Alexander Roßnagel, Gerrit Hornung, Christoph Schnabel

Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht

Der neue elektronische Personalausweis wird unter anderem die Möglichkeit der Authentisierung des Ausweisinhabers in Online-Verbindungen bieten. Diese Funktion bietet weitreichende Möglichkeiten im E-Government und im E-Commerce, beinhaltet aber auch datenschutzrechtliche Risiken. Der Beitrag untersucht rechtliche Fragen der Authentisierungsfunktion und legt dabei einen Schwerpunkt auf das Datenschutzrecht. Er beruht auf einem Gutachten, das die Verfasser im Herbst 2007 für das Bundesministerium des Innern angefertigt haben.

Prof. Dr. Alexander Roßnagel

Vizepräsident der Universität Kassel, Prof. für Öffentliches Recht, Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken
E-Mail: a.rossnagel@uni-kassel.de

Dr. Gerrit Hornung, LL.M.

Geschäftsführer von provet und Wissenschaftlicher Mitarbeiter an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

Ass. iur. Christoph Schnabel, LL.M.

Mitglied von provet und Wissenschaftlicher Mitarbeiter an der Universität Kassel
E-Mail: c.schnabel@uni-kassel.de

1 Hintergrund

Der elektronische Personalausweis soll den bisherigen Personalausweis so fortentwickeln, dass er seine Grundaufgabe des Identitätsnachweises in Zukunft auch in elektronischen Rechts- und Geschäftsprozessen erfüllen kann. Dazu wird er drei grundsätzliche Funktionalitäten vereinen.[1] Die hoheitliche Ausweisfunktion wird – wie schon beim elektronischen Reisepass – um biometrische Daten des Gesichts und zweier Finger erweitert. Die Authentisierungsfunktion ermöglicht den elektronischen Nachweis der Identität sowohl in Online-Anwendungen als auch in lokalen Verarbeitungsprozessen. Die optionale Signaturfunktion schafft für die Ausweisinhaber die Voraussetzungen dafür, im elektronischen Rechtsverkehr Erklärungen abzugeben, die hinsichtlich Integrität und Authentizität dauerhaft beweisbar sind.

Während die Einführung biometrischer Daten im Wesentlichen dieselben technischen und rechtlichen Fragen aufwirft wie beim neuen Reisepass,[2] ergeben sich bei den Signatur- und Authentisierungsfunktionen grundlegend neue Probleme des Verfassungs-, Verwaltungs-, Datenschutz- und Signaturrechts.[3] Die folgenden Ausführungen beschränken sich auf die datenschutzrechtliche Bewertung der Authentisierungsfunktion.

2 Authentisierungskonzept und Anwendungsbeispiele

Die Authentisierungsfunktion wird standardmäßig bereitgestellt, der Ausweisinhaber kann sie aber ablehnen. Stimmt er zu, so erhält er die Möglichkeit, durch Eingabe einer PIN die Daten (die bislang aufgedruckten Daten mit Ausnahme der Personalausweisnummer, überdies ggf. Attribute wie bestimmte Altersgrenzen oder Wohnort) mithilfe der Authentisierungsfunktion einem Diensteanbieter zu übermitteln.[4] Allerdings wird nicht jeder Anbieter auf die Daten zugreifen können, sondern nur solche, die zuvor von einem „Access-Verifier" – der zumindest in der

1 S. näher *Reisen*, DuD 2008 (in diesem Heft).

2 S. zu diesem *Roßnagel/Hornung*, DÖV, 2005, 983 ff.; *Pallasky*, Datenschutz in Zeiten globaler Mobilität, 2007, 30 ff.; zur Biometrie in Personalausweisen *Reichl/Roßnagel/Müller*, Digitaler Personalausweis, 2005; *Hornung*, Die digitale Identität, 2005.

