Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann

Kartenleser für den neuen deutschen Personalausweis

Vor- und Nachteile unterschiedlicher Lesertypen

Die Nutzung der Online-Authentisierungs-Funktion des neuen deutschen Personalausweises erfordert die Verwendung eines Chipkartenlesers. Dessen Sicherheitseigenschaften stehen dabei im Zusammenhang mit den anderen Komponenten des „Systems Personalausweis". Der folgende Beitrag stellt die Eigenschaften der verschiedenen Lesertypen gegenüber und bewertet auf dieser Basis deren Vor- und Nachteile.

Dr. Jens Bender

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI)
E-Mail: Jens.Bender@bsi.bund.de

Dr. Dennis Kügler

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI)
E-Mail: Dennis.Kuegler@bsi.bund.de

Dr. Marian Margraf

Referent im Bundesministerium des Innern (BMI)
E-Mail: Marian.Margraf@bmi.bund.de

Dr. Ingo Naumann

Bis Juni 2010 tätig als Referent im BSI, zuletzt abgeordnet zur ENISA. Jetzt Systems Security Engineer bei den Vereinten Nationen in Wien.
E-Mail: naumann@ieee.org

Einleitung

Am 1. November 2010 wird in Deutschland der neue Personalausweis mit integriertem kontaktlosen Chip eingeführt. Dieser Chip dient der Unterstützung von drei Funktionen:

- eine Biometriefunktion ausschließlich für die hoheitliche Verwendung (wie z.B. die Grenzkontrolle);
- der elektronische Identitätsnachweis (kurz eID-Funktion oder eID) oder auch Online-Authentisierung realisiert eine gegenseitige Authentisierung zweier Kommunikationspartner über das Internet, so dass beide Parteien wissen, mit wem sie kommunizieren;
- die qualifizierte elektronische Signatur (QES) nach deutschem Signaturgesetz stellt das Äquivalent zur eigenhändigen Unterschrift im elektronischen Rechts- und Geschäftsverkehr dar.

Der rechtliche Rahmen wird dabei durch das Personalausweisgesetz vorgegeben [1]. Die technische Umsetzung wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Form von Technischen Richtlinien, Common-Criteria-Schutzprofilen und Certificate Policies spezifiziert [2].

1 eID und Signatur

Für den Privatanwender relevant sind die eID-Funktion und die Signaturfunktion. Um einen Rahmen für die folgende Diskussion der Sicherheitseigenschaften zu setzen, wird zunächst an einem Beispiel das Zusammenspiel und die Abgrenzung dieser Funktionen an einem „nicht-elektronischen" Beispiel, der Abwicklung eines Bankgeschäfts, dargestellt.

Dabei stellen in einem ersten Schritt die beiden (Geschäfts-) Partner – Kunde und Bank – gegenseitig ihre Identität fest. Für den Kunden ist dies offensichtlich: Er betritt das Gebäude einer bestimmten Bank. Die Bank wiederum identifiziert den Kunden z. B. anhand seines Personalausweises. Somit hat eine gegenseitige Authentisierung stattgefunden, ohne dass dies rechtliche Wirkung entfalten würde.

Erst in einem zweiten Schritt wird ein Vertrag geschlossen oder eine Transaktion autorisiert. Ein Vertrag kommt grundsätzlich durch zwei Willenserklärungen zustande: Angebot durch den Dienstanbieter und Annahme durch den Kunden. In vielen Fällen ist die Schriftform für diese Erklärungen nicht notwendig, d. h. sobald sich beide Seiten handelseinig sind, kommt auch ohne Unterschrift ein Vertrag (durch konkludentes Handeln) zu Stande.

