

ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E. V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E. V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E. V. BERLIN-BONN ·
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Stellungnahme des Zentralen Kreditausschusses zur geplanten Einführung des elektronischen Personalausweises

(Entwurf der Bundesregierung für ein Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften
– BR-Drs 550/08 sowie Grobkonzept – Version 2.0 zur Einführung des elektronischen Personalausweises in Deutschland)

3. November 2008

Die deutsche Kreditwirtschaft begrüßt die mit dem Gesetzesvorhaben der Bundesregierung angestrebte Einführung des elektronischen Personalausweises (ePA), da damit ein wichtiger Beitrag zur Sicherung und Vereinfachung des elektronischen Rechts- und Geschäftsverkehrs im Internet geleistet wird. Die Bundesregierung stützt sich in der Gesetzesvorlage auf die Annahme, dass zum Zeitpunkt der Einführung des elektronischen Personalausweises bereits Anwendungen der Wirtschaft und der öffentlichen Verwaltungen für den elektronischen Identitätsnachweis bereit stehen, damit sogleich für den Bürger ein greifbarer Nutzen für diese neue Funktion des Personalausweises erkennbar ist. In diesem Zusammenhang wird insbesondere das Online Banking als eine prädestinierte Anwendung für den elektronischen Identitätsnachweis genannt¹. Damit tatsächlich der angestrebte Nutzen erreicht wird, sollten aus Sicht der deutschen Kreditwirtschaft folgende Punkte im weiteren Gesetzgebungsverfahren berücksichtigt werden:

1. Einsatz des ePA im Online-Banking

Im Hinblick auf den Einsatz des elektronischen Personalausweises im Online Banking ist festzustellen, dass der elektronische Identitätsnachweis keine Banktransaktionsdaten, sondern nur vom ePA ausgegebene Identifikationsdaten absichern kann. Im Grobkonzept für die Einführung des elektronischen Personalausweises in Deutschland wird zwar dargelegt, dass mit Hilfe des Berechtigungszertifikates des Diensteanbieters eine sichere Verbindung aufgebaut und diese dazu genutzt werden könne, die auf die Identifizierung folgende Transaktion abzusichern. Jedoch geht

¹ so u.a. in Kapitel 8.2.1 des Grobkonzeptes für die Einführung des elektronischen Personalausweises in Deutschland

aus den bisher veröffentlichten Unterlagen nicht hervor, wie beispielsweise Angriffe, bei denen Banking-Trojaner auf dem PC des Kunden in Echtzeit Transaktionsdaten verändern, mit dem elektronischen Identitätsnachweis wirksam unterbunden werden können.

Dem Zentralen Kreditausschuss sollten die detaillierten technischen Protokolle des ePA inklusive eines umfassenden und begutachteten Sicherungskonzeptes rechtzeitig im Vorfeld zur Verfügung gestellt werden, um nachfolgend eine mögliche Eignung des ePA für den Einsatz im Online Banking weitergehend bewerten zu können.

2. Bedeutung des ePA für bestehende Authentisierungsinfrastrukturen in der Kreditwirtschaft und etwaige Einsparungseffekte

Die Bundesregierung geht davon aus, dass Diensteanbieter durch die Nutzung des elektronischen Identitätsnachweises auf den Einsatz eigener Authentisierungsinfrastrukturen verzichten könnten und sich damit deutliche Einsparungspotenziale ergäben². Hierbei muss jedoch bedacht werden, dass eine Authentisierungsinfrastruktur auf Basis des elektronischen Personalausweises voraussichtlich nur ergänzend im Online Banking und parallel zu den etablierten kreditwirtschaftlichen Verfahren zum Einsatz kommen kann, da davon ausgegangen werden muss, dass selbst bei einer entsprechenden Einführungsstrategie zunächst nicht alle Kunden den elektronischen Personalausweis im Internet nutzen werden.