3 Diese werden im Gutachten für das Bundesministerium des Innern ausführlich behandelt; zur Signaturfunktion s. bereits *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller (Fn. 2), 91 ff., 219 ff.; *Hornung*, (Fn. 2), 319 ff.

4 Zu technischen Sicherheitsmerkmalen s. *Bender/Kügler/Margraf/Naumann*, DuD 2008 (in diesem Heft).

Anfangszeit eine staatliche Stelle sein wird – ein Zugriffszertifikat zugeteilt bekommen haben. Das Zugriffszertifikat beschränkt den Zugriff des Diensteanbieters technisch auf die Daten, die für die Erbringung des jeweils konkreten Dienstes tatsächlich notwendig sind. Es wird auch Angaben über den Diensteanbieter, dessen Datenschutzaufsichtsbehörde, Angaben zu seinen Berechtigungen für den Zugriff auf einzelne Datenfelder und den Erhebungs- und Verarbeitungszweck enthalten.

Die neuartige Authentisierungsfunktion kann überall dort eingesetzt werden, wo bisher rechtlich oder faktisch die Vorlage des Personalausweises verlangt wird, ohne dass die gleichzeitige Anwesenheit der zu authentisierenden Person aus anderen Gründen als der Vorlage des Ausweises selbst zwingend erforderlich ist. Dies betrifft vor allem die Stellung von Anträgen oder die Anmeldung zu Prüfungen.[5] Soweit diese Verfahren online abgewickelt werden können, kann die Authentisierung grundsätzlich mithilfe des elektronischen Personalausweises online vorgenommen werden.

Ein wichtiges Anwendungsbeispiel der Authentisierungsfunktion und ihrer datenschutzfreundlichen Ausgestaltung stellt der Zugriff auf Inhalte dar, die nur Personen ab einem bestimmten Alter – vor allem Erwachsenen – zugänglich gemacht werden dürfen. So stellen etwa pornographische Angebote einen erheblichen Anteil am Electronic Commerce im Internet. In Deutschland müssen hierfür die strengen Anforderungen des Jugendmedienschutzes beachtet werden. In Deutschland ansässige Anbieter müssen zuverlässige Altersverifikationssysteme betreiben, um nicht gegen § 4 Abs. 2 JMStV, § 15 Abs. 2 JuSchG und § 184 StGB zu verstoßen.[6] An diese werden in der Rechtsprechung hohe Anforderungen gestellt.[7] Auch bei Gratis-Angeboten ist eine Identifikation der Nutzer erforderlich, was aufgrund der sozialen Ächtung, die mit dem Konsum von Pornographie einhergeht, zu einem erheblichen Wettbewerbsnachteil für deutsche Anbieter führt. Diese Probleme können durch die Authentisierungsfunktion des elektronischen Personalausweises in Zukunft vermieden werden.

3 Freie Wahl der Authentisierungsfunktion

Die Authentisierungsfunktion wird auf dem elektronischen Personalausweis zwar standardmäßig bereitgestellt, der Ausweisinhaber kann aber entscheiden, ob er die Funktion überhaupt nutzen möchte. Der Brief mit der PIN, die zur Verwendung benötigt wird, wird mit der Mitteilung übersandt, dass der Ausweis zur Abholung bereitliegt. Wenn ein Bürger die Authentisierungsfunktion nicht nutzen möchte, teilt er dies bei Abholung seines neuen Personalausweises mit und übergibt den noch verschlossenen PIN-Brief der Behörde.

Die Freiwilligkeit der Anwendung ist im Sinn informationeller Selbstbestimmung vorbildlich. Ein einziger Kritikpunkt könnte darin zu sehen sein, dass es sich bei dem vorgeschlagenen Verfahren um eine Opt-out-Lösung handelt. Opt-out-Verfahren sind grundsätzlich datenschutzrechtlich bedenklich, weil die Gefahr besteht, dass die Möglichkeit der Verweigerung übersehen oder aus Nachlässigkeit nicht wahrgenommen wird.[8] Allerdings erscheinen diese Probleme beim elektronischen Personalausweis beherrschbar, weil eine Informationskampagne die Einführung des neuen Ausweises begleiten wird und ein aktives Tun (Abholen des Ausweises) erforderlich ist, in dessen Rahmen ein persönlicher Kontakt erfolgt.

