Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

Jens Fromm, Petra Hoepner, Jonas Pattberg, Christian Welzel

»3 JAHRE ONLINE-AUSWEISFUNKTION – LESSONS LEARNED«

Kompetenzzentrum Öffentliche IT

IMPRESSUM

Autoren:
Jens Fromm, Petra Hoepner, Jonas Pattberg, Christian Welzel

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3436-7173
Telefax: +49-30-3436-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Oktober 2013

DANKSAGUNG

Das Kompetenzzentrum ÖFIT von Fraunhofer FOKUS dankt den folgenden Behörden, Organisationen und Firmen für die hilfreichen Anregungen, Kommentare und Diskussionen: Bundesministerium des Innern (BMI), Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesverwaltungsamt (BVA), Bundesdruckerei, BearingPoint, BITKOM, Deutsches Industrie-Forum zur eID-Infrastruktur, ecsec GmbH. Unser besonderer Dank gilt dem Referat IT 4 »Pass- und Ausweiswesen, Identifizierungssysteme« des BMI sowie den folgenden Personen: Jens Bender, Frank Byszio, Detlef Hühnlein, Hanno Koop, Frank Morgner, Caroline Neufert, Andreas Reisen, Ivonne Scherfenberg, Martin Schröder und Klaus Wolter.

Dieses Dokument gibt ausschließlich die Meinung der Autoren wieder und repräsentiert nicht notwendigerweise den Standpunkt der Kommentatoren.

INHALTSVERZEICHNIS

1. PHILOSOPHIE UND ENTSCHEIDUNGEN

Der neue Personalausweis (nPA) feiert seinen dreijährigen Geburtstag. Seine Einführung gilt als eines der größten IT-Projekte der öffentlichen Hand in Deutschland.[1] Eine neue IT-Infrastruktur für über 60 Millionen Bundesbürgerinnen und Bundesbürger wurde geschaffen. Insgesamt wurden ca. 23 000 Mitarbeiterinnen und Mitarbeiter in über 5300 Personalausweisbehörden für die neuen Arbeitsprozesse geschult; eine neue Produktionsinfrastruktur in der Bundesdruckerei wurde eingerichtet und organisatorische Prozesse für die Vergabe von Berechtigungen etabliert.

Der neue Personalausweis bildet mit seiner Online-Ausweisfunktion eine elektronische Identitätsfunktion (eID-Funktion) ab, die es dem Bürger ermöglicht, sich im Internet auszuweisen. Einen Überblick über das Gesamtsystem, die Funktionsweise und die technischen Lösungen findet man in verschiedenen White Papers.[2]

Schon in der Konzeptionsphase des neuen Personalausweises wurden grundlegende Entscheidungen hinsichtlich der Philosophie der Online-Ausweisfunktion getroffen. Die elektronischen Identitätsfunktionen anderer Länder wurden untersucht, um von deren Erfahrungen zu profitieren. Beispielsweise wurden zur Einführung des nPA kostenlose Kartenleser bereitgestellt, damit fehlende Kartenleser nicht die Einführung behindern würden.[3] Diverse Begleitstudien wurden durchgeführt. Ebenfalls sollten durch ein Unterstützungsprogramm für Diensteanbieter aus Wirtschaft und Verwaltung Online-Dienste bereits zum Start des neuen Personalausweises angeboten werden.

Auf Grund von Erfahrungen und Anforderungen wurden folgende Designprinzipien festgelegt:[4]

- Amtlicher Ausweis mit Online-Ausweisfunktion: Eine dedizierte Karte wird an die Bürgerinnern und Bürger ausgegeben, im Gegensatz zu einer elektronischen Identitätsfunktion die auf andere Karten aufgebracht werden kann.[5]
- Datenschutz mit vollständiger Kontrolle durch den Ausweisinhaber:[6] Der Ausweisinhaber entscheidet, welche Daten weitergegeben werden.
- Sicherheit als Grundlage: Nicht als Add-on.
- Ausschließlich Identifikation: Keine Karte für alles, wie z. B. Geldkarte, Versicherungskarte, Club-Karte, d.h. der Chip enthält keine Speicherbereiche für sonstige Daten.
- Keine X.509 Authentisierungszertifikate:[7] Diese werden aus Datenschutzgründen nicht für die Identifikation verwendet, damit die personenbezogenen Personalausweisdaten nicht »beglaubigt« an Dritte weitergereicht werden können.
- Dezentrale Architektur: Daher keine zentralisierte Datenbank.
- Prinzip der Freiwilligkeit: Bürgerinnen und Bürger können die Online-Ausweisfunktion jederzeit aktivieren und deaktivieren.
- Vertrauen durch Gegenseitigkeit: Die Online-Ausweisfunktion soll Vertrauen schaffen, indem sowohl Bürger als auch Diensteanbieter sich gegenseitig vertrauenswürdig identifizieren.

[1] BMI: Ein Jahr neuer Personalausweis, Pressemitteilung, 31.10.2011, http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/10/npa.html

[2] Kompetenzzentrum Neuer Personalausweis, White Paper, http://www.ccepa.de/whitepaper

[3] European Commission: eGovernment in Belgium, eGovernment Factsheets, January 2007, http://documentostics.com/component/option,com_docman/task,doc_view/gid,1151/ »To date, the eID is not intensively being used since only 8% of Belgian web users own a card reader and less than 1% of these internet users use their eID online.«

[4] Jens Bender: Der neue Personalausweis. Warum er so ist wie er ist, Vortrag CeBIT/03.03.2011, http://www.cio.bund.de/DE/Strategische-Themen/IT-Investitionsprogramm/Aktivitaeten/CeBIT-2011/Vortraege/nPa_bsi_download.pdf?__blob=publicationFile

[5] Beispielsweise in Österreich ist die Bürgerkarte in verschiedenen Ausprägungen möglich: als Signaturkarte wie die Bankomatkarte oder die eCard oder auf dem Mobiltelefon als sogenannte Handy-Signatur, http://oesterreich.gv.at/site/cob__28545/5244/Default.aspx

[6] Die weibliche Form ist der männlichen Form gleichgestellt; lediglich aus Gründen der Vereinfachung wurde teilweise nur die männliche Form gewählt.

[7] X.509 ist ein internationaler Standard für Public-Key-Infrastrukturen zum Erstellen digitaler Zertifikate. Ein Authentisierungszertifikat bestätigt die Identität und den öffentlichen kryptografischen Schlüssel einer Person. Die Authentizität und Integrität des Zertifikats kann durch kryptografische Verfahren geprüft werden.

Trotzdem liegt die Nutzung der Online-Ausweisfunktion insgesamt unter den Erwartungen. Folgende Kennzahlen zeigen die derzeitige Situation:[8]

- über 21 Mio. neue Personalausweise (nPA) und 2,2 Mio. elektronische Aufenthaltstitel (eAT) ausgegeben;
- Berechtigungszertifikate für 147 Dienste von 106 Diensteanbietern vergeben; davon 40 % E-Government- und 60 % E-Business-Dienste;
- Einschaltquote, d. h. Aktivierung der Online-Ausweisfunktion, liegt bei ca. 28 %.

Allerdings führt nicht jede aktivierte Online-Ausweisfunktion auch zu deren Einsatz bei der Nutzung von Diensten.

Was sind also die Gründe, dass die Online-Ausweisfunktion noch nicht so häufig genutzt wird? Was hat man nach drei Jahren gelernt? Wie kann man die Akzeptanzproblematik, die mit der die Diffusion[9] von Innovationen einhergeht (wie beispielsweise von der Kreditkarte und dem Sicherheitsgurt bekannt), positiv beeinflussen?

