir hiermit Stellung zum oben aufgeführten Gesetzesentwurf zur Einführung elektronischer Identifizierungseinheiten (E-ID).

Grundsätzlich haben wir allergrösste Vorbehalte gegen die vorgeschlagene Aufgabenteilung zwischen Staat und Privaten bei der Vergabe von E-IDs, zumal diese E-IDs zwingend u. a. für Vote électronique oder für E-Health-Anwendungen vorgeschrieben werden sollen. Genauso, wie die Unternehmens-Identifikationsnummer (UID) durch den Staat vergeben wird, ist auch eine E-ID für natürliche Personen zwingend ausschliesslich durch den Staat - ohne Einbezug von Privaten - zu vergeben.

grundrechte.ch fordert deshalb, den vorliegenden Entwurf in diesem Sinne vollständig zu überarbeiten, so wie dies ursprünglich der Bundesrat am 19. Dezember 2012 dem EJPD in Auftrag gegeben hat.

Nicht zuletzt vor dem Hintergrund der jüngsten massiven Cyberattacken (wanna cry) geben wir zu bedenken, dass jede neue Datenbank neue Begehrlichkeiten (Missbrauch, Manipulation, Erpressung, Handel mit Daten) erweckt. Fachleute sind sich einig, dass es keine Garantie gibt, Datenbanken vor Angriffen von aussen hundertprozentig zu schützen. Umso sorgfältiger muss der Staat mit den Personendaten seiner Bürgerinnen und Bürger umgehen.

Die E-ID darf auf keinen Fall die herkömmlichen Ausweispapiere (ID, Pass, Ausländerausweis) ersetzen. Die Wahlfreiheit, mit welcher Methode, mit welchem amtlichen Dokument sich jemand gegenüber öffentlichen Ämtern oder privaten Firmen ausweisen will, muss zwingend erhalten

bleiben. Nur so kann das Grundrecht auf informationelle Selbstbestimmung auf lange Zeit gewahrt und geschützt werden.

Wenn überhaupt eine E-ID eingeführt werden soll, darf dies auf gar keinen Fall an private profitorientierte Unternehmen ausgelagert werden. Der Staat ist die einzige Institution, die - analog der Ausstellung amtlicher Ausweise - dazu berechtigt sein darf. Es muss unbedingt gewährleistet bleiben, dass das Ausstellen eines rechtsgültigen ID Nachweises, in welcher Form auch immer, eine unveräusserliche Aufgabe des Staates bleibt und damit sichergestellt wird, dass kein Datenmissbrauch möglich ist.

Die Vorlage geht auch bezüglich der zu verarbeitenden Daten für eine E-ID viel zu weit. Es ist nicht ersichtlich, weshalb derart viele Personendaten quasi auf Vorrat gesammelt und den privaten Anbietern zur Verfügung gestellt werden sollen. Insbesondere die Versichertennummer nach Artikel 50c des Bundesgesetzes über die Alters- und Hinterlassenen-Versicherung sowie das Gesichtsbild und das Unterschriftsbild aus der nationalen Ausweisdatenbank sind hochsensible höchstpersönliche Daten und werden einzig für andere, ganz bestimmte eingeschränkte Zwecke unter Zusicherung der Vertraulichkeit erfasst.

Ohne jemandem etwas unterstellen zu wollen, gibt es bereits genügend aktuelle Beispiele, wonach Personendaten längst nicht nur für den ursprünglich angegebenen Zweck verwendet werden. Die im Gesetzesentwurf vorgesehene **Kontrolle durch die beim Bund angesiedelte Anerkennungsstelle ist ungenügend**. Sie wäre kaum in der Lage, die korrekte Verwendung aller Personendaten sicher zu stellen - zumal diese sogar von den Identity Providern an Betreiber von E-ID-verwendende Dienste weitergegeben werden dürften.

Die Ausstellung einer E-ID muss auch unter diesem Kontrollaspekt eine reine Bundesaufgabe bleiben. Nur so kann sichergestellt werden, dass der Umgang mit diesen sensiblen Daten jederzeit auch einer parlamentarischen Aufsicht und Kontrolle unterstellt bleibt und das Gesetz, sofern notwendig, nachgebessert werden kann, ohne dass dadurch bestehende Verträge mit privaten Dritten verletzt würden.

Zusammenfassend halten wir fest, dass wir die Vorlage insgesamt ablehnen. Die Einführung einer E-ID muss zwingend eine staatliche Aufgabe bleiben. Sie darf unter keinen Umständen an private Dritte ausgelagert werden. Staatlich anerkannte Identitätsausweise müssen, in welcher Form auch immer, ausschliesslich vom Staat selbst ausgestellt und nachgeführt werden. Das Kostenargument darf hier nicht zum Tragen kommen.

Zudem muss der Bund sicherstellen, dass die Bürgerinnen und Bürger jederzeit das Recht haben, selber zu entscheiden, mit welchem Dokument sie sich ausweisen wollen. Dies gilt auch für die Authentifizierungs-Vorgaben von privaten Firmen. Der Bund ist in der Pflicht, diese anzuweisen, das Recht auf informationelle Selbstbestimmung, die digitale Selbstbestimmung zu wahren. Die im Bericht erwähnten Projekte „Passepartout fürs Internet“ von Credit Suisse, UBS und Swisscom sowie „SwissID“ von der Post und den SBB sehen eine Zwangsverpflichtung der KundInnen zu einer digitalen E-ID vor! **Sie alle verletzen dieses Grundrecht massiv! Der Bundesrat ist daher aufgefordert, die gesetzlichen Grundlagen zu schaffen bzw. das Datenschutzrecht so anzupassen, dass die Kundinnen und Kunden die Angebote auch ohne SwissID wahrnehmen können.**

Mit freundlichen Grüssen

Viktor Györffy, Präsident grundrechte.ch

NÜGLARUS
C/O HANDELSKAMMER GLARUS
POSTGASSE 27
8750 GLARUS

WWW.NÜGLARUS.CH

Eidgenössisches Justiz- und
Polizeidepartement
Frau Bundesrätin Simonetta Sommaruga
Bundesrain 20
3003 Bern

per E-Mail: copiur@bj.admin.ch

Glarus, 29. Mai 2017

Stellungnahme zum Vorentwurf Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)

Sehr geehrte Frau Bundesrätin

Die Initiative NüGlarus hat zum Ziel den Kanton Glarus bei seiner wirtschaftlichen Entwicklung insbesondere im Bereich von Innovation und Co-Innovation zu unterstützen. Die Initiative versteht sich als lösungsorientierter Ideen- und Impulsgeber für Wirtschaft, Gesellschaft und Politik. Die Vereinfachung der Behördengänge und von administrativen Prozessen in und mit privaten und öffentlichen Unternehmen ist dabei zentral.