Das Begleitschreiben zum PIN-Brief muss (vergleichbar mit der Unterrichtung nach § 6 SigG)[9] optisch und sprachlich so gestaltet sein, dass für jeden Bürger die Bedeutung und Funktion der Authentisierungsfunktion, die Möglichkeit der Rückgabe des Briefs und die Rechtsfolgen einer Nicht-Rückgabe klar ersichtlich sind. Dies ist aus zwei Gründen erforderlich: Zum einen hat sich der Staat dazu entschlossen, eine sichere Infrastruktur für die Authentisierung aufzubauen. Eine Infrastruktur ist aber immer nur so sicher wie das schwächste Glied der Kette. Bei elektronischen Informations- und Kommunikationssystemen, die vielen Nutzern offen stehen, ist der Schwachpunkt in der Regel der Nutzer selbst. Zum anderen trifft den Staat hier auch eine Verkehrssicherungspflicht. Durch den Aufbau der Authentisierungsinfrastruktur schafft er ein System, das sich für die Bürger bei mangelnder Aufklärung und unbedarfter Nutzung auch zur Gefahrenquelle entwickeln kann. Der Staat muss dies soweit wie möglich verhindern und dies nicht nur im Interesse der Stabilität des gesamten Systems, sondern auch zum Schutz des einzelnen Bürgers.

Die Mitarbeiter in der Personalausweisbehörde müssen bei der Übergabe aktiv nachfragen, ob der Bürger die Authentisierungsfunktion wünscht; dies ist durch geeignete Dienstvorschriften sicherzustellen. Wird der PIN-Brief zurückgegeben, so ist dieser zu vernichten und der Vorgang zu dokumentieren. Außerdem sollte der Bürger einen Antrag auf Sperrung der Authentisierungsfunktion stellen müssen.

4 Freiwillige Nutzung

Hinsichtlich der Nutzung der Authentisierungsfunktion im Einzelfall gilt ebenfalls, dass die jeweils erforderliche Mitwirkung die informationelle Selbstbestimmung des Ausweisinhabers sichert. Seine Mitwirkung wird durch die beiden Merkmale Besitz (des Ausweises) und Wissen (der Authentisierungs-PIN) sichergestellt. Die Erhebung der Authentisierungsdaten durch einen Dienstleister oder eine Behörde darf nach § 4 Abs. 3 BDSG nur erfolgen, wenn der Betroffene über die Person des Empfängers, den Verwendungszweck, die zu erhebenden Daten und die Empfänger möglicher Übermittlungen unterrichtet ist.[10] Um diese Anforderung zu erfüllen, muss dem Ausweisinhaber vor dem Auslesen der Daten optisch dargestellt werden,

5 Zu Anwendungsbeispielen s. auch *Helmbrecht/Thielmann/Ziemer* (Hrsg.), Elektronischer Personalausweis und E-Identity, Bericht des Berliner Gesprächs des Münchner Kreises am 26. März 2007.

6 S. zu den entsprechenden Rechtsfragen *Liesching*, MMR 2005, 465 ff.; *ders*., K&R 2006, 394 ff.; *Vassilaki*, K&R 2006, 211 ff.

7 *BGH*, Urteil v. 18.10.2007 – I ZR 102/05, noch unveröffentlicht, Pressemitteilung 149/2007, abrufbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&pm_nummer=0149/07 .

8 S. z.B. *Wiesner*, DuD 2007, 604 ff.; *Weichert*, VuR 2006, 452f.; das *OLG München,* MMR 2007, 47, hat allerdings eine Opt-out-Klausel als mit § 4a BDSG vereinbar beurteilt.

