



## Beilage c - VERTRAULICH

# Auswertung der Ämterkonsultation zu einem neuen Bundesgesetz über die staatlichen elektronischen Identifikationsmittel "eID-Gesetz"

Übersicht zu den eingereichten Stellungnahmen

Bern, 24. Juli 2014

**In der Ämterkonsultation wurden folgende Dienststellen begrüßt:**

- BK (Sektion Recht, Verwaltungsinterne Redaktionskommission, EDÖB)
- GS EDA
- EDI (GS, BSV)
- GS VBS
- EFD (GS, ISB, EFV, EPA, BBL, BIT, FINMA)
- WBF (GS, SECO, BfK, KTI)
- UVEK (GS, BAKOM).

**Liste der eingegangenen Stellungnahmen**

- BK (Sektion Recht, Verwaltungsinterne Redaktionskommission, EDÖB)
- EDA
- EDI (BAG, BFS, BSV)
- EJPD (GS, BJ, fedpol, BFM)
- VBS (NDB)
- EFD (ISB, EFV, EPA, BBL, BIT, FINMA)
- WBF (GS, KTI)
- UVEK (BAKOM)

**Keine Bemerkungen zu den Unterlagen der Ämterkonsultation**

- BFS
- GS-WBF (nach Rücksprache mit seco)
- KTI

Allgemeine Bemerkungen	Absender EDÖB	Notizen
<p>Le projet de loi eID et le rapport explicatif ne sont pas suffisamment détaillés sur certains points:</p> <ul style="list-style-type: none"> <li>• Seulement les données contenues dans l'eID sont clairement mentionnées. Les autres données contenues dans le système d'information sur les eID et dans le registre des certificats ne sont pas mentionnées.</li> <li>• Le projet de loi eID et le rapport explicatif ne donne aucune indication quant aux éventuels accès aux fichiers susmentionnés.</li> <li>• Le rapport explicatif ne précise malheureusement au point 1.3 comment le code contenu dans l'eID permet la création d'un pseudonyme différent pour chaque service utilisé. On ne sait en particulier pas où ces pseudonymes seront stockés (IDK, eID-Informationssystem, eID-Server) ? En outre, s'agit-il bien du même code lorsque le rapport parle de saisie d'un nombre secret (NIP) et du même pseudonyme quand il évoque une personne enregistrée sous un nom d'utilisateur ?</li> <li>L'utilisation du numéro AVS en tant qu'identificateur universel de personnes dans toute l'administration et en dehors (dans le secteur privé comme cela est prévu dans le projet de loi eID) présente des risques considérables pour la protection de la personnalité en raison du fait que l'on renonce ainsi à empêcher tout appariement non autorisé de données par des moyens techniques. Nous plaçons en faveur de l'utilisation d'un identificateur sectoriel de personnes. Ce procédé a déjà été transposé avec succès dans la loi fédérale sur le dossier électronique du patient (LDEIP).</li> <li>Cette voie est également ouverte à tous les autres cas requérant une identification de personnes de manière univoque sans lourde charge administrative et financière supplémentaire.</li> <li>=&gt; <u>Stellungnahme EDÖB</u>, siehe auch hinten bei den allgemeinen Bemerkungen zum Gesetzesentwurf und zu den Erläuterungen.</li> </ul>	<p>EDA</p>	
<p>Wir sind grundsätzlich mit dem Geschäft einverstanden, haben jedoch folgende Bemerkungen zum Bundesratsantrag (siehe unten).</p> <p>Besten Dank dass wir am Vernehmlassungsverfahren teilnehmen dürfen. Wir senden Ihnen gerne unsere, aus den Direktionsbereichen gesammelten, Hinweise. Es handelt sich dabei nicht um konkrete Anpassungsbegehren, sondern die nachfolgenden Informationen sollen dem EJPD vor allem die Schnittstellen zu Themen das BAG aufzeigen:</p> <p>1) Gemäss Registerverordnungen MedBG (SR 811.117.3) soll die AHV-Nummer systematisch verwendet werden (vgl. Art. 4 Bst. e der Registerverordnung MedBG). Die gesetzliche Grundlage wird mit der laufenden Revision des Medizinalberufgesetzes (SR 811) geschaffen (vgl. neuer Art.</p>	<p>BAG</p>	

<p>51 Abs. 4bis MedBG, BBl 2013 6225). Zudem fragen wir uns, ob die Registerverordnung MedBG angepasst werden müsste, wenn das eID-Gesetz in der vorliegenden Form in Kraft treten wird. In der Registerverordnung MedBG wir nämlich von Personen, die Einsicht in ihre Registerdaten wollen, verlangt, dass sie Benutzernamen und Passwort beantragen müssten, wenn neu die Personen elektronisch mit der eID oder auch HPC Benutzernamen und Passwort bestellen würden? Im BAG ist zudem - analog zur Registerverordnung MedBG - eine Verordnung zum Psychologieberuferegister in Arbeit. Sie wird voraussichtlich im Herbst 2014 in die Ämterkonsultation geschickt werden.</p>		
<p>2) Die AHN13 ist Teil der eID (Art. 3 Abs. 1 Bst. j). Wenn die eID als Identifikationsmittel gemäss dem Bundesgesetz über das elektronische Patientendossier (EPDG, vom Ständerat in der Sommersession verabschiedet, voraussichtliches Inkrafttreten 1.1.2017) eingesetzt werden soll, gilt es genau abzuklären, wer welche Nummer (AHVN13 und Patientenidentifikationsnummer) für was gebrauchen darf. Für die Identifikation im Rahmen des EPDG wurde die Verwendung der AHN13 explizit verworfen (Botschaft zum EPDG, S. 5359 f. und 5378 ff.), stattdessen kommt eine neu zu vergebende Patientenidentifikationsnummer zum Einsatz. Daher darf die AHN13 nicht via eID als Identifikator verwendet werden. Technisch sollte es daher machbar sein, dass die AHN13 im Rahmen des EPDG nicht ausgelesen werden kann (ausser in den Ausnahmefällen nach Art. 5 Abs. 2 EPDG). Damit stellt sich die Anschlussfrage, ob allenfalls die Patientenidentifikationsnummer ein (freiwilliges) Attribut der eID sein soll. Ein Nebeneinander der beiden Nummern resp. Trägermedien ist wohl unvermeidbar, da die Patientenidentifikationsnummer nur bei Eröffnung eines elektronischen Patientendossiers gemäss EPDG vergeben wird und der Bezug der eID freiwillig ist.</p>		
<p>3) In den Registern (z.B. MedReg) wird weiterhin der Heimatort als identifizierendes Merkmal geführt, auf der eID wird dieses Merkmal durch den Geburtsort ersetzt. Falls diese Register geändert werden müssen ist mit relativ hohen Informatikkosten zu rechnen. Wir möchten Anregen, dass im Projektbudget für allfällige Datenbankumstellungen ein Budgetposten reserviert wird, welcher den Ämtern (BAG) bei einer allfälligen Umstellung zur Verfügung gestellt werden kann.</p>		BSV
<p>Dans le cadre de la présente consultation des offices, l'OFAS prend position quant aux intérêts des assurances sociales et plus particulièrement quant à la question de l'utilisation du numéro AVS et aux risques en terme d'atteinte à la protection de la personnalité qui y sont liés. A cet égard,</p>		



<p>l'OFAS se permet de rappeler que le numéro d'assuré AVS a été conçu comme un numéro de sécurité sociale, qui doit servir en premier lieu la mise en œuvre des assurances sociales, sans qu'il en soit fait une utilisation abusive. Dans la modification de la LAVS du 23 juin 2006 relative au nouveau numéro d'assuré AVS (RO 2007 5259 et message FF 2005 515), les bases légales concernant, d'une part, l'utilisation systématique du numéro AVS comme numéro de sécurité sociale, et, d'autre part, l'utilisation systématique du numéro AVS dans d'autres domaines, ont été créées (art.50d et 50e LAVS). Des mesures de précaution relatives à l'utilisation du numéro AVS ont par ailleurs été clairement définies (art. 50g LAVS), dans l'optique éventuelle que le numéro d'assuré se développe pour devenir un numéro <i>administratif</i> d'identification de personne utilisé exclusivement par la Confédération, les cantons et les communes, étant entendu que ce développement resterait soumis à un contrôle démocratique.</p>		
<p>Le Conseil fédéral dans sa réponse à l'interpellation du Groupe BD 13.3492 s'est montré d'avis que l'utilisation systématique du numéro AVS en tant qu'identificateur universel dans un contexte de cyberadministration devait faire l'objet d'un examen approfondi. Un groupe de travail inter-départemental de la Confédération (« universell einsetzbarer behördlicher Personenidentifikator ») a été constitué, dans lequel l'OFJ est dûment représenté. L'OFAS s'oppose par conséquent à l'actuelle présentation d'un avant-projet autorisant de fait la transmission du numéro AVS, sans base légale formelle, non seulement entre organes de l'Etat, mais aussi potentiellement en ce qui concerne <i>tout le domaine privé</i>, ceci sans analyse approfondie. Comme le Préposé à la protection des données, l'OFAS juge en effet que l'utilisation du numéro AVS en tant qu'identificateur <i>universel</i> de personnes présente des risques considérables défavorables à la protection de la personnalité en raison du fait que l'on ne pourrait pas empêcher des appariements non autorisés de données par des moyens techniques. Des données personnelles sensibles pourraient ainsi devenir accessibles par simples recoupements. N'importe quelle entreprise privée serait en mesure d'utiliser le numéro AVS sans que le respect des mesures de protection exigées à juste titre par l'art. 50g LAVS puisse être imposé.</p>		
<p>Danke für die Unterlagen, die m.E. gut abgefasst und für das Vernehmlassungsverfahren geeignet sind. Ich frage mich unter Vorbehalt, dass ich etwas übersehen haben sollte, ob es sich nicht lohnen würde, im Bundesratsantrag und in den Erläuterungen zum Vorentwurf ausdrücklich</p>	<p>GS-EJPD</p>	

<p>hervorzuheben, dass es sich bei der eID um ein wichtiges Element für eine erfolgreiche Umsetzung der vom Bundesrat beschlossenen Informationsgesellschaftsstrategien handelt (Informationsgesellschaft Schweiz; E-Government; E-Commerce; E-Health; Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken), indem namentlich die Sicherheit und das Vertrauen gefördert würden. Auch ein Hinweis auf den Nutzen zur Umsetzung der parlamentarisch-wirtschaftlichen Initiative „ePower für die Schweiz“ dürfte sich m.E. durchaus empfehlen. Zudem bitte ich Euch die Bemerkungen aus dem ISC-EJPD zum Thema „Sicherheit und Benutzung“ näher zu prüfen und zu berücksichtigen (siehe Bemerkungen BRA).</p>	
<p>Wir danken Ihnen für die Gelegenheit zur Stellungnahme zum Entwurf des eID-Gesetzes. Dieser hat uns wie auch die Verwaltungsinterne Redaktionskommission (VIRK) vor zahlreiche Fragen gestellt. Zudem erscheint uns die Struktur des Gesetzesentwurfs noch nicht überzeugend (vgl. die einleitenden Bemerkungen in der Stellungnahme der VIRK). Wir bezweifeln, ob der Entwurf in der aktuellen Konsultationsrunde vernehmlassungsreif werden kann und bitten Sie daher, vor der Eröffnung der Vernehmlassung eine zusätzliche Konsultationsrunde durchzuführen. Selbstverständlich sollten zuerst die vorliegende und in der Stellungnahme der VIRK aufgeworfenen Fragen und Vorschläge diskutiert und verarbeitet werden.</p>	<p>BJ, RS II</p>
<p>a. <i>Liste der möglichen Trägersweise?</i> Der Entwurf regelt nicht, welche Ausweise mit der eID versehen werden können, und delegiert diese Regelung auch nicht z.B. an den Bundesrat. Die Regelung kann aber nicht vernünftig angewendet werden (und ihre rechtliche und logische Kohärenz kann nicht geprüft werden), wenn nicht bekannt ist, welche Trägersweise das Gesetz zulassen soll.</p> <p>b. <i>Verwendungszweck der eID regeln? / Systematische Änderung anderer Erlasse</i> Der Entwurf regelt den Verwendungszweck der eID und insbesondere der in ihr gespeicherten AHV-Nummer nicht; ebenso bleiben die Rechtswirkungen ihres Einsatzes ungeklärt. Der Gesetzgeber soll die eID offenbar einmal kreieren und abwarten, zu was sie sich gewissermassen organisch entwickelt. Wir haben Zweifel, ob dieses Regelungskonzept funktionieren kann. Man vergleiche Artikel 1 Absatz 2 AwG, wonach der Pass und die Identitätskarte der Inhaberin oder dem Inhaber zum Nachweis der Schweizer Staatsangehörigkeit und der eigenen Identität dienen. Daraus, dass im Anhang des Entwurfs einige Gesetze so geändert werden, dass die eID in verschiedenen Situationen explizit als Identitätsnachweis akzeptiert werden muss, kann man wohl</p>	

schliessen, dass die allgemeine Zweckbestimmung der Trägersweise gemäss AwG (und damit die rechtliche Wirkung ihres Einsatzes) auf die eID offenbar nicht anwendbar ist. Auch die Erläuterungen stellen nicht klar, ob unter der Rubrik *Änderung anderer Erlasse* systematisch alle Bundesgesetze geändert werden, die heute die Identifikation mit einem traditionellen Ausweispapier vorsehen.

**c. Verhältnis zu AwG und AuG**

Sollte man nicht die geltenden Bestimmungen zu den Datenchips (ePass), die ja ohnehin parallel in AwG und AuG stehen, ins neue Gesetz integrieren? Es dürfte schwer vermittelbar sein, warum die eine elektronische Zusatzfunktion der Ausweise in AwG und AuG parallel geregelt wird und die andere im separaten eID-Gesetz.

**d. Verhältnis zu ZertES und SuisseID; Signatur- und Verschlüsselungsfunktion?**

Wir können den Erläuterungen keine überzeugende Begründung entnehmen, warum über die bereits bestehenden Regelungen und Aktivitäten in den Bereichen ZertES und SuisseID nun noch eine dritte, in der Umsetzung anspruchsvolle Ebene geschichtet werden soll. Läge es nicht nahe, die auf der eID zwangsläufig vorhandene Technik und den hohen rechtlichen, finanziellen und organisatorischen Aufwand nicht nur für die Authentifizierung, sondern auch für das Verschlüsseln und das Signieren von Dokumenten nutzbar zu machen?

**Insbesondere Datenschutz**

**a) Grundsätzliche Einschätzung der Sensibilität der bearbeiteten Daten**

Mit der AHV-Nummer soll eine Information in der eID enthalten sein, die unabhängig von der Definition der besonders schützenswerten Personendaten (Art. 3 Bst. c DSG) auf jeden Fall besondere Aufmerksamkeit verdient. Ihr systematischer Einsatz in breiten Bereichen erleichtert das Verknüpfen von Daten aus verschiedenen Quellen und damit das Anlegen von Persönlichkeitsprofilen (Art. 3 Bst. d DSG). Angesichts dessen scheinen uns sowohl der Gesetzesentwurf als auch die Erläuterungen zu wenig Gewicht auf den Schutz der aus der eID auslesbaren Daten zu legen.