Mit dem neuen E-ID Gesetz wird definiert wie künftig digitale Identitäten vergeben und genutzt werden. Die Schweiz hat im Vergleich zu anderen Ländern in diesem Bereich grosse Verspätung. Der Handlungsbedarf ist enorm.
Onlineprozesse vereinfachen die Kommunikation und den Austausch von Informationen, ermöglichen Effizienzgewinne bei Behörden und Unternehmen und entsprechen einem Bedürfnis von Kundinnen und Kunden bzw. Bürgerinnen und Bürgern. Im Gegensatz zu einer physischen Transaktion in einem Geschäft oder bei einer Behörde, lässt sich die Identität der beteiligten Parteien im Onlinebereich aber nur schwierig oder gar nicht feststellen. Entsprechende IDs haben sich bisher am Schweizer Markt nicht durchgesetzt und im Onlinehandel hat sich die Kreditkarte als «Ausweis» etabliert.
Mit der fortschreitenden Digitalisierung von Wirtschaft, Behörden und Gesellschaft ist diese Situation nicht mehr haltbar. Es besteht dringender Bedarf nach einem digitalen Pendant zum Reisepass für die Online-Welt. Diese elektronische Identitätskarte oder E-ID wird jedoch nur dann Erfolg haben, wenn sie rasch und flächendeckend für viele Dienste und Angebote der Wirtschaft und der Behörden verwendet werden kann.

Dazu ist ein gutes Zusammenspiel von Staat und Wirtschaft ausschlaggebend. **Wie der Telekombranchenverband Asut fordert NüGlarus, dass die Identifikation der Personen mit staatlichen Registern und Daten zu erfolgen hat. Damit die Vertrauensgrundlage für die E-ID in der Bevölkerung für alle Anwendungsszenarien wie z.B. Fernabstimmungen an Gemeindeversammlungen geschaffen wird, soll der Staat auch selbst effektiv eine E-ID anbieten. Zusätzlich soll die E-ID bei Behördenkontakten als verbindlich erklärt werden.**

NÜGLARUS
C/O HANDELSKAMMER GLARUS
POSTGASSE 27
8750 GLARUS

WWW.NÜGLARUS.CH

1. ***Neues Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)***

a) E-ID: Wer

Eine elektronische Identitäten kann durch

1) staatliche Akteure (Bund/Kantone/Gemeinden)
2) private Akteure
3) staatliche und privatwirtschaftliche Akteure

ausgegeben werden.

Physische Identitäten (Pass/ID/Personenregister) werden heute von Bund und Gemeinden zur Verfügung gestellt. Sie überprüfen die Identität der Bewohner und geben eine sichere physische Identität aus.

Vordringlichstes Ziel muss es nach Jahren von Misserfolgen nun sein, der Schweizer Bevölkerung auf Wunsch und ohne zusätzlichen Aufwand (und zu tiefen Kosten) neben der physischen Identität auch eine elektronische Identität zur Verfügung zu stellen, welche in der Schweiz bzw. weltweit mit allen Systemen kompatibel ist.

Dazu bieten sich insbesondere Kundenbeziehungen an, die bereits bestehen und wo eine Identitätsakontrolle bereits erfolgte um die elektronische Identität rasch zu verbreiten. D.h. insbesondere mit Bund/Kantonen/Gemeinden sowie mit Banken, Telekomanbietern und allenfalls Akteuren des öffentlichen Verkehrs.

Ziel muss es jedoch auch sein, dass die nächste Generation von Schweizern auf Wunsch gar keine physischen Identitäten mehr einsetzen und eines Tages sogar beziehen muss. Das heisst: auch das Eröffnen einer Telekomkundenbeziehung oder eines Bankkontos soll dereinst mit elektronischer Identität möglich sein.
Sollten private Akteure nur mittels einer Eröffnung der Kundenbeziehung per physischer Identität, also Pass, IDK oder Ausländerausweis in der Lage sein eigene E-IDs auszugeben, würde dies einem Anreiz entsprechen andere E-IDs zu diesem Zweck nicht zu akzeptieren. Dies muss unbedingt verhindert werden. Dies ist in letzter Konsequenz nur möglich, wenn auch eine staatliche digitale Grundidentität zur Verfügung gestellt wird.

Ebenfalls für eine auch staatliche Identität spricht, dass es in der Augen der Stimmbürger subjektiv wohl nur einen Anbieter gibt, der z.B. eine Abstimmung (zum Bespiel eine Fernabstimmung an einer Gemeindeversammlung) nach allen Regeln garantieren könnte. Das ist der Staat.
Auch für eine staatliche elektronische Identität spricht, dass letztere innerhalb von nur 10 Jahren rundumerneuert wird. Damit hätten 100% der Bevölkerung innerhalb von nur 10 Jahren praktisch ohne Zusatzbemühungen die Möglichkeit an eine digitale Identität zu kommen. Das ist einer der Gründe weshalb neue digitale Dienste in Estland derart verbreitet sind.

Bei der höchsten Sicherheitsstufe erfolgt die Registrierung für die E-ID mit persönlicher Vorsprache beim IdP oder mit Videoidentifikation gestützt auf einen staatlichen physischen Ausweis. Zusätzlich wird die Echtheit des Ausweises und mindestens ein biometrisches Merkmal (Fingerabdruck-, Gesichts- oder Stimmenerkennung) **gestützt auf eine behördliche Quelle** überprüft (Ausweisgültigkeit und Gesichtsbild oder anderes biometrisches Erkennungsmerkmal). Dazu braucht es eine starke Kooperation zwischen dem E-ID Anbieter und der staatlichen Identifikationsstelle. Wie effizient diese Zusammenarbeit sein wird ist zum jetzigen Zeitpunkt unklar.

NüGlarus unterstützt im Hinblick auf eine hohe Verbreitung der digitalen Identität die Möglichkeit, dass private Anbieter wie Banken und Telekomanbieter in der Schweiz diese zur Verfügung stellen können und dass diese grundsätzlich untereinander und mit EU Anbietern interoperabel sein sollen.

Damit die Schweiz ihren grossen Rückstand auf andere Länder rasch gut machen kann, ist jedoch auch eine staatliche digitale Identität notwendig, bzw. soll eine solche in Zukunft ohne Zusatzaufwand auf Wunsch auf der Identitätskarte (oder dem Pass) aufgeschaltet werden können. Die E-ID soll allen Bürgerinnen und Bürgern zur Verfügung stehen und zwar auch solchen, die keine E-ID eines privaten Anbieters wollen. Nur wenn der Staat eine Basis-E-ID zur Verfügung stellt und zwar so rasch als möglich (mit dem Inkrafttreten des Gesetzes), ist zudem gewährleistet, dass es effektiv eine E-ID gibt – unabhängig von den privaten Angeboten. Für ein staatliches E-ID-Angebot müssen dabei dieselben Rahmenbedingungen gelten, wie für eine private E-ID eines zertifizierten Identity Providers. Ansonsten besteht die Gefahr einer Wettbewerbsverzerrung. Um eine Wettbewerbsverzerrung zu vermeiden, sind die Kosten vollständig beim Aufschalten der staatlichen E-ID auf die Identitätskarte zu erheben (es soll dafür kein physisches Vorsprechen auf einer Amtsstelle notwendig sein).
Auf Wunsch sollen die Bürger auch in der Lage sein für E-ID auf ihrer Identitätskarte statt dem öffentlichen Anbieter einen privaten Anbieter zu wählen.