9 S. dazu *Roßnagel*, in: ders., Recht der Multimediadienste, § 6 SigG Rn. 1 ff.

10 Zu den entsprechenden Anforderungen s. *Sokol*, in: Simitis, BDSG, 6. Auflage 2006, § 4 Rn. 39 ff. m.w.N.

wer die Daten auslesen will, welche der im elektronischen Personalausweis gespeicherten Daten betroffen sind und zu welchem Zweck das Auslesen erfolgt.

Als Mittel hierzu erscheint das Zugriffszertifikat geeignet, das durch eine staatliche oder staatlich kontrollierte Stelle nach einer Erforderlichkeitsprüfung vergeben wird.[11] Aus dem Zertifikat sind die erforderlichen Angaben ersichtlich; diese werden durch die ausgebende Stelle für den Bürger nachprüfbar bestätigt. Es ist technisch sicherzustellen, dass die Daten erst nach der Anzeige des Zertifikats (und der darauffolgenden PIN-Eingabe) aus dem elektronischen Personalausweis ausgelesen werden. Mit der PIN-Eingabe gibt der Ausweisinhaber die Daten zum Abruf durch die Behörde oder den Dienstleister frei.

5 Vergabe von Zugriffszertifikaten

Das Modell der Access-Verifier leistet eine Art Vorprüfung der Datenverarbeitungsprozesse des Diensteanbieters. Überprüft wird die Erforderlichkeit des Zugriffs auf die Authentisierungsdaten insgesamt und einzelne Datenfelder.[12] Durch das Zugriffszertifikat erfolgt eine unabhängige Bestätigung der Identität der verantwortlichen Stelle (der Diensteanbieter), der abzurufenden Daten und des Verwendungszwecks. Anders als bisher muss der Bürger im Internet nicht mehr auf die eigenen Angaben eines Diensteanbieters vertrauen. Auch Hilfskonstruktionen wie Online-Siegel und andere Bestätigungen durch Dritte können insoweit entfallen. Dies erleichtert jede Form der Rechtsverfolgung des Ausweisinhabers. Durch die Angabe der zuständigen Aufsichtsbehörde wird insbesondere die Durchsetzung der datenschutzrechtlichen Betroffenenrechte vereinfacht.

Der datenschutzrechtliche Nutzen des Zertifikatsmodells hängt allerdings direkt von dem Prüfungsmaßstab ab, den der Access-Verifier seiner Prüfung zugrunde legt. Je tiefer die Prüfung erfolgt, desto aufwändiger ist sie und desto leichter werden Diensteanbieter sich von dem Prüfungserfordernis abschrecken lassen. Je weniger tief die Prüfung ist, desto geringer wird das Vertrauen der Ausweisinhaber in den Inhalt der ausgestellten Zertifikate sein.

Nach den Planungen soll eine „Plausibilitätsprüfung der datenschutzrechtlichen Erforderlichkeit" erfolgen. Dies wäre eine schwächere Form als eine echte Erforderlichkeitsprüfung[13] und könnte datenschutzrechtlich bedenklich sein. Auf der anderen Seite dürfte es im Rahmen der Prüfung in den meisten Fällen darum gehen, zu entscheiden, ob eine „eineindeutige" Identifizierung des Ausweisinhabers erforderlich ist oder nur bestimmte Attribute wie Volljährigkeit oder Wohnort benötigt werden, die auch anonym übermittelt werden können. Wenn ersteres bejaht wird, müssen – da die Personalausweisnummer entsprechend der derzeitigen Rechtslage in § 4 Abs. 2 PersAuswG nicht verwendet werden soll – ohnehin de facto alle für die Authentisierung vorgesehenen Daten ausgelesen werden. Die Frage der Erforderlichkeit der Identifizierung wird regelmäßig auch im Rahmen einer Plausibilitätsprüfung entscheidbar sein.