[8] Klaus Wolter, Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt: Die Online-Ausweisfunktion, Vergabepraxis und Verfahren, Vortrag, Zukunftskongress Staat & Verwaltung, Berlin, 25.06.2013, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Praesentationen/130625_Zukunftskongress-VfB-Wolter.html

[9] Everett M. Rogers: Diffusion of Innovation, Fifth Edition, Free Press, 2003. »Diffusion is the process in which an innovation is communicated through certain channels over time among the members of a social system. It is a special type of communication, in that the messages are concerned with new ideas.«

2. LESSONS LEARNED

Ziel dieses Rückblicks ist es, die Erfahrungen mit der Einführung des neuen Personalausweises aus heutiger Sicht zu reflektieren. Erfolge und Fehler werden analysiert, um Stärken und deren Ausbaumöglichkeiten sowie Schwächen und deren Verbesserungsmöglichkeiten zu erkennen.

2.1 MOTIVATION, TRANSPARENZ UND AUFKLÄRUNG FÜR ALLE BETEILIGTEN

Für den Erfolg einer elektronischen Identitätstechnologie müssen alle beteiligten Akteure motiviert werden, diese einzusetzen.

Derzeit variieren die Einschaltquoten für die Online-Ausweisfunktion zwischen verschiedenen Personalausweisbehörden. Hohe Einschaltquoten kommen hauptsächlich aus Kommunen, die selbst Online-Dienste für den neuen Personalausweis anbieten und somit direkt den Nutzen für die Aktivierung verdeutlichen. Mangelnde Auskunftsfähigkeit kann allerdings auch das Gegenteil bewirken.[10]

Ursachen für geringe Einschaltquoten sind potenzielle Ängste, Misstrauen und Skepsis von Bürgern gegenüber elektronischen Systemen des Staates. Diese müssen ernst genommen werden. Wesentlich für deren Abbau sind Transparenz und Überprüfbarkeit der eID-Technik durch den Bürger selbst bzw. durch unabhängige Organisationen. Ein Schritt in diese Richtung ist, dass Bürger ihre elektronischen Daten auf dem Chip des Personalausweises auch am eigenen Computer und nicht nur in der Personalausweisbehörde einsehen können. Das ist allerdings erst seit 2013 möglich, da hierfür eine Änderung der Personalausweisverordnung erforderlich war.[11] Diese Selbstauskunft sollte nicht nur kommunal, sondern auch zentral vom Bund angeboten werden.

Häufig halten auch Unsicherheit und zu geringes Verständnis der Online-Ausweisfunktion die Bürger von deren Anwendung zurück. Kritisch wird daher auch gesehen, dass die »Bewerbung der eID-Funktion bis heute überwiegend über Nischenmedien, wie dedizierte Ausweisportale oder auf Webseiten der in diesem Umfeld tätigen IT-Unternehmen stattfindet«.[12] Wesentlich ist es also, den Nutzen für den Bürger verständlich zu kommunizieren. Das umfasst Informationsmaterialien, Demo-Dienste, Beratung und Unterstützung und zwar nicht nur zur Einführung, sondern mindestens bis alle Bürger einen neuen Personalausweis besitzen, d. h. mindestens 10 Jahre lang.

Wichtiger Bestandteil der Aufklärung ist auch die Auseinandersetzung im kritischen Dialog. Gerade bei staatlichen Großprojekten ist immer auch mit öffentlicher Kritik zu rechnen. Um dem zu begegnen, ist ein regelmäßiger Dialog und transparenter Umgang mit der Technologie genauso notwendig wie eine neutrale Auseinandersetzung mit der Kritik.

Darüber hinaus ist die Motivation der Bürger zur Nutzung der Online-Ausweisfunktion zu beachten. Es muss die Frage beantwortet werden: Aus welchen Gründen soll ein Bürger den Ausweis einsetzen, welche Vorteile hat er davon? Neben Aspekten der Sicherheit und der Bequemlichkeit wären auch Kosteneinsparungen beziehungsweise ermäßigte Gebühren ein Anreiz, die Diensteanbieter an Bürger weitergeben könnten. Gerade die Verwaltung kann hier als Vorreiter fungieren.

---

[10] Susanne Asheuer, Joy Belgassem, Wiete Eichhorn, Rio Leipold, Lucas Licht, Christoph Meinel, Anne Schanz, Maxim Schnjakin: Akzeptanz und Nutzerfreundlichkeit der AusweisApp: Eine qualitative Untersuchung, Hasso Plattner Institut, Universität Potsdam, Technische Berichte Nr. 69, 2013. http://opus.kobv.de/ubp/volltexte/2013/6397/pdf/tbhpi69.pdf, S.30: »Die Mitarbeiter waren oft nicht in der Lage, den Bürgern den Nutzen der Online-Ausweisfunktion vor Augen zu führen. Stattdessen wurden unklare Angaben gemacht oder inkorrekte Anwendungsmöglichkeiten genannt. Manche Mitarbeiter äußerten in Befragungen, dass sie froh seien selbst noch den alten Ausweis zu besitzen.«

[11] Kommune21: Selbstauskunft schafft Transparenz, Mitteilung vom 4. März 2013, http://www.kommune21.de/meldung_15486_Selbstauskunft+schafft+Transparenz.html

[12] O. Keitzel, W. Zimmer, E. de Vries, H. Kubicek und M. Wind: Die eID-Funktion als Vertrauensanker im E-Commerce, Mittelstandsoffensive Neuer Personalausweis, Expertise und Handlungsempfehlungen für die Etablierung zentraler eID-Infrastrukturen für den Mittelstand, Berlin 2012, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Begleitstudien/Studie_E-Commerce.pdf?__blob=publicationFile

Auch Wirtschaft und Verwaltung als potenzielle Diensteanbieter benötigen besonders am Anfang Aufklärung und Unterstützung. Kostentransparenz für den Einsatz der Online-Ausweisfunktion ist so früh wie möglich zu schaffen, damit betriebswirtschaftliche Prozesse eingeleitet werden können. Unsicherheiten von Diensteanbietern hinsichtlich organisatorischer Anforderungen und gesetzlicher Vorgaben für den Einsatz der Online-Ausweisfunktion, wie zum Beispiel die Erforderlichkeit von Sicherheitskonzepten oder Haftungsfragen, sind frühzeitig zu klären. Diesbezügliche Beratung und Unterstützung ist genauso wichtig wie für die technische Umsetzung.

2.2 LERNPROZESSE AKZEPTIEREN, STÄNDIGE VERBESSERUNG UND PERMANENTE BEGLEITUNG

Ein Großprojekt wie der neue Personalausweis mit einer komplexen Infrastruktur bestehend aus vielen neuen Systemen und Komponenten sollte zwar nach einer Einführungsphase funktionieren, bedarf aber einer kontinuierlichen, strategischen Weiterentwicklung mit definierten »smarten«[13] Zielen.

Wesentlich ist es, die Akzeptanz der Online-Ausweisfunktion weiter zu steigern und damit entscheidendes Vertrauen dauerhaft zu gewinnen. Vom Bundesministerium des Innern (BMI) wurden als Ziele für 2012 eine höhere Einschaltquote und mehr Anwendungsmöglichkeiten für die Online-Ausweisfunktion und für 2013 mehr Anwendungsmöglichkeiten für De-Mail und Online-Ausweisfunktion sowie ein leichterer Zugang zur Nutzung festgelegt.[14] Unter anderem mit der E-Government-Initiative wurden Maßnahmen zum Erreichen dieser Ziele eingeleitet.[15]

Um die Nutzerakzeptanz der Online-Ausweisfunktion durch verschiedene Maßnahmen nicht nur punktuell zu verbessern, sondern insgesamt auch wirksam zu bewerten und zu prüfen, sind die Mechanismen des Qualitätsmanagements nach DIN EN ISO 9001 sinnvoll. Ständige Verbesserung mit der Methode »Planen-Durchführen-Prüfen-Handeln« ist dabei ein Grundprinzip. Es ist also keineswegs erforderlich, dass ein Prozess oder System von Anfang an perfekt funktioniert. Wichtig ist ein konstruktiver Umgang mit Unzufriedenheit und Fehlern. Zu diesem Zweck wurde für die Bürger der Bürgerservice eingerichtet, der telefonisch und per E-Mail erreichbar ist. Auch für Diensteanbieter aus Wirtschaft und Verwaltung ist ein Verbesserungsmanagement erforderlich. Das Einrichten einer permanenten Begleitungsstelle (z. B. im Bundesverwaltungsamt (BVA)) wäre hier angeraten.

