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