Für die Ausgabe einer staatlichen E-ID durch eine Gemeinde auf Basis der Identitätskarte ist kein neuer Artikel im Gesetz notwendig! Gemeinden/Kantone können diese allenfalls auch in Zusammenarbeit auf Basis der Identitätskarte ausgeben, solange diese den Wettbewerb nicht verzerren.
Wir fordern Pilot-Gemeinden auf, dies rasch nach Annahme dieses Gesetzes zu tun und werden hierbei auch Unterstützung anbieten. Es ist hier auch die Möglichkleit zu prüfen, dass dgitale Identiäten von anderen Identitätsanbietern als dem Staat auf der Gemeinde mit der Ausgabe der Identitätskarte ausgegeben werden. Ähnliches gilt für die Prozesse beim Handelsregisteramt für juristische Personen.

Sowohl staatliche wie private elektronische Identitäten sollten nach dem **opt-out Prinzip** gewährt werden um die Verbreitung zu fördern. D.h. wer mit der neuen Identitäskarte oder EC-Karte keine E-ID erhalten will, muss dies explizit so angeben. Studien zeigen, dass die Verbreitung über eine solche simple Regel sehr stark ansteigen kann. Mit einer raschen grösseren Verbreitung würden auch in der Schweiz endlich neue sichere digitale Geschäftsmodelle möglich.

b) E-ID: Wie
Alle elektronisches Identitäten in der Schweiz müssen gemäss Gesetz interoperabel sein. Das ist gut so. Es ist auch sicherzustellen, dass übliche EU Identitäten interoperabel sind. Zudem muss der Gesetzgeber intevenieren, wenn sich die Anbieter nicht über die kommerziellen Aspekte einig werden (Interkonnektion). Grundsätzlich sollten keine Kosten bei der Nutzung einer E-ID eines Identitätsproviders durch einen Diensteanbieter anfallen, um die Verbreitung von neuen Technologien nicht zu verlangsamen. Neue Probleme wie beim Roaming sind unbedingt von Anfang an zu vermeiden! Diese Preisstruktur könnte im Gesetz von Anfang an festgeschrieben werden («Bill-and-keep» Interkonnektion). Die Abrechnung kann wie im Gesetz beschrieben dem Markt überlassen werden. Die Preisstrukturr ist jedoch wie beschrieben festzulegen, damit die Nutzung gefördert wird und es nicht zu einem Marktversagen kommt (grosse E-ID-Provider könnten bei Ihren eigenen Retaildienstleistungen z.B. kleine E-IdPs nicht mehr akzeptieren (oder die hohen Interkonnektionsgebühren nicht bezahlen wollen).

Um die vollständige Interoperabilität und Interkonnektion sicherzustellen, ist ein zusätzlicher Artikel notwendig, der das Bill-and-Keep Prinzip festschreibt:

> ***Entwurf Art 23.3 E-ID Gesetz (neu)***
>
> **[3] IdPs sind grundsätzlich frei darin, Gebühren für die ihnen entstandenen Kosten zu erheben.**
> **Es dürfen jedoch weder von privaten noch öffentlichen Anbietern Terminierungsgebühren (Kosten auf Seiten des Dienstleisters) erhoben werden.**

Das heisst jede einzelne zusätzliche Nutzung der E-ID ist für jeden Dienstleister in der Schweiz und im Ausland kostenlos.

NÜGLARUS
C/O HANDELSKAMMER GLARUS
POSTGASSE 27
8750 GLARUS

WWW.NÜGLARUS.CH

c) Behörden müssen E-ID zwingend akzeptieren

Schliesslich ist die Verwendung der E-ID im Verkehr mit Behörden zwingend vorzuschreiben. Überall dort, wo im Verkehr mit Behörden eine Ausweispflicht oder Ähnliches besteht, soll die Verwendung der E-ID zwingend vorgeschrieben werden. Damit wird die Anwendung der E-ID bevorzugt und e-Government-Prozesse werden unterstützt. Dies trägt zu einer raschen Verbreitung der E-ID bei und führt zu Effizienzgewinnen bei der öffentlichen Hand und in der Privatwirtschaft. Ausnahmen für die E-ID-Pflicht sind im Einzelfall möglich, aber bewilligungspflichtig.

Für Rückfragen und weitergehende Informationen stehen wir jederzeit gern zur Verfügung.

Roberto Balmer
Präsident
E: robi@nüglarus.ch
M: 044 / 586 81 12

@NueGlarus

Linkedin

Facebook

Glarus, 29. Mai 2017

Commentaires sur la Loi fédérale sur les moyens d'identification électronique reconnus (Loi e-ID)

Auteurs:
Dans le cadre du *Open Geneva Hackathons* qui s'est déroulé à Genève du 12 au 14 mai 2017 (http://opengenevahackathons.org/), un hackathon s'est tenu sur le *Prototypage de Politiques du Numérique* (https://jhmorin.wixsite.com/faclabbattelleoghack). Une équipe s'est concentrée sur la question de l'*identité numérique* en faisant un travail d'analyse sur cette question. Les contributeurs ont convenus de partager le résultat de ce travail dans le cadre de la procédure de consultation sur la loi e-ID ouverte jusqu'au 29 mai 2017.

Les contributeurs à ce travail sont :

- Bruno Chanel – bruno@brunochanel.com
- Jörn Erbguth – joern@erbguth.net
- Guillaume Saouli – guillaume.saouli@partipirate.ch (personne de contact)
- Alexis Roussel – alexis.roussel@bity.com
- Vincent Pignon – Vincent.Pignon@etat.ge.ch
- Jean-Henry Morin – Jean-Henry.Morin@unige.ch

Résumé succinct du commentaire

*Nous estimons que **l'intégralité de cette loi doit être revue** en plaçant l'Etat au cœur du dispositif d'identité, dans sa fonction régalienne qui en aucun cas ne souffrirait d'être externalisée à l'économie privée.*

Introduction

Dans le cadre de la digitalisation de la société, la reconnaissance et la gestion de l'identité est un élément essentiel de la continuité de l'état de droit et représente par conséquent une des pierres angulaires de la société.

Il est surprenant et inquiétant de voir que le travail du DFJP se borne à réduire l'individu à un simple consommateur. Il s'agit là d'une spoliation fondamentale de la personne, et une restriction de ses droits.