Daher sind Einsparungseffekte nicht zwingend zu erwarten. Vielmehr wären mit der Unterstützung des ePA zunächst höhere Kosten für die Kreditwirtschaft verbunden. Da zudem nach Aussage der Bundesregierung die Kosten für den Aufbau und Betrieb der Public-Key-Infrastruktur für Berechtigungszertifikate sowie die Kosten für deren Ausstellung über Gebühren der Diensteanbieter getragen werden sollen, dürfte die von der Kreditwirtschaft zu tätige Investitionsentscheidung außerdem maßgeblich von diesen Kosten abhängen. Mithin sind eine valide Abschätzung der Kosten³ und insbesondere konkrete Aussagen über Art und Höhe der Bepreisung der Berechtigungszertifikate von entscheidender Bedeutung. Dem Vernehmen nach wird derzeit vom BMI ein Konzept erstellt, wie die Ausgabe der Berechtigungszertifikate bepreist werden soll. Um eine größtmögliche Marktakzeptanz herbeizuführen, sollte die Wirtschaft bei der Festlegung des Preismodells beteiligt werden.

² so z.B. in der Begründung zum Gesetzentwurf auf Seite 19.

³ Die in der Gesetzesbegründung enthaltene Kostenschätzung ist an vielen Stellen nicht nachvollziehbar. Beispielsweise wird von 500.000 Beantragungen von Berechtigungen pro Jahr ausgegangen. Pro Berechtigung sollen jedoch alle zwei bis drei Tage neue Berechtigungszertifikate ausgegeben werden, die in die Systeme der Diensteanbieter sicher integriert werden müssen. Dieser Kostenfaktor wird jedoch nicht erwähnt.

In diesem Zusammenhang wäre auch zu berücksichtigen, dass die Kreditwirtschaft seit Jahren den Aufbau einer Kartenleserinfrastruktur für das Online Banking gefördert hat. Mehr als eine Million Online-Banking-Nutzer in Deutschland nutzen bereits heute chipkartenbasierte Verfahren im Internet. Diese bestehende Infrastruktur ist für den geplanten kontaktlosen Ausweis nicht nutzbar. Die Einführung des elektronischen Personalausweises als kontaktlose Chipkarte würde vielmehr zum Aufbau einer zweiten kontaktlosen Infrastruktur führen und wirkt damit den bisherigen Aktivitäten der Kreditwirtschaft entgegen. Da auch andere Kartenprojekte der eCard-Strategie wie die elektronische Gesundheitskarte kontaktbehafte Chipkarten einsetzen, würde es sich aus Sicht der Kreditwirtschaft anbieten zu prüfen, ob nicht in Hinblick auf eine gemeinsame Kartenstrategie der ePA als Hybridkarte ausgerichtet werden könnte. Dies dürfte zudem den Aufbau einer für alle Arten von Chipkarten interoperablen Einsatzumgebung beim Bürger erheblich erleichtern.

Die Kreditwirtschaft hat sich in der Vergangenheit immer für die Auslegung des elektronischen Personalausweises als Hybridkarte ausgesprochen. Eine einseitige Förderung der kontaktlosen Chipkartentechnologie würde der – ursprünglich auch mit der Wirtschaft abgestimmten – eCard-Strategie der Bundesregierung zuwider laufen.

3. Nutzung des ePA bei der Kontoeröffnung

Seitens der Bundesregierung wird als ein weiteres kreditwirtschaftliches Anwendungsszenario die Kontoeröffnung über das Internet genannt⁴. Die diesbezüglichen rechtlichen Anforderungen an Kreditinstitute ergeben sich im Wesentlichen aus dem Geldwäschegesetz (GwG), der Abgabenordnung (AO) und aus den zivilrechtlichen Anforderungen an den Vertragsabschluss. Fraglich ist, ob durch den vorliegenden Entwurf des Personalausweisgesetzes (PAuswG) diese Anforderungen als erfüllt gelten können und auch durch die Bankenaufsicht mitgetragen werden.

In § 18 PAuswG, Absatz 3 werden abschließend die Daten aufgezählt, welche im Rahmen des elektronischen Identitätsnachweises übermittelt werden dürfen. Demnach können weder die Staatsangehörigkeit noch Art, Nummer und ausstellende Behörde des zur Identifizierung herangezogenen Dokumentes im Rahmen der elektronischen Identifizierung erfasst werden. Um – wie in Artikel 5 „Änderung des Geldwäschegesetzes“ vorgesehen – eine Kontoeröffnung über das Internet mit dem ePA zu ermöglichen, muss demnach sichergestellt sein, dass sich die in § 8 GwG formulierte Anforderung an die Erfassung von Art, Nummer und ausstellende Behörde des zur Identifizierung herangezogenen Dokumentes nicht auf die Identifizierung nach § 6 Absatz 2 Nr. 2 Satz 1 GwG bezieht, bei der der Vertragspartner des zur Identifizierung Verpflichteten nicht physisch

⁴ so z.B. Grobkonzept, Kapitel 8.2.1

anwesend sein muss. Die Staatsangehörigkeit könnte implizit aus der Art des Dokumentes abgeleitet werden, da der ePA nur für deutsche Staatsangehörige ausgegeben wird.