Die Angabe von Erhebungs- und Verarbeitungszweck im Zugriffszertifikat ist sehr nützlich, weil sie für den Ausweisinhaber Transparenz schafft und zugleich dem Diensteanbieter die zulässigen Verarbeitungszwecke vor Augen führt. Andererseits wird der Zweck des Abrufs der Daten der Authentisierungsfunktion regelmäßig die „sichere Identifizierung beim Vertragsabschluss" sein. Zwar wird sich der dahinter liegende Geschäftszweck im Regelfall aus dem Kontext ergeben und für den Ausweisinhaber daher transparent sein. Doch darf diese Pauschalangabe nicht dazu führen, dass zur „eineindeutigen" Identifizierung de facto alle Diensteanbieter alle Daten erhalten. Die Prüfung der Erforderlichkeit des Zugriffs auf alle Felder der Authentisierungsfunktion muss sich auch an dem Gebot des § 3a BDSG zur Datenvermeidung und Datensparsamkeit und – für Telemedien – dem Gebot des § 13 Abs. 6 TMG, die anonyme und pseudonyme Inanspruchnahme und Bezahlung von Telemedien zu ermöglichen, ausrichten.

Daher kommt eine Beschränkung des Zugriffs auf einzelne Felder nicht nur nach der Prüfung, ob eine anonyme Volljährigkeits- oder Wohnortbestätigung (letzteres für regionale Angebote, zum Beispiel alle Anwohner einer bestimmten Stadt) zur Erfüllung des Geschäftszwecks des Diensteanbieters hinreichend ist, in Betracht. Vielmehr kann eine solche Begrenzung oder gar eine Ablehnung des Antrags erforderlich sein, wenn im Verhältnis zwischen Anbieter und Nutzer beispielsweise keine Gegenleistung des Ausweisinhabers gefordert wird, wenn der Ausweisinhaber vorleisten muss, wenn für die Kommunikation keine postalische Anschrift notwendig ist oder wenn eine pseudonyme oder gar anonyme Kommunikation den Geschäftszweck genauso gut erfüllt wie eine identifizierende. Andererseits muss der Aufwand für solche Prüfungen beherrschbar bleiben. Dies dürfte möglich sein, wenn sich mit der zunehmenden Erfahrung des Access-Verifiers Standards für die Beurteilung von Klassen von Diensteanbietern und Identifizierungszwecken herausbilden.

Letztlich liegt der besondere Wert des angedachten Systems aber vermutlich weniger in der Erforderlichkeitsprüfung hinsichtlich einzelner Datenfelder, als in der garantierten Transparenz hinsichtlich der zugriffsberechtigten Institutionen, die das Anmeldeerfordernis garantiert. Ferner schützt das Zertifikat vor Phishing und ähnlichen unlauteren Angriffen. Darüber hinaus kann eine Beschränkung der Datenweitergabe auf Anbieter innerhalb des Anwendungsbereichs der europäischen Datenschutzrichtlinie erfolgen,[14] und die Angabe der Aufsichtsbehörde im Zugriffszertifikat erleichtert die Durchsetzung datenschutzrechtlicher Betroffenenrechte.

Generell gibt das Zugriffszertifikat – für den elektronischen Rechtsverkehr perspektivisch sehr wichtig – dem Ausweisinhaber eine Möglichkeit an die Hand, die Identität seines Interaktionspartners sicher zu validieren. Dies erleichtert (oder ermöglicht erst) die Rechtsverfolgung und -durchsetzung, falls es im Laufe der Interaktion zu einem Rechtsstreit kommt.

11 S. dazu unten 5.

12 Es handelt sich nicht um eine Vorabkontrolle im Sinn von § 4d Abs. 5 BDSG, ist dieser allerdings verwandt.

13 S. zum Begriff der Erforderlichkeit im Datenschutzrecht *Gallwas*, in: Haft/Hassemer/Neumann/Schild/Schroth, Strafgerechtigkeit, Festschrift für Arthur Kaufmann, 1993, 819 ff.; *Globig*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 4.7 Rn. 57.