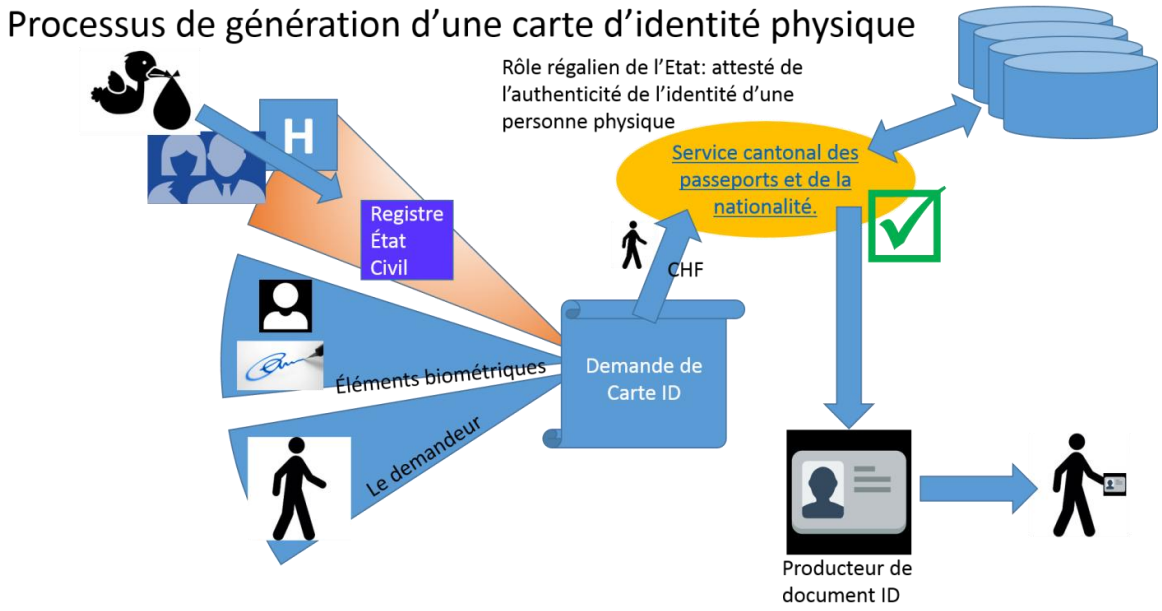
Alors que la société se numérise de plus en plus, la relation du citoyen aux institutions se fait aussi de plus en plus de manière électronique, que ce soit pour l'acte démocratique, qu'est le vote, le dépôt de plainte, ou la relation aux administrations dans leur ensemble, il apparaît clairement dans son projet que le DFJP a fait l'impasse sur ces développements.

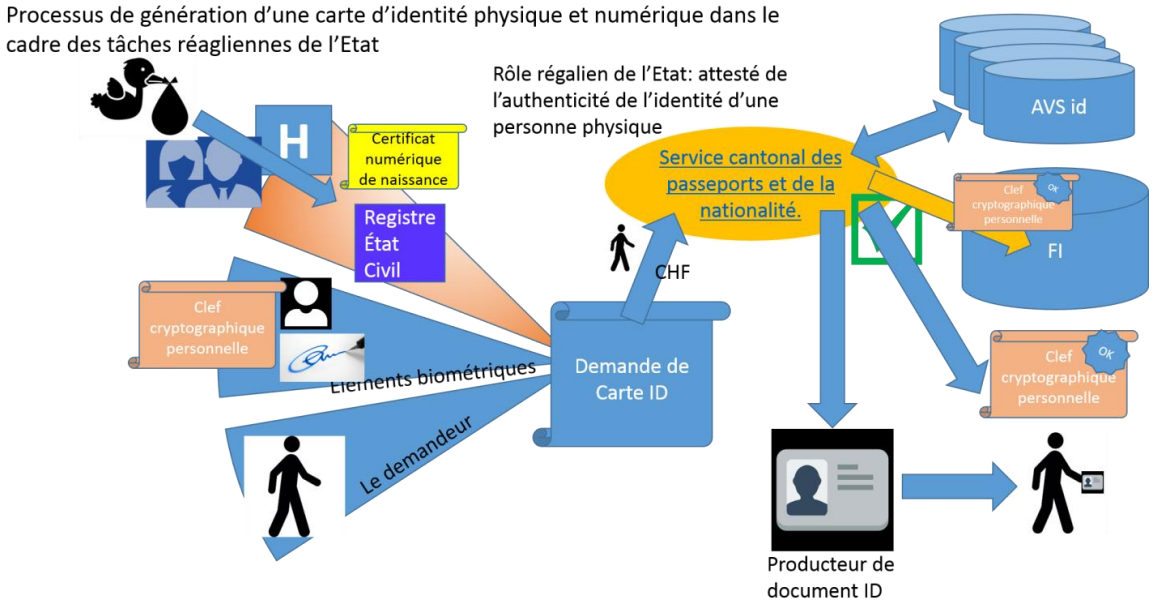
Nous sommes d'avis qu'il est essentiel que l'identité soit au cœur de la digitalisation de la société, et non un élément marginal pouvant être traité légèrement et dont la mise en œuvre est laissée à des acteurs privés. Dans le monde analogique, l'État est le seul fournisseur d'identité,

il ne peut pas subsidiariser son rôle au titre qu'une barrière est franchie, et qu'il faille agir au niveau d'"Internet".

L'Etat est le garant de l'identité d'une personne en garantissant la véracité de 3 éléments:

1. La filiation
2. Les éléments biométriques, tel que la photo, la signature, les empreintes digitales, la taille
3. La matérialité de la personne (sa présence lors de la demande)





Même si dans la relation technique, des tierces parties privées peuvent intervenir, il n'en reste pas moins que l'identité numérique ne peut pas être attribué par une telle entité privée, puisqu'en démocratie, elle ne peut que se borner à reconnaître la personne et son identité et non la lui attribuer.

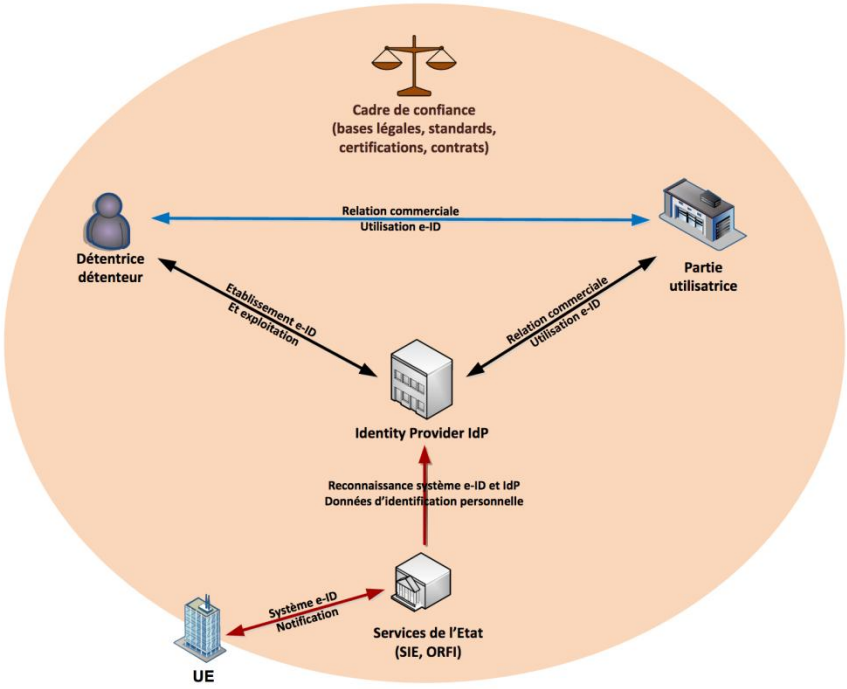


Schéma 1: Instances et relations les plus importantes d'un écosystème e-ID

La base de travail du DFJP néglige également cet élément fondamental dans son approche, et manque ainsi l'opportunité d'amener notre état de droit dans l'ère numérique.

Dans le cadre de la réflexion menée pendant ce Hackathon, nous avons identifié plusieurs éléments clefs qui nécessitent des clarifications et des modifications. Elles sont consignées ci-dessous.