Das Beispiel lässt sich in die Online-Welt übertragen. Hier werden heute üblicherweise für den ersten Schritt eine Nutzer-Authentisierung mittels Nutzername und Passwort (oder PIN) eingesetzt, wobei dies eine schon bestehende Beziehung zwischen Nutzer und Dienstanbieter voraussetzt. Sofern der Nutzer noch nicht bekannt ist, wird von Online-Anbietern häufig auf eine Lieferung per Nachnahme zurückgegriffen, um die fehlende Identi-

Tabelle 1 | eID und Signatur

	Traditionell	Elektronisch	
		1-Faktor	2-Faktor
Verifikation der Identität	Vorlage des Ausweises	Passwort	eID
Transaktion	Unterschrift	TAN	QES

fizierung auszugleichen. Der Dienstanbieter wird dabei meist über die Webadresse und ein SSL-Zertifikat identifiziert. Für den zweiten Schritt der Transaktionsauthentisierung werden oft TAN-Verfahren eingesetzt.

Allen diesen Verfahren ist gemeinsam, dass es sich um Ein-Faktor-Authentisierungen handelt. Einige Dienstanbieter, vornehmlich Banken, bieten auch eine Zwei-Faktor-Authentisierung mit einem entsprechend deutlich höheren Sicherheitsniveau an. Hierfür sind jeweils die beiden Faktoren Besitz (physikalisches Token, z. B. Chipkarte, USB-Dongle) und Wissen (normalerweise ein Passwort) erforderlich.

Der neue Personalausweis bietet diese Möglichkeit fortan auch ohne vorherige Registrierung durch den Dienstanbieter. Dafür sind die beiden Faktoren Besitz (Ausweis) und Wissen (eID-PIN bzw. Signatur-PIN) notwendig.

2 Die Online-Authentisierung

Die Online-Authentisierung bildet die oben dargestellte gegenseitige Authentisierung von Ausweisinhaber und Dienstanbieter kryptografisch ab. Der Dienstanbieter benötigt ein Berechtigungszertifikat, das durch den Chip selbst überprüft wird. Dieses Berechtigungszertifikat enthält neben Angaben zum Dienstanbieter auch die maximal möglichen Zugriffsrechte.

Im ersten Schritt der Online-Authentisierung wird dieses Zertifikat dem Ausweisinhaber angezeigt. Hier besteht auch die Möglichkeit, die Rechte des Dienstanbieters weiter einzuschränken. Sind die Zugriffsrechte zur Zufriedenheit des Ausweisinhabers festgelegt und ist er mit der Datenübertragung zum Dienstanbieter einverstanden, so startet er die Online-Authentisierung durch die Eingabe seiner persönlichen geheimen PIN. Die PIN wird durch den Ausweis mit Hilfe des PACE-Protokolls verifiziert, einem kryptografischen Protokoll, bei dem die PIN selbst nicht im Klartext übertragen wird.

Im nächsten Schritt überprüft der Ausweis die Gültigkeit des Berechtigungszertifikates mit Hilfe der Terminalauthentisierung, für die der Dienstanbieter den Besitz des zum Zertifikat gehörigen geheimen Schlüssels nachweisen muss. Nach der Überprüfung der Authentizität des Dienstanbieters erfolgt die Überprüfung der Echtheit des Ausweises durch die Chipauthentisierung in Verbindung mit der passiven Authentisierung.

Ergebnis der Terminal- und Chipauthentisierung ist (neben dem Echtheitsnachweis des Ausweises) ein Ende-zu-Ende verschlüsselter und integritätsgesicherter Kanal zwischen Chip und Dienstanbieter. Ausschließlich innerhalb dieses Kanals kann der Dienstanbieter entsprechend seiner Rechte personenbezogene Daten aus dem Ausweis auslesen. Weder ein Angreifer im Internet noch auf dem lokalen Rechner (z. B. mittels eines Trojaners) des Ausweisinhabers kann diese Daten mitlesen oder manipulieren.