14 S. unten 8.

6 Ungültige Zugriffszertifikate und Ausweise

Zugriffszertifikate dürfen nicht unbegrenzt, sondern nur für eine bestimmte Zeit ausgestellt werden, so dass sie irgendwann ablaufen und erneuert werden müssen. Außerdem kann es vorkommen, dass sich nach der Ausstellung herausstellt, dass ein Diensteanbieter falsche Angaben gemacht hat oder die Daten missbraucht. In diesem Fall sollte die Möglichkeit bestehen, ein Zugriffszertifikat zu sperren. Die Gültigkeit der Zugriffszertifikate ist deshalb durch die Applikation zu prüfen, die auf dem System abläuft, das der Ausweisinhaber nutzt. Da dies regelmäßig der heimische Computer sein wird, erscheint diese Lösung vertretbar.

Ebenso wie ein Zugriffszertifikat kann auch ein elektronischer Personalausweis ungültig werden. Eine entsprechende Kontrolle könnte durch eine Sperrliste ungültiger Ausweise erreicht werden. Die Alternative dazu besteht – wie bei der qualifizierten elektronischen Signatur – in der Abfrage der aktuellen Gültigkeit des elektronischen Personalausweises (OCSP-Abfrage). Da dieser jedoch, anders als bei der Signatur, durch eine einzige Stelle (letztlich den Bund) herausgegeben wird, entstünde so ein vollständiges Register aller im Umlauf befindlichen elektronischen Personalausweise. Dies ist nach geltendem Recht (§ 3 Abs. 2 und 3 PersAuswG) unzulässig. Von einer Änderung dieser Bestimmungen sollte aus datenschutzrechtlichen Gründen (Gefahr der Profilbildung durch Verwendung eines einheitlichen Personenkennzeichens)[15] abgesehen werden. Durch die Ausweispflicht entstünde ansonsten ein zentrales, vollständiges Personenregister aller deutschen Ausweisinhaber.

Dieses Risiko besteht bei einer Sperrliste nicht. In ihr wird nur eine Teilmenge der Ausweise gespeichert. Überdies sind Einträge nach Ablauf der Gültigkeitsdauer des Personalausweises zu löschen, also im Höchstfall (etwa beim Diebstahl direkt am Ausstellungstag) nach maximal zehn Jahren. Allerdings kann eine solche Liste – je nach der Zahl der enthaltenen Ausweise und der Anzahl und Art der mit diesen vor der Sperrung getätigten Rechtsgeschäfte – ebenfalls wesentliche personenbezogene Daten enthalten. Die damit verbundenen Probleme können entscheidend vermindert werden, wenn die Sperrliste nicht alle Daten der Authentisierungsfunktion, sondern beispielsweise nur eine eindeutige Nummer enthält. So wird datenschutzrechtlichen Belangen ebenso Rechnung getragen wie dem Bedürfnis nach einer verlässlichen Infrastruktur.[16] Die Sperrliste könnte eine staatliche Stelle oder die Bundesdruckerei GmbH (beziehungsweise ein anderer Hersteller) im Zusammenhang mit der zentralen Speicherung aller Personalausweisnummern nach § 3 Abs. 3 PersAuswG übernehmen.