Références:

- La loi : https://www.admin.ch/ch/d/gg/pc/documents/2842/Vorlage_eid_d.pdf
- Rapport : https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/e-id/vn-ber-d.pdf
- eIDAS (Niveau Europeen) : http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32014R0910
- ISO 20022.ch https://www.iso-20022.ch/lexikon/e-id-gesetz/
- La LDI – Loi sur les Documents d'Identité https://www.admin.ch/opc/fr/classified-compilation/19994375/index.html

Commentaires :

1. La gestion de l'identité est une tâche régalienne fondamentale de l'état de droit, elle ne peut pas être déléguée à des opérateurs privés. Comme le montre la LDI Loi sur les documents d'identité, la LeID est lacunaire et n'est pas conséquente.
2. Une identité numérique ne peut pas être fragmentée avec des niveaux différenciés de confiance,
3. La gestion d'une identité électronique ne peut pas simplement être confiée à une personne morale de droit suisse dans la mesure où des lois d'autres pays pourraient imposer des actions pouvant remettre en cause la confiance nécessaire pour opérer une telle infrastructure critique selon l'origine de la propriété de la personne morale en question.
4. Les Fournisseurs d'Identités pourraient avoir accès à des données personnelles (e.g., religion) sans nécessairement pouvoir justifier que les personnes concernées sont leurs clients.
5. Le délai de mise-à-jour des informations sur l'identité est totalement farfelu (Art. 8) : une semaine à une année de délai est beaucoup trop long par rapport à la criticité de l'usage de telles informations.
6. Le risque de faillite d'un Fournisseur d'Identité est un danger. En effet, l'identité électronique d'une personne ne survit pas la faillite de ce dernier, ce qui ne peut pas être acceptable étant donné que l'identité d'une personne ne peut pas être aliénée et être dépendante des aléas d'une personne morale privée.
7. L'interopérabilité est une exigence critique. Les premiers acteurs vont définir des standards de fait auxquels les suivants vont devoir adhérer.
8. L'Art 24.1 prévoit que les relations entre titulaire de l'e-ID, de l'exploitant d'un service utilisateur et du FI soient régis les articles du code des obligations, cela implique que les deux derniers peuvent s'appuyer sur la liberté de régler et exclure leur responsabilité dans leurs conditions générales. La détention d'un document d'identité électronique ne peut pas être gouverné par le code des obligations, ni d'ailleurs les opérations de validation d'une identité ou une authentification. Comme le montre en essence la LDI.
9. Art. 10, al 2, comment est-il prévu de contrôler le « consentement éclairé » du titulaire de l'e-ID ?

DÉTAILS :

4.2 Il existe des cas de figure où des Fournisseurs d'Identité sont des filiales/succursales de société étrangère ; il ne peut être loisible de laisser de telle société opéré des infrastructures aussi sensibles alors qu'elles peuvent être soumise à des impératifs légaux supérieurs, comme c'est d'ailleurs le cas avec les filiales de sociétés états-uniennes cise à l'étranger et dont l'extraterritorialité n'est pas reconnue par les lois américaines, en particulier le Patriot Act, tout comme d'ailleurs par la jurisprudence pénale fédérale des USA. Un tel cas de figure ne peut pas être accepté puisque l'intégrité et la confiance dans le système de gestion d'identité peuvent être compromises sans qu'aucune partie suisse ne puisse intervenir.
Pour rappel, le gouvernement zougois a arrêté toute collaboration avec des sociétés

américaines possédant une filiale en Suisse à cause de cet état de fait, alors qu'il ne s'agissait que de la gestion d'informations fiscales.

5.1 A l'instar des documents d'identité physique, comment est-il possible d'envisager des niveaux de fiabilités diverses ? La preuve d'une identité ne peut pas être à géométrie variable. Est-ce qu'il existe une pièce d'identité physique dont les qualités sont réduites ? Non. Même si technologiquement, l'utilisation d'une identité électronique peut s'effectuer de diverses manières, il est inenvisageable d'offrir des identités au rabais. Soit l'autorité reconnaît l'identité d'une personne soit elle ne la reconnaît pas, mais elle ne peut pas donner une reconnaissance partielle à un élément insécable tel que la doctrine en matière d'identité le définit.

5.2 Les niveaux mentionnés ne sont ni clairement défini, et les critères ne sont pas stipulés. Pourquoi définir plusieurs niveaux, alors qu'il s'agit de cas d'usage d'une identité électronique, plutôt que la détermination d'une identité numérique. Il est clair que le point 5.2 confond cas d'usage d'une application s'appuyant sur une exploitation partielle d'une identité électronique, avec la nécessité de définir un document d'identité électronique permettant toutes les utilisations. Cela est inacceptable.

6 Comme mentionner dans l'introduction, un e-id ne peut pas être attribué mais doit être reconnu, sur la base d'éléments fournis par le demandeur et corroboré par les registres des autorités d'état civil, et les éléments biométriques propres au demandeur. Cette tâche ne peut pas être confiée à des opérateurs privés.

7 La version de l'e-id fournie peut avoir un identifiant, mais en aucun cas la personne demanderesse. Faire un tatouage électronique de la personne avec un identifiant unique n'est pas acceptable, car cela ne correspond pas à la doctrine d'établissement de l'identité d'une personne.

6 & 7 Les éléments stipulés dans ces deux articles de la Leid sont contraires au droit supérieur et à l'esprit de la constitution. Par ailleurs, ils sont également contraires à la doctrine en matière d'établissement de l'identité d'une personne.

8.1 Les cas d'usage ne peuvent pas contraindre le contrôle d'intégrité d'une identité électronique, mais également du registre des identités électroniques ; ce processus doit être permanent, et se dérouler au minimum une fois par semaine.
8.2 C'est de la responsabilité de l'Etat et non à son agent de s'assurer que la gestion des informations d'un e-id y inclus sa révocation. Un e-id est un acte officiel, son annulation n'est pas du resort d'un agent privé.
8.3 L'Etat n'a pas à percevoir d'émolument supplémentaire lorsque des données personnelles sont modifiées, puisqu'il perçoit déjà, par ailleurs, un émolument pour cette mise à jour.

9 L'Etat doit utiliser l'e-ID d'une personne et non le numéro AVS pour toutes ses relations. L'utilisation d'un identifiant tel que l'AVS en dehors des cas d'application de ce dernier, contrevient à la protection de la sphère privée de la personne et son intégrité. L'administration doit pouvoir construire un référentiel de personnes en s'appuyant sur un élément dont l'intégrité, et la non-répudiabilité sont contrôlés de manière plus stricte qu'un identifiant de bénéficiaire d'assurance. L'e-ID est cet élément.

10.2 Les FI n'ont pas à transmettre de données personnelles à un utilisateur, mais ils doivent se borner à valider si oui ou non, les éléments d'information fournis par le détenteur d'un e-ID sont valables.

Modification d'autres actes

1. Loi du 22 juin 2001 sur les documents d'identité

2. Code civil

3. Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants

4. Loi fédérale du 18 mars 2016 sur la signature électronique
La loi ne prend pas en compte le niveau de confiance attribué aux eid (voir section 2 article 5 de la Le-id).