Kennzahlen sind ebenfalls ein Mechanismus des Qualitätsmanagements, da nicht nur das Veranlassen, sondern auch das Überprüfen von Maßnahmen anhand von Kennzahlen entscheidend sind. Eine solche Kennzahl ist die Einschaltquote für die Online-Ausweisfunktion. Weitere wichtige Kennzahlen könnten definiert und überprüft werden:[16] Prozentsatz der tatsächlichen Nutzer der Online-Ausweisfunktion, Altersrelation zu Einschaltquote, Zeitpunkt der Erstnutzung nach Erhalt des Ausweises, Prozentsatz der Nutzer, die einen Dienst erneut nutzen usw. Insbesondere Behörden und E-Government-Dienste können hier wertvolle Kennzahlen liefern, da diese im Verantwortungsbereich des Staates liegen und daher leichter statistische Daten zur Verfügung stellen können. So könnte man gezielt Informationen nicht nur zur Einschalt- sondern auch zur Nutzungsquote sammeln, um Maßnahmen noch gezielter ergreifen zu können.

[13] Die Planung von Zielen kann mit der sogenannten SMART-Regel erfolgen. SMART bedeutet: Spezifisch (situations- und personenorientiert), Messbar (überprüfbar), Aktionsorientiert (auf konkrete Handlungen bezogen), Realistisch (überschaubar und inhaltlich begrenzt), Terminiert (zeitlich festgelegt).

[14] Frank-Rüdiger Srocke: E-Government immer öfter mit eID-Funktion, Vortrag, CeBIT – Forum Public Sector Park, Hannover, 7. März 2013, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Praesentationen/130304_CeBIT_FORUM_EGov_mit%20eID_Srocke_final.pdf?__blob=publicationFile

[15] E-Government-Initiative, Webseite, http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Initiative/e-government-initiative_node.html und http://www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/E-Government-Initiative/egovernment_initiative_node.html

[16] Gemäß DIN EN ISO 9004 ist die Wahl geeigneter Leistungskenngrößen und geeigneter Überwachungsmethoden für den Erfolg des Mess- und Analyseprozesses von entscheidender Bedeutung. Aufgrund der dezentralen Infrastruktur für den nPA sind die möglichen Kennzahlen und die Methoden für ihre Erfassung und Überwachung (beispielsweise mittels Online-Messung, Interviews, Fragebögen) noch zu untersuchen. U. a. sind datenschutzrechtliche Aspekte dabei ein wichtiges Kriterium.

Wenn beispielsweise junge Menschen die Online-Ausweisfunktion eher nutzen als ältere, dann sollten besondere Anreize für jugendliche Erstnutzer geschaffen werden. Auch kann in dieser Altersgruppe die »Vorbildfunktion« für andere den Diffusionsprozess positiv beeinflussen. Insgesamt sind Maßnahmen wichtig, die nach dem Abholen des Personalausweises von der Behörde eine schnelle Erstnutzung einleiten, um diese Hürde zu überwinden. Etwa können in Bürgerämtern aufgestellte Automaten einen Funktionstest anbieten mit initialem Setzen einer PIN sowie einer Selbstauskunft.

2.3 STAATLICHE SOFTWARE – JA, ABER OFFEN, NUTZERFREUNDLICH UND UNABHÄNGIG

Für den Start des neuen Personalausweises war die Bereitstellung einer kostenlosen Software erforderlich, um diesen überhaupt online nutzen zu können. Diese staatliche Software wurde ehemals als Bürgerclient und später als AusweisApp bezeichnet. Die Einführung der AusweisApp gestaltete sich problematisch und gilt bis heute als neuralgischer Punkt im gesamten System.

Sicherheitslücken direkt nach dem Start, Abhängigkeiten vom Betriebssystem, vom Browser und von bestimmten Browserversionen und diverse Verzögerungen, bis die AusweisApp auch für Linux (nach sieben Monaten) und MacOS (über ein Jahr) zur Verfügung stand, haben dem Vertrauen in die Software geschadet. Eine Sicherheitszertifizierung der AusweisApp durch den Anbieter (Personalausweisverordnung Anhang 5 »Übersicht über die zu zertifizierenden Systemkomponenten«) ist zwar optional, wird aber empfohlen. Die Zertifizierung ist jedoch auch nach drei Jahren noch nicht abgeschlossen.[17] Der Bundesrechnungshof forderte, dass »vom Bund angebotene Software die gesetzlichen Vorgaben erfüllt und ohne Haftungsrisiken genutzt werden kann«. Daraufhin wurde eine Information zur Sicherheit der AusweisApp vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht.[18]

Insbesondere in Deutschland ist ein gewisses Misstrauen gegenüber staatlicher Software aus Furcht vor Überwachung vorhanden; eine AusweisApp von einem unbekannten nicht-staatlichen Hersteller ist allerdings ebenfalls nicht vertrauenswürdiger. Kulturell bedingt wird ein hohes Maß an Sicherheit und Privatheit gefordert. Aus diesem Grund wäre es von Anfang an wünschenswert gewesen, wenn die AusweisApp als Open-Source-Software vorhanden gewesen wäre. Ängste hätten reduziert und bestimmte Mängel durch die Community verhindert werden können.

Nach und nach entstehen jetzt quelloffene Alternativen[19] zur staatlichen AusweisApp und Implementierungen des eCard-API-Frameworks[20], wie PersoApp[21], Open eCard[22], AutentApp[23], eIDClientCore[24] oder Open eID[25]. So wird eine breite Basis geschaffen, um sowohl neue Endgeräte als auch andere Software anzubinden. Diese verschiedenen Entwicklungen sind begrüßenswert, jedoch ist darauf zu achten, dass die Bürgerinnen und Bürger dadurch nicht verwirrt werden. Diesbezügliche Informationen und Erläuterungen sollten durch den Bund bereitgestellt werden.

[17] Bundesrechnungshof, Jahresbericht 2012, Bemerkungen 2012 zur Haushalts- und Wirtschaftsführung des Bundes – Weitere Prüfungsergebnisse –, 16. April 2013, Seite 5 »Fragen zur Softwaresicherheit beim neuen elektronischen Personalausweis seit Jahren ungeklärt«, https://www.bundesrechnungshof.de/de/veroeffentlichungen/bemerkungen-jahresberichte/2012-weitere-pruefungsergebnisse/inhalt/2012-bemerkungen-gesamtbericht-weitere-pruefungsergebnisse-pdf

[18] BSI, AusweisApp, https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/AusweisApp/AusweisApp.html

[19] Heise Newsticker: Neuer Personalausweis: Projekte für neuen eID-Client, 24.07.2013, http://www.heise.de/newsticker/meldung/Neuer-Personalausweis-Projekte-fuer-neuen-eID-Client-1922815.html

[20] BSI TR-03112, Das eCard-API-Framework, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html

[21] Projekt PersoApp, https://www.persoapp.de/

[22] Open eCard Team c/o ecsec GmbH, https://www.openecard.org/de/

[23] bos GmbH&Co. KG, AutentApp, http://www.autentapp.de/

[24] Bundesdruckerei, eIDClientCore, http://sar.informatik.hu-berlin.de/BeID-lab/eIDClientCore/

[25] Fraunhofer, Open eID, http://sourceforge.net/projects/open-eid/

2.4 PROBIEREN GEHT ÜBER STUDIEREN – BERATUNG UND TESTMÖGLICHKEITEN DAUERHAFT ANBIETEN

Ein neues System, neue Anwendungen und unbekannte Funktionen müssen erprobt werden können, um Erfahrungen zu sammeln und Vertrauen zu entwickeln.