7 Verwendung eines Personenkennzeichens

Das deutsche Verfassungsrecht steht Datensätzen, die als einheitliche Personenkennzeichen (PKZ) verwendet werden können, anders als viele andere Staaten sehr kritisch gegenüber. Derartige Kennzeichen können Instrumente der Profilbildung über das Verhalten von Personen sein und dadurch tief in deren Persönlichkeitsrechte eingreifen. Werden Daten bei unterschiedlichen Stellen erhoben, verarbeitet und genutzt, wird die Zusammenführung dieser verteilt gespeicherten Datenbestände erleichtert, wenn bei den jeweiligen Stellen bereits eine Verknüpfung mit demselben Personenkennzeichen erfolgte.[17] In der deutschen Diskussion wird ein solches Kennzeichen regelmäßig für unzulässig gehalten, da dieses gewollt oder ungewollt die Brücke zur permanenten Kontrolle der Betroffenen schlage, die bis hin zur Steuerung ihres Verhaltens gehen könne.[18]

Allerdings begegnet man heutzutage in einer Reihe von Lebensumständen Datensätzen, die eindeutige Identifizierungen erlauben. Das so genannte Verbot eines einheitlichen Personenkennzeichens verbietet aber nicht die Verwendung derartiger Datensätze insgesamt, sondern nur ihre Verwendung gerade als einheitliche Personenkennzeichen, das heißt als umfassende Identifizierungsmerkmale für große Gruppen von Betroffenen über Verarbeitungs- und Zuständigkeitsgrenzen hinweg. Im Kern geht es damit um die strikte Einhaltung der Regeln der Zweckbindung und der informationellen Gewaltenteilung.[19] Diese rechtlichen Nutzungsbeschränkungen sind – soweit möglich – technisch und organisatorisch zu sichern.

Dementsprechend wäre es zulässig, den elektronischen Personalausweis mit bereichsspezifischen Kennungen zu versehen;[20] unzulässig ist die Verwendung der Daten als eindeutiges Personenkennzeichen. Eine Möglichkeit, dieses Ziel zu erreichen, wäre die Generierung bereichsspezifischer Kennzeichen durch den elektronischen Personalausweis selbst. Dadurch könnte bei der Wiederanmeldung an einer Online-Anwendung dieses Kennzeichen übermittelt werden, ohne dass eine erneute Übertragung aller Daten des Authentisierungszertifikats erforderlich ist.[21] So wird verhindert, dass diese Daten zur Rückverfolgung und Profilbildung eingesetzt werden können.

Die Verwendung des elektronischen Ausweises als Mittel der Zusammenführung verteilt gespeicherter Daten und allgemeines Personenkennzeichen ist dagegen zu verhindern. Für den bisherigen Personalausweis sind entsprechende Schutzvorschriften in § 3 Abs. 4 sowie § 4 Abs. 2 und Abs. 3 PersAuswG vorgesehen, die sinngemäß in die elektronische Welt übertragen werden müssen.

15 S. z.B. *Süßmuth/Koch*, Pass- und Personalausweisrecht, 4. Auflage, 2006, § 3 Rn. 4; *Hornung* (Fn. 2), 55f.; 159 ff.

16 Aus rechtlicher Sicht bleibt das Problem bestehen, dass die Diensteanbieter in der Pflicht stehen, in regelmäßigen – sehr kurzen – Zeitabständen die Sperrliste herunterzuladen. Dies ist aber kein datenschutzrechtliches, sondern ein vertrags- und haftungsrechtliches Problem.

17 S. bereits *Kirchberg*, ZRP 1977, 137 ff.; zur informationstechnischen Verwendung *Steinmüller*, DVR 1983, 215 ff.

18 *Simitis*, in: ders. (Fn. 10), Einl. Rn. 12; *BVerfGE* 27, 1 (6); 65, 1, 53 (57); Rechtsausschuss des Bundestages, BT-Drs. 7/5277, 3; s. auch *Kirchberg*, ZRP 1977, 137 m.w.N.; *Steinmüller*, DVR 1983, 205, 242 ff.; *Weichert*, RDV 2002, 172.

19 S. auch *Weichert*, RDV 2002, 173.

20 Das Konzept der österreichischen Bürgerkarte verfolgt in starkem Maße den Ansatz bereichsspezifischer Kennungen, s. etwa *Kotschy*, DuD 2006, 201 ff.