Eine ausführliche Beschreibung der Online-Authentisierung findet sich in [3]. Die verwendeten kryptografischen Protokolle (PACE, Terminal- und Chipauthentisierung) werden in [4] definiert, das Gesamtsystem Personalausweis wird in [5] beschrieben. Einen Vergleich der Sicherheits- und Datenschutzeigenschaften verschiedener elektronischer Ausweise in Europa bietet [6].

3 Die Umgebung des Nutzers

Für die Nutzung der Online-Authentisierung benötigt der Ausweisinhaber neben dem Ausweis selbst und der zugehörigen PIN einen Rechner mit Internetanschluss und einer Client-Software sowie ein Personalausweis-kompatibles Kartenlesegerät. Diese Umgebung muss folgende Funktionen zur Verfügung stellen:

- Anzeige des Berechtigungszertifikates und Möglichkeit der Abwahl von Datenfeldern durch den Ausweisinhaber;
- PIN-Eingabe und Durchführung des PACE-Protokolls zwischen Ausweischip und Kartenlesegerät bzw. Rechner des Nutzers;
- Durchleiten der Kommandos für die Terminal- und Chipauthentisierung zwischen Chip und Dienstanbieter sowie der verschlüsselten Kommunikation zum Auslesen der freigegebenen Daten bzw. Funktionen.

Das Auslesen personenbezogener Daten erfolgt immer Ende-zu-Ende-verschlüsselt und integritätsgesichert zwischen Chip und Dienstanbieter, d. h. weder Lesegerät noch Client-Software sind für die Vertraulichkeit oder den Manipulationsschutz der personenbezogenen Daten verantwortlich. Das PACE-Protokoll läuft lokal in der Umgebung des Benutzers ab.

Daraus lassen sich folgende benötigte Sicherheitsfunktionen ableiten:

- Schutz der PIN-Eingabe gegen Abhören
- Schutz der Anzeige (und Datenfelderabwahl) gegen Verfälschung

Aufgrund der Nutzung des öffentlichen Internet ist ein Verhindern der Durchführung einer Online-Authentisierung durch das Unterbrechen der Verbindung (Denial-of-Service) immer möglich. Dieser Angriff wird im Folgenden daher nicht weiter betrachtet.

Als Chipkartenleser stehen für den Personalausweis nun verschiedene Typen zur Auswahl:

- Basisleser ohne Sicherheitsfunktionen. Da bedingt durch die kontaktlose Schnittstelle kein fester Formfaktor vorgegeben ist, ist dieser Typ sehr flexibel. So können Leser dieses Typs z. B. leicht in Laptops oder Tastaturen integriert werden, so dass kein zusätzliches Gerät notwendig ist.
- Standardleser mit integriertem PIN-Pad und Fähigkeit zur Durchführung des PACE-Protokolls. Standardleser können weiterhin optional ein Display enthalten.
- Komfortleser enthalten verpflichtend PIN-Pad und Display und unterstützen als einziger Lesertyp die qualifizierte Signatur mit dem Personalausweis.

Diese Lesertypen werden in der Technischen Richtlinie „Anforderungen an Chipkartenleser mit ePA-Unterstützung“ definiert [7]. Die je nach Typ jeweils nicht im Leser umgesetzten Sicherheitsfunktionen werden in der Client-Software integriert, die in der Technischen Richtlinie „eCard-API-Framework“ definiert wird [8]. Der Bund stellt eine zertifizierte Implementierung dieser Richtlinie in Form

einer Applikation, der „AusweisApp", kostenfrei zur Verfügung.

Im Folgenden werden die verschiedenen Chipartenleser-Typen in Bezug auf die genannten Sicherheitsfunktionen analysiert.

3.1 Sichere Anzeige

Im Zuge der Online-Authentisierung werden dem Ausweisinhaber wesentliche Angaben aus dem Berechtigungszertifikat des Dienstanbieters angezeigt, u. a. der Namen des Dienstanbieters, Angaben zum Zweck der Datenübermittlung sowie Hinweise auf die zuständige Datenschutzbehörde. Eine weitere wesentliche Angabe ist eine Liste der vom Dienstanbieter gewünschten Datenfelder, die dieser aus dem Ausweis auslesen will. Diese Liste kann vom Bürger weiter eingeschränkt werden, er kann allerdings keine Datenfelder hinzufügen, die nicht durch das Berechtigungszertifikat des Dienstanbieters abgedeckt sind.