Conclusions

En conclusion et indépendamment des commentaires évoqués ci-dessus, nous estimons que ***l'intégralité de cette loi doit être revue*** en plaçant l'État au cœur du dispositif d'identité, dans sa fonction régalienne qui en aucun cas ne souffrirait d'être externalisée à l'économie privée, comme le démontre très justement la LDI, qui doit servir de référence pour la construction de la LeID.

Vernehmlassungsantwort zum *E-ID-Gesetz*

Zürich, 28. Mai 2017

Sehr geehrte Damen und Herren,

Gerne möchte ich als Privatperson zum neuen Gesetz Stellung nehmen. Insgesamt erachte ich diese Vorlage als gelungen und hoffe auf eine baldige Rechtskraft dieses Gesetzes.

Artikel 5 ist zentral für die E-ID und auch aus rechtsstaatlicher Sicht essentiell Wichtiges wird mit Ziffer 4 auf die Verordnungsstufe delegiert. Gerne möchte ich daher ein paar Bemerkungen in dieser Hinsicht anbringen auch wenn später mutmasslich wiederum eine Vernehmlassung zu den diesbezüglichen Ausführungserlassen stattfinden wird.

Der Bericht bezeichnet den deutschen ePA als «Messlatte für neue staatliche E-ID weltweit». Es werden auch die Kosten und Umständlichkeit in der Benutzung angeführt - Argumente, die - in allenfalls leicht vermindertem Masse - auch regelmässig zur aktuellen SuisseID genannt werden. Insbesondere auch die Herausgeber von SuisseID und scheinbar auch der neuen SwissID finden Gefallen an Cloud-Signaturen und -Identitäten – offenbar auch für das Sicherheitsniveau «hoch».

Die Unterschiede bezüglich des *benötigten Vertrauens in Dritte beim Betrieb* dieser Cloud-Ansätze im Vergleich zum ePA und anderen auf den Konzepten klassischer PKI beruhender System scheinen mir zu wenig erläutert.

Bei den *klassischen Systemen* beschränken sich die hoheitlichen (bzw. hoheitlich delegierter) Funktionen auf

a) den kurzen Zeitpunkt der Ausstellung (typischerweise dem Verbinden eines kryptografischen 'Public Keys' [einer quasi zufälligen Zahl z.B. nach dem RSA Algorithmus] mit der Identität durch die Signatur eines X509 Zertifikats)
b) und der Bereitstellung von standardisierten Revokationsinformationen während der darauf folgenden Jahre der Anwendung um z.B. den Schaden durch den Verlust der Private-Keys minimieren zu können.

Danach ist die Anwendung durch Hardware und Algorithmen im Kontrollbereich des Benutzers gewährleistet, die bei sorgfältiger Durchführung gegenüber illegitimem Einfluss von Dritten vergleichsweise resistent sind.

Bei den «modernen» Ansätzen wie z.B. Cloud-Signaturen liegt der private Schlüssel nicht mehr beim Benutzer und auch die Software und Algorithmen, die Identifikation und Signatur erlauben / erstellen, sind vollständig unter der Kontrolle von Dritten. Das heisst, dass bei jeder Identifikation und Signatur Dritte auf einem dem Ausstellungsvorgang gleichwertigem Vertrauens-Niveau tätig sein müssen. Auch ist allfällig inkorrekte Tätigkeit dieser Dritten für den Endbenutzer erheblich schwieriger nachzuweisen.

Die Schweiz kann sich glücklich schätzen, dass in den letzten Jahrzehnten die rechtsstaatlichen und demokratischen Institutionen nie offensichtlich ernsthaft in

Bedrängnis geraten sind (mutmasslich auch nicht durch das organisierte Verbrechen) und daher die Vorteile bezüglich Kosten und Benutzerfreundlichkeit eines «Cloud»-basierten Ansatzes voll zum Tragen gekommen wären. Ausserhalb von Kern-Europa würde die Beurteilung gerade in den letzten Jahren und Monaten für verschiedene Regionen leider anders ausfallen – dort können sich die Bürger glücklich schätzen, wenn eine Ausstellung am Tag X ohne illegitime Einflussnahme «geklappt» hat und danach die Einflussmöglichkeiten auf die tägliche Anwendung durch Dritte erheblich kleiner als im Cloud-Ansatz sind, auch wenn dies zu einem Mehrfachen an Support-Aufwand führt.

Wichtig ist daher für die Ausführungsgesetzgebung, dass es für das Sicherheitsniveau «hoch» immer auch eine technische Umsetzungsvariante geben muss, bei der die «Private Keys» (oder deren Äquivalent) sich physisch im Kontrollbereich des Nutzers befinden – ebenso wie die Algorithmen/Software von deren Anwendung.
Ein Anspruch des Bürgers auf eine solchermassen ausgestaltete E-ID des Niveaus «hoch» muss Eingang in das Gesetz finden - z.B. in einem Absatz 1a) von Artikel 13 (Subsidiäres E-ID-System des Bundes).

Ralf Hauser, 8032 Zürich

P.S.: Die angestrebte «Aufgabenteilung zwischen Staat und Markt» begrüsse ich ausdrücklich!

HÄUSLER
STEFAN, lic.iur,
Fürsprecher

Stampachgasse 51
3065 Bolligen
Tel: 031 921 00 46
haeusler@caminando.ch

Eidgenössisches Justiz- und Polizeidepartement EJPD
copiur@bj.admin.ch

Bolligen, 20. Mai 2017

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

Sehr geehrte Frau Bundesrätin,
Sehr geehrte Damen und Herren

Bekanntlich läuft zurzeit ein Vernehmlassungsverfahren zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz). Nachdem ich mich bis vor rund einem Jahr in meiner Funktion als Grundbuchinspektor des Kantons Bern mit zahlreichen e-Government Projekten auseinandersetzte – insbesondere mit der Einführung des elektronischen Geschäftsverkehrs – masse ich mir in diesem Bereich eine gewisse Fachkompetenz an und erlaube mir, als Privatperson eine Stellungnahme abzugeben.

Ich möchte dabei jedoch nicht auf die einzelne Bestimmungen und Details eingehen, sondern mich im Folgenden auf einige wichtige Grundsätze und Prinzipien beschränken.

1. Es ist zu begrüssen, dass der Bundesrat mit dem vorliegenden Gesetzesentwurf eine formelle Regelung über die elektronischen Identitäten anstrebt. Die Entwicklungen im technischen Bereich und die zahlreichen Projekte von staatlichen Stellen im Bereich e-Government als auch von privaten Dienstleistungsanbietern im Bereich der online-Kundenbetreuung (Banken, Versicherungen, etc.) verlangen klare Voraussetzungen für die Identifizierung von Personen auf dem digitalen Weg. Die letzten Jahre waren diesbezüglich von Rechtsunsicherheit und Rechtunklarheit geprägt und die geltenden Grundlagen waren lediglich Personen verständlich, die sowohl technisch als auch juristisch versiert sind. Für strategische Entscheide verantwortliche Führungskräfte, für Sachbearbeiter in öffentlichen Verwaltungen oder bei privaten Dienstleistungsanbietern geschweige denn für Private ist unklar, was gilt und wie mit diesem Thema umgegangen werden soll.