21 S. aus technischer Sicht *Bender/Kügler/Margraf/Naumann*, DuD 2008 (in diesem Heft).

8 Zugriff durch ausländische Dienstleister

Ein weiteres Problem ist die Frage, ob die Vergabe der Zugriffszertifikate aus datenschutzrechtlicher Sicht auf deutsche Anbieter beschränkt werden sollte, um die hohen deutschen Datenschutzstandards zu sichern. Allerdings wird es schon aus Gründen der europäischen Dienstleistungsfreiheit (Art. 49 EGV) kaum möglich sein, innerhalb der Europäischen Gemeinschaft ansässige Diensteanbieter von der Nutzung auszuschließen. Angesichts der einheitlichen Mindeststandards innerhalb der Gemeinschaft und des europäischen Wirtschaftsraums (Datenschutzrichtline[22] und Datenschutzrichtlinie für elektronische Kommunikation[23]) erscheint dies akzeptabel. Beide Richtlinien fordern spezifische Rechtsgrundlagen, Zweckbindung, Transparenz, Verhältnismäßigkeit, Datensicherheit, Betroffenenrechte und unabhängige Kontrollen.[24]

Bei Diensteanbietern außerhalb der Mitgliedsstaaten sind nach § 4b Abs. 2 Satz 2 BDSG Übermittlungen unzulässig, wenn ein „angemessenes Datenschutzniveau nicht gewährleistet ist". Ein spezifisches Problem des elektronischen Personalausweises besteht bei grenzüberschreitender Datenverarbeitung nicht.

9 Zusammenfassung und Ausblick

Das Konzept der Authentisierung mittels des elektronischen Personalausweises verbindet eine generelle, vertrauenswürdige Vorabprüfung der Identität der Diensteanbieter und der Erforderlichkeit des von ihnen geplanten Zugriffs mit der Mitwirkung des Ausweisinhabers vor dem einzelnen Datenabruf, die durch die Sicherungselemente Besitz und Wissen geschützt wird. Soweit ersichtlich, ist dieses Modell weltweit ohne Vorbild. Es gibt den Ausweisinhabern die Möglichkeit, die Identität ihrer Kommunikationspartner nachprüfbar festzustellen, ihre Verarbeitungszwecke zu erkennen und die zuständige datenschutzrechtliche Aufsichtsbehörde zu erfahren. Das Verfahren wird die Durchsetzung datenschutzrechtlicher und anderer Ansprüche der Ausweisinhaber wesentlich erleichtern.

Insgesamt ist das Modell der staatlichen oder staatlich beaufsichtigten Vergabe von Zugriffszertifikaten für den elektronischen Personalausweis deshalb positiv zu bewerten. Allerdings ist auf eine Einschränkung hinzuweisen: Die Vergabe dieser Zertifikate bietet keinerlei Schutz dagegen, dass neben der Authentifizierung mittels des elektronischen Personalausweises noch eine Vielzahl anderer personenbezogener Daten – etwa über Web-Formulare – abgefragt werden. Dies ist jedoch kein Problem des elektronischen Personalausweises, sondern eine allgemeine Frage des Handelns im Rechts- und Geschäftsverkehr im Internet.

22 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281/31 v. 23.11.1995; s. zum Hintergrund z.B. *Simitis*, in: ders. (Fn. 10), Einl. Rn. 208 ff.; *ders.*, NJW 1997, 281 ff.; *Burkert*, in: Roßnagel (Fn. 13), Kap. 2.3, Rn. 44 ff.; *Dammann/Simitis*, EG-Datenschutzrichtlinie, 1997, Einl.

23 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EG L 201/37 v. 31.7.2002.

24 Näher *Brühann*, in: Roßnagel (Fn. 13), Kap. 2.4, Rn. 15 ff.; *Gola/Klug*, Grundzüge des Datenschutzrechts, 2003, 18 ff.