Um die Technik zu erproben, wurden die E-Business- und E-Government-Diensteanbieter bereits vor Erstausgabe des nPA durch die geschlossenen und offenen Anwendungstests eingebunden. Zur Betreuung der Anwendungstests wurde ein Kompetenzzentrum eingerichtet. Gleichzeitig wurde ein Feldtest in ca. 30 Personalausweisbehörden für hoheitliche Prozesse durchgeführt. Ziel war es, möglichst viele Anwendungen bereits bei der Erstausgabe des nPA zur Verfügung zu haben.

Auch wenn diese Anwendungstests erste Anreize geschaffen haben, sind doch nicht so viele Anwendungen daraus entstanden, wie erhofft. Problematisch waren insbesondere auch die Kosten für den Betrieb eines eID-Servers oder eID-Services für die Diensteanbieter. Kleine und mittlere Unternehmen (KMU) und kleinere Behörden waren finanziell oder technisch nicht in der Lage, diesen Dienst zu nutzen. Modelle für das gemeinsame Nutzen eines Berechtigungszertifikats sind erst nach der Einführung des nPA entstanden. In 2012 wurden rechtliche Probleme ausgeräumt, sodass kommunale Zweckverbände ein Berechtigungszertifikat ohne Einschränkung erhalten können, um Bürgerkonten für ihre Mitgliedskommunen einzurichten und zu betreiben.[26] Die Kommunen benötigen keine eigenen Zertifikate mehr und werden so von der aufwändigen Beschaffung und Verwaltung der Berechtigungszertifikate entlastet.

Eine ähnliche Konstellation für KMUs beispielsweise über Industrie- und Handelskammern wäre zwar denkbar, ist aber rechtlich derzeit nicht möglich. Allerdings wird mit diesen Gemeinschaftszertifikaten das datenschutzfreundliche Prinzip – Informationen pro Dienst nicht pro Diensteanbieter – zugunsten der Kostenreduktion eingeschränkt. Generell sollten diesbezüglich weitere Betriebs- und Geschäftsmodelle entwickelt werden, um die Kosten und Komplexität für bestimmte Diensteanbieter, wie KMUs und kleine Kommunen, zu reduzieren, jedoch weiterhin die dienstspezifische Information zu übermitteln.

Um die Anzahl von Online-Diensten von Anfang an zu erhöhen, wäre eine Verpflichtung von Behörden, zur Authentisierung für Online-Verwaltungsdienstleistungen den nPA zu akzeptieren, eine gute Möglichkeit gewesen. Die Hürde im E-Government den nPA einzusetzen ist niedriger, da Bürger an den Einsatz ihres Ausweises in einer Behörde gewöhnt sind. Erst mit der Verabschiedung des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (E-Government-Gesetz)[27] in 2013 erfolgte für die Behörden des Bundes ein Schritt in diese Richtung. Ab 1. Januar 2015 sind Bundesbehörden verpflichtet, die Nutzung des elektronischen Identitätsnachweises zu ermöglichen und dafür die auf Seiten der Behörden notwendige Infrastruktur bereitzustellen.[28]

Um auch zukünftig weitere neue Diensteanbieter zu gewinnen, sind dauerhaft Beratungsangebote, Testmöglichkeiten und diesbezügliche Ressourcen für die Einbindung des nPA erforderlich. Anbieten würde sich hier beispielsweise die Vergabestelle für Berechtigungszertifikate (VfB) im BVA als kompetente und unabhängige Stelle für eine umfassende Beratung und Betreuung.

Die Testmöglichkeiten für Diensteanbieter werden derzeit über Test-Infrastrukturen von den jeweiligen eID-Service-Anbietern angeboten. Allerdings erfordert deren Nutzung vorab schon eine Entscheidung für einen bestimmten eID-Service-Anbieter. Auch hier wäre eine Beratung hinsichtlich der verschiedenen Möglichkeiten durch eine unabhängige Stelle sinnvoll.

[26] BMI, Lösung für Berechtigungszertifikate mit Modellcharakter in NRW, Mitteilung, 26.09.2012, http://www.personalausweisportal.de/SharedDocs/Kurzmeldungen/DE/2012/NRW_Sammelzertifikate.html

[27] E-Government-Gesetz, Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 25. Juli 2013, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/egovg_verkuendung.pdf?__blob=publicationFile

[28] BMI: Wann treten die Regelungen des E-Government-Gesetzes in Kraft ?, http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/EGovernmentGesetz/01_in_kraft_treten.html?nn=3315448

Darüber hinaus bedarf es unkomplizierter Bezugsprozesse für nPA- und eAT-Testausweise in unterschiedlichen Generationen und Ausprägungen sowie für Testzertifikate zu festgelegten Konditionen. Dies ist insbesondere auch für freie Entwickler notwendig, um eine Entwickler-Community für neue Anwendungen aufzubauen. Um von Testausweisen abstrahieren zu können, wird derzeit auch ein Open-Source-eID-Simulator entwickelt.[29]

Auch für die Bürgerinnen und Bürger sind unverbindliche Anwendungsmöglichkeiten in Form von Diensten erforderlich, um den Umgang mit dem nPA erlebbar zu machen. So könnten schon in den Bürgerämtern bei der Ausgabe der Ausweise erste positive Erfahrungen vermittelt und Mehrwerte besser dargestellt werden. Neben der Selbstauskunft wären beispielsweise auch regionale Anwendungen und Dienste, die die Vorteile der Altersverifikation und der Pseudonymfunktion zeigen, geeignet. So könnte der Wunsch nach Freischaltung der Online-Ausweisfunktion befördert werden. Noch einfacher wäre es, wenn nur freigeschaltete nPA ausgegeben würden, sofern dies rechtlich möglich ist. Eine Deaktivierung müsste der Bürger dann selbst veranlassen. Test- und Probedienste sollten natürlich auch vom heimischen Computer aufrufbar sein.

2.5 GESETZLICHE ANPASSUNGEN FRÜHZEITIG DURCHFÜHREN

Gesetzliche Grundlagen bilden die Basis für das Handeln der Verwaltung. Werden neue elektronische Funktionen in Verwaltungsprozessen eingeführt, so müssen rechtliche Hindernisse beseitigt werden, die elektronische Verfahren blockieren oder behindern. Gesetzesänderungen aber erfordern Zeit !

Diverse gesetzliche Anpassungen waren notwendig um die Online-Ausweisfunktion nutzen zu können. Neben dem Personalausweisgesetz und der Personalausweisverordnung wurden beispielsweise auch das Melderechtsrahmengesetz, die Signaturverordnung und das Geldwäschegesetz so angepasst, dass zur Legitimations- und Identitätsprüfung der neue Personalausweis genutzt werden kann.