2. Presseberichten zum E-ID-Gesetz zufolge soll die von Post und SBB angestrebte E-ID (SwissID) für den Bürger kostenlos sein. Dies ist zu begrüssen. Wenn die Bürger zur Verwendung der E-ID motiviert werden sollen, darf dies für den Einzelnen keine Kosten generieren. Werden für das Ausstellen oder Verwenden der E-ID Gebühren verlangt,

wird die Bereitschaft seitens der Bürger massiv reduziert sein. Wie erwähnt konnte dieser Grundsatz Presseberichten entnommen werden. In den Vernehmlassungsunterlagen lassen sich zu dieser Frage jedoch keine Hinweise finden. Der Die Kosten- und Gebührenfrage ist somit unbedingt im Gesetz zu verankern. Unter welchen Voraussetzungen allenfalls Gebühren verlangt werden könnten, ist unten unter Ziffer 4.b erläutert.

3. Die Bestätigung einer Identität einer Person ist grundsätzlich eine hoheitliche Aufgabe, welche durch die zuständige staatliche Stelle vorzunehmen ist und nicht delegiert werden kann. Angesichts der Bedeutung einer Identitätsbescheinigung werden denn auch zu Recht hohe (Sicherheits-)Anforderungen an das Ausstellen einer Identitätskarte und eines Passes gestellt.

4. Dieser Grundsatz muss unbedingt auch auf das Ausstellen einer elektronischen Identität angewandt werden. Wenn diese Aufgaben an nicht-staatliche Anerkennungsstellen (Identity Provider; IdP) übertragen werden, wird von diesem wichtigen Grundsatz abgewichen. Davon ist jedoch aus folgenden Gründen abzusehen:
    a. Der Erfolg einer digitalen Identität und deren Verbreitung hängt massgeblich von deren Akzeptanz in der Bevölkerung ab. Die Bevölkerung ist es sich gewohnt, dass offizielle Bestätigungen, speziell im Bereich der Identität und der Bescheinigung persönlicher Daten von staatlicher Seite erfolgen. Sind dafür plötzlich im Bereich der digitalen Welt private IdP zuständig, entsteht ein grosses Misstrauen. Der Umstand, dass es dann sogar mehrere IdP gibt, die auf dem Markt auftreten und die in einer Art Wettbewerb stehen, wird die Bürger zusätzlich verunsichern. Die durchschnittliche Bevölkerung wird nicht in der Lage sein zu verstehen, dass von privaten IdP ausgestellte elektronische Identitäten eine gleichwertige Stellung haben, wie die durch die öffentliche Verwaltung ausgestellten Identitätsdokumente (Identitätskarte / Pass). Das Ziel, im Bereich der digitalen Identität Rechtklarheit und –sicherheit zu schaffen, kann dadurch nicht erreicht werden – zumindest nicht auf dem angestrebten Niveau.
    Der Umstand, dass die Post und die SBB mit ihrem Produkt SwissID bereits vorgeprescht sind, darf kein Grund sein, das Ausstellen einer digitalen Identität ausschliesslich staatlichen Stellen zuzuweisen. Wenn Private antizipierend ohne entsprechende gesetzliche Grundlage im Hinblick auf ein mögliches künftiges Geschäftsfeld agieren, tun sie dies auf eigenes Risiko. Ein „fait accompli“ darf keine Rechtfertigung dafür sein, eine gesetzliche Regelung doch anders als ursprünglich geplant zu erlassen. Dass es sich bei Post und SBB um öffentliche rechtliche Körperschaften des Bundes handelt, ändert an diesem Umstand nichts.

    b. Für den Bürger ist nicht verständlich und nachvollziehbar, wenn er sich für das Erlangen herkömmlicher Identitätsdokumente (Identitätskarte, Pass) an eine staatliche Stelle wenden muss, für das Erlagen einer digitale Identität hingegen an einen privaten IdP. Es wäre für den Bürger wesentlich einfacher, wenn er die digitale Identität nicht nur von der gleichen Stelle wie die Identitätskarte oder den Pass (kantonale Passbüros, Personenstandsämter, Ausweiszentren, etc.) zugeteilt erhielte, sondern die E-ID sogar im gleichen Prozess ausgestellt werden könnte, wie die Identitätskarte oder den Pass. Nebst der Einfachheit hätte diese

Lösung auch den Effekt, dass die digitale Identität eine sehr hohe Akzeptanz erhielte.
Hinzu kommt, dass die für Pass und Identitätskarte zuständigen kantonalen Ämter und Dienststellen schon über eine sehr gute Infrastruktur verfügen, um das Publikum zu empfangen und deren Identität zu überprüfen. Zur Ausstellung einer E-ID müssen sie lediglich noch mit den entsprechend notwendigen Zusatzprogrammen ausgerüstet werden. Damit sind keine Investitionen in die Infrastruktur notwendig. Auch die personellen Ressourcen müssen – wenn überhaupt – vermutlich nur gering erhöht werden.
Sollte der obenerwähnte Grundsatz der Gebührenfreiheit nicht eingehalten werden können, hätte diese Lösung den Vorteil, dass für eine von staatlicher Stelle ausgegebene Identität eher Bereitschaft besteht, die Kosten für die Ausstellung der E-ID zu tragen. Schliesslich müssen die Bürger heute für das Ausstellen einer herkömmlichen Identitätskarte ebenfalls Gebühren entrichten. Wenn diese Gebühr bescheiden angehoben und dafür auch eine elektronische Identität erhältlich wäre, hätte dies keinen Einfluss auf Akzeptanz und Verbreitung der E-ID.

c. Es ist unerlässlich, dass jede Person von ihrer Geburt bis zu ihrem Tod nur über eine einzige digitale Identität verfügt, so wie es zum Beispiel auch mit guten Gründen bei der Sozialversicherungsnummer (AHVN13) der Fall ist. Ansonsten wird es zu einem heillosen Durcheinander kommen, wenn eine Person plötzlich über mehrere Identitäten verfügt. Dieser Effekt wäre schliesslich wieder ein Umstand, der zu unerwünschter Rechtsunsicherheit führt, weil bei Auftauchen mehrerer Identitäten nicht klar wäre, ob es sich nun um die gleiche Person handelt oder nicht. Das Einhalten dieser Prämisse muss mit dem beabsichtigen Gesetz zwingend gewährleistet sein.

d. Wenn mehrere IdP auf dem Markt auftreten können, kann nicht sichergestellt werden, dass eine Person nur über eine digitale Identität verfügt. Herrscht unter den IdP ein Wettbewerb, werden die Bürger auch die Möglichkeit haben müssen, den IdP wechseln zu können. Die Anforderung, wonach jede Person nur über eine einzige digitale Identität verfügen darf, kann jedoch nicht gewährleistet werden, wenn mehrere Anbieter bestehen. Nur mit einer staatlichen Stelle, welche auch mit einer Clearingstelle zu versehen ist, kann diese Prämisse eingehalten werden.