Das Display eines Kartenlesers bietet üblicherweise die Möglichkeit, wenige Zeilen Text (meist zwei) anzuzeigen. Dies reicht nicht aus, um die im Zertifikat enthaltenen Daten umfassend und übersichtlich darzustellen. Daher kann das Leserdisplay in der Praxis maximal zur nochmaligen, stichprobenartigen Überprüfung der bereits durch die Client-Software angezeigten Daten dienen.

Da eine Online-Authentisierung immer ein gültiges Berechtigungszertifikat eines Dienstanbieters voraussetzt, ist es nicht möglich, durch ein Verfälschen der Anzeige unberechtigt personenbezogene Daten des Ausweisinhabers zu erhalten. Es ist höchsten möglich, mit Hilfe einer falschen Angabe dem Nutzer vorzutäuschen, weniger personenbezogene Daten auszulesen, als tatsächlich übermittelt werden, oder eine Authentisierung gegenüber einem anderen Dienstanbieter durchzuführen, als vom Nutzer gedacht. In jedem Fall kann der Dienstanbieter aber nur die im Berechtigungszertifikat vorgesehenen Felder auslesen.

3.2 PIN-Eingabe

Die Vertraulichkeit der PIN kann durch verschiedene Angriffsmethoden verletzt werden:

- Ausnutzen des Verhaltens des Ausweisinhabers, wenn dieser z. B. die PIN aufgeschrieben zusammen mit dem Ausweis verwahrt;
- elektronisches Mitlesen der PIN bei der Eingabe, je nach eingesetztem Leser erfordert dies eine Manipulation der Leserfirmware bzw. den Einsatz eines Trojaners (Keyloggers) auf dem Rechner des Ausweisinhabers;
- Ausspähen der PIN bei der Eingabe unabhängig von der Art des eingesetzten Lesegeräts.

Für die Bewertung dieses Angriffs müssen wir zunächst die Auswirkungen eines Angriffs auf die PIN untersuchen.

Wesentlicher Unterschied zu klassischen Authentisierungsverfahren ist hier, dass der Angreifer in jedem Fall zusätzlich zur Kenntnis der PIN auch Zugriff auf den Ausweis benötigt, um eine Authentisierung durchführen zu können. Dies kann

Tabelle 2 | Angriffe auf Authentisierungsverfahren

Verwendetes Authentisierungsverfahren	Passwort	Online-Authentisierung	
Angriffe und Maßnahmen		Basisleser	Leser mit PIN-Pad
Abgreifen von Passwort/PIN	Trojaner/Keylogger, je nach verwendetem Verfahren auch direktes Mitlesen der Übertragung des Passwortes	Trojaner/Keylogger	Firmwaremanipulation des Lesers
Missbrauch von Passwort/PIN	Voller Zugriff auf alle passwortgeschützten Zugänge bei Dienstanbietern	Kein Missbrauch möglich ohne gleichzeitigen Zugriff auf die Karte	
Gegenmaßnahmen	Ändern aller Passwörter, Verwenden einer Zwei-Faktor-Authentisierung	Ändern der PIN, Ausweis nach Benutzung vom Leser nehmen, bei Verlust des Ausweises Sperren des Ausweises	
Umleitung der Authentisierung bzw. der personenbezogenen Daten	Umleitung zu beliebigen Angreifern sowohl durch Trojaner als auch externe Angriffe (z.B. DNS-Spoofing) möglich	Umleitung nur zu Dienstanbietern mit Berechtigungszertifikat möglich, erfordert Verfälschung der Anzeige des Zertifikates durch einen Trojaner	
Weiter mögliche Auswirkungen eines Trojaners	Lesen und Manipulation aller auf dem Rechner gespeicherten Daten, Mitlesen des Bildschirms, Mitlesen aller Tastatureingaben, Mitlesen der kompletten Internetkommunikation		
Gegenmaßnahmen	Verwendung aktueller Antivirensoftware und Firewall, Installation aller Sicherheitsupdates		