**b) Verhältnis zwischen den Pflichten der eID-Inhaber und der vertrauenden Beteiligten**

Il existe un déséquilibre important entre les obligations du titulaire de eID et la partie utilisatrice (comparer art. 6 et art. 16 du projet). Cette dernière n'a pas d'obligation de préserver la sécurité des traitements de données qu'elle effectue alors qu'elle est responsable de ces traitements. Elle



<p>n'a pas non plus l'obligation de prendre des mesures pour évaluer les risques et mettre en oeuvre un niveau de sécurité adéquat. Or, comme le mentionne le ch. 67 du préambule de la proposition de règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final:</p> <p>«Une violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer une grave perte économique et des dommages sociaux importants, y compris une usurpation d'identité, à la personne physique concernée».</p> <p>Il s'agirait d'approfondir cette question et d'équilibrer les droits et les obligations des protagonistes ainsi que d'anticiper les conséquences d'une violation de la sécurité des données voire d'une usurpation d'identité. Dabei ist zu berücksichtigen, dass die vertrauenden Beteiligten in den meisten Anwendungsszenarien den grössten Teil der nötigen Informatikinfrastruktur kontrollieren, während die eID-Inhaber als einfache Nutzer selten einen grossen Einfluss haben werden.</p> <p>c) <u>Durchsetzung: Rechtsfolgen von Pflichtverletzungen (insb.: Strafbestimmungen?)</u></p> <p>Les questions de responsabilité sont abordées de manière lacunaire à notre avis, uniquement dans le cas d'une violation du devoir de diligence du titulaire de l'eID (voir les remarques concernant le commentaire ad art. 6 qui se limite aux obligations résultant d'actes illicites au sens de l'art. 41 du Code des obligations).</p> <p>Wie zu Artikel 16 angemerkt, überrascht die Abwesenheit von gesetzlichen Rechtsfolgen von Pflichtverletzungen der vertrauenden Beteiligten, seien sie Private oder Behörden.</p> <p>Zu prüfen und in den Erläuterungen zu diskutieren ist insbesondere, ob Strafbestimmungen neu geschaffen oder angepasst werden müssen (dazu StR-StPR einbeziehen).</p>		
<p>Danke für die Möglichkeit zur Stellungnahme in diesem spannenden Geschäft. Wir haben ja regen Kontakt in dieser Sache und sind natürlich im Grundsatz mit der Vorlage einverstanden. Dennoch möchte ich es nicht versäumen, seitens fedpol / Projekt eine offizielle Stellungnahme abzugeben.</p> <p>In den letzten Tagen haben wir von verschiedener Seite, unter anderem von einer Person, welche bei der Implementierung der deutschen eID (nPA) eng mitgearbeitet hat, sowie einer Stelle im Umfeld der SuisseID, deutliche Hinweise auf Implementierungsrisiken bei der geplanten eID bekommen. Diese wichtigen Hinweise betreffen hauptsächlich zwei Bereiche, welche unbedingt noch vor der kommenden Vernehmlassung genau abgeklärt werden müssen:</p> <p><u>Usability:</u> Es wurde bestätigt, dass die angedachte Funktionalität unserer eID eindeutig in die</p>	fedpol	



<p>richtige Richtung geht. So sind „Einfachfunktionen ohne Pin“ und „Verifikation von Attributen“ unbedingt empfehlenswert. Offen ist aber erneut die Frage, ob vor dem Hintergrund „Snowden“ nicht doch auch eine Verschlüsselungsfunktion auf der eID sein sollte. Als sehr empfehlenswert wurde uns genannt, parallel zum Produkt eID auch eine konkrete und für die Kunden attraktive (unmittelbar nützliche) Anwendung zu lancieren. Es wäre also u.U. sinnvoll, gleich mit dem eID-Gesetz eine solche Anwendung vorzusehen und nicht nur auf separate Anträge zu verweisen, welche dann irgendwann kommen. In Deutschland gibt es heute rund 100 Anbieter von Dienstleistungen, welche die eID (nPA) nutzen wollen/können. Davon sind rund die Hälfte staatlich und die andere Hälfte schwergewichtig im privaten Versicherungsmarkt angesiedelt.</p> <p><u>Support:</u> Offenbar ist der Aufwand für die Unterstützung und Wartung des eID-Anwender-Clients auf verschiedensten IT-Infrastrukturen der Endkunden ein Albtraum. Wenn wir keine Einschränkungen, zum Beispiel auf NFC-fähige Smartphones, vornehmen und in der Folge klassische PCs, Laptops etc. mit Lesegeräten ausschliessen, dann werden wir grosse Probleme im Feld und enttäuschte Endkunden haben. Das in Deutschland beobachtete Phänomen ist, dass die von Staat herausgegebene Ausweis-App immer nur mit ganz bestimmten und sehr oft veralteten Versionen von Browsern eingesetzt werden kann. Interessanterweise bietet der Staat in Deutschland den Endkunden zusätzlich keinerlei Support für die eID-Funktionalität, was aufgrund der geschilderten Probleme für mich ein absolutes no-go ist und wohl dazu beiträgt, dass nur ein Drittel aller Personen die eID-Funktionalität überhaupt einschalten lassen und davon weniger als 1% die Ausweis-App auch nur herunterladen und installieren. Über die effektive Nutzung habe ich immer noch keine verlässlichen Informationen.</p> <p>Dies gesagt, ergibt sich für uns folgende Konsequenz: wir müssen die Machbarkeit und Risiken einzelner Aspekte in den nächsten rund drei Monaten noch vertieft abklären. Erst danach können wir abschliessend die Kongruenz des eID-Gesetzes mit dem eID-Konzept abstimmen. Ich muss also leider einen gegenüber der aktuellen Planung einen erhöhten Zeitbedarf anmelden.</p>		
<p>Wir möchten dazu aus Sicht des NDB an dieser Stelle nochmals bemerken, dass die neuen Bestimmungen und die technische Ausgestaltung weiterhin eine praktikable Ausstellung von Ausweisdokumenten zum Aufbau und zur Aufrechterhaltung von Tarnidentitäten nach Art. 14 c (vgl. insb. Abs. 6) BWIS ermöglichen sollen.</p>		NDB
<p>Wir sind mit dem Antragsentwurf grundsätzlich einverstanden, haben aber folgende Bemerkungen: Ein kritisches Thema, nicht aus technischer aber sicher aus rechtlicher und politischer Sicht, ist die</p>		ISB

<p>Aufnahme der Sozialversicherungsnummer bzw. AHV-Nummer als Attribut. Dies wird sicherlich zu einer erheblichen politischen Diskussion führen und stellt ein gewisses Risiko dar (Referendum). Eine Alternative wäre der EDÖB-kompatible Weg mit der „sektoriellen ID“; eine andere Möglichkeit wäre es, die AHV-Nummer lediglich als optionales Attribut (nur auf Wunsch des Benutzers) zu definieren. In diesem Zusammenhang wäre auch zu überlegen, ob nicht weitere Attribute ebenso als optional aufgeführt werden könnten, wie z.B. biometrische Daten.</p>		
<p>Wir nehmen einen allfälligen späteren – gegenfinanzierten – Ressourcenbedarf zur Kenntnis und begrüessen es, dass Sie diesen erst beim Vorliegen gesicherter Grundlagen anlässlich der Inkraftsetzung des Gesetzes unterbreiten werden. Den Stellenbedarf bei der Verabschiedung der Botschaft zu beantragen, erachten wir jedoch als noch zu früh, da die Beratungen im Parlament ebenfalls noch Einfluss auf die Umsetzung haben können.</p>	EPA	
<p>Grundsätzlich begrüessen wir den Varianten-Entscheid des EJPD zugunsten einer staatlichen eID. Analog zur IDK als konventionelles Identifikationsmittel, soll das elektronische Identifikationsmittel durch den Staat ausgestellt werden. Gestützt darauf soll die Privatwirtschaft in effizienter Weise eigene Identifikationsmittel sowie Signaturdienste anbieten und damit flexibel auf den Markt und die neuen Technologien reagieren können. Zukünftig sollen zwei IDK-Modelle angeboten werden, eines ohne und eines mit Chip. Der Chip wird die staatliche elektronische Identität und biometrische Daten, vergleichbar mit dem E-Pass, enthalten.</p> <p>Das BBL begrüsst insbesondere die vorgebrachten sicherheitsrelevanten Aspekte, welche im Vordergrund stehen. So soll die staatliche eID die höchste Qualitäts- und Sicherheitsstufe haben, die auch sensitiven Anwendungen wie E-Health und Vote Electronique genügt. Grundsätze: hohe Vertrauenswürdigkeit kommt vor hoher Funktionalität, hoher Flexibilität, tiefen Kosten und einfachster Bedienung. Diesbezüglich wird auf das übergeordnete Ziel hingewiesen, nämlich die Sicherheit und das Vertrauen im elektronischen Geschäftsverkehr herzustellen. In diesem Sinne hat das EFD, BBL, bereits zum Aussprachepapier des EJPD vom Januar 2014 «Einführung einer staatlichen elektronischen Identität (eID) zusammen mit der neuen Identitätskarte. Vorentscheide und weiteres Vorgehen.» Stellung bezogen.</p> <p><b>Sicherheitsansprüche der Schweizer Bürger</b>          Das BBL hat sich ebenfalls bereits im Rahmen des BRB vom 16. Dezember 2011 «Schweizer Pass und Identitätskarte, Entscheide über das weitere Vorgehen» für die Sicherheit im Umgang und</p>	BBL	

dem Transport von biometrischen Personendaten ausgesprochen. Die biometrischen Daten, resp. die elektronische Identität des Schweizer Bürgers, sollen sich von der Erfassung bis zur Personalisierung in staatlicher Obhut befinden (Kantone, Bund). D.h. in einer integrierten End-to-End-Lösung mit der Sicherheit des medienbruchfreien Datentransportes innerhalb des Einflussbereiches der staatlichen Hoheit. Die Akzeptanz für eine eID mit biometrischen Daten wird durch die Gewährleistung der Personalisierung innerhalb hoheitlicher Sicherheitsdispositive nachhaltig gefördert. Wie bei der Personalisierung des Schweizer Passes soll deshalb auch bei der eID mit biometrischen Daten die umfassende Datensicherheit für den Schweizer Bürger gewährleistet werden.

#### **Sicherheitsüberlegungen**

Die Sensibilisierung bezüglich der Datensicherheit ist stark gestiegen. Die Fraktion der CVP-EVP hat am 27. November 2013 die Interpellation «13.4023 – Informatikpläne des Bundes» eingereicht, welche sich mit Sorge über die Ausschreibung einer Auslagerung von Datentransportdiensten äussert. Dabei hat der Bundesrat in seiner Antwort vom 26.02.2014 festgehalten, dass basierend auf den Erkenntnissen zur aktuellen Bedrohungslage und aus Gründen der Staatssicherheit, Betriebsleistungen für besonders kritische und zentrale Infrastrukturen der Bundesverwaltung wo möglich nur an Unternehmen vergeben, welche ausschliesslich unter Schweizer Recht handeln, sich zur Mehrheit in Schweizer Eigentum befinden und ihre Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen. Der Bundesrat hat dies in seinem Beschluss vom 29.01.14 zusammen mit weiteren Massnahmen festgehalten. Aufgrund dessen wurde das VBS (NDS) beauftragt eine Analyse und Einschätzung der Bedrohungslage für die gesamte Leistungserstellung von IKT-Leistungen für die BV vorzunehmen. Das EFD (ISB) wurde beauftragt, zusammen mit den Departementen und der BK gestützt auf die Einschätzung der Bedrohungslage durch den NDB, Grundsätze zur Leistungserstellung der in der Bundesverwaltung eingesetzten IKT-Leistungen zu erarbeiten und dem Bundesrat vorzulegen. Mit diesen neuen Vorgaben wird es im Bereich von sensiblen Personendaten bei öffentlichen Ausschreibungen schwierig geeignete Bewerberinnen und Bewerber zu finden. Ebenfalls hat sich Herr NR L. Stamm in seiner Motion «12.3303 – Zwingende Herstellung der IDK durch die öffentliche Hand» vom 16. März 2012 kritisch mit dieser Thematik auseinandergesetzt. Im Kern der Motion besagt diese, dass die Erstellung von Ausweisen wie Identitätskarten und



Pässe zu den engsten hoheitlichen Aufgaben gehört. Diese dürfen nicht an Dritte ausgelagert werden, wenn dabei die Vertraulichkeit der Daten nicht hundertprozentig sichergestellt wird. Zusammenfassend ist festzuhalten, dass erst bei einer zentralen Personalisierung der eID beim Bund die Förderung eines sicheren elektronischen Geschäftsverkehrs unter Privaten und Behörden bestmöglich gewährleistet ist (vgl. Art. 1 Abs. 2 Bst. a des Vorentwurfes des Bundesgesetzes über die staatlichen elektronischen Identifikationsmittel vom 19. Juni 2014 [VE eID-Gesetz]). Erst dann ist es auch gerechtfertigt, InhaberInnen einer eID Sorgfaltspflichten im Umgang mit dieser aufzuerlegen (vgl. Art. 6 VE eID-Gesetz).

Interessanterweise wird im erläuternden Bericht zum Vorentwurf unter Pkt. 1.5.3 der neue elektronische Personalausweis in Deutschland als gutes Beispiel aufgeführt, welcher die Komplexität in technischer und organisatorischer Hinsicht gemeistert hat. Bereits sind rund 25. Mio. neue Personalausweise ausgegeben worden. Dabei wurde 2008 von der Bundesrepublik Deutschland im Hinblick auf die Wahrung der nationalen sicherheitspolitischen Interessen die sog. Bundesdruckerei nach acht Jahren privatwirtschaftlicher Ausrichtung, wieder in den Besitz des Bundes zurückgeführt. Der Rückwerb dieser Institution schaffte auch eine sicherheitspolitische Voraussetzung zur Vergabe der Herstellung des elektronischen Personalausweises an die Bundesdruckerei, was faktisch einer hoheitlichen Tätigkeit gleichkommt.

#### **Wirtschaftlichkeitsüberlegungen**

Gemäss dem Antrag an den Bundesrat vom 16. Dezember 2011 sollen aus Sicherheitsgründen zwei Standorte beim Bund für die Personalisierung des Schweizer Passes und zwei Standorte in der Privatwirtschaft für die Personalisierung der Identitätskarte eingerichtet werden. Der Schweizer Bürger müsste die Kosten für vier Standorte über die Gebühren für seine Ausweisschriften bezahlen. Wenn die Identitätskarte beim Bund personalisiert wird, reichen zwei Standorte aus. An beiden Standorten können Schweizer Pässe und Identitätskarten mit biometrischen Daten personalisiert werden. Synergien der bestehenden Infrastrukturen, wie Ausrüstungen für den geschützten Datentransport von den Kantonen zum EJPD und ins BBL, Sicherheitsproduktionsräume und -lager, Transportmittel sowie der vorhandenen Personalressourcen mit einschlägigem Know-How, können genutzt werden.