e. Es wird vermutlich unumgänglich sein, dem Bürger in irgendeiner Form die E-ID auszuhändigen. Den Vernehmlassungsunterlagen lässt sich jedoch nicht entnehmen, ob dies in Form eines Hardwaretokens (USB-Stick oder Chipkarte) oder aber softwaremässig (z.B. über eine mobile Applikation oder serverbasiert) erfolgen soll. Diese Frage sollte zwingend gesetzlich geregelt werden, damit es bei der Umsetzung des E-ID Gesetzes keine Diskussionen geben wird.
Sollte die E-ID auch in Form eines Hardwaretokens abgegeben werden, so ist zwingend zu prüfen, ob das entsprechende Zertifikat nicht in den Chip auf der offiziellen Identitätskarte integriert werden kann. Aus Sicht des Bürgers wäre es sehr praktisch und von hoher Akzeptanz, wenn die Identitätskarten sowohl im

herkömmlichen Sinn als auch im elektronischen Rechtsverkehr eingesetzt werden können.

f. Ich bin zudem davon überzeugt, dass die Implementierung der digitalen Identität in die bestehenden Register (Infostar, etc.) einfach und günstig zu realisieren wäre. Diese Register werden schon heute durch die für die Identitätsausstellung zuständigen Stellen verwendet und erhielten entsprechend lediglich zusätzliche Funktionalitäten. Die Prozesse könnten einfach ergänzt und die notwendigen Funktionalitäten einfach implementiert werden. Dies wäre nicht nur einfacher, sondern auch eine viel günstigere Lösung. Dagegen sind die in der Botschaft zum E-ID-Gesetz skizzierten Prozesse und technischen Lösungsmöglichkeiten (S. 7) kompliziert und dadurch kostenintensiv und unübersichtlich. Es ist auch aus diesem Grund ein einziges Register (z.B. Infostar) anzustreben, in welchem nebst den herkömmlichen Daten einer Person auch deren elektronische Identität geführt werden kann. Das wäre günstiger und einfacher. Zudem wären die Verantwortlichkeiten viel klarer geregelt als bei der vorgeschlagenen Lösung.

5. Den Überlegungen zum Datenschutz kann leider nicht gefolgt werden. Dies aus folgenden Gründen
   a. Die vorgeschlagene Lösung versucht, einen vermeintlich hohen Datenschutz zu generieren. Aber gerade bei der Auslagerung der Ausstellung der digitalen Identität an IdP wird hier unnötig ein zusätzliches Risiko eingegangen. Das Vertrauen des Bürgers in den Staat ist denn diesbezüglich auch höher, als bei privaten IdP.

   b. In allen Diskussionen betreffend Digitalisierung und Datenschutz wird es als unerschütterlicher Grundsatz angesehen, dass personenbezogene Daten auf keinen Fall miteinander verknüpft werden sollen und dürfen. Schon nur die hypothetische Möglichkeit zur Verknüpfung von Daten kann zur Verhinderung einer innovativen Idee führen. Dieser Angstmacherei führt zu einer Verhinderung des Fortschrittes und lässt die Schweiz im internationalen Vergleich auch künftig nur hinterherhinken. Es ist höchste Zeit, gewisse Grundsätze des Datenschutzes ernsthaft in Frage zu stellen. Die eindeutige Zuordnung von Personen (Subjekten) zu unzähligen Objekten (dingliche und obligatorische Rechte, Eigenschaften) wird immer wichtiger. Dies haben die Diskussionen um die Personenidentität beim automatischen Informationsaustausch (AIA) oder aber der ZGB Revision im Zusammenhang mit der eindeutigen Identifikation von Personen in den elektronischen Grundbuch-Systemen gezeigt. Es kann doch nicht sein, dass für jedes neue Gebiet, in welchen Personendaten elektronisch verarbeitet werden, dieselben Diskussionen geführt werden müssen und die Forderung nach einem neuen unabhängigen Identifikator für natürliche Personen gestellt wird. Leider fehlt es zurzeit an einer modernen Strategie bezüglich Personenidentifikation und –identität (inkl. den elektronischen Signaturen). Diese Bereiche gehören meines Erachtens untrennbar zueinander und sollten im heutigen Umfeld des Web 3.0, der industriellen Revolution 4.0, Big Data, Open Government Data, Internet of Things, Blockchains etc. neu diskutiert werden. Die heute geltenden Regelungen des Datenschutzes und deren sehr restriktive Interpretation verhindern nicht nur die Innovation, sondern erweisen sich je länger je mehr als unzeitgemäss. Die

Bevölkerung ist sich den Umgang mit digitalen Elementen je länger je mehr gewohnt und insbesondere die jüngere Generation hat weniger Berührungsängste. Angesichts des verhältnismässig doch grossen Vertrauens in die staatlichen Stellen ist es nun höchste Zeit zu diskutieren, ob nicht ein einziges System sämtliche Personendaten der Schweiz verwalten soll, in welchem einer Person verschiedene Teilnummern für verschiedene Anwendungsfälle (Gesundheitswesen, Versicherungs-/Bankenwesen, privater Einsatz). Das wäre nicht nur günstiger sondern auch effizienter. Statt sich auf anachronistische Datenschutzbestimmungen zu stützen, sollte zum Schutz der Daten der Fokus vielmehr auf die IT-Security und deren Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität gelegt werden. Die Diskussion, was heute unter einem zeitgemässen Datenschutz zu verstehen ist, muss zwingend geführt werden. Mit der Schaffung des E-ID-Gesetzes besteht dazu eine einmalige Gelegenheit, da in diesem Rahmen auch allfällige Änderungen am Datenschutzgesetz (DSG) möglich wären.

Zusammenfassend möchte ich festhalten, dass das Ausstellen einer digitalen Identität zwingend als staatliche Aufgabe zu verstehen ist, die nicht ausgelagert werden darf. Es handelt sich nicht nur um die ureigene Aufgabe einer staatlichen Stelle sondern ist auch aus Gründen der Akzeptanz, der Effizienz und schliesslich auch – bei der Implementation der notwendigen Funktionalitäten in bestehende Register – und der Wirtschaftlichkeit die beste Lösung. Die Synergien, welche bei der gleichzeitigen Ausstellung von herkömmlichen Identitätsdokumenten mit der digitalen Identität entstehen, führen nur zu einem geringen Mehraufwand bei der öffentlichen Verwaltung. Allenfalls muss zur Erweiterung der bestehenden Systeme eine höhere Investition getätigt werden, als bei der Übertragung an IdP. Hingegen dürfte der technische und organisatorische Betrieb wesentlich günstiger sein, da es weniger technische und organisatorische Schnittstellen gibt und keine Investitionen in die Infrastrukturen getätigt werden müssen.
Und schliesslich sind auch die unzeitgemässen Prämissen des Datenschutzes grundsätzlich zu überdenken. Es ist höchste Zeit, ein einziges zentrales Personenregister zu führen, in welchem die Identität einer Person und deren Identifikatoren für verschieden Teil- oder Rechtsgebiete inklusive deren elektronische Signaturen verwaltet werden können.

Ich ersuche Sie um Kenntnisnahme und verbleibe mit freundlichen Grüssen

Mit freundlichen Grüssen

lic.iur. Stefan Häusler, Fürsprecher
(leider ohne rechtsgültige digitale Signatur)