entweder durch direkten physikalischen Zugriff geschehen (Diebstahl des Ausweises) oder durch Ausnutzung des Nutzerverhaltens, wenn dieser den Ausweis auf dem Kartenleser liegen lässt oder auf den Kartenleser legt, da er gerade eine Authentisierung durchführen möchte.

In keinem Fall kann der Angreifer auf personenbezogene Daten des Ausweises zugreifen, wenn er nicht selbst über ein Berechtigungszertifikat verfügt. Ein Auslesen ist nur durch einen Dienstanbieter mit Berechtigungszertifikat möglich. Ist der Angreifer selbst Dienstanbieter (oder arbeitet er mit einem zusammen), so kann er zwar personenbezogene Daten erlangen, ist allerdings selbst über das Berechtigungszertifikat und die zugehörige Registrierung bei der Vergabestelle für Berechtigungszertifikate (VfB) schnell zu identifizieren. In diesem Fall wird ihm mindestens das Berechtigungszertifikat entzogen werden, so dass eine weitere missbräuchliche Nutzung ausgeschlossen wird.

Der mögliche Schaden wird weiter dadurch beschränkt, dass die eID-Funktion nur der Verifikation der Identität dient, es wird keine Transaktion (wie z. B. ein Kauf) autorisiert.

4 Gegenmaßnahmen

Aus der Analyse der genannten Angriffe ergeben sich unmittelbar einige Gegenmaßnahmen.

- Wesentliche und wichtigste Sicherheitsmaßnahme ist die Absicherung des Rechners durch Antivirensoftware, die Benutzung einer (Personal) Firewall und die Installation aktueller *Sicherheitsupdates. Diese Maßnahmen werden vom BSI unabhängig von der Verwendung der Online-Authentisierung grundsätzlich empfohlen [9]. Auch in der Rechtsprechung wird eine Pflicht des Nutzers zur angemessenen Sicherung eines am Internet angeschlossenen Rechners bestätigt (z.B. LG Köln 5.12.2007, 9 S 195/07).
- Der Ausweis sollte nach der Nutzung vom Leser genommen werden. Diese Maßnahme ist auch bei anderen Kartensystemen (z. B. Signaturkarten oder kryptografische USB-Token) üblich.
- Die Kontrolle über den Ausweis sollte niemals aufgegeben, insbesondere sollte er nicht hinterlegt werden. Das neue Personalausweisgesetz enthält in § 1 (1) Satz 3 die Regelung, dass der Ausweisinhaber nicht zu einer Hinterlegung aufgefordert werden darf [1], wie es zur Zeit noch in manchen Hotels üblich ist.
- Besteht der Verdacht einer kompromittierten PIN, kann der Ausweisinhaber jederzeit seine PIN ändern. Mit Kenntnis der aktuellen PIN kann dies am eigenen Rechner erfolgen, ohne ist dies in der Ausweisbehörde möglich.
- Zusätzlich ist jederzeit die Sperrung des Ausweises über die Ausweisbehörde oder die Sperrhotline möglich (siehe auch [10]).

Diese Maßnahmen spiegeln sich auch in § 27 des Personalausweisgesetzes wider [1].

5 Risikoabschätzung

Wesentlicher Punkt bei der Bewertung eines Angriffs auf die PIN ist die Verwendung der Karte als zusätzliche Absicherung: Mit der PIN alleine kann der Angreifer nichts erreichen, er benötigt auch Zugriff auf den Ausweis selbst. Weiter kann der Angreifer auch bei Kenntnis der PIN und Zugriff auf den Ausweis nicht die personenbezogenen Daten auslesen. Er benötigt weiter die Zusammenarbeit mit einem Dienstanbieter, da ohne Berechtigungszertifikat keine Daten ausgelesen werden können.