#### **Vorgehensvorschlag des BBL**



<p>Das BBL schlägt deshalb vor, die öffentliche Ausschreibung der eID gleich wie beim Schweizer Pass 2003 auszugestalten. Die Wirtschaft soll die Konzeption, die Ausrüstungen für die Personalisierung und das Material für die Identitätskarte im Wettbewerb anbieten und liefern. Insbesondere können auf diese Weise auch ausländische Lieferantenangebote zugelassen werden. Ein echter Wettbewerb unter den Anbietern wird möglich. Die Personalisierung der eID beim Bund bindet nur ca. 10 bis 20 % der Wertschöpfung. Der überwiegende Teil von ca. 80 bis 90 % wird aber von erfahrenen Firmen aus der Privatwirtschaft mit Innovationskraft bezogen werden. Damit ist sichergestellt, dass diese Firmen in der Forschung und Entwicklung auch weiterhin tätig bleiben.</p> <p>Bereits in seiner Antwort des Bundesrates vom 17.02.2010 auf die Anfrage 09.1180 von Luzi Stamm „Biometrische Pässe. Sicherheit der sensiblen Daten“ hielt der dieser fest, dass <i>gemäss dem geltenden sowie auch dem per 1. März 2010 in Kraft tretenden revidierten Ausweisgesetz (SR 143.1; inklusive revidierter Ausweisverordnung, SR 143.11) die Ausstellung von Ausweisen eine staatliche Aufgabe ist. Diese wird von Bund und Kantonen gemeinsam vollzogen, wobei das EJPD die Herausgeberin der Ausweise ist. Gestützt auf die Bestimmungen des BoeB liegt es somit in der Zuständigkeit des Bundes zu entscheiden, welche Leistungen er mittels einer Ausschreibung bei der Privatindustrie beschaffen will (z. B. Lieferung von Passbestandteilen und Maschinen) und welche Leistungen er selber erbringen will, bzw. im Interesse der öffentlichen Ordnung und Sicherheit selber erbringen muss (namentlich die Produktion von biometrischen Pässen). Gestützt auf diese Kompetenz soll daher, wie oben ausgeführt, die Produktion des biometrischen Schweizer Passes weiterhin beim Bundesamt für Bauten und Logistik in Zusammenarbeit mit der Privatindustrie (PPP) erfolgen. Aufgrund dieser Ausgangslage geht das EFD, BBL, davon aus, dass die künftige eID ebenfalls demselben hoheitlichen Standard verpflichtet sein muss.</i></p>	
<p>Das BIT begrüsst den Entwurf des neuen eID-Gesetzes ausdrücklich und dankt dem BJ für die Gelegenheit Stellung zu nehmen.</p> <p>Wir möchten dem Interesse des BIT Ausdruck verleihen, die operative Rolle als zuständige Stelle für die Herausgabe und Verwaltung der Berechtigungszertifikate wahrzunehmen. Mit der aufgebauten Swiss Government PKI verfügt das BIT über die Kompetenzen einen solchen Dienst zu betreiben und die Funktionalität der künftigen eID-Lösung sicherzustellen. Dabei stimmen wir auch der im Bundesratsantrag vorgeschlagenen Finanzierung der Investitions-, Betriebs- und Personalkosten durch Deckungsbeiträge zu.</p>	<p>BIT</p>

De l'avis de la FINMA, le devoir d'identification fait partie des propositions de mesures les plus importantes pour la mise en œuvre des Recommandations révisées du Groupe d'action financière (GAFI-Standards; voir : <http://www.sif.admin.ch/dokumentation/00509/00510/00622/00624/00868/index.html?lang=de>). Il s'agit notamment de relever dans ce contexte que la note interprétative de la recommandation 10 du GAFI décrit les relations d'affaires sans présence physique des parties comme impliquant des risques plus élevés. Nous nous permettons en outre d'attirer votre attention sur la recommandation 15 du GAFI selon laquelle « Les pays et les institutions financières devraient identifier et évaluer les risques de blanchiment de capitaux ou de financement du terrorisme pouvant résulter (a) du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution, et (b) de l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants. ». L'introduction proposée du E-ID dans le domaine LBA doit donc reposer sur une analyse approfondie des risques de blanchiment qui peuvent découler de cette nouvelle technologie.

Dans le cas où une telle analyse permet de conclure qu'il est possible de gérer et limiter de manière appropriée les risques de blanchiment qui peuvent découler de l'introduction du eID dans le domaine des services financiers, la FINMA est d'avis que les points suivants devront encore au minimum être pris en compte :

- 1) Nous saluons le fait que la solution étatique ait été retenue plutôt qu'une solution privée. Cela permet de garantir une première identification de meilleure qualité à la base de la délivrance de la pièce d'identité, respectivement de la eID.
- 2) Le risque de transmission des moyens d'identification subsiste. L'article 6 de la Loi eID qui prévoit des devoirs de diligence pour le titulaire du document d'identité n'est pas suffisant car aucune conséquence juridique n'est prévue en cas de non-respect de ces obligations. Un complément devra être apporté dans la Loi eID sur ce point. La possibilité d'introduire p.ex. une disposition pénale doit être examinée.
- 3) Le devoir d'identification au sens de la LBA porte également sur l'adresse du cocontractant (voir p.ex. art. 39 et ss OBA-FINMA). L'article 3 de la Loi eID, dans lequel le contenu de la eID est détaillé, devra être complété avec l'adresse de domicile du titulaire. Si tel ne devait pas être le cas, le nouvel al. 3bis de l'article 3 LBA devra être complété dans le sens que la vérification de l'adresse du domicile doit être faite en complément de l'identification au moyen de la eID (p.ex. par l'envoi

FINMA

<p>d'un courrier à l'adresse indiquée par le cocontractant).</p> <p>4) Au regard de la réglementation en matière de lutte contre le blanchiment, les documents d'identification reçus par l'intermédiaire financier doivent être munis d'une photo (voir p.ex. art. 40 al. 3 OBA-FINMA). L'article 3 de la Loi eID devra également être complété de manière à ce que la eID contienne la photo d'identité sous format électronique. En effet, la possession d'une photo est indispensable pour le cas où l'intermédiaire financier doit procéder dans le cadre de la surveillance de la relation à des clarifications complémentaires vis-à-vis du cocontractant (contact par vidéo-conférence par exemple).</p> <p>5) L'obligation de documentation des intermédiaires financiers doit être respectée en tout temps (cf. Art. 7 GwG). En d'autres termes, l'intermédiaire financier doit pouvoir enregistrer dans son dossier client les données transmises par le biais du eID et exigées par la LBA.</p> <p>6) Finalement, nous attirons votre attention sur le fait que la traduction française du nouvel al. 3bis LBA n'est pas claire : « <u>elles peuvent</u> » devrait a priori être remplacé par « <u>ils peuvent</u> » car cela se rapporte aux intermédiaires financiers en général et pas uniquement aux institutions d'assurance citées à l'alinéa 3.</p>		
<p>Nous sommes d'accord avec votre proposition et n'avons qu'un commentaire de détail à faire au sujet de l'art. 5.</p> <p>A part la loi sur la signature électronique et son ordonnance d'exécution, nous n'avons par ailleurs pas, dans notre domaine d'activité, d'autres dispositions légales à signaler dans lesquelles serait prévue une obligation de comparaître personnellement.</p>	BAKOM	



Bemerkungen zum Bundesratsantrag (BRA)	Absender	Notizen
<p>Wir empfehlen Ihnen eine Kürzung des Antrags zu prüfen, da der Detaillierungsgrad für den Bundesrat sehr hoch ist. Sofern keine Kürzung vorgenommen wird, ist eine Zusammenfassung erforderlich.</p> <p>Zudem bitte ich Euch die Bemerkungen aus dem ISC-EJPD zum Thema „Sicherheit und Benutzung“ näher zu prüfen und zu berücksichtigen: <i>Im Antrag wird gefordert, eine eID mit hoher resp. höchsten Sicherheitsanforderungen zu realisieren, welche unter anderem auch für ein eVoting verwendet werden kann. Es wird aber (im Gegensatz zu Deutschland) auch aus Kostengründen auf eine Funktion mit digitaler Signatur verzichtet. Umgesetzt wird „nur“ die (starke) Authentisierung (Chip kann die Identität bestätigen). Wir bezweifeln, ob sich eVoting ohne Signaturen umsetzen lässt (eingegangene Stimmen müssen nach der Abstimmung zweifelsfrei nachgezählt werden können – und dies wird unseres Wissens heute mit digitalen Signaturen resp. blinden Signaturen auf Basis von X509 Zertifikaten vorgenommen); oder es müsste noch ein zusätzlicher Signaturdienst aufgebaut werden.</i></p>	EDA	
<p><b>Ziffer 2 BRA (eID im europäischen Umfeld)</b></p> <p>Für die EU, die sich der Realisierung eines schrankenlosen einheitlichen europäischen Binnenmarktes verpflichtet hat, ist dieses Anliegen besonders wichtig. Dazu wurde die <u>Verordnung (EU) Nr. .../2014 über Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)</u> erlassen.</p> <p>=&gt; Hier müsste die genaue Bezeichnung (mit ABl.-Referenz in der FN) angegeben werden. Zurzeit hat der Rat die Verordnung noch nicht gebilligt und auch die Unterzeichnung steht noch aus.</p> <p>Geplant war eine Verabschiedung im EP im Juli und erst danach im Rat.</p> <p>=&gt; Gelöscht: EU-</p> <p>Auch wenn vorläufig offen ist (1), ob, wann und wie die Schweiz sich staatsvertraglich in dieses System einbinden wird, soll das schweizerische eID-System von Beginn an so konzipiert werden, dass es <u>grundsätzlich notifiziert werden könnte</u> (2).</p> <p>=&gt; (1) Warum vorläufig?</p> <p>=&gt; (2) Nicht verständlich. Sieht die VO selbst ein Notifikationsverfahren vor? Oder denkt man an eine Übernahme im Rahmen von Schengen?</p>	GS-EJPD	
	BJ, ERSD	



<p>Wir fänden es gut und nützlich, wenn im <u>Antrag an den Bundesrat</u> (z.B. in Abschnitt 2) oder im erläuternden Bericht zum Vorentwurf (z.B. in Abschnitt 1.5.3) darauf eingegangen wird, ob bzw. wie stark in Deutschland der ePA auch wirklich genutzt wird. Die Darstellung erscheint uns ein bisschen zu optimistisch. Insbesondere müsste darauf hingewiesen werden, dass 2/3 der ePA-Besitzer die eID-Funktion willentlich deaktiviert hat.</p> <p>Die Formulierung in Abschnitt 2 des Antrages, wonach die eID als Online-Ausweis „auf dem von Natur aus grenzenlosen Internet eingesetzt“ wird, erscheint uns etwas zu umgangssprachlich. Insbesondere stört uns das Adjektiv „grenzenlos“ und wir schlagen vor, dieses ersatzlos zu streichen.</p>	<p>ISB</p>
<p><b>Ziffer 4 BRA (Grundzüge der Vorlage)</b></p> <p>Im Hinblick darauf, dass die eID-Funktion künftig allen Einwohnerinnen und Einwohnern der Schweiz zugänglich sein soll, und darum – wenn auch in separaten Projekten – künftig eventuell auch in den verschiedenen Ausländerausweisen enthalten sein wird, beantragen wir den Erlass eines separaten eID-Gesetzes.</p> <p>=&gt; Der Entscheid darüber ist nicht gefällt. Gelöscht: insbesondere</p>	<p>BFM</p>
<p><b>Ziffer 5 BRA (Finanzielle, personelle und weitere Auswirkungen)</b></p> <p>Zu Ziffer 5: Sie führen aus, für die künftige Betriebsorganisation müssten höheren Kosten und zusätzlichen Stellen veranschlagt werden. Da dazu jede Begründung fehlt, ist dies nicht nachvollziehbar.</p>	<p>EDA</p>
<p><b>Ziffer 6 BRA (Neuer Auftrag für die Konzeption eines umfassenden 'Identitäts-Ökosystems')</b></p> <p>Teile davon können der Privatwirtschaft überlassen werden, der Staat muss aber ebenfalls weitere Beiträge leisten, darunter insbesondere:</p> <p>1) Die Koordination bei der Konzeption und Einführung eines nationalen Identitäts-Ökosystems, das mit den in Entwicklung begriffenen IAM-Konzepten des Bundes und der <u>vorstehend (Ziff. xxx) erwähnten Verordnung (EU) Nr. .../2014</u> abgestimmt ist;</p> <p>=&gt; Richtige Benennung der VO =&gt; Gelöscht: EU-</p>	<p>BJ, ERSD</p>
<p>Wir sind mit dem Antragsentwurf grundsätzlich einverstanden, haben aber folgende Bemerkungen und Anträge:</p> <p>In Abschnitt 6 des Antrages an den Bundesrat („Neuer Auftrag für die Konzeption eines umfassenden Identitäts-Ökosystems“) und möglichst auch im Beschluss sollte eine proaktive</p>	<p>ISB</p>

<p>Zusammenarbeit mit allen beteiligten Stellen gefordert werden, insbesondere unter Einbezug des ISB und der Kantone. Wir haben entsprechende Ergänzungsvorschläge in Kap. 6 formuliert (Änderungsmodus). Im Rahmen der gegebenen Möglichkeiten ist das ISB gerne bereit, den Aufbau eines Identitäts-Ökosystems zu unterstützen.</p> <p>In diesem Zusammenhang empfehlen wir, praktischen Aspekten der Benutzerfreundlichkeit und der Möglichkeit zum Einsatz der eID in Abhängigkeit der Verfügbarkeit von Lesemethoden und -geräten ausreichende Beachtung zu schenken, damit sich ein Identitäts-Ökosystem überhaupt entwickeln kann.</p>		
<p>Im Kapitel zu den finanziellen und personellen Auswirkungen des Antragsentwurfs bzw. erläuternden Berichts erwähnen Sie, dass ...</p> <p>1) Die Gesamtprojektkosten, die [mit dem Budget 2013 plafondserhöhend] bewilligten Mittel und den Umfang des Verpflichtungskredits nicht übersteigen werden, dass aber eine intertemporale Verschiebung der Mittel notwendig ist.</p> <p>-&gt; Wir stellen fest, dass diese intertemporale Verschiebung im Rahmen des diesjährigen Budgetierungsprozesses umgesetzt wurde (oder droht eine erneute Verschiebung? uAwg).</p> <p>2) Für die Betriebsorganisation (eID-Kompetenzzentrum) mit höheren Kosten und zusätzlichen Stellen gerechnet werden muss. Der genaue Ressourcenbedarf werde bei der Verabschiedung der Botschaft ausgewiesen und beantragt. Im erläuternden Bericht quantifizieren Sie die erforderlichen Ressourcen mit 26 zusätzlichen Stellen (3 Mio.) und 1.2 Millionen (Betriebskosten Systeme).</p> <p>-&gt; Wir bitten Sie, Antrag und erläuternden Bericht soweit abzustimmen, dass der unterschiedlich quantifizierte Mittelbedarf deckungsgleich ist. Wir ersuchen Sie, uns zusätzliche Informationen zum Stellenmehrbedarf zukommen zu lassen, damit wir dies mit dem EPA besprechen und aufgrund dieser zusätzlichen Informationen (hinterlegtes Mengengerüst, etappierter Aufbau, etc.) noch Stellung dazu nehmen können. Wir bitten Sie, zur Erhöhung der Transparenz eine tabellarische Übersicht in den Antrag an den Bundesrat einzufügen (wieviel für was ab wann; wieviel schon/noch nicht bewilligt/eingestellt).</p> <p>Sie werden verstehen, dass in einer Zeit, in der das Parlament die Personalkostenentwicklung kritisch beobachtet und dem Bundesrat Sparaufträge erteilt, ein Mehrbedarf besonders kritisch unter die Lupe genommen wird. Wir behalten uns ausdrücklich vor, aufgrund der zusätzlichen Informationen abschliessend Stellung zu nehmen.</p> <p>3) Die Investitions-, Betriebs- und Personalkosten (Antragsentwurf: „gemäss den Vorgaben des</p>	<p>EFV</p>	

Parlaments": welchen Vorgaben?) als Deckungsbeitrag auf die Gebühren für die Ausweise umgelegt werden.

-> Wir bitten Sie, in den Entwürfen festzuhalten, dass wie bis anhin kostendeckende Gebühren erhoben werden sollen (s. Antrag oben). Insofern ist der Begriff Deckungsbeitrag zu streichen.

#### **Ziffer 6 Antragsentwurf (Ziffer 6 E-Beschlussdispositiv)**

Im Antrag an den Bundesrat ist auf Seite 5 unter Ziffer 6 der Punkt 3 zu streichen. Der erläuternde Bericht ist entsprechend anzupassen.

#### Begründung:

Für uns ist nachvollziehbar, dass bei Einführung einer eID eine gesamtschweizerische Konzeption zu Koordinationszwecken benötigt wird. Ebenfalls ist klar, dass geprüft werden sollte, welche staatliche Dienste für die Verwendung der eID geeignet sind und dass die so identifizierten Dienste in einem zweiten Schritt zu Online- Diensten ausgebaut werden sollten. Allerdings sind wir der Meinung, dass es nicht Aufgabe des Bundes sein kann, privatwirtschaftliche Angebote für den Einsatz der eID zu fördern. Die Privatwirtschaft wird die Vorteile der eID erkennen und ihre Dienstleistungen entsprechend anpassen.

