Der elektronische Identitätsnachweis
Einsatzmöglichkeiten des neuen Personalausweises im privat-wirtschaftlichen Umfeld

Marian Margraf

Personalausweise werden heute nicht nur zur Feststellung z. B. der Identität bei der Grenz- oder Personenkontrolle durch Polizei oder Zoll eingesetzt, sondern finden auch häufig im privatwirtschaftlichen Umfeld Anwendung. Die im Chip des zukünftigen elektronischen Personalausweises enthaltenen Funktionen a) elektronischer Identitätsnachweis und b) qualifizierte elektronische Signatur, werden dafür sorgen, dass die herkömmliche Nutzung von Personalausweisen in der »Papierwelt« auf die elektronische Welt übertragen wird. Der Artikel geht auf die Hauptideen des elektronischen Identitätsnachweises ein, erläutert insbesondere die Unterschiede zur qualifizierten elektronischen Signatur und zeigt konkrete Einsatzszenarien.

1. Einleitung

Ab 01.11.2010 wird der neue Personalausweis in Deutschland ausgegeben. Wesentliche Neuerungen dieses Dokumentes sind, neben der zukünftigen Form im Scheckkartenformat, die Integration eines kontaktlosen Chips mit ISO 14443-Schnittstelle, der sowohl eine Anwendung für den hoheitlichen Bereich enthält, z. B. im Rahmen einer Grenzkontrolle, als auch zwei Anwendungen für die Nutzung im privatwirtschaftlichen Umfeld. Einen Überblick über die elektronischen Funktionen gibt Abb. 1.

Bei der Gestaltung der elektronischen Funktionen wurden in besonderer Weise die Anforderungen an Datenschutz und Datensicherheit beachtet und umgesetzt. Ein zuverlässiger Schutz personenbezogener Daten kann nur durch ein Zusammenspiel rechtlicher Bestimmungen, organisatorischer Maßnahmen und technischer Umsetzungen gewährleistet werden. Auch für die bisherige Nutzung des Ausweises in der Papierwelt hat das bis heute gültige Personalausweisgesetz verschiedene Bestimmungen zum Umgang mit dem Dokument vorgesehen. So ist z. B. eine Kopie des Ausweises nur in Ausnahmefällen gestattet. Die Seriennummer eines Ausweises darf nicht für einen automatisierten Abgleich in Datenbanken genutzt werden und der maschinenlesbare Bereich steht außerhalb hoheitlicher Anwendungen nicht zur Verfügung.

Identifizierung für hoheitl. Anwendungen	**Authentisierung** für E-Business/E-Govern.	**Signatur** für E-Business/E-Govern.
Gesichtsbild Fingerabdruck Name, Vorname Geburtsdatum usw.	Name, Vorname Adresse Alter/Altersverifikation Pseudonym usw.	qualifizierte elektronische Signatur nach deutschem Signaturgesetz

Abb. 1: Überblick über die elektronischen Funktionen des neuen Personalausweises.

Diese Regelungen wurden in dem neuen Personalausweisgesetz übernommen. Darüber hinaus müssen aber, gerade für die Absicherungen der neuen elektronischen Funktionen, zusätzliche Sicherheitsmechanismen realisiert werden. Daher wurden bei dem Design der Funktionen des Chips insbesondere die folgenden Anforderungen umgesetzt:

- Eine Datenübermittlung erfolgt stets verschlüsselt.
- Datenübermittlungen erfolgen nur im Einvernehmen mit dem Inhaber.
- Eine Nutzung des Personalausweises durch Dritte ist nicht möglich.
- Der Inhaber weiß, wem gegenüber er seine Daten übermittelt.
- Es werden nur die Daten übermittelt, die auch benötigt werden.
- Die Nutzung kann weder von einer staatlichen noch von anderen Stellen überwacht werden.
- Mit dem Personalausweis ist auch eine pseudonyme Anmeldung möglich.
- Ein globales eindeutiges, den Personalausweis oder den Inhaber zuordenbares Merkmal, existiert nicht.

Gerade der letzte Punkt erfordert eine besondere Umsetzung zur Sperrung abhanden gekommener Ausweise, siehe Abschnitt 3.3.

In den folgenden Kapiteln werden die elektronischen Funktionen des neuen Personalausweises im Einzelnen beschrieben, wobei hauptsächlich auf den elektronischen Identitätsnachweis und dessen Unterschiede zur qualifizierten elektronischen Signatur eingegangen wird. Zum Abschluss werden dann mögliche Einsatzszenarien erläutert.

2. Anwendungen des Personalausweises im privatwirtschaftlichen Umfeld

Neben der Feststellung der Identität bei der Grenz- oder Personenkontrolle, z. B durch Polizei oder Zoll, werden Personalausweise auch regelmäßig im privatrechtlichen Umfeld genutzt. Der Grundgedanke ist dabei immer derselbe. Der Ausweisinhaber weist sich gegenüber einer anderen Person, hier z. B. gegenüber einem Geschäftspartner oder einem Behördenvertreter, mit dem für seine Person ausgestellten Dokument aus und zeigt damit, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Üblicherweise ist Ausweisinhabern bekannt, wem gegenüber sie ihre Identität nachweisen. Im geschäftlichen oder behördlichen Umfeld betritt man die Räumlichkeiten einer Institution oder lässt sich von der Person gegenüber ebenfalls einen Ausweis zeigen. Auf dieser Grundlage nehmen Ausweisinhaber an, dass die Personen gegenüber im Auftrag der so verkörperten Institutionen handeln.

Es findet also eine gegenseitige Authentisierung statt. Bei dieser Art des Identitätsnachweises handelt es sich allerdings lediglich um eine Momentaufnahme, bei der keine der beiden Parteien ohne weiteres im dauerhaften Besitz eines von Dritten anerkannten Beweises über die Identität und den Willen des anderen bleibt. Ein solcher Beweis wird durch eine eigenhändige Unterschrift geschaffen, welche bei Bedarf in Verwaltungs- oder Gerichtsverfahren herangezogen werden kann.

Ziel des neuen Personalausweises, der seit 01.11.2010 in Deutschland ausgegeben wird, ist es, diese herkömmliche Nutzung von Ausweisen in der »Papierwelt« auf die elektronische Welt auszuweiten. Dazu stehen optional zwei Funktionen für Diensteanbieter im E-Government- und E-Businessbereich zur Verfügung:

Der elektronische Identitätsnachweis (kurz eID-