Gesetzliche Anpassungen werden weiterhin vorgenommen: Um zum Beispiel Führungszeugnisse nicht mehr nur persönlich in der zuständigen Meldebehörde sondern auch mit der Online-Ausweisfunktion beantragen zu können, wurde im Juni 2013 eine Änderung des Bundeszentralregistergesetzes verabschiedet.[30]

Eine weitere Hürde zur Etablierung elektronischer Verwaltungsprozesse ist auch die Schriftform. Regelmäßig wird in der Verwaltungspraxis ein unterschriebenes Dokument auch dann verlangt, wenn die Schriftform nicht gesetzlich vorgeschrieben ist (»gefühlte« Schriftform).[31] Bisher war hier nur die qualifizierte elektronische Signatur (QES) zugelassen, die allerdings von den Bürgern wenig genutzt wurde. Eine wichtige Gesetzesänderung, die die Online-Ausweisfunktion des neuen Personalausweises und des elektronischen Aufenthaltstitels als elektronisches Äquivalent der Schriftform zulässt, ist erst in 2013 mit dem E-Government-Gesetz geschaffen worden.

---

[29] Holger Funke und Tobias Senger, An open source eID simulator, in: Detlef Hühnlein und Heiko Roßnagel (Hrsg.), Open Identity Summit 2013, Kloster Banz, 10-11 September 2013, Lecture Notes in Informatics, Proceedings, Volume P-223, 2013

[30] Elektronische Antragstellung für Führungszeugnisse, Beschluss Bundestag, 13. Juni 2013, http://www.bmj.de/SharedDocs/Kurzmeldungen/DE/2013/20130614_Bundestag.html

[31] Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKR-Gesetz: Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften (NKR-Nr. 2030), 28. August 2012, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/ModerneVerwaltung/stellungnahme_nkr_egovg.pdf?__blob=publicationFile

Trotzdem soll das Unterschreiben mit dem Personalausweis – wie auch von Anfang an beworben – noch möglich sein. Die ursprünglich vorgesehene Online-Aktivierung der QES ist allerdings bis heute nicht möglich, jedoch befindet sich die elektronische Unterschrift mit dem Personalausweis in der Testphase.[32] Die ursprüngliche Vorstellung sogenannte Adhoc-Signaturen bereitzustellen, d. h. nur wenige Tage oder Monate gültige qualifizierte elektronische Signaturen, ist aus Nutzersicht weiterhin sehr kompliziert. Gründe dafür liegen in den rechtlichen Bedingungen, die für den Prozess der Aktivierung einer QES auf dem Ausweis derzeit explizit einen manuellen Zwischenschritt vorsehen.

2.6 SPANNUNGSFELD SICHERHEIT VS. NUTZERFREUNDLICHKEIT

Der Personalausweis ist ein hoheitliches Dokument mit einem sehr hohen Sicherheitsniveau. Für die elektronische Identifikation und Authentisierung mit der Online-Ausweisfunktion war Sicherheit und Privatheit ein wesentliches Designmerkmal. Aus diesem Grunde wurde eine neue, hochkomplexe, sichere Infrastruktur für den elektronischen Identitätsnachweis geschaffen, die die Personalausweisbeantragung, die Produktion und Personalisierung, die Berechtigungsinfrastruktur einschließlich dienstespezifischer Sperrlisten und letztendlich die Nutzung von Diensten durch den Bürger umfasst.

Schon anfangs wurde die Nutzerfreundlichkeit zwar als wichtig eingestuft, trotzdem wurde eine Usability-Studie erst kurz vor Inbetriebnahme des neuen Systems in Auftrag gegeben.[33] Die Studie empfiehlt unter anderem: »Usability fängt dort an, wo der Bürger das Startpaket zur AusweisApp ausgehändigt bekommt: auf dem Amt. Dieses Startpaket beinhaltet den neuen Personalausweis, das Kartenlesegerät, einen USB-Stick mit vorinstallierter AusweisApp und Gerätetreibern sowie eine kleine Broschüre, die die Schritte bis zur ersten Nutzung der AusweisApp beschreibt.« So einfach ist es bis heute nicht geworden! Ein automatisierter Installationsablauf fehlt.

Noch kämpfen die Bürger mit dem Download und der Installation der AusweisApp, dem Kauf und der Installation eines geeigneten Kartenlesers, den unterschiedlichen Betriebssystemen und alten Versionen von Browsern, dem richtigen Verständnis für Transport-PIN, PIN, PUK, CAN usw. Wer hier nicht auf der Strecke bleibt, nutzt dann vielleicht die Online-Ausweisfunktion. Fazit: Die Erstnutzung muss noch einfacher werden. Zumindest der oben beschriebenen Browserabhängigkeit wurde mit einer Anpassung der technischen Richtlinien bereits aktiv begegnet. Ein weiterer Faktor ist der Wiedererkennungswert durch die Orientierung an marktgängigen Lösungen.[34]

Es stellt sich die Frage, ob diese Schwierigkeiten als Folge der hohen Sicherheitsanforderungen einzuordnen sind. Die Antwort darauf ist nicht eindeutig. Der Zusammenhang zwischen Sicherheit und Usability wird von Yee so dargestellt:[35] Sicherheit schränkt den Zugriff auf Operationen ein, die unerwünschte Ergebnisse haben, während Usability den Zugang zu Operationen verbessert, die erwünschte Ergebnisse haben. Er führt weiter aus, dass ein Konflikt erst dann entsteht, wenn Informationen fehlen, die entscheiden lassen, ob ein bestimmtes Ergebnis erwünscht war. Diese Entscheidung ist komplizierter, wenn beispielsweise Fehlermeldungen nicht verständlich sind oder die Funktionalität zu umfassend ist. Hier wäre eine Möglichkeit, Sicherheit und Nutzerfreundlichkeit besser miteinander zu harmonisieren durch Reduzierung von Funktionalität. Beispielsweise könnten alle Funktionen für die elektronische Signatur nur bei Bedarf installiert werden und nicht obligatorisch. Nach dem Motto »Weniger ist mehr« würde die Komplexität verringert werden und die Installation und Benutzbarkeit der Online-Ausweisfunktion wäre gegebenenfalls einfacher und verständlicher.

[32] Personalausweisportal, Elektronische Unterschrift für den neuen Personalausweis im Testbetrieb, Mitteilung, 21. November 2012, http://www.personalausweisportal.de/SharedDocs/Kurzmeldungen/DE/2012/sign-me.html

[33] Jasper Hugo Grote, Daniela Keizer, Dominik Kenzler, Patrick Kenzler, Christoph Meinel, Maxim Schnjakin, Lisa Zoth: Vom Client zur App, Ideenkatalog zur Gestaltung der Software zum Einsatz des neuen Personalausweises, Hasso-Plattner-Institut im Auftrag des Bundesministeriums des Innern, 30. September 2010, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Begleitstudien/Studie_Usability_Volltext.pdf;jsessionid=0B260AAFA45C490B6426176A96C2A8F5.2_cid334?__blob=publicationFile

[34] KGSt, KoopA ADV: Erfolgsfaktoren für E-Government-Lösungen: Nutzungsanreize, Marketing und mehr, Bericht 1/2006, Seite 43, http://www.verwaltungsreform-bw.de/SiteCollectionDocuments/Erfolgsfaktoren%20f%C3%BCr%20E-Government.pdf

[35] Ka-Ping Yee: Aligning Security and Usability, IEEE Security & Privacy, Volume 2, Issue 5, September 2004

2.7 DIE EINE LEUCHTTURM-ANWENDUNG EXISTIERT NICHT – ABER VIELE ANWENDUNGEN (DAS HENNE-EI-PROBLEM)

Ohne Online-Dienste keine Nachfrage für die Online-Ausweisfunktion, keine Nachfrage für die Online-Ausweisfunktion verhindert wiederum neue Online-Dienste – das Henne-Ei-Problem war bekannt. Um diese Kausalkette zu durchbrechen, wurde schon in der Anwendungstestphase nach Leuchtturmanwendungen gesucht.