Ausserdem ist zu beachten, dass im Rahmen von E-Government Schweiz bereits viele Projekte lanciert sind, die schliesslich ebenfalls das Ziel des möglichst einfachen elektronischen Verkehrs zwischen Privaten und Behörden verfolgen. Ein hoher Koordinationsaufwand mit den federführenden Organisationseinheiten dieser Projekte ist deshalb zu erwarten.

Wir ersuchen Sie zudem, im Antrag an den Bundesrat das Ziel des Prüfauftrags (Punkte 1 und 2) ausführlicher zu beschreiben und dabei die Möglichkeit einer Finanzierung durch die Nutzniesser aufzuzeigen. Im Kapitel zu den finanziellen Auswirkungen ist der Prüfauftrag zumindest zu erwähnen und in einer Grössenordnung zu quantifizieren. Wir gehen davon aus, dass sich ein Nutzen aus der Verwendung des Systems ergibt; deshalb erübrigen sich u.E. (finanzielle) Anreize.



<b>Ziffer 7 BRA (Vernehmlassungsverfahren)</b>	
<p>Die Vernehmlassung zum eID-Gesetz erfolgt im Rahmen der Vorbereitung eines Erlasses von Gesetzesbestimmungen im Sinne von Artikel 164 Absatz 1 der Bundesverfassung. Das Vernehmlassungsverfahren findet deshalb gestützt auf Artikel 3 Absatz 1 des Vernehmlassungsgesetzes (VG) statt.</p> <p>=&gt; In Fussnote vollständiger Titel und SR des Erlass einfügen.</p> <p>Somit genügt diese Dauer auch den Anforderungen von Artikel 7 Absatz 2 <u>VG</u>.</p> <p>=&gt; Gelöscht: Vernehmlassungsgesetz</p>	BJ, ERSD

Bemerkungen zum Beschlussdispositiv	Absender	Notizen
<p>Dispositif de décision</p> <p>Il faut supprimer la mention de la publication à la fin du projet de dispositif de décision, conformément aux Directives sur les affaires du Conseil fédéral.</p> <p>Link à ces directives en matière d'ouverture de la procédure de consultation : <a href="http://intranet.bk.admin.ch/roter_ordner/06775/06813/index.html?lang=de">http://intranet.bk.admin.ch/roter_ordner/06775/06813/index.html?lang=de</a></p>	<p>BK</p>	

	Absender	Notizen
<p><b>Allgemeine Bemerkungen zum Gesetzesentwurf</b></p> <p>Le projet de loi eID et le rapport explicatif ne sont pas suffisamment détaillés sur certains points:</p> <ul style="list-style-type: none"><li>• Seulement les données contenues dans l'eID sont clairement mentionnées. Les autres données contenues dans le système d'information sur les eID et dans le registre des certificats ne sont pas mentionnées.</li><li>• Le projet de loi eID et le rapport explicatif ne donne aucune indication quant aux éventuels accès aux fichiers susmentionnés.</li></ul> <p>Aus rechtlicher Sicht gibt es zum Vorentwurf des eID-Gesetzes nicht viel zu sagen. Der Datenschutz scheint gewährleistet zu sein.</p> <p>Ob die vorgesehenen Sorgfaltspflichten bzw. deren Umschreibung (vgl. Art. 6), namentlich die „zumutbare Massnahmen“ sowie der „Stand der Technik“ eine praktikable Regelung sind, um Missbräuche zu verhindern, kann zum jetzigen Zeitpunkt nicht gesagt werden.</p> <p>Es ist vorgesehen, dass Diplomaten- und Dienstpässe auch an Personen ohne schweizerisches Bürgerrecht abgegeben werden können. Ob die neue formell-gesetzliche Grundlage im bestehenden AwG zu schaffen ist, scheint fragwürdig zu sein. Einerseits befasst sich das AwG nicht mit Diplomatenpassen, sondern primär mit Ausweisen für „normale“ schweizerische Staatsangehörige. Andererseits wäre das Bedürfnis für Diplomaten- oder Dienstpässe für Ausländer gemäss EDA auf 10 bis 15 Personen beschränkt, wofür sich eine separate, spezialgesetzliche Regelung anbieten würde.</p> <p><u>Regeste:</u> Ausländerausweise sind derzeit nicht im Projekt enthalten. Daher kann der Verweis auf Art. 121 BV gestrichen werden.</p>	EDÖB	
	fedpol	
	BFM	



Bemerkungen zu den einzelnen Bestimmungen des Gesetzesentwurfs	Absender	Notizen
<p><b>Artikel 1 Entwurf eID-Gesetz (Zweck und Gegenstand)</b></p> <p><b>Artikel 1 Absatz 1</b></p> <p><i>Art. 1 Abs. 1 Bst. a: Wer gibt Ausländerausweise heraus?</i>                      Werden auch alle Ausländerausweise vom Bund herausgegeben? Wenn gewisse dieser Ausweise von den Kantonen oder Gemeinden herausgegeben würden, wäre der Entwurf nicht anwendbar und die betreffende Ausweise könnten nicht mit einer eID versehen werden.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 2 Entwurf eID-Gesetz (Begriffe)</b></p> <p><i>Geheimnummer/Spermerkmal: Ziffern- oder Zeichenfolge?</i>                      Ist es sinnvoll, die Geheimnummer und das Spermerkmal auf Gesetzesstufe auf Ziffern einzuschränken, oder sollte man der Technik dort mehr Spielraum lassen und auch andere Zeichen (Buchstaben, Sonderzeichen ...) zulassen? Unabhängig von der Antwort wäre es gut, diesen Punkt in den Erläuterungen anzusprechen.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 2 Buchstaben i und j</b></p> <p><i>Artikel 2 i und j: Bei Geheimnummer und Spermerkmal wird von einer Zifferfolge gesprochen; im Gesetzestext sollte man hier technikunabhängiger formulieren, z. B. Zeichenanstatt Ziffernfolge. In der Fussnote könnte dann ein Verweis auf den derzeitigen Stand der Technik stehen (derzeit Nummern).</i></p>	<p>ISB</p>	
<p><b>Artikel 3 Entwurf eID-Gesetz (Inhalt der eID)</b></p> <p><i>Artikel 3: Die Liste der Attribute ist schlank und abschliessend. Das bedeutet, dass es viele Anwendungsfälle geben wird, in denen externe Attribut-Provider zum Einsatz kommen müssen und weitere Attribute / Eigenschaften von Personen zu bestätigen. Diese Attribut-Provider müssen dann beim Aufbau eines Identitäts-Ökosystems mit berücksichtigt werden. Es werden nur die Attribute der Identität dargestellt; es wäre wünschenswert, wenn alle gespeicherten Attribute des Ausweises (vermutlich Ausweisnummer, PIN, Spernummer, Herausgeber o.a.) ebenso aufgelistet werden. (vgl. Erläuterung S. 4 und 13f). Schliesslich fragen wir uns, wieso anstelle des Heimatortes der Geburtsort als Attribut auftritt, und ob bei der Umstellung vom Heimatort auf den Geburtsort nicht mit grösseren Problemen zu rechnen ist.</i></p>	<p>ISB</p>	

<p>- Le devoir d'identification au sens de la LBA porte également sur l'adresse du cocontractant (voir p.ex. art. 39 et ss OBA-FINMA). L'article 3 de la Loi eID, dans lequel le contenu de la eID est détaillé, devra être complété avec l'adresse de domicile du titulaire. Si tel ne devait pas être le cas, le nouvel al. 3bis de l'article 3 LBA devra être complété dans le sens que la vérification de l'adresse du domicile doit être faite en complément de l'identification au moyen de la eID (p.ex. par l'envoi d'un courrier à l'adresse indiquée par le cocontractant).</p> <p>- Au regard de la réglementation en matière de lutte contre le blanchiment, les documents d'identification reçus par l'intermédiaire financier doivent être munis d'une photo (voir p.ex. art. 40 al. 3 OBA-FINMA). L'article 3 de la Loi eID devra également être complété de manière à ce que la eID contienne la photo d'identité sous format électronique. En effet, la possession d'une photo est indispensable pour le cas où l'intermédiaire financier doit procéder dans le cadre de la surveillance de la relation à des clarifications complémentaires vis-à-vis du cocontractant (contact par vidéo-conférence par exemple).</p>	<p>FINMA</p>
<p><b>Artikel 3 Absatz 1 Buchstabe d</b>  <b>Art. 3 Abs. 1 Bst. d: Geburtsort</b>          Nach Artikel 2 AwG wird auf den Trägersausweisen von Schweizern der Heimatort angegeben; nach dem Entwurf soll in der eID – auch bei Schweizern – der Geburtsort eingetragen werden. Die Erläuterungen sagen aber nichts zur Frage, ob dieses Auseinanderfallen des Inhalts von Trägersausweis und eID zu praktischen Problemen führen kann und wie diese allenfalls gelöst werden könnten. Auf den ersten Blick schiene es plausibler, bei der bisherigen Lösung zu bleiben und zu differenzieren: Heimatort für Schweizer, Geburtsort für Ausländer.</p>	<p>BJ, RS II</p>
<p><b>Artikel 3 Absatz 1 Buchstabe e</b>  <b>Art. 3 Abs. 1 Bst. e: Nationalität in der Einzahl</b>          Kann es Fälle geben, wo zwei Nationalitäten angegeben werden müssen, insb. bei Personen, die zwei oder mehr ausländische Nationalitäten besitzen und einen Ausländerausweis erhalten?</p>	<p>BJ, RS II</p>
<p><b>Artikel 3 Absatz 1 Buchstabe j</b>          Article 3, alinéa 1, lettre j          Pour les raisons indiquées ci-dessus, le numéro AVS doit être biffé de la liste des attributs d'identification. Si un identificateur univoque devait être nécessaire, il faudrait mettre en place un identificateur sectoriel.</p>	<p>EDÖB</p>

<p>Die AHVN13 ist Teil der eID (Art. 3 Abs. 1 Bst. j). Wenn die eID als Identifikationsmittel gemäss dem Bundesgesetz über das elektronische Patientendossier (EPDG, vom Ständerat in der Sommersession verabschiedet, voraussichtliches Inkrafttreten 1.1.2017) eingesetzt werden soll, gilt es genau abzuklären, wer welche Nummer (AHVN13 und Patientenidentifikationsnummer) für was gebrauchen darf. Für die Identifikation im Rahmen des EPDG wurde die Verwendung der AHVN13 explizit verworfen (Botschaft zum EPDG, S. 5359 f. und 5378 ff.), stattdessen kommt eine neu zu vergebende Patientenidentifikationsnummer zum Einsatz. Daher darf die AHVN13 nicht via eID als Identifikator verwendet werden. Technisch sollte es daher machbar sein, dass die AHVN13 im Rahmen des EPDG nicht ausgelesen werden kann (ausser in den Ausnahmefällen nach Art. 5 Abs. 2 EPDG). Damit stellt sich die Anschlussfrage, ob allenfalls die Patientenidentifikationsnummer ein (freiwilliges) Attribut der eID sein soll. Ein Nebeneinander der beiden Nummern resp. Trägermedien ist wohl unvermeidbar, da die Patientenidentifikationsnummer nur bei Eröffnung eines elektronischen Patientendossiers gemäss EPDG vergeben wird und der Bezug der eID freiwillig ist.</p>	<p>BAG</p>
<p>Selon l'art. 3, al. 1, let. j, de l'avant-projet, l'un des attributs d'identification serait désormais le numéro AVS, ce que le commentaire se limite à mentionner, sans plus de détails. Or, l'identification était jusqu'ici possible sans devoir recourir au numéro AVS et le commentaire n'indique pas pour quoi ce ne serait plus possible à l'avenir. L'OFAS conteste donc la nécessité de cette mention et s'y oppose. Il ne s'agit au surplus pas d'une base légale formelle permettant l'utilisation systématique du numéro AVS au sens de l'art. 50e LAVS, car l'avant-projet ne détermine pas le cercle concret des utilisateurs légitimés, ni l'usage qui serait fait du numéro AVS.</p> <p>Quant à l'introduction de l'art. 51, al. 3bis, LAVS, proposant de dispenser les employeurs de vérifier les indications portées par les salariés dans la demande de certificat d'assurance, elle doit être rejetée. Ledit certificat requiert encore d'autres éléments qui ne figurent pas sur la liste des attributs définis à l'art. 3, al. 1, de l'avant-projet, comme par exemple le nom de célibataire, le sexe, l'adresse, l'identité des parents, et le motif de la demande. Les employeurs participent à l'exécution de la LAVS et ont de ce fait certaines tâches, notamment celle mentionnée à l'art. 51, al. 3, LAVS. L'eID ne permet en l'occurrence pas de remplacer le devoir de contrôle de l'employeur sur l'ensemble des données qui sont à transmettre à la caisse de compensation, dans le but de garantir que l'employé pour lequel l'employeur demande un certificat d'assurance est correctement iden-</p>	<p>BSV</p>



<p>tifié et que cette identification est elle-même correctement transmise à la caisse de compensation. La dispense proposée entraverait donc la bonne exécution de l'AVS et des assurances sociales qui y sont rattachées.</p> <p><u>Aux motifs de ce qui précède, l'OFAS demande:</u></p> <ul style="list-style-type: none"> <li>- de biffer l'art. 3, al. 1, let. j, de l'avant-projet et</li> <li>- de biffer l'introduction de l'art. 51, al. 3bis, LAVS</li> </ul> <p>Pour conclure dans ce contexte, l'OFAS plaide en faveur de l'examen d'autres possibilités, comme l'utilisation d'un identificateur sectoriel de personnes qui serait déduit du numéro AVS et que la Centrale de compensation mettrait à disposition des utilisateurs qui doivent recourir à un identificateur univoque de personnes.</p>		
<p><b>Artikel 3 Absatz 2</b></p> <p><u>Art. 3 Abs. 2 (Fassung VIRK): Andere Inhalte der eID neben den Identitätsattributen</u></p> <p>Die VIRK hat eine Bestimmung über den Inhalt der eID aus Artikel 11 (Funktionen/Anwendungen) zu Artikel 3 (Inhalt der eID) verschoben. In den Erläuterungen steht zudem, die eID enthalte eine Reihe von Sicherheitsdaten. Müsste man diese in Artikel 3 nicht erwähnen?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 4 Entwurf eID-Gesetz (Einsicht)</b></p> <p><b>Artikel 4 Absatz 1</b></p> <p>a) Muss man tatsächlich zur Stelle gehen, wo man den Ausweis einmal bestellt hat (so lesen wir den Entwurf), oder kann man zu jedem beliebigen Passbüro («Antragstelle»)?</p> <p>b) Laut den Erläuterungen soll «der Bund» die – kantonalen – «Antragstellen» mit Lesegeräten ausrüsten. Das müsste man genauer darstellen: Verantwortlichkeiten, Finanzierung...</p> <p>c) Warum soll man Einsicht nur in die Identitätsattribute erhalten und nicht in alle auf der eID gespeicherten Daten? Diese Daten beziehen sich rein schon durch ihr Vorhandensein auf der eID auf eine bestimmte Person und sind daher Personendaten im Sinn von Artikel 2 Buchstabe a DSGVO. In der Logik des Datenschutzrechts ist es nicht folgerichtig, die Einsicht in diese Daten zu verweigern.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 4 Absatz 2</b></p> <p><b>Article 4, alinéa 2</b></p> <p>Cette disposition indique que les données d'identification seront stockées de manière centralisée. Nous partons de l'idée que ces données d'identification seront traitées dans le système d'information mentionné à l'article 7, alinéa 1. Il serait souhaitable de mentionner cette précision au</p>	<p>EDÖB</p>	