Bei der Kontoeröffnung kommt der Dokumentation, dass das Kreditinstitut seiner Identifizierungspflicht nachgekommen ist, große Bedeutung zu. Hierfür wäre klarzustellen, dass der Herkunftsnachweis der Identitätsdaten ausschließlich durch die Prozesssicherheit beim Diensteanbieter und dessen Protokollierung gewährleistet werden kann, da der elektronische Identitätsnachweis selbst keinen dauerhaft abgesicherten Nachweis über die Herkunft der Daten liefert.

Ferner ist Folgendes zu berücksichtigen: Bei der Kontoeröffnung im Internet muss darüber hinaus ein zivilrechtlich gültiger Vertrag abgeschlossen werden. Dieser unterliegt an sich zwar grundsätzlich keinem besonderen gesetzlichen Formerfordernis, insbesondere nicht dem Schriftformgebot nach § 126 BGB. Bei bestimmten Bankgeschäften ist das Schriftformgebot allerdings einzuhalten. Dies gilt derzeit beispielsweise bei Verbraucherdarlehensverträgen im Sinne des § 492 BGB oder der Stellung einer Bürgschaft gemäß § 766 BGB. Außerdem ist zu bedenken, dass allein zur Dokumentation und Beweissicherung Kontoeröffnungsverträge – auch im Fernabsatz – in der Regel schriftlich abgeschlossen werden, das heißt eine entsprechende Vertragsurkunde ist vom Kunden zu unterzeichnen. Zugleich wird damit auch eine Unterschriftenprobe des Kunden eingeholt, um im Rahmen der Geschäftsbeziehung bei beleghaft erteilten Aufträgen die Echtheit der Unterschrift prüfen zu können. Bislang erfolgt im Fall der Eröffnung von Online Konten ein solcher schriftlicher Abschluss des Kontoeröffnungsvertrages – und damit verbunden die Einholung der Unterschriftenprobe – in der Praxis meist unter Verwendung des PostIdent-Verfahrens. Dabei wird die Identifizierung des Kunden anhand des Personalausweises durch Postbedienstete durchgeführt und eine Unterschrift des Kunden eingeholt. Die bei der Identifizierung erhobenen Daten nebst Unterschrift werden dann an das Kreditinstitut übermittelt.

Der elektronische Identitätsnachweis des ePA kann deshalb das PostIdent-Verfahren oder andere vergleichbare Verfahren unter Einschaltung geeigneter Dritter bei der Identifizierung nur dann vollständig ersetzen, wenn auch eine Unterschriftenprobe zusammen mit den Identitätsdaten elektronisch gesichert übermittelt wird. Dies ist bislang nicht vorgesehen. Es würde es sich deshalb anbieten, Kreditinstituten die Berechtigung einzuräumen, zusammen mit Daten des elektronischen Identitätsnachweises auch die Unterschriftenprobe sowie einen geeigneten Nachweis über die Herkunft der Daten – beispielsweise dem dienste- und kartenspezifischen Kennzeichen – elektronisch gesichert aus dem ePA auszulesen.

Im PAuswG sollten darum die rechtlichen Voraussetzungen geschaffen werden, eine Unterschriftsprobe zusammen mit Daten des elektronischen Identitätsnachweises, beispielsweise dem dienste- und kartenspezifischen Kennzeichen, elektronisch gesichert aus dem ePA auslesen zu dürfen.