Es bestand der Wunsch, Geschäftsvorfälle mit hohem Nutzerpotenzial mit dem neuen Personalausweis zu verbinden. Internationale E-Commerce-Diensteanbieter zeigten jedoch wenig Interesse, eine deutsche Lösung in ihr Portfolio einzubinden, da die Zielgruppe zu klein war.[36] Banken und Kreditinstitute bieten zwar Dienstleistungen an, die eine sichere Identifizierung und Authentifizierung benötigen, hatten allerdings schon diverse eigene Sicherheitslösungen für das Online-Banking implementiert. Sogar im E-Government waren staatliche Dienstleistungen, die den neuen Personalausweis unterstützen, nur spärlich angeboten worden. Auch hier stellt die Einbindung der eID-Funktion des nPA einen zusätzlichen Aufwand dar, da ein »zweiter« Zugangskanal für E-Government-Dienste technisch und organisatorisch eingerichtet werden muss. Eine weitere Hürde sind auch die Kosten, die Diensteanbieter für die Online-Ausweisfunktion aufbringen müssen.

Im Nachhinein stellt sich also die Frage, ob die Suche nach DEN Leuchtturmanwendungen überhaupt sinnvoll ist. Wichtig ist das stetige Erweitern des Portfolios von Diensten. Dafür wurde beispielsweise 2012 die E-Government-Initiative vom Bundesministerium des Innern ins Leben gerufen. Generell sind im Laufe der letzten drei Jahre viele neue Dienste entstanden,[37] die für bestimmte Lebenslagen interessant sind. Der Erfolg der Online-Ausweisfunktion lässt sich jedoch nicht nur an der Anzahl der vorhandenen Dienstleistungen messen, sondern es ist wesentlich, dass Anwendungen geschaffen werden, die sowohl Interesse bei den Bürgern erzeugen als auch für Diensteanbieter vorteilhaft sind.

Wichtige Anwendungsszenarien sollten von Anfang an betrachtet und deren Anforderungen berücksichtigt werden. Eines der Hauptanwendungsgebiete der Online-Ausweisfunktion sind elektronische Verwaltungsprozesse im Kontext E-Government. Einige dieser Prozesse erfordern die Angabe des Geburtsnamens einer Person. Die Online-Ausweisfunktion hatte diesen zunächst nicht als elektronisch übermittelbares Feld vorgesehen. Die entsprechende Anpassung des Personalausweisgesetzes ist mit dem E-Government-Gesetz im Jahr 2013 erfolgt. Bereits ausgegebene Ausweise können jedoch nicht mehr angepasst werden. Im Ergebnis werden damit unterschiedliche Generationen von Ausweisen im Feld sein.

Neue Ideen und Prototypen entstehen für den neuen Personalausweis: beispielsweise die nPA-Box[38] zum Speichern digitaler Dokumente in bayerischen Bürgerkonten, die Unterstützung von kommunalen Bürgerbegehren durch die BuergerCloud[39], Android-Smartphones[40] mit NFC-Chips, mit denen sich die Online-Ausweisfunktion des Personalausweises ohne Kartenleser nutzen lässt, oder ein Open-Source-eID-Client[41] für Android. Auch Brückentechnologien wie Bluetooth-fähige Kartenleser können einen wichtigen Beitrag leisten, wie sie etwa vom OpeneID-Projekt unterstützt werden. Mittlerweile sind auch im Bankensektor schon Einsatzmöglichkeiten vorhanden, beispielsweise zur Kontoeröffnung oder zum Geldabheben.[42] Ebenfalls

[36] Andreas Poller, Ulrich Waldmann, Sven Vowé, and Sven Türpe: Electronic Identity Cards for User Authentication – Promise and Practice, IEEE Security and Privacy, January/February 2012, Vol. 10, No. 1, pp. 46-54

[37] Kompetenzzentrum Neuer Personalausweis, Übersicht über Online-Anwendungen, http://www.ccepa.de/onlineanwendungen

[38] IT-Beauftragte der Bayerischen Staatsregierung Anstalt für Kommunale Datenverarbeitung in Bayern Unternehmensberatung H&D GmbH: Die nPA-BOX – Der persönliche Datensafe im Internet, Konzeptstudie im Rahmen Bayerischer Bürgerkonten, 11. April 2013, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10._Sitzung/nPA-Box.pdf

[39] BuergerCloud – Demokratie aus der Wolke, http://buergercloud.de

[40] AGETO AG, Personalausweis per NFC: AGETO und NXP schaffen Basis für mobilen Einsatz des neuen Personalausweises ohne Kartenlesegerät, Pressemitteilung, 5. März 2013, http://www.ageto.de/presse/pressemitteilungen/91-ageto-ag/433-ageto-und-nxp-schaffen-basis-fuer-mobilen-einsatz-des-neuen-personalausweises-ohne-kartenlesegeraet

[41] Detlef Hühnlein, Dirk Petrautzki, Johannes Schmölz et al.: On the design and implementation of the Open eCard App. In: N. Suri, M. Waidner (Hrsg.): Sicherheit, Schutz und Zuverlässigkeit (SICHERHEIT 2012), 07.-09.03.2012, GI-Edition – Lecture Notes in Informatics (LNI) 195, pp. 95-110

[42] Webseite, Bankgeschäfte mit dem neuen Personalausweis, www.npa-banken.de

wird die Signaturfunktion endlich erprobt.[43] Auch am Einsatz des nPA an Automaten oder zur Zutrittskontrolle wird gearbeitet. Hier ist teilweise die PIN-Eingabe ein Handicap, da diese geschützt erfolgen muss und den Prozess »verlangsamt«. Aus Datenschutzgründen ist jedoch der Einsatz der Online-Ausweisfunktion ohne PIN-Eingabe bisher nicht möglich. Im eIDEE-Wettbewerb werden neue Anwendungen prämiert und mit dem nPA können hier auch Bürger ihre Favoriten wählen.[44]

2.8 TECHNISCHE ENTWICKLUNGEN FRÜHZEITIG ERKENNEN UND EINBEZIEHEN

Jedes Großprojekt basiert zum Entwurfs- und Einführungszeitpunkt auf einem bestimmten technischen Wissen sowie auf verfügbaren technischen Produkten. Aufgrund der langen Vorbereitungszeit sind aber gegebenenfalls zum Inbetriebnahmezeitpunkt neue interessante Entwicklungen auf dem Markt zu verzeichnen.

Am Beispiel der Entwicklung von Mobiltelefonen (1994 erste SMS, 1997 erstes Handy mit Farbdisplay, 2007 erstes iPhone) kann man erkennen, dass zum Zeitpunkt der Planung des neuen Personalausweises Smartphones mit ihrer großen Funktionalität noch nicht existierten, diese sich jetzt jedoch zunehmend zum persönlichen Assistenten entwickeln. Natürlich stellt sich daher heute die Frage, wie sich der neue Personalausweis und das Smartphone sinnvoll ergänzen.

Für die Verbreitung und nachhaltige Nutzung einer technischen Innovation ist es generell wichtig, dass aktuelle Technologieentwicklungen gesichtet und neue Trends frühzeitig erkannt und einbezogen werden. So können Akzeptanz- und Begeisterungsfaktoren die Nutzung der Innovation durch den Bürger positiv beeinflussen. Dies ist insbesondere für Sicherheitsinnovationen wie dem nPA notwendig, da Sicherheitsprodukte anfangs schwer zu motivieren sind. Beispielsweise war in den 60er Jahren der Sicherheitsgurt im Auto noch umstritten; durch ständige Neu- und Weiterentwicklungen wie Seitenaufprallschutz, Airbag oder CityStop haben es die Autohersteller jedoch verstanden, Sicherheit als Qualitätskriterium zu etablieren.