**moins dans le rapport explicatif.**

		POLY

<p>In Art. 4 Absatz 2 des eID-Gesetzentwurfs oder im erläuternden Bericht müsste spezifiziert sein, welche Identitätsdaten zentral gespeichert werden bzw. ob diese Daten deckungsgleich mit den auf der Karte gespeicherten Daten sind.</p>	<p>ISB</p>	
<p><b>Artikel 5 Entwurf eID-Gesetz (Meldepflicht)</b>  <b>Art. 5: Differenzierte Meldepflichten</b>          Artikel 5 sieht je nachdem, welche unerwünschte Situation eingetreten ist, eine Meldung an Fedpol oder an die kantonale «Antragstelle» oder an beide vor. Wir erachten es nicht als realistisch, von den betroffenen Privaten zu erwarten, dass sie Meldungen an unterschiedliche Stellen absetzen. Man sollte im Sinn einer praxistauglichen Lösung entweder die kantonalen «Antragstellen» oder Fedpol als alleinige Anlaufstellen für die Ausweisinhaber vorsehen (Koordination mit vorgesehener Beratungsfunktion von Fedpol nach Art. 10 Abs. 2 beachten). Eine Alternative wäre, zumindest für die Meldepflichten nach Artikel 5 den Betroffenen die Wahl zu lassen, ob sie sich an die kantonale «Antragstelle» oder an Fedpol wenden. Keine dieser Lösungen sollte in der Umsetzung besonders aufwändig sein, weil die verschiedenen Stellen ohnehin an ein einheitliches Informationssystem angeschlossen sein müssen und weil das Erfassen einer Verlustmeldung keine besonders hohen Anforderungen stellen dürfte.</p>	<p>BJ, RS II</p>	
<p>Nous ne comprenons en effet pas très bien la différence qui est faite entre les alinéas 2 et 3 de cette disposition, qui nous paraissent se référer en définitive au même cas de figure. Il nous paraîtrait plus logique de dire à l'al. 2 qu'en cas de perte ou de vol du type de document d'identité porteur de l'eID, le titulaire doit informer immédiatement l'émetteur au sens de l'art. 7 (dans tous les cas, et non seulement si des tiers risquent d'avoir eu connaissance du code confidentiel). Quant à l'al. 3, il devrait régler le cas où le type de document d'identité porteur de l'eID n'a pas été perdu ou volé, mais que le titulaire sait ou présume, sur la base de soupçons fondés, que des tiers pourraient (momentanément) avoir eu accès à son eID.</p>	<p>BAKOM</p>	
<p><b>Artikel 5 Absatz 1</b>          Die Meldung des Verlustes oder Diebstahls eines Trägerausweises mit eID richtet sich nach den Vorschriften zum entsprechenden Ausweis. Gelöscht: es</p>	<p>BFM</p>	



<p><b>Artikel 5 Absatz 3</b></p>			
<p><b>Art. 5 Abs. 3: Meldepflicht bei Zugang Dritter zur eID</b></p>			
<p>Diese Bestimmung hat vermutlich keinen eigenen Gehalt, zumindest nicht gegenüber Absatz 2 in der Fassung der VIRK. Es ist allerdings unklar, was «Zugang haben» bedeutet?</p>			
<ul style="list-style-type: none"> <li>- Die Karte rein faktisch aus dem Portmonee des Trägers nehmen können, z.B. als Familienmitglied?</li> <li>- Die Geheimzahl wissen?</li> <li>- Den RFID-Chip unbemerkt aktivieren und für die nicht mit der Geheimzahl geschützten Anwendungen nutzen können?</li> </ul>			
<p>Das Erste kann man unmöglich verhindern, das Zweite kann leicht unbemerkt geschehen und beim Dritten kann man nicht davon ausgehen, dass sich alle mit Alu-Folien oder ähnlichen Hausmitteln vor unbemerktem Zugriff auf die Karte schützen werden.</p>			
<p>Unklar ist ausserdem, wer Dritter ist. Alle ausser dem Inhaber, inkl. Familienmitglieder, Spitex, Arbeitskollegen und Putzfrau?</p>			
<p>Das Gleiche gilt, wenn die Inhaberin oder der Inhaber weiss oder den begründeten Verdacht hat, dass eine Dritte oder ein Dritter Zugang zur eID hatte oder haben könnte.</p>		BFM	
<p>In Art. 5 Absatz 3 des eID-Gesetzes müsste genauer spezifiziert sein, was genau damit gemeint ist, dass „eine Dritte oder ein Dritter Zugang zur eID haben könnte.“ Ist damit der Zugang nur zur Karte oder auch zur Geheimzahl gemeint? Im erläuternden Bericht wird davon gesprochen, dass es insbesondere um die Kenntnis der Geheimzahl gehe, die Aussage müsste aber präzisiert und konkretisiert werden.</p>		ISB	
<p><b>Artikel 6 Entwurf eID-Gesetz (Sorgfaltpflichten)</b></p>			
<p>Le risque de transmission des moyens d'identification subsiste. L'article 6 de la Loi eID qui prévoit des devoirs de diligence pour le titulaire du document d'identité n'est pas suffisant car aucune conséquence juridique n'est prévue en cas de non-respect de ces obligations. Un complément devra être apporté dans la Loi eID sur ce point. La possibilité d'introduire p.ex. une disposition pénale doit être examinée.</p>		FINMA	

<p><b>Artikel 6 Absatz 1</b></p> <p>Art. 6 Abs. 1: Sorgfaltspflicht, den ausschliesslichen Zugriff auf den Trägerausweis mit eID sowie auf die Geheimnummer sicherzustellen</p> <p>Vgl. Art. 5 Abs. 3: Wie streng soll diese Pflicht sein? Den physischen Zugriff auf die Karte kann man nicht wirklich ausschliessen. Zudem muss man mindestens dem Lesegerät eines Anbieters sehr wohl Zugriff auf die Karte geben, wenn man sie einsetzt. Zumindest in dieser Situation kann nicht die Rede sein von ausschliesslichem Zugriff durch den Inhaber.</p> <p>Ausserdem entsprechen sich dt. und frz. nicht (sicherstellen: obligation de résultat; veiller à: obligation de moyen).</p>	<p>BJ, RS II</p>	
<p><b>Artikel 6 Absatz 2</b></p> <p>Art. 6 Abs. 2: Verantwortung der Inhaber für die Sicherheit der technischen Umgebung</p> <p>Wir halten es nicht für realistisch, den Inhabern grundsätzlich die Verantwortung für die Sicherheit der technischen Umgebung zu übertragen, auch nicht mit der Einschränkung «durch zumutbare Massnahmen». In Anwendungsszenarien, wo der Inhaber die eID an seinem eigenen Lesegerät (z.B. Smartphone) vorweist, hat die Bestimmung sicher einen sinnvollen Anwendungsbereich: Der Benutzer muss die Software auf seinem Gerät aktuell halten. Hingegen kann er auch in dieser Situation allfällige vom Kommunikationspartner («vertrauenden Dienst/Beteiligten») zur Verfügung gestellte Software nicht wirklich kontrollieren. Keinerlei Einfluss auf die Sicherheit des Lesegeräts und dessen Software hat er, wenn dieses vom Kommunikationspartner gestellt wird. Auf die Sicherheit der Daten auf dem weiteren Bearbeitungsweg hat er ebenfalls keinerlei Einfluss.</p> <p>Wir könnten uns allenfalls folgende Formulierung vorstellen:</p> <p>«Sie oder er hat durch zumutbare Massnahmen zu gewährleisten, dass die eID in ihrem oder seinem unmittelbaren Einflussbereich so eingesetzt wird, dass die angestrebte Nutzung nach dem jeweiligen Stand der Technik sicher ausgestaltet ist.»</p> <p>Vgl. auch die Bemerkung zu Art. 16 / Sorgfaltspflichten</p>	<p>BJ, RS II</p>	
<p><b>Artikel 6 Absatz 3</b></p> <p>In Art. 6 Absatz 3 des eID-Gesetzesentwurfs ist nicht klar, was die Antragstelle konkret macht, wenn ihr ein Fehler gemeldet wird. Wird dann zwingend eine neue IDK mit eID ausgestellt?</p>	<p>ISB</p>	

<p><b>Artikel 7 Entwurf eID-Gesetz (Herausgeber)</b>                  Article 7                  L'article 7 et le rapport explicatif ne sont pas suffisamment précis quant au système d'information sur les eID. Ce système d'information sera-t-il interconnecté avec d'autre système d'information de fedpol comme par exemple ISA ? Il n'est de plus pas possible de déterminer quelles données personnelles seront traitées dans ce système d'information, quelles autorités ou personnes privées auront accès au système d'information et à quelles données. Ces différents points devront être précisés au niveau de la loi.</p>	<p>EDÖB</p>	
<p>Überdies ist gemäss Vorentwurf des eID-Gesetz, vgl. Art. 7, neben dem als Herausgeber genannten EJPD, das Bundesamt für Bauten und Logistik für die als Personalisierung zuständige Stelle der eID aufzuführen:                  Art. 7 Herausgeber und Personalisierungsstelle                  1 Herausgeber der eID ist das Bundesamt für Polizei (fedpol). Es führt ein Informationssystem über die ausgestellten eID und betreibt die für die Herausgabe, Verwaltung und Auskunftserteilung notwendige Infrastruktur.                  2 Die zuständige Stelle für die Personalisierung der eID mit biometrischen Daten ist das Bundesamt für Bauten und Logistik (BBL).</p>	<p>BBL</p>	
<p><b>Artikel 7 Absatz 1</b>                  Art. 7 Abs. 1: Herausgeberstellung von Fedpol                  Es ist nicht klar, was diese Herausgeberstellung rechtlich und praktisch bedeutet und in welchem Verhältnis das Herausgeben (der eID?) zum Ausstellen (des Trägers ausweises?) steht.                  Art. 7 Abs. 1 erster Satz: Betrieb der für die Herausgabe und Verwaltung der eID sowie für die Erteilung von Auskünften notwendigen Infrastruktur                  Es wirkt seltsam, im Gesetz primär die Infrastruktur für diese Aufgaben zu nennen, statt die Aufgaben selber. Warum wird das so geregelt?                  Art. 7 Abs. 1 zweiter Satz: Informationssystem                  Das Informationssystem muss detaillierter geregelt werden. Vgl. den Leitfaden unter</p>	<p>BJ, RS II</p>	



<p>www.bj.admin.ch &gt; Themen &gt; Staat &amp; Bürger &gt; Legistik &gt; Legistische Hauptinstrumente &gt; Leitfaden für die Erarbeitung der Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten.</p> <p><b>Artikel 7 Absatz 2</b></p> <p><b>Art. 7 Abs. 2: Keinerlei Kontrolle der Gültigkeitsabfragen?</b></p> <p>a) Muss im Gesetz vorgesehen werden, dass die Möglichkeit, die Gültigkeit von eIDs abzufragen, gegen Missbrauch gesichert werden muss? Der praktische Einsatz solcher Sicherungen würde möglicherweise gegen die vorgesehene Gesetzesbestimmung verstossen, wonach die Überprüfung jederzeit, zuverlässig und kostenlos möglich sei muss.</p> <p>b) Muss man festlegen, wer die Gültigkeit eine eID überprüfen darf? Etwa nur ihr Inhaber und die Inhaber von Berechtigungszertifikaten, die einen konkreten Kommunikationsvorgang mit der betreffenden eID nachweisen?</p>		<p>BJ, RS II</p>	
<p><b>Artikel 8 Entwurf eID-Gesetz (Prozess)</b></p> <p><b>Art. 8: Persönliche Vorsprache, Ausstellng zusammen mit dem Trägersausweis</b></p> <p>Warum muss die persönliche Vorsprache im eID-Gesetz geregelt werden, wenn sie am Schluss dann doch nach den Ausführungsbestimmungen zum AwG und zum AuG ablaufen soll (so die Erläuterungen)? Müsste man nicht eher Absatz 1 streichen und stattdessen nach Absatz 2 die Aussage ergänzen, dass das Verfahren gemäss AwG/AuG abzuwickeln ist (etwa: «Das Ausstellungsverfahren richtet sich nach den auf den jeweiligen Trägersausweis anwendbaren Bestimmungen»)?</p>		<p>BJ, RS II</p>	
<p>In <u>Art. 8</u> ist bei der Ausgestaltung des Prozesses darauf zu achten, dass das höchste Niveau der „Vertrauensstellung“ erreicht wird (Level of Assurance LOA 4 gemäss eCH-0170 und eCH-0171). Zudem sollte der Prozess auch auf der Seite der Antragstellenden zu keiner grossen zusätzlichen Belastung führen.</p>		<p>ISB</p>	
<p><b>Artikel 8 Absatz 3</b></p> <p><b>Art. 8 Abs. 3 Gebühren:</b> Es ist nicht sinnvoll, im Gesetz bloss zu schreiben, es könne eine kostendeckende Gebühr erhoben werden. Wenn es nur um Gebührenforderungen von Bundesverwaltungsbehörden für ihre Leistungen ginge, bräuchte man auf Gesetzesstufe nichts zu regeln, weil Artikel 46a RVOG eine passende und im Detail ausgereifte Regelung dazu enthält. Einzelne Elemente dieser in diesem Fall ohnehin anwendbare Regelung herauszugreifen, schafft nur Verwirrung. So ist vorliegend nicht klar, was «kostendeckend» bedeutet: Darf der</p>		<p>BJ, RS II</p>	

<p>Gebührenertrag die Kosten des Verwaltungszweigs nicht überschreiten (das ist das allgemeine gebühren-rechtliche Kostendeckungsprinzip) oder wird der Bundesrat angewiesen, die Gebührenansätze so festzulegen, dass die vollen Kosten des Verwaltungszweigs gedeckt werden? Wenn es hingegen um das Zusammenspiel von Behörden und Gebühren des Bundes und der Kantone geht, muss man dieses näher regeln: Welches Gemeinwesen stellt Gebühren wofür in Rechnung, und welchen Anteil davon gibt es gegebenenfalls an die andere Ebene weiter? Das Gesetz muss mindestens den Bundesrat beauftragen, diese Fragen zu regeln. Möglicherweise wird sich in diesem Zusammenhang ergeben, dass entsprechende Regelungen im AwG und im AUG ergänzt oder angepasst werden sollten; das eID-Gesetz könnte dann darauf verweisen und vorsehen, dass für die eID ein Aufschlag erhoben wird.</p>	<p>ISB</p>	
<p>Wir beantragen, Art. 8 Abs. 3 des Gesetzesentwurfs wie folgt zu formulieren:  <i>Für die Ausstellung einer eID kann <u>wird</u> eine kostendeckende Gebühr erhoben werden.</i>                  Begründung:                  Das geltende Recht geht bei den Ausweisen von einer kostendeckenden Gebühr aus. Von diesem Grundsatz ist auch bei der eID nicht abzuweichen.</p>	<p>EFV</p>	
<p><b>Artikel 9 Entwurf eID-Gesetz (Gültigkeit, Sperrung und Ungültigkeitserklärung)</b>                  Article 9                  Le rapport explicatif ne mentionne pas quelles données figureraient sur la liste de blocage publique. Il est nécessaire d'indiquer à l'article 9 quelles données seront rendues accessibles de manière publique.</p>	<p>EDÖB</p>	
<p><b>Artikel 9 Absatz 1</b>                  In Art. 9 Absatz 1 wird festgehalten, dass die eID die gleiche Gültigkeitsdauer wie der Trägerschein hat (in der Regel also 10 Jahre). Damit hat die eID eine im Zertifikatsgeschäft unüblich lange Lebensdauer. Im erläuternden Bericht müsste entsprechend geklärt werden, ob bzw. wieso aus dieser unüblich langen Lebensdauer nicht Risiken resultieren und wie diese Risiken allenfalls reduziert werden können.</p>	<p>ISB</p>	