In jedem Fall besteht also durch die Verwendung der zwei Faktoren Ausweis und PIN ein deutlicher Sicherheitsgewinn gegenüber den heute üblichen rein wissensbasierten Verfahren, da bei letzteren der Angreifer unmittelbar im Besitz aller notwendiger Informationen zum Ausnutzen des Angriffs ist.

Dem Sicherheits-Vorteil eines Lesers mit PIN-Pad stehen die Vorteile des Basislesers gegenüber: wesentlich geringere Kosten für den Ausweisinhaber sowie leichtere Integrierbarkeit in z. B. Laptops oder Tastaturen. So verringert der Basisleser die Einstiegshürde erheblich und führt daher voraussichtlich zu einem sowohl allgemeinen als auch individuellen Sicherheitsgewinn aufgrund einer größeren Verbreitung der Online-Authentisierung mit dem Personalausweis. Die Unterstützung der verschiedenen Lesertypen erlaubt es jedem Bürger, anwendungsbezogen den für ihn geeigneten Leser auswählen.

Vollständig verhindert werden können Angriffe auf die PIN (Ausspähen, Ausnutzung des Nutzerverhaltens) allerdings auch durch die Verwendung von Lesegeräten mit PIN-Pad nicht. Zudem birgt ein Trojaner-Angriff weitere, wesentlich weiter reichende Gefahren. So kann z. B. ein Angreifer vollen Zugriff auf alle auf einem Rechner gespeicherten Dateien nehmen oder die gesamte Kommunikation des Rechners mit dem Internet mitlesen (alle E-Mails, Webseiten usw.). Das Mitlesen und natürlich auch die Manipulation des gesamtem Netzverkehres ist für einen

solchen Angreifer auch möglich, wenn die Kommunikation verschlüsselt erfolgt, da die Verschlüsselung, sofern keine Hardware-Token wie z. B. der neue Personalausweis eingesetzt werden, auf dem angegriffenen Rechner erfolgt.

6 Auswirkungen auf Rechtsgeschäfte

Die Online-Authentisierung entspricht dem Vorzeigen des Personalausweises und ist technisch entsprechend ausgestaltet. Kryptografisch ist die Authentisierung nur für den Zeitpunkt der Authentisierung gültig, insbesondere kann der Dienstanbieter die Authentisierung nicht gegenüber Dritten nachweisen. Die Online-Authentisierung ist damit eine reine Authentisierung und keine Willenserklärung.

Sofern ein Vertrag über das Internet abgeschlossen werden soll, ist also neben der Online-Authentisierung die Abgabe einer Willenserklärung notwendig. Sofern die Schriftform erforderlich ist, bietet sich hier die qualifizierte elektronische Signatur an, die vom neuen Personalausweis unterstützt wird und jederzeit auch nach Ausweisausgabe nachgeladen werden kann. Ist die Schriftform nicht erforderlich, können auch andere Methoden (wie schon heute üblich) eingesetzt werden.

Wird ein Ausweis missbräuchlich verwendet, liegt eine Täuschung des Dienstanbieters in der Person des Kunden vor. Die vom Angreifer abgegebene Willenserklärung ist für den Inhaber des Ausweises nicht bindend.

6.1 Zertifizierung von Kartenleser und AusweisApp

Zur Verifikation können Kartenleser und Client-Software gemäß den entsprechenden Sicherheitsrichtlinien zertifiziert werden. Das BSI empfiehlt grundsätzlich den ausschließlichen Einsatz zertifizierter Komponenten.