Um bei einer Kontoeröffnung im elektronischen Geschäftsverkehr die bisherigen Medienbrüche zu vermeiden, würde es sich zudem anbieten, den Kontoeröffnungsvertrag vollelektronisch mit Hilfe der qualifizierten elektronischen Signatur abzuschließen. Das hierfür erforderliche qualifizierte Zertifikat muss vom Bürger jedoch ausdrücklich beantragt werden und ist kostenpflichtig. Daher kann zu Beginn der Einführung des ePA nicht von einer vollständigen Ausstattung aller ePA mit qualifizierten Zertifikaten ausgegangen werden. Außerdem muss das qualifizierte Zertifikat dem Antragsteller eindeutig zugewiesen werden können; in der Regel reichen hierfür die Angaben zum Zertifikatsinhaber im Zertifikat nicht aus. Um als Kreditinstitut bei der Zuordnung von qualifizierten Zertifikat zum Antragsteller Medienbrüche zu vermeiden, sollten Kreditinstitute daher berechtigt sein, das qualifizierte Zertifikat zusammen mit Daten des elektronischen Identitätsnachweises, beispielsweise dem dienste- und kartenspezifischen Kennzeichen, elektronisch gesichert aus dem ePA auslesen zu dürfen. Darüber hinaus sollte der Diensteanbieter bei der Ausgabe eines neuen ePA nach Ablauf der Gültigkeit des alten ePA die Möglichkeit haben, die Kontinuität zwischen altem und neuem ePA herzustellen.

Im PAuswG sollten die rechtlichen Voraussetzungen geschaffen werden, das qualifizierte Zertifikat zusammen mit Daten des elektronischen Identitätsnachweises, beispielsweise dem dienste- und kartenspezifischen Kennzeichen, elektronisch gesichert aus dem ePA auslesen zu dürfen.

4. Verwendung des ePA im Zusammenhang mit Vertragsabschlüssen im Internet

In den öffentlichen Verlautbarung der Bundesregierung wird der Eindruck vermittelt, der elektronische Identitätsnachweis des ePA könne auch für Willenserklärungen im Rahmen des elektronischen Geschäftsverkehrs im Internet genutzt werden. Um vorzubeugen, dass der Bürger nicht genau zwischen elektronischer Identifizierung und rechtsverbindlicher elektronischer Unterschrift nach Signaturgesetz unterscheiden kann, sollte der Bürger bei der Ausgabe des ePA insbesondere über die Bedeutung der jeweils mit den unterschiedlichen elektronischen Funktionen verbundenen PIN ausdrücklich unterrichtet werden.

5. Konkretisierung technischer Verfahrensdetails per Rechtsverordnung

In dem vorliegenden Entwurf des PAuswG werden bereits einige technische Rahmenbedingungen festgelegt. Folgende Punkte des Gesetzesentwurfs sollten dabei aus Sicht der Kreditwirtschaft geprüft werden:

- Das Berechtigungszertifikat des Diensteanbieters soll nach § 18 Absatz 4 PAuswG neben Name und Anschrift die E-Mail-Adresse des Diensteanbieters enthalten. Hierbei stellt sich die Frage, welche Rechtsfolgen mit der Angabe der E-Mail-Adresse verbunden sein sollen. Für die Identifizierung von Diensteanbietern im elektronischen Geschäftsverkehr hat sich die Webadresse (URL) durchgesetzt.
- Aufgrund der hohen Austauschfrequenz (alle zwei bis drei Tage) muss die Bereitstellung der Berechtigungszertifikate über einen vollständig automatisierten Prozess erfolgen können. In der Pilotierungsphase könnte es sich außerdem anbieten, die Gültigkeitsdauer der Berechtigungszertifikate der Risikosituation entsprechend flexibel durch die Vergabestelle festlegen zu lassen und die Gültigkeitsdauer nicht auf Ebene des Gesetzes festzulegen.
- Nach § 27 Absatz 3 PAuswG soll das Bundesamt für Sicherheit in der Informationstechnik die Systeme und Komponenten der Einsatzumgebung für den ePA zertifizieren. Diese Aufgabe sollten auch privatwirtschaftliche Prüflabore übernehmen können.

Nach § 34 PAuswG sollen weitere technische Details zum ePA in einer Rechtsverordnung geklärt werden. Da diese Details oft entscheidend für die Praktikabilität und Kosten des Verfahrens sind, sollte die Wirtschaft an der Abstimmung der Rechtsverordnung beteiligt werden.