<p><b>Artikel 9 Absatz 2</b></p>	<p><b>Art. 9 Abs. 2: Sperrliste und andere Techniken</b> Laut den Erläuterungen zu Artikel 7 soll die Sperrung von eIDs mittels Sperrliste nur eine Möglichkeit unter mehreren denkbaren Sperrtechniken sein. Diese Flexibilität verliert man, wenn man sie hier dann doch als einzig zulässige vorschreibt.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 10 Entwurf eID-Gesetz (eID-Kompetenzzentrum)</b></p>	<p><b>Art. 10 Kompetenzzentrum</b> Was soll die organisationsrechtliche Stellung dieses Zentrums sein? Wenn es nur um eine neue Aufgabe von Fedpol geht, dann sollte man einfach dieses Zentrum nennen und ihm die Aufgabe zuweisen. Ob die zuständige Abteilung von Fedpol dann z.B. «Kompetenzzentrum» genannt wird, wird dadurch nicht präjudiziert (siehe Rz. 153 GTR).</p>	<p>BJ, RS II</p>	
<p><b>Artikel 10 des Gesetzesentwurfs ist mit einem neuen Absatz 3 zu ergänzen: Der Aufwand des eID-Kompetenzzentrums wird über Gebühren finanziert.</b></p>	<p>Begründung: Auch der Betrieb des Kompetenzzentrums ist im Sinne der Kostendeckung über Gebühren zu finanzieren.</p>	<p>EFV</p>	
<p><b>Artikel 10 Absatz 1 Buchstabe b</b></p>	<p><b>Art. 10: technische Interoperabilität</b> Warum wird in Bezug auf Anfragen ausländischer Behörden nur die technische Interoperabilität herausgegriffen (Abs. 1 Bst. b)? Wenn es z.B. rechtliche oder organisatorische Fragen gibt, wird man sich doch ebenfalls an Fedpol wenden dürfen? Warum ist die detaillierte, differenzierte Aufzählung von möglichen Fragestellern überhaupt nötig? Sofern es darum geht, die Aufgabenteilung zwischen Fedpol und den kantonalen «Antragstellen» zu regeln, fehlt offensichtlich die Seite der Antragstellen.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 10 Absatz 2</b></p>	<p><b>Art. 10 Abs. 2: Aufgabenübertragung auf «Dritte»</b> a) Wer sind «Dritte»? Private? b) Warum ist so eine Aufgabenübertragung nötig? Das müsste in den Erläuterungen aufgezeigt werden. c) Wenn tatsächlich eine Aufgabenübertragung auf Private zulässig sein soll, so müssen verschiedene Fragen geregelt werden (Aufsicht, Finanzierung, Wahrung der Wettbewerbsneutralität...; siehe Rz. 837–857 des Gesetzgebungsleitfadens, 3. Auflage 2007).</p>	<p>BJ, RS II</p>	



<p><b>Artikel 11 Entwurf eID-Gesetz (Funktionen und Anwendungen der eID)</b>  <b>Artikel 11 Absatz 3</b></p>		
<p>Art. 11 Abs. 3: «Der Bundesrat bestimmt die einzuhaltenden Standards»                  Was ist mit Standard gemeint? Geht es um technische Normen oder soll der Bundesrat auch eine autonome Regelung erlassen können? Braucht es überhaupt eine Delegationsnorm oder kann der Bundesrat die vorgesehene Regelung ohnehin direkt gestützt auf Artikel 182 BV erlassen?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 12 Entwurf eID-Gesetz (Auslesen der Daten)</b>  <b>Artikel 12 Absatz 3</b></p>		
<p>Art. 12 Abs. 3: «Angaben, welche die Überprüfung der Gültigkeit der eID erlauben»                  Mindestens in den Erläuterungen sollte man aufzeigen, was das für Daten sein dürfen. Oder ist es einfach das Sperrmerkmal (das man dann natürlich so nennen sollte)? Wenn es um datenschützerisch relevante Daten geht, sollte auch der Gesetzestext etwas genauer sagen, was es für Daten sind.</p>	<p>BJ, RS II</p>	
<p>Bei jeder Anwendung werden Angaben <u>übermittelt</u>, welche die Überprüfung der Gültigkeit der eID <u>erlaubt</u>.</p>	<p>BFM</p>	
<p>Gelöscht: übermittelt, erlauben.</p>		
<p><b>Artikel 13 Entwurf eID-Gesetz (Verwendung der eID für staatliche Dienste)</b>  <b>Art. 13: Verhältnismässigkeitsprinzip</b></p>		
<p>a) Der Entwurf konkretisiert hier das Verhältnismässigkeitsprinzip, das ohnehin gilt. Die Formulierung könnte aber manchen Leser dazu verleiten, in der Bestimmung eine gesetzliche Grundlage für den Einsatz der eID und die damit verbundene Datenbearbeitung zu sehen. Unseres Erachtens wäre das unzulässig; der Gesetzestext sollte aber klarer sein.                  b) Warum wird die Verhältnismässigkeit nur bei der Datenbearbeitung durch Behörden vorgesehen (anders als in Art. 4 Abs. 2 DSGVO)?                  c) Wie sollen die vorgesehenen Einschränkungen durchgesetzt werden? Weder das Gesetz noch die Erläuterungen äussern sich dazu.</p>	<p>BJ, RS II</p>	

<p>In Art. 13 suggeriert Absatz 2, dass staatliche Dienstangebote, für die ein Identitätsnachweis notwendig ist, zwingend die eID nutzen müssen, und dass entsprechend keine anderen Authentifikationsmöglichkeiten unterstützt werden dürfen. Wir erachten diese ausschliessende Forderung als relativ stark und einschneidend und fragen uns, ob das so wirklich gewollt ist. Zudem sollte klargestellt werden, dass der Verweis auf Artikel 11 so zu verstehen ist, dass es sich bei der dortigen Aufzählung um eine Rangliste handelt (zuerst a. anonyme Authentifizierung, dann b. pseudonyme Authentifizierung, etc.).</p>	<p>ISB</p>
<p><b>Artikel 14 Entwurf eID-Gesetz (Zuständige Stelle)</b>          Gemäss Abschnitt 5 (Art. 14 und 15) ist nicht klar, ob je Unternehmen ein Berechtigungszertifikat ausreicht. Was ist z.B. wenn ein Unternehmen für sich oder im Auftrag von Dritten verschiedene Dienste anbietet? Was ist grundsätzlich der Wert und Nutzen eines Berechtigungszertifikates, wenn dieses von keiner Prüfung abhängt?</p>	<p>ISB</p>
<p><b>Artikel 14 Absatz 1</b>          Art. 14 Abs. 1: «Der Bundesrat beauftragt eine Stelle...»          Der Bundesrat sollte im Moment, wo er den Gesetzesentwurf vorstellt, wissen, welche Behörde diese Aufgabe übernehmen soll. Diese ist denn auch im Gesetzesentwurf direkt zu nennen (Rz. 152 GTR).          Falls hingegen eine Aufgabenübertragung auf Private erlaubt werden soll, so gilt dasselbe wie zu Artikel 10 Absatz 2.</p>	<p>BJ, RS II</p>
<p><b>Artikel 14 Absatz 2</b>          Art. 14 Abs. 2: Register der Berechtigungszertifikate          Dieses Register wird hier als bekannt vorausgesetzt, obwohl es nicht geregelt wird. Es gelten dieselben Bemerkungen wie zu Artikel 7 Absatz 1 zweiter Satz (Regelung eines Informationssystemes).</p>	<p>BJ, RS II</p>
<p><b>Artikel 15 Entwurf eID-Gesetz (Verfahren)</b>          Article 15          Comme pour le système d'information sur les eID, les explications sur le registre des certificats sont peu détaillées. Devra notamment être réglé, quelles données sont traitées et qui a accès à celles-ci.</p>	<p>EDÖB</p>

<p>Gemäss Abschnitt 5 (Art. 14 und 15) ist nicht klar, ob je Unternehmen ein Berechtigungszertifikat ausreicht. Was ist z.B. wenn ein Unternehmen für sich oder im Auftrag von Dritten verschiedene Dienste anbietet? Was ist grundsätzlich der Wert und Nutzen eines Berechtigungszertifikates, wenn dieses von keiner Prüfung abhängt?</p>	<p>ISB</p>	
<p><b>Artikel 15 Absatz 3</b>                  Art. 15 Abs. 3: <i>Widerruf bei Missbrauch</i>                  Die Generalklausel «Missbrauch» ist sehr unscharf. Sie sollte wenn möglich präzisiert werden. Was gilt etwa bei nicht strafbaren Datenschutzfreveltaten, die in der Praxis zumindest bei privaten «vertrauenden Beteiligten» ja an der Tagesordnung sein dürften?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 15 Absatz 3 Buchstabe b</b>                  Art. 15 Abs. 3 Bst. b und 16 Abs. 2: «unberechtigt an Dritte weitergeben»?                  Was bedeutet «unberechtigt»? An welche Dritten darf das Berechtigungszertifikat weitergegeben werden, und wo ist das geregelt bzw. soll es geregelt werden?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 16 Entwurf eID-Gesetz (Rechte und Pflichten der vertrauenden Dienste)</b>                  Art. 16: <i>Rechtsfolge von Pflichtverletzungen</i>                  Ist es sinnvoll, dass abgesehen vom möglichen Widerruf des Berechtigungszertifikats (Art. 15 Abs. 3) keine Sanktionen für die Verletzung von Pflichten der vertrauenden Beteiligten vorgesehen sind? Angesichts des sehr leichten Zugangs zu den Berechtigungszertifikaten (was Umgehungsmanöver erleichtern dürfte) und der grossen Verantwortung der Stellen, die auf eID-Daten zugreifen können, überrascht die Regelung.</p>	<p>BJ, RS II</p>	
<p><b>Artikel 16 Absatz 2</b>                  Art. 15 Abs. 3 Bst. b und 16 Abs. 2: «unberechtigt an Dritte weitergeben»?                  Was bedeutet «unberechtigt»? An welche Dritten darf das Berechtigungszertifikat weitergegeben werden, und wo ist das geregelt bzw. soll es geregelt werden?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 17 Entwurf eID-Gesetz (Vollzug)</b>                  Artikel 17 Absatz 2                  Art. 17 Abs. 2: <i>Administrative und technische Vorschriften?</i>                  Ist es nötig, Fedpol die Kompetenz zum Erlass solcher Bestimmungen zu übertragen? Wenn ja, sollten die Erläuterungen aufzeigen, wessen Rechte und Pflichten in diesen Bestimmungen in technischer und administrativer Hinsicht konkretisiert werden sollen, und inwiefern.</p>	<p>BJ, RS II</p>	



Allgemeine Bemerkungen zu den Erläuterungen	Absender	Notizen
<p>Der erläuternde Bericht zum Gesetzesentwurf hält die Eckpunkte fest, die der Bundesrat (BR) für die Ausgestaltung der künftigen eID festgelegt hat. Unter den drei Punkten ist die Unterstützung hochsensitiver Anwendungen - darunter Vote électronique - vorgesehen. Die vorliegende Stellungnahme bezieht sich auf den Gesetzesentwurf mit Blick auf die Bedürfnisse von Vote électronique.</p> <p>Etwa 3 Prozent der Stimmberechtigten können zur Zeit bei eidgenössischen Urnengängen über das Internet abstimmen. In seinem dritten Bericht über die elektronische Stimmabgabe hat der BR 2013 seine Strategie für die Weiterentwicklung der elektronischen Stimmabgabe über das Internet festgelegt. Darauf gestützt hat der BR die Verordnung über die politischen Rechte (VPR) angepasst und die Bundeskanzlei (BK) hat eine neue Verordnung über die elektronische Stimmabgabe (VEleS) erlassen. Die neuen Rechtsgrundlagen sind am 15. Januar 2014 in Kraft getreten. Bedingung für die Ausdehnung der elektronischen Stimmabgabe ist die sogenannte "Verifizierbarkeit". Mit Blick auf eine medienbruchfreie (ohne Verwendung des via Post zugestellten Stimmmaterials) Stimmabgabe hat die BK die Bedürfnisse von Vote électronique im Vorfeld des vorliegenden Gesetzesentwurfs eingebracht.</p> <p>Ein sicheres und weit verbreitetes Authentifizierungsmittel, das das Vertrauen der Bevölkerung geniesst, bildet eine der Grundvoraussetzungen für die medienbruchfreie Stimmabgabe. Dadurch wird sichergestellt, dass nur Stimmberechtigte Personen an einem Urnengang teilnehmen können. Allerdings muss auch die Frage nach der Sicherheit der einzelnen Transaktionen gestellt werden. In Bezug auf die elektronische Stimmabgabe erfordert die Verifizierbarkeit zusätzliche Mechanismen mit Blick auf die Sicherung der einzelnen Transaktionen (der Stimmen). Auch im e-Banking werden Mechanismen zur Sicherung der einzelnen Transaktionen eingesetzt. In diesem Sinne hat es die BK begrüsst, dass das Aussprachepapier eine Prüfung in Aussicht gestellt hat, ob ein hochsicheres Lesegerät abgegeben werden soll. Nur mit einem geeigneten Gerät kann die elektronische Stimmabgabe zeitgemäss und zukunftssträftig unterstützt werden. Gleichzeitig hätte es dazu beigetragen, die Vertrauenswürdigkeit des elektronischen Geschäftsverkehrs ganz allgemein zu fördern - insbesondere die Vertrauenswürdigkeit des Geschäftsverkehrs, der auf der Grundlage der eID erfolgen soll: Falls unter Verwendung der eID getätigte Transaktionen manipuliert werden, würden die Verwendung der eID und die Glaubwürdigkeit der Aussagen über die Sicherheit der eID mutmasslich ebenfalls in Mitleidenschaft gezogen. Die Abgabe eines</p>	<p>BK</p>	

<p>geeigneten Lesegeräts wurde zu unserem Bedauern letztlich verworfen. Im Lichte verschiedener belegter und unbelegter Zweifel über die Vertrauenswürdigkeit des Internets würden wir es begrüßen, wenn der erläuternde Bericht klar zum Ausdruck bringen würde, dass der vorliegende Gesetzesentwurf ausschliesslich die Grundlage für eine sichere Authentifizierung schafft. Die sichere Verwendung der eID, im Sinne der Sicherheit der eigentlichen Transaktionen, wird nicht adressiert. Angehende Dienstleister sollen dies bei der Einführung von eID-gestützten Dienstleistungen berücksichtigen.</p>		
<p>Le projet de loi eID et le rapport explicatif ne sont pas suffisamment détaillés sur certains points:</p> <ul style="list-style-type: none"> <li>• Seulement les données contenues dans l'eID sont clairement mentionnées. Les autres données contenues dans le système d'information sur les eID et dans le registre des certificats ne sont pas mentionnées.</li> <li>• Le projet de loi eID et le rapport explicatif ne donne aucune indication quant aux éventuels accès aux fichiers susmentionnés.</li> <li>• Le rapport explicatif ne précise malheureusement au point 1.3 comment le code contenu dans l'eID permet la création d'un pseudonyme différent pour chaque service utilisé. On ne sait en particulier pas où ces pseudonymes seront stockés (IDK, eID-Informationssystem, eID-Server) ? En outre, s'agit-il bien du même code lorsque le rapport parle de saisie d'un nombre secret (NIP) et du même pseudonyme quand il évoque une personne enregistrée sous un nom d'utilisateur ? L'utilisation du numéro AVS en tant qu'identificateur universel de personnes dans toute l'administration et en dehors (dans le secteur privé comme cela est prévu dans le projet de loi eID) présente des risques considérables pour la protection de la personnalité en raison du fait que l'on renonce ainsi à empêcher tout appariement non autorisé de données par des moyens techniques. Nous plaçons en faveur de l'utilisation d'un identificateur sectoriel de personnes. Ce procédé a déjà été transposé avec succès dans la loi fédérale sur le dossier électronique du patient (LDEIP). Cette voie est également ouverte à tous les autres cas requérant une identification de personnes de manière univoque sans lourde charge administrative et financière supplémentaire.</li> </ul>	<p>EDÖB</p>	

<p><i>allg.: Chancen und Risiken</i></p> <p>Glaubt man den Erläuterungen, so wird die eID ein grosser Fortschritt für die Sicherheit elektronischer Kontakte zwischen den verschiedensten Kommunikationsparteien. Es wäre interessant zu erfahren, welche Risiken die eID ebenfalls mit sich bringt. Denkbar wäre etwa, dass das erfolgreiche Usurpieren einer – vermeintlich – mit einer eID abgesicherten Identität drastischere Folgen haben könnte als ein «traditioneller» Identitätsdiebstahl. Interessant wäre zudem eine technisch fundierte Einschätzung, wie gut die Chancen stehen, dass die eingesetzte Technik (Authentifizierung, verschlüsselte Übermittlung zum Lesegerät usw.) während der ganzen Lebensdauer der Trägersweise sicher bleibt.</p>	<p>BJ, RS II</p>	
<p>Wir fänden es gut und nützlich, wenn im Antrag an den Bundesrat (z.B. in Abschnitt 2) oder im <u>erläuternden Bericht zum Vorentwurf</u> (z.B. in Abschnitt 1.5.3) darauf eingegangen wird, ob bzw. wie stark in Deutschland der ePA auch wirklich genutzt wird. Die Darstellung erscheint uns ein bisschen zu optimistisch. Insbesondere müsste darauf hingewiesen werden, dass 2/3 der ePA-Besitzer die eID-Funktion willentlich deaktiviert hat.</p> <p>Gemäss <u>Abschnitt 1.2</u> des erläuternden Berichts soll von der neuen IDK eine Variante mit und eine Variante ohne Chip angeboten werden. Dabei ist bei der Version mit Chip immer sowohl die eID-Funktion als auch die biometrischen Daten auf dem Chip. Da diese beiden Funktionen keine Abhängigkeit aufweisen sollte die Auswahl bei der Variante für den Bürger auch entkoppelt werden. Es sollte eine IDK mit eID-Funktion aber ohne biometrische Daten und auch umgekehrt angeboten werden.</p> <p>In <u>Abschnitt 1.3</u> des erläuternden Berichts wird die Bezeichnung NATEL verwendet. Da es sich hierbei um eine eingetragene Marke der Swisscom handelt, sollte besser der Begriff „Mobiltelefon“ verwendet werden. Zudem wird in diesem Abschnitt argumentiert, dass es in gewissen Fällen genügt, die IDK mit der eID an das Lesegerät zu halten. Hier ist nicht klar, welche Daten dann ausgelesen werden können, und wie sichergestellt ist, dass nur Daten ausgelesen werden, die der Benutzer auch freigegeben hat. Diese Punkte müssten vertieft werden.</p>	<p>ISB</p>	
<p>Im Antrag an den Bundesrat ist auf Seite 5 unter Ziffer 6 der Punkt 3 zu streichen. Der erläuternde Bericht ist entsprechend anzupassen (Begründung, siehe oben Bemerkungen zum Bundesratsantrag).</p>	<p>EFV</p>	



<p>Interessanterweise wird im erläuternden Bericht zum Vorentwurf unter Pkt. 1.5.3 der neue elektronische Personalausweis in Deutschland als gutes Beispiel aufgeführt, welcher die Komplexität in technischer und organisatorischer Hinsicht gemeistert hat. Bereits sind rund 25 Mio. neue Personalausweise ausgegeben worden. Dabei wurde 2008 von der Bundesrepublik Deutschland im Hinblick auf die Wahrung der nationalen sicherheitspolitischen Interessen die sog. Bundesdruckerei nach acht Jahren privatwirtschaftlicher Ausrichtung, wieder in den Besitz des Bundes zurückgeführt. Der Rückwerb dieser Institution schaffte auch eine sicherheitspolitische Voraussetzung zur Vergabe der Herstellung des elektronischen Personalausweises an die Bundesdruckerei, was faktisch einer hoheitlichen Tätigkeit gleichkommt.</p>	<p>BBL</p>	
<p><b>Ziffer 1.1 Ausgangslage</b>                  Mehrere Gründe sprechen dafür, die neue Identitätskarte mit einer eID zu versehen:                  Die EU hat eine Verordnung für die gegenseitige Anerkennung und Interoperabilität von eID-Systemen der Mitgliedländer verabschiedet. Dies zeigt, dass auch die EU diesem Werkzeug eine grosse Bedeutung beimisst.                  =&gt; Prüfen, ob bereits erfolgt (genauere Angaben zum Rechtsakt hinzufügen).</p>	<p>BJ, ERSD</p>	
<p><b>Ziffer 1.2 Entstehung des vorliegenden Gesetzesentwurfs</b></p>		
<p><b>Ziff. 1.2, zweiter Absatz, Bst. b:</b> «Die eID muss mittelfristig auch allen in der Schweiz aufenthaltsberechtigten Ausländerinnen und Ausländern zugänglich sein» Ist aufenthaltsberechtigigt die richtige Kategorie?</p>	<p>BJ, RS II</p>	
<p>Im Hinblick darauf, dass die eID-Funktion künftig allen Einwohnerinnen und Einwohnern der Schweiz zugänglich sein soll, und darum – wenn auch in separaten Projekten – künftig <u>eventuell</u> auch in den verschiedenen Ausländerausweisen enthalten sein könnte, entschied man sich für ein separates eID-Gesetz.                  =&gt; Gelöscht: insbesondere</p>	<p>BFM</p>	

<p><b>Ziffer 1.3 Konzept und Funktion der eID</b></p> <p><i>Ziff. 1.3 am Ende: Diverse eGov-Anwendungen</i></p> <p>Es sollte darauf hingewiesen werden, dass in jedem Bereich, in dem die eID von Behörden eingesetzt werden soll, die Zulässigkeit des Vorhabens unter allen relevanten Gesichtspunkten geprüft werden muss. Dazu gehören in jedem Fall die Frage, ob die vorgesehene Datenbearbeitung eine gesetzliche Grundlage hat (insbesondere bei Verwendung der AHV-Nummer), und die Frage, ob die Behörde das Vorweisen eines amtlichen Ausweises, genauer einer eID, verlangen darf.</p>	<p>BJ, RS II</p>	
<p><b>Ziffer 1.4 Ziele des Gesetzesentwurfs</b></p> <p>Teile davon können der Privatwirtschaft überlassen werden; der Staat muss aber ebenfalls weitere Beiträge leisten, namentlich:</p> <p>1) Die Koordination bei der Konzeption und Einführung eines gesamtschweizerischen eID-Ökosystems, das mit den in Entwicklung begriffenen IAM-Konzepten des Bundes und der vorstehend (Ziff. 1.1) erwähnten Verordnung (EU) Nr. xxx/2014 abgestimmt ist.</p> <p>Die Schweiz ist zwar nicht EU-Mitglied, aber in Anbetracht unserer engen Verflechtung mit vielen EU-Staaten und der globalen Natur von Online-Diensten im Internet wird in diesem Bereich Konformität und Kompatibilität mit dem europäischen Umfeld angestrebt.</p> <p>=&gt; Eventuell auch klarstellen, dass darüber hinaus keinerlei staatsvertragliche Verpflichtung zur Übernahme bestehen (Die VO ist namentlich nicht Schengen-relevant).</p> <p>Der IDK und der eID sind gemeinsam, dass sie eindeutig und insbesondere vertrauenswürdig einer konkreten Person zugeordnet sein müssen.</p> <p>=&gt; Gelöscht: ist</p>	<p>BJ, ERSD</p>	
<p><b>Ziffer 1.5 Staatliche elektronische Identifikationsmittel</b></p> <p>Die Schweiz befindet sich mit der Einführung eines elektronischen Identifikationsmittels nicht allein. In der am [Datum] verabschiedeten Verordnung (EU) Nr. .../2014 zu eID und Vertrauensdiensten und mit entsprechenden technischen Standards werden Rahmenbedingungen spezifiziert, die garantieren, dass die Interoperabilität zwischen den einzelnen länderspezifischen Systemen gewahrt wird. Das geplante eID-System richtet sich an diesen internationalen Vorgaben aus, so dass die schweizerische eID auch im internationalen Kontext eingesetzt werden kann.</p>	<p>BFM</p>	<p>BJ, ERSD</p>

<p>=&gt; Genaue Bezeichnung der verabschiedeten Verordnung inkl. ABl.-Fundstelle) angeben. Die in der FN angegebene Referenz ist ungenügend, da sie sich auf den Vorschlag und nicht den verabschiedeten Rechtsakt bezieht. Zudem hat das EP die Verordnung im April noch nicht verabschiedet (sondern nur seinen Standpunkt festgelegt). Zur Verabschiedung bedarf es der Unterschrift der Präsidenten von Rat und EP, nachdem beide Organe im Plenum der definitiven Fassung zugestimmt haben. Dies ist bisher nicht erfolgt.</p>		
<p><b>Ziffer 1.5.2 Europäische Harmonisierung und Interoperabilität</b>          Für die EU, die sich der Realisierung eines einheitlichen europäischen Binnenmarktes verpflichtet hat, ist dieses Anliegen besonders wichtig. <u>Da sie keine Kompetenz besitzt, die Ausweise für Staatsangehörige zu reglementieren</u>, hat sie vorerst die Aufenthaltspapiere für Drittstaatenangehörige detailliert standardisiert.          =&gt; Das trifft so nicht zu. Die EU-Ausweisverordnung (VO Nr. 2252/2004), eine WE des Schengen-Besitzstands, regelt durchaus die Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten.          =&gt; Gelöscht: schrankenlosen</p>	<p>BJ, ERSD</p>	
<p>Auch die Schweiz hat am 21. Mai 2008 diesen Standard im Rahmen <u>einer Schengen-Weiterentwicklung</u> übernommen. <u>Mit der Verordnung (EG) Nr. 380/2008 Verordnung wurden biometrische Daten auf einem Datenchip des einheitlichen Aufenthaltstitels, der in der Schweiz seit dem 12. Dezember 2008 für gewisse Drittstaatsangehörige auf Grundlage der Verordnung (EG) Nr. 1030/2002 ausgestellt wird, eingeführt.</u></p>	<p>BFM</p>	
<p><b>Ziffer 1.5.2.1 European Citizen Card (ECC)</b>          Nachdem die ersten europäischen Länder ihre elektronischen Identitätskarten zwar ähnlich aber doch unterschiedlich aufgebaut hatten, wurde schon vor etwa <u>zehn Jahren</u> der Ruf nach Standardisierung und Interoperabilität laut.          =&gt; Gelöscht: 10 Jahre</p>	<p>BFM</p>	
<p><b>Ziffer 1.5.2.2 eIDAS</b>          Am 3. April 2014 hat das Europäische Parlament den Vorschlag der Kommission für eine Verordnung über Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (COM(2012)0238) in erster Lesung behandelt und verabschiedet (Dokument P7_TA-PROV(2014)0282).          =&gt; Die Verordnung ist damit noch nicht verabschiedet, siehe dazu Bemerkung in Kom. Nr. 3.</p>	<p>BJ, ERSD</p>	



<p>Nebst der Regelung und Zertifizierung der Anbieterinnen und Anbieter der elektronischen Signatur und weiterer Vertrauensdienste in der <u>Art der bisherigen Richtlinie</u> enthält die neue Verordnung in den Artikeln 6 ff. =&gt; Welche?</p> <p>Die <u>eIDAS-Verordnung</u> bildet die rechtliche Grundlage für den länderübergreifenden eID-Einsatz, den das schon länger existierende und nachstehend in Ziffer 1.5.2.3 beschriebene Projekt STORK entwickelt. =&gt; Begrifflichkeit im ganzen Dokument abgleichen.</p> <p>Nach heutiger Planung soll die eIDAS-Verordnung Mitte 2016 in Kraft treten, zusammen mit umfangreicher Umsetzungs-Gesetzgebung auf tieferer Stufe. =&gt; Die Angaben zur Verabschiedung und zum Inkrafttreten sind noch sehr unklar, und für den unbefangenen Leser widersprüchlich.</p> <p>Selbstverständlich gibt es für die Schweiz keine rechtliche <u>Verpflichtung</u> zur Übernahme, <u>Umsetzung oder Anwendung</u> der EU-Verordnung. =&gt; Gelöscht: Verbindlichkeit</p> <p>Auch wenn <u>vorläufig</u> offen ist, ob, wann und wie die Schweiz sich staatsvertraglich in dieses System einbinden wird, soll das schweizerische eID-System von Beginn an so konzipiert werden, dass es grundsätzlich notifiziert werden könnte. =&gt; Warum vorläufig? Stehen entsprechende Entscheide an?</p> <p><b>Ziffer 1.5.3 Der neue elektronische Personalausweis in Deutschland</b></p> <p>Wie sich das Gesamtsystem in der breiten Anwendung <u>durchsetzen</u> wird, kann man zurzeit erst langsam abzuschätzen beginnen. Im Moment wird primär bemängelt, dass die Zertifizierung als Dienstanbieterin oder -anbieter zu aufwendig und zu teuer sei. =&gt; In welchem Verhältnis steht dieser deutsche Standard mit dem der EU und dem vorliegenden Projekt?</p>		
	<p>BJ, ERSD</p>	

<p><b>Ziffer 3.1.2 Personelle Auswirkungen</b>  <b>Ziff. 3.1.2 zweiter Absatz: Personelle Auswirkungen</b>                  Beziehen sich die Aussagen zu den Gebührenerhöhungen nur auf die Personalkosten oder auch auf die übrigen Kosten nach Ziffer 3.1.1?  <b>Ziff. 3.1.2 zweiter Absatz: «Vorgaben der für die Ausweise verantwortlichen Fachstellen»</b>                  Was sind das für Fachstellen, und gestützt worauf können sie Vorgaben machen?</p>	<p>BJ, RS II</p>	
<p><b>Ziffer 3.1.3 Andere Auswirkungen</b>  <b>Ziff. 3.1.3: Andere Auswirkungen</b>                  Z.B. hier sollte man aufzeigen, ob und inwiefern in den betreffenden Rechtsbereichen die Identifikation mittels eID unter dem neuen Recht zulässig und ausreichend wäre, insbesondere wenn die AHV-Nummer eingesetzt werden soll.</p>	<p>BJ, RS II</p>	
<p><b>Ziffer 3.4 Auswirkungen auf die Gesellschaft</b>  <b>Ziff. 3.4: Einsatz der eID gegen Phishing und Spam?</b> Es sollte aufgezeigt werden, wie der Einsatz der eID gegen Phishing und Spam wirken kann. Es ist auf den ersten Blick nicht ersichtlich, wie eine Karte, die nur eine Authentisierungsfunktion aufweist, diese Erscheinungen bremsen könnte.</p>	<p>BJ, RS II</p>	
<p><b>Ziffer 3.5 Auswirkungen auf die Umwelt</b>                  Die Vorlage hat keine direkten Auswirkungen auf die Umwelt. Grundsätzlich sollte ein vermehrter Wechsel von physischer zu elektronischer Abwicklung von Geschäften <u>per Saldo Ressourcen einsparen und sich entsprechend vorteilhaft für die Umwelt auswirken.</u>                  =&gt; Das ist eine etwas gar lapidare Behauptung, die ohne nähere Substantiierung der Gründe wenig aussagekräftig bleibt.</p>	<p>BJ, ERSD</p>	