Bei der Zertifizierung werden zunächst die korrekte Zusammenarbeit der einzelnen Komponenten untereinander und mit dem Ausweis durch Konformitätstests untersucht. Weiter wird die korrekte Implementierung der jeweiligen Sicherheitsfunktionen betrachtet, bei Lesegeräten also das PIN-Pad und das Display, soweit vorhanden. Sofern ein Leser die Möglichkeit eines Firmware-Updates bietet, so wird auch dieses auf Manipulationssicherheit analysiert.

6.2 Qualifizierte Signatur

Die eID-Funktion dient ausschließlich der Authentisierung des Ausweisinhabers. Im Gegensatz dazu dient die qualifizierte Signatur der rechtsverbindlichen Signatur eines elektronischen Dokumentes mit den entsprechenden Rechtsfolgen. Aus dieser grundsätzlich anderen Zielrichtung der qualifizierten Signatur ergibt sich auch eine gegenüber der eID-Funktion andere Sicherheitsbewertung.

Für die qualifizierte Signatur ist die Verwendung eines Kartenlesers mit integriertem PIN-Pad unerlässlich, so wie dies auch bei anderen Signaturkarten üblich ist. Allerdings wird bei letzteren die Verwendung eines entsprechenden Lesers im Gegensatz zum neuen Personalausweis nicht technisch erzwungen.

Für die Signaturfunktion des Personalausweises wird erstmals durch die Karte selbst die Verwendung eines geeigneten Lesers überprüft. Dazu enthalten Komfortleser einen sicheren Schlüsselspeicher, der ein Zertifikat und den zugehörigen privaten Schlüssel für die Leserauthentisierung enthält. Ein entsprechendes Zertifikat erhalten ausschließlich nach Signaturgesetz bestätigte Komfortleser. Somit wird auch für diese Funktion mit dem Personalausweis ein zusätzlicher Sicherheitsgewinn erzielt.

Fazit

Auch wenn Kartenleser mit PIN-Pad einen Sicherheitsvorteil gegenüber Lesern ohne PIN-Pad bieten, so tritt dieser Vorteil doch gegenüber dem massiven Sicherheitsgewinn des Personalausweises auch mit Basisleser gegenüber den heute üblichen Passwort-Verfahren zurück. Aufgrund der nicht unerheblichen Kostenunterschiede zwischen Lesern mit und ohne PIN-Pad erscheint das Ausschließen von Basislesern mit dem Ergebnis, dass viele Bürger bei den Passwort basierenden Verfahren bleiben, nicht gerechtfertigt.

Um die Einführung der elektronischen Funktionen des Personalausweises zu unterstützen, fördert der Bund die Verbreitung von Kartenlesern durch ein Zuwendungsverfahren im Rahmen des Konjunkturpaketes II. In diesem Verfahren werden alle Lesertypen gefördert.

Literatur

[1] *Gesetz über Personalausweise und den elektronischen Identitätsnachweis* (Personalausweisgesetz – PauswG) vom 18. Juni 2009 (BGBl. I S. 1346)

[2] BSI: Webseite zu elektronischen Ausweisen; https://www.bsi.bund.de/ElektronischeAusweise

[3] Bender, J., Kügler, D., Margraf, M., Naumann, I.: *Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis*. DuD – Datenschutz und Datensicherheit, 32(3), 2008

[4] BSI: Technische Richtlinie TR-03110, *Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*

[5] BSI: Technische Richtlinie TR-03127, *Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*

[6] ENISA: Position Paper, *Privacy Features of European eID Card Specifications*. 2009

[7] BSI: Technische Richtlinie TR-03119, *Anforderungen an Chipkartenleser mit ePA-Unterstützung*

[8] BSI: Technische Richtlinie TR-03112, *eCard-API-Framework*

[9] BSI für Bürger; https://www.bsi-fuer-buerger.de

[10] Bender, J., Kügler, D., Margraf, M., Naumann, I.: *Das Sperrmanagement im neuen deutschen Personalausweis*. DuD – Datenschutz und Datensicherheit, 34(5), 2010