[43] Bundesdruckerei, sign-me – Online-Signatur mit dem neuen Personalausweis, http://www.bundesdruckerei.de/de/199-sign-me

[44] eIDEE-Wettbewerb, »eIDEE – Wettbewerb für den digitalen Handschlag« ist eine Initiative der Bundesdruckerei GmbH, https://www.digitaler-handschlag.de/

3. ZUKÜNFTIGE POTENZIALE UND HERAUSFORDERUNGEN

Die sichere elektronische Kommunikation zwischen Bürgern, Verwaltung und Privatwirtschaft bildet die Grundlage für die digitale Gesellschaft des 21. Jahrhunderts. Der neue Personalausweis ist ein Schritt hin zu vertrauenswürdigen Identitäten. Aber es existieren noch viele Herausforderungen und bisher unbekannte Möglichkeiten auf diesem Weg. Im Folgenden sind technische und organisatorische Potenziale aufgeführt, die kurz-, mittel- oder langfristig den Einsatz der Online-Ausweisfunktion befördern könnten.

Für den Bürger

Die Einführung von temporären und permanenten Bürgerkonten bietet Bürgern die Möglichkeit, sich zu identifizieren und gegebenenfalls auch wichtige Dokumente zu verwalten oder weitere E-Government-Transaktionen vorzunehmen.[45] So könnte optional auch eine Historie ausgeführter eID-Transaktionen angelegt werden. Da Bürgerkonten meist kommunal angeboten werden, sollte bei einem Umzug auch das Bürgerkonto mit »umziehen« können, d. h. Austauschformate und Softwarewerkzeuge sind erforderlich. Neben einer ausführlichen Beratung und den Testmöglichkeiten des Personalausweises auf den Bürgerämtern und der Selbstauskunft auf dem Personalausweisportal sind auch neue Ideen erwünscht, wie beispielsweise das Begleiten von Erstnutzern mit einem »First-User-Wizard« oder das unverbindliche Ausprobieren mit der Anwendung »Ausprobieren wird belohnt«, [46] die mit einer Spendenfunktion verbunden wird. Neben neuen Anwendungen sollte auch die Bedienbarkeit der eID-Software weiter verbessert werden. Schwierigkeiten bei Anwendern verursacht beispielsweise, dass die PIN nicht über die PUK neu gesetzt werden kann, wie es vom Mobilfunk bekannt ist und dass nicht festgestellt werden kann, ob die initiale Transport-PIN noch unversehrt ist.

Generell muss der neue Personalausweis an prominenten Stellen auch weiterhin beworben werden. Positive Kommunikation in Zusammenhang mit neuen Angeboten ist notwendig.

Mobile Nutzung

»Jeder vierte Bundesbürger (24 %) kann sich vorstellen, seinen Ausweis zu Hause zu lassen und sich unterwegs mit seinem Smartphone zu identifizieren«.[47] Es ist daher essenziell, dass der neue Personalausweis mobil mit Smartphones verwendet werden kann. Hier bieten sich verschiedene Einsatzmöglichkeiten für die Kombination der beiden Techniken an: (1) Apps für Funktionen rund um den Personalausweis[48] wie beispielsweise die PIN-Aktivierung, (2) Verwendung des mobilen Endgeräts als Kartenleser[49] oder (3) Speicherung und Nutzung von Identitäten auf dem mobilen Endgerät.[50]

Zentrale Koordinierungs- und Beratungsstelle

Derzeit sind verschiedene Behörden (BMI, BVA, BSI, Bundesnetzagentur) und Firmen (Bundesdruckerei, OpenLimit etc.) mit diversen Aufgaben und Prozessen rund um den Personalausweis betraut. Strategisch ist dabei das BMI zuständig, technisch das BSI und rechtlich-organisatorisch das BVA. Um die Planung und Weiterentwicklung gemeinsam zu steuern, sollten Forschung, Entwicklung, Steuerung, Wissensmanagement, Beratung und Service-Hotline von einer zentralen Stelle koordiniert

[45] Vitako, Beantragung von Zertifikaten für das Auslesen von Daten aus dem neuen Personalausweis, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Material-Dienstleister/Beispielprozess_Buergerkonto.pdf?__blob=publicationFile

[46] Susanne Asheuer, Joy Belgassem, Wiete Eichhorn, Rio Leipold, Lucas Licht, Christoph Meinel, Anne Schanz und Maxim Schnjakin: Studie zur Konzeption einer Internetplattform für den neuen Personalausweis, Hasso-Plattner-Institut für Softwaresystemtechnik im Auftrag des Bundesministeriums des Innern, 21.5.2013, http://www.hpi.uni-potsdam.de/fileadmin/hpi/FG_ITS/papers/Journal/Personalausweisstudie.pdf

[47] BITKOM, Smartphone als Ausweis, http://www.bitkom.org/de/presse/8477_76612.aspx

[48] bos KG, Personalausweis lernt Android, 15.5.2012, http://www.egovernment-computing.de/kommunikation/articles/364276/

[49] J. Braun, M. Horsch, A. Wiesmaier und D. Hühnlein: Mobile Authentisierung und Signatur, DACH Security 2011, http://www.cdc.informatik.tu-darmstadt.de/mona/pubs/201109_DACH11_Mobile_Authentisierung_und_Signatur.pdf

[50] Frank Dietrich: Mobile Nutzung des neuen Personalausweises, 22. SIT SmartCard Workshop, 9.2.2012, http://www.smartcard-workshop.de/content/dam/smartcard/de/documents/WS12/21_WS2012_Folien_MobileNutzungn-PA_Dietrich.pdf

werden. Der Aufbau und Betrieb dieser Koordinierungs- und Beratungsstelle könnte beispielsweise im BVA angesiedelt sein.

Bundes-eID-Server für Behörden

Für die Umsetzung des E-Government-Gesetzes wird die Nachfrage zur Anbindung der Online-Ausweisfunktion insbesondere aus der Bundesverwaltung steigen. Dafür wäre der Aufbau und Betrieb eines eigenen Bundes-eID-Servers sinnvoll. Unterschiedliche Dienste von Behörden könnten einfacher und kostengünstiger angebunden werden. Der eID-Service könnte bei einem zentralen IT-Dienstleister des Bundes wie beispielsweise der Bundesstelle für Informationstechnik (BIT) des Bundesverwaltungsamtes betrieben werden und deren bestehende Infrastruktur des Hochleistungsrechenzentrums nutzen.

Konformitätstests

Derzeit entstehen verschiedene Open- (oder auch Closed-) Source-Entwicklungen für den neuen Personalausweis. Als problematisch könnte sich jedoch erweisen, dass sich die unterschiedlichen Implementierungen nicht oder nur teilweise konform zu den Technischen Richtlinien des BSI oder anderen eingesetzten Standards verhalten. Um einerseits Implementierungen zu fördern, andererseits aber eine »Beaufsichtigung« der verschiedenen Entwicklungen und nachträgliche Anpassungen zu vermeiden, sollten Testmöglichkeiten zur Verfügung stehen, zum Beispiel in Form von Testbeds und Testsuiten für funktionale oder Konformitätstests, PlugFest Events oder auch kostenlose Testausweise für Entwickler im wissenschaftlichen oder gemeinnützigen Bereich. Basierend auf den Testergebnissen wäre eine Konformitätsbestätigung in Form eines Zertifikats oder Siegels auch denkbar.

EU-Bürger einbeziehen

Der elektronische Identitätsnachweis mit dem neuen Personalausweis und dem elektronischen Aufenthaltstitel sind für Deutsche und Drittstaatenangehörige einsetzbar. Ausgeschlossen von der Online-Ausweisfunktion sind jedoch EU-Bürger, die weder den nPA noch den eAT besitzen. Anwendungen, die für alle Nationalitäten funktionieren müssen, sind daher nicht für die Online-Ausweisfunktion geeignet bzw. erfordern noch den Einsatz von weiteren Verfahren zur Identifizierung und Authentisierung. Angedacht, aber nicht eingeführt, ist eine Unionsbürgerkarte für gemeldete EU-Bürger.[51] Obwohl technisch einfach umsetzbar, erfordert diese Lösung jedoch entsprechende rechtliche und organisatorische Regelungen.

Interoperabilität in der EU

Viele EU-Mitgliedstaaten haben ein elektronisches Identifizierungssystem eingeführt. Diese eID-Systeme unterscheiden sich allerdings in verschiedenen Aspekten, wie Technik, eID-Daten oder ausstellende Institutionen. Bisher fehlte eine gemeinsame Rechtsgrundlage, die jeden Mitgliedstaat dazu verpflichten würde, von anderen Mitgliedstaaten ausgestellte elektronische Identifizierungsmittel für den Zugang zu Online-Diensten anzuerkennen und zu akzeptieren. Dies soll durch die zukünftige eIDAS-Verordnung geändert werden.[52] Mit der Verordnung sollen sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen grenzüberschreitend ermöglicht werden, indem die gegenseitige Anerkennung und Akzeptierung notifizierter elektronischer Identifizierungssysteme und wichtiger elektronischer Vertrauensdienste auf EU-Ebene geregelt werden. Offen ist, ob das System des neuen Personalausweises nach dem aktuellen Entwurf der Verordnung notifizierbar ist.[53] Trotzdem muss die grenzüberschreitende Authentisierung erprobt werden. Erste Ergebnisse für eine grenzüberschreitende Authentisierung mit europäischen eIDs wurden im EU-STORK-Projekt gesammelt.[54] Im Nachfolgeprojekt STORK2.0 ist Deutschland nicht vertreten. Europäische Lösungen müssen jedoch auch erprobt werden – bilaterale grenzüberschreitende Dienste sind ein erster Ansatz (z. B. »Dienst Regelingen« in den Niederlanden) und müssen ausgebaut werden.

[51] Bernd Kowalski: Perspektiven für die eID-Funktion des Personalausweises, Vortrag Ministerialkongress, Berlin, 8. September 2011, http://www.ministerialkongress.de/3b_Kowalski_MinKon_BSI_nPA_0809_2011_FINAL.pdf
[52] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung), 4. Juni 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:DE:PDF
[53] Frank Byszio, Detlef Houdeau, Gisela Meister und Klaus-Dieter Wolfenstetter: Elektronische Identifikation in Europa: die neue EU-Verordnung, Datenschutz und Datensicherheit – DuD, März 2013, pp 169-172
[54] EU STORK Projekt, 2008-2011, http://www.eid-stork.eu/

Standardisierung von Technologien, Verfahren und Protokollen

Um interoperable Lösungen zu erreichen, sind standardisierte Schnittstellen, Protokolle oder Technologien erforderlich. Das Verwenden von Standards ist dabei genauso wichtig wie die aktive Teilnahme an der Standardisierung, um beispielsweise die positiven Ergebnisse formal zu etablieren. Auch wenn die eIDs der verschiedenen Länder unterschiedlich sind, sollten insbesondere die datenschutzfördernden Funktionen (gegenseitige Identifikation, Altersbestätigung, Pseudonymfunktion) des neuen Personalausweises international besser etabliert werden.

Von der Authentifizierung zur sicheren Transaktion

Die Authentifizierung von Personen ist nur ein erster Schritt zu einer sicheren Kommunikation. Beispielsweise ist aus Sicht des Bankenverbands der Einsatz des nPA im Online-Banking und bei Bezahlverfahren mit Zahlungsgarantie noch nicht möglich,[55] da neben sicherer Identifizierung hier auch immer eine sichere Autorisierung der Transaktion erfolgen muss. Wie von TAN-Generatoren bekannt, sollten in die Transaktion die Überweisungsdaten (Kontonummer, Betrag etc.) einfließen, damit der Zahler diese überprüfen kann. Bisher werden allerdings die Übermittlung der Transaktionsdaten und die Autorisierung von den nPA-Kommunikationsprotokollen nicht unterstützt, obwohl technische Grundlagen vorhanden sind.[56]

nPA als Wurzelidentität

Der Einsatz des Personalausweises für jeden beliebigen Online-Dienst ist derzeit unwahrscheinlich, da zu viele Handlungsschritte erforderlich sind: wie Personalausweis aus der Brieftasche entnehmen, Kartenleser anschließen, PIN eingeben. Für Dienste, die ursprünglich ein persönliches Erscheinen erforderten, wie eine vertrauenswürdige Erstregistrierung, oder für den eigenen Schutz durch anonyme Nachweise (Alter, Wohnort) wird dieser Aufwand von Bürgerinnen und Bürgern eher akzeptiert werden. Für Online-Dienste, die schon heute durch Nutzername und Passwort bedienbar sind, ist die Online-Ausweisfunktion zu komplex. Hier sind vom nPA »abgeleitete« sichere Identitäten,[57] die weder Kartenleser noch nPA erfordern, sinnvoll.

nPA als Teil des Identitätsmanagements

Die personenbezogenen Daten im neuen Personalausweis umfassen nur einen Teilbereich unseres Lebensumfelds. Nicht berücksichtigt werden beispielsweise Firmenzugehörigkeit, Kinder, Bankdaten, Vereinsmitgliedschaften usw. Diese Eigenschaften, auch als Identitätsattribute bezeichnet, müssen für die Nutzung von bestimmten Dienstleistungen im Internet ebenfalls vertrauenswürdig und sicher nachgewiesen werden können. Eine nutzerkontrollierte, virtuelle Zusammenführung weiterer Identitätsdaten mit der vom Personalausweis dokumentierten elektronischen Identität wäre hier erforderlich und sollte durch ein geeignetes Identitätsmanagement unterstützt werden. Vertrauenswürdige Dritte, z. B. Identity-Provider könnten erforderliche Nachweise bereitstellen. Jedoch ist dies derzeit rechtlich nicht möglich.

Verschlüsselungszertifikate für vertrauliche Kommunikation

Die Nutzung des nPA für eine kryptografisch verschlüsselte Ende-zu-Ende-Kommunikation wäre eine zweckmäßige Erweiterung für viele Bürger, die bisher noch keine Erfahrung mit Verschlüsselung haben. Die Generierung und Verwaltung der kryptografischen Schlüssel und des Verschlüsselungszertifikats könnten wie auch für Signaturzertifikate auf dem nPA erfolgen. Jedoch erfordert die Unterstützung von Verschlüsselung noch weitere Überlegungen hinsichtlich einer weiteren PIN, Bereitstellung von Verzeichnisdiensten für die Verschlüsselungszertifikate, Migration der Schlüssel auf einen neuen nPA nach dessen Ablauf, externe Sicherung der Schlüssel im Falle des Verlusts des nPA, Software für die Nutzung usw.

---

[55] Ulrike Linde, Christoph Maggioni und Mark Rüdiger: Der neue Personalausweis im Banking, http://www.bundesdruckerei.de/sites/default/files/documents/2012/anwendungen_id_fachbeitrag__mit_gekaufter_lizenz_linde_maggioni_ruediger.pdf

[56] In der BSI-TR-03112-7 (eCard-API-Framework – Protocols) existiert im EAC-Protokoll bereits ein TransactionInfo-Feld. Der Zugriff auf das Feld wird allerdings für den eID-Server in der BSI-TR-03130 nicht unterstützt.

[57] Martin Schröder und Frank Morgner: eID mit abgeleiteten Identitäten, DuD – Datenschutz und Datensicherheit, August 2013, pp 530-534, http://www.dud.de/Premium-Inhalt/40/2619/eID-mit-abgeleiteten-Identit-#228;ten.html

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Jens Fromm
Leiter Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
jens.fromm@fokus.fraunhofer.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 1310 (Grafik: Fraunhofer FOKUS)