<p><b>Ziffer 4.1 Verfassungsmässigkeit</b></p> <p>Beim eID-Gesetz handelt es sich um einen neuen Erlass. Analog zur Kompetenzdelegation im Ausweisgesetz kann sich der Erlass auf Artikel 38 Absatz 1 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV, SR 101) stützen. Artikel 38 BV gibt dem Bund die umfassende Kompetenz zur Regelung des Erwerbs und Verlusts des Bürgerrechts und somit auch die Kompetenz zur Ausgabe eines Ausweises, der die schweizerische Staatsangehörigkeit nachweist (BBl 2000 4751).</p> <p>=&gt; Gelöscht: und im Ausländergesetz</p> <p>=&gt; Gelöscht: resp. Artikel 121 Absatz 1</p> <p>=&gt; Gelöscht: Der Bund hat gestützt auf Artikel 121 Absatz 1 BV auch eine umfassende Kompetenz zur Gesetzgebung im Ausländerbereich (BBl 2002 3709)</p>	<p>BFM</p>	
<p><b>Ziffer 4.3 Delegation von Rechtsetzungsbefugnissen</b></p> <p><i>Ziff. 4.3: Delegation von Rechtsetzungsbefugnissen</i></p> <p>Hier müsste das Konzept aufgezeigt werden, nach dem die Gesamtmenge der nötigen Rechtsnormen auf die verschiedenen Normstufen verteilt werden soll. Selbstverständlich könnte dabei auch mit Verweisen auf den Detailkommentar gearbeitet werden, wenn die entsprechenden Erklärungen sich dort fänden.</p> <p>Die äusserst knappen Ausführungen treffen zudem nicht zu: Nach Artikel 17 Absatz 2 soll Fedpol Regelungsbefugnisse übertragen bekommen, nicht das EJPD.</p>	<p>BJ, RS II</p>	



<p><b>Ziffer 4.4 Datenschutz</b></p> <p><b>e) Einzelfragen zu den Erläuterungen, Ziff. 4.4</b></p> <ul style="list-style-type: none"><li>- Zweiter Aufzählungsstrich: Die Aussage trifft nur für das Auslesen und das Bestätigen von Identitätsattributen zu. Die anonyme und die pseudonyme Authentifizierung und das Bestätigen von abgeleiteten Behauptungen können ohne Zutun des Inhabers geschehen, auch unbemerkt.</li><li>- Dritter und vierter Aufzählungsstrich: Es ist gewiss zu begrüßen, dass die eID einen fein dosierten, an der Verhältnismässigkeit ausgerichteten Einsatz technisch erlauben soll. Hingegen garantiert das Bestehen der dargestellten technischen Möglichkeiten keineswegs, dass die vertrauenden Beteiligten tatsächlich immer die schonendste Einsatzvariante nutzen. Die am wenigsten schonende (das Auslesen aller Identitätsattribute inkl. AHV-Nummer) dürfte in fast allen Szenarien technisch am einfachsten und praktischsten sein, und wie bereits dargestellt fehlt jeder Mechanismus, der die Durchsetzung der Verhältnismässigkeit garantieren könnte.</li><li>- Fünfter Aufzählungspunkt: «Zwar findet keine umfassende Prüfung der Dienstanbieterinnen und anbieter statt ...». Es findet gar keine Prüfung statt; die Dienstanbieter werden einzig anhand ihrer UID identifiziert.</li><li>- Sechster Aufzählungsstrich: Le commentaire cite des liaisons chiffrées et des protections contre la manipulation sans que ces mesures ne soient imposées, à notre avis, par la loi. Le projet de loi ne cite pas même les obligations usuelles en matière de sécurité de données à la Confédération. Wie soll die Anwendung der sicheren Verfahren sichergestellt werden?</li></ul>	BJ, RS II	
--	-----------	--

Bemerkungen zu den einzelnen Bestimmungen der Erläuterungen (Ziffer 2)	Absender	Notizen
<p><b>Artikel 1 Absatz 1</b></p> <p>Buchstabe a zeigt zudem auf, dass sich eine eID auf verschiedenen vom Bund herausgegebenen Ausweisen befinden kann. In erster Linie ist das die Identitätskarte, später <u>könnten</u> die Ausländerausweise dazu kommen, und von der Konzeption her wäre es auch <u>möglich</u> weitere Ausweise, wie beispielsweise der Pass oder der Führerausweis, damit <u>auszurüsten</u>.</p> <p>=&gt; Gelöscht: sollen =&gt; Gelöscht: könnten =&gt; Gelöscht: auch =&gt; Gelöscht: ausgerüstet werden</p>	BFM	
<p><b>Artikel 1 Absatz 2</b></p> <p>Dies gelingt durch die Übernahme der geltenden Standards auf internationaler Ebene, die eine Interoperabilität bei der Anwendung der eID sicherstellen <u>sollen</u>.</p>	BFM	
<p><b>Artikel 2</b></p> <p>Bei der Wahl der Terminologie musste einerseits auf die aktuelle Regelung der Ausweisschriften, insbesondere das Ausweisgesetz Rücksicht genommen werden. Neue Begriffe wurden <u>so gut wie möglich</u> mit den Regelungen der EU und der umliegenden Länder abgeglichen.</p> <p>=&gt; Was heisst das genau? Inwiefern ist der Abgleich nicht gelungen? Wo gibt es noch Unterschiede?</p>	BJ, ERSD	
<p><b>Artikel 3</b></p> <p>Hingegen soll auf der eID der Geburtsort anstelle des Heimatorts als Identitätsattribut verzeichnet werden. <u>Das</u> entspricht der internationalen Praxis.</p> <p>=&gt; Gibt es hier normative Vorgaben, auf die Bezug genommen werden könnte?</p>	BJ, ERSD	
<p><b>Artikel 5 Absatz 1</b></p> <p>Zu Art. 5 Abs. 1: <i>Darstellung des geltenden Rechts</i></p> <p>Die Erläuterungen sollten aufzeigen, welche Regelungen auf Verlust und Diebstahl aller erfassten Trägerausweistypen anwendbar sind.</p>	BJ, RS II	

<p><b>Artikel 6</b></p> <p><i>Zu Art. 6: Haftung nach Art. 41 OR</i></p> <p>Sind diese Ausführungen mit ZZ abgesprochen? Es scheint uns, dass Artikel 41 OR zumindest auf jene Fälle nicht anwendbar ist, wo einer Behörde aufgrund einer Pflichtverletzung eines eID-Inhabers ein Schaden entsteht.</p>	BJ, RS II	
<p><b>Artikel 6 Absatz 3</b></p> <p><i>Zu Art. 6 Abs. 3: Ablauf bei der Änderung von Identitätsattributen</i></p> <p>Der Ablauf, der bei der Änderung von Identitätsattributen von Amtes wegen ablaufen und die eID miterfassen soll, sollte hier mitsamt seinen Rechtsgrundlagen dargestellt werden.</p>	BJ, RS II	
<p><b>Artikel 7 Absatz 3</b></p> <p><i>Zu Art. 7 Abs. 3: Prüfung ungültiger eIDs</i></p> <p>Hier sollte erklärt werden, warum es nötig ist, dass auch ungültige eIDs überprüft werden können.</p>	BJ, RS II	
<p><b>Artikel 9</b></p> <p>Article 9</p> <p>Le rapport explicatif ne mentionne pas quelles données figureront sur la liste de blocage publique. Il est nécessaire d'indiquer à l'article 9 quelles données seront rendues accessibles de manière publique.</p>	EDÖB	
<p><b>Artikel 10</b></p> <p><i>Art. 10: Schnittstellen gemäss Erläuterungen?</i></p> <p>Laut den Erläuterungen betreibt Fedpol «auch die notwendigen Schnittstellen zu den kantonalen und kommunalen Behörden». Wie muss man sich diese Schnittstellen vorstellen? Sind technische Geräte, Datenübermittlungswege oder organisatorische Vorkehren gemeint?</p>	BJ, RS II	
<p><b>Artikel 11</b></p> <p><i>Zu Art. 11, letzter Absatz: Nutzungsbedingungen</i></p> <p>Das vorgesehene Vorgehen ist bei Angeboten privater Anbieter üblich, passt aber nicht für die Ausstellung von staatlichen Identitätsdokumenten. Die Rechte und Pflichten der Antragsteller ergeben sich nicht aus irgendwelchen Allgemeinen Geschäftsbedingungen (AGB), sondern abschliessend aus der Gesetzgebung. Diese ist so auszugestalten, dass sie alle nötigen Bestimmungen enthält. Der Hinweis auf die Bestätigung der «Akzeptanz der Nutzungsbedingungen» ist ersatzlos zu streichen.</p>	BJ, RS II	



<p><b>Artikel 15</b></p> <p><b>Zu Art. 15: Vertrauenswürdigkeit aufgrund UID?</b></p> <p>Der Verzicht auf ein «aufwändiges Zertifizierungsverfahren» (wohl eher: Bewilligungs- oder Zulassungsverfahren) wird damit begründet, dass das Innehaben einer UID (die einzige Voraussetzung für den Zugriff auf die eID!) die Identifikation der betreffenden Akteure erlaube. Das greift wohl zu kurz. Die Existenz einer UID-Einheit bietet kaum Gewähr für einen verantwortungsvollen Umgang mit den Möglichkeiten, die die eID bieten soll (insb. routinemässiges Auslesen der AHV-Nummer). Selbstverständlich kann auch ein aufwändiges Zulassungsverfahren mit strengen Voraussetzungen und intensiver Aufsicht einen verantwortungsvollen Umfang nicht mit Sicherheit garantieren. Aber es sollten doch die Vor- und Nachteile diskutiert werden, die ein Zulassungssystem mit echten Anforderungen und deren Prüfung durch die Zulassungsbehörde mit sich bringen würde.</p> <p><b>Zu Art. 15: Ausländische vertrauende Beteiligte</b></p> <p>Die eID soll ja insbesondere auch für internationale Kontakte genutzt werden können. Wie gelangen ausländische vertrauende Beteiligte an ein Berechtigungszertifikat? Gibt es hier Unterschiede für Private und Behörden?</p>	<p>BJ, RS II</p>	
<p><b>Artikel 16</b></p> <p><b>Zu Art. 16: Prüfung der Gültigkeit der Berechtigungszertifikate durch die eID</b></p> <p>Es sollte (natürlich auf einem für Laien zugänglichen technischen Niveau) dargestellt werden, wie die eID prüfen kann, ob ein Berechtigungszertifikat gültig ist, insbesondere ob es widerrufen wurde.</p> <p><b>Zu Art. 16: Software-Development-Kit</b></p> <p>Es bestehen rechtliche Zweifel, ob es zulässig ist, dass der Staat quelloffene Software zur Verfügung stellt (was wohl beabsichtigt ist). Ein Gutachten von Georg Müller und Stefan Vogel im Auftrag des ISB zu dieser und verwandten Fragen soll nach den Sommerferien verfügbar werden. Je nachdem kann es sinnvoll sein, das vorgesehene Software-Angebot im Gesetz explizit vorzusehen (falls es sich verfassungsrechtlich als zulässig erweist, versteht sich).</p>	<p>BJ, RS II</p>	
<p><b>Artikel 17</b></p> <p><b>Zu Art. 17 / Ziff. 4.3</b></p> <p>Der Verweis auf Ziffer 4.3 führt nicht zu interessanten Erläuterungen zur Vollzugsklausel. Insbesondere findet sich keine Begründung des begründungsbedürftigen Absatz 2.</p>	<p>BJ, RS II</p>	

<p><b>Ziffer 2.3.1.2 Änderung von Art. 4a AwG</b></p> <p><b>Ziff. 2.3.1.2: Änderung von Art. 4a AwG</b></p> <p>Wir haben Zweifel, ob die Ausführungen zum technischen Aufwand, der durch die Änderung verursacht wird, zutreffen. Die Aufhebung der Beschränkung auf die kantonalen Behörden gilt nicht nur für Anträge auf Ausweise mit eID, sondern auch für die ePass-Funktion, die die Erfassung biometrischer Daten voraussetzt. Würde somit die Änderung nicht dazu führen, dass die betreffenden Gemeinden auch die Biometrie-Geräte anschaffen müssten?</p>	<p>BJ, RS II</p>
---	------------------

Anträge	Absender	Notizen
<p>Aux motifs de ce qui précède, l'OFAS demande:</p> <ul style="list-style-type: none"> <li>- de biffer l'art. 3, al. 1, let. j, de l'avant-projet et</li> <li>- de biffer l'introduction de l'art. 51, al. 3bis, LAVS</li> </ul> <p>Pour conclure dans ce contexte, l'OFAS plaide en faveur de l'examen d'autres possibilités, comme l'utilisation d'un identificateur sectoriel de personnes qui serait déduit du numéro AVS et que la Centrale de compensation mettrait à disposition des utilisateurs qui doivent recourir à un identificateur univoque de personnes.</p>	<p>BSV</p>	
<p>Das BBL beantragt die Überarbeitung des erläuternden Berichts zum Vorentwurf in folgendem Sinne:</p> <ul style="list-style-type: none"> <li>- Die Personalisierung von Ausweisschriften mit biometrischen Daten ist eine hoheitliche Aufgabe des Bundes. Deshalb soll die künftige biometrische eID analog dem Schweizer Pass beim BBL personalisiert werden.</li> <li>- Die öffentliche Ausschreibung ist analog der Ausschreibung für den CHP03 auszugestalten, so dass die Konzeption der eID sowie die Lieferung der Materialien und Maschinen durch die Privatwirtschaft erfolgen und die Personalisierung beim EFD/BBL wahrgenommen wird (vgl. Vorgehensvorschlag, Ziff. 4.).</li> </ul> <p>Überdies ist gemäss Vorentwurf des eID-Gesetz, vgl. Art. 7, neben dem als Herausgeber genannten EJPD, das Bundesamt für Bauten und Logistik für die als Personalisierung zuständige Stelle der eID aufzuführen:</p> <p>Art. 7 Herausgeber und Personalisierungsstelle</p> <p>1 Herausgeber der eID ist das Bundesamt für Polizei (fedpol). Es führt ein Informationssystem über die ausgestellten eID und betreibt die für die Herausgabe, Verwaltung und Auskunftserteilung notwendige Infrastruktur.</p> <p>2 Die zuständige Stelle für die Personalisierung der eID mit biometrischen Daten ist das Bundesamt für Bauten und Logistik (BBL).</p>	<p>BBL</p>	



<p><b>Diverses</b></p> <p><u>Documents de la consultation</u></p> <p>Avec les documents de la consultation des offices, nous vous prions à l'avenir de toujours livrer les lettres d'accompagnement, la liste des destinataires, ainsi que la fiche d'information avec un résumé de l'affaire dans les trois langues. En l'espèce, nous devons examiner ces documents dès que possible, mais encore avant l'ouverture de la procédure de co-rapport. Nous vous prions donc de nous les envoyer pour examen dès que possible.</p> <p><u>Link à la fiche d'information :</u> <a href="http://intranet.bk.admin.ch/themen/gesetz/01330/index.html?lang=de&amp;download=NHZLpZeg7t.lnp610NTU042l2Z6Inlacy4Zn4Z2qZpnO2Yug2Z6gpJCHdIJ3fWym162epYbg2c_JJKbNoKSn6A--">http://intranet.bk.admin.ch/themen/gesetz/01330/index.html?lang=de&amp;download=NHZLpZeg7t.lnp610NTU042l2Z6Inlacy4Zn4Z2qZpnO2Yug2Z6gpJCHdIJ3fWym162epYbg2c_JJKbNoKSn6A--</a></p> <p><u>Link aux informations sur la procédure de consultation :</u> <a href="http://intranet.bk.admin.ch/roter_ordner/06775/06813/index.html?lang=de">http://intranet.bk.admin.ch/roter_ordner/06775/06813/index.html?lang=de</a></p> <p><u>Publication des documents de la consultation</u></p> <p>Afin que nous puissions publier les documents sur le site officiel de la Confédération des procédures de consultation, nous vous prions de les envoyer à <a href="mailto:vernehmlassungsunterlagen@bk.admin.ch">vernehmlassungsunterlagen@bk.admin.ch</a> dans les trois langues en format pdf (format Word pour la fiche d'information) immédiatement après que la décision du Conseil fédéral sera prise, soit le jour même.</p>	BK	
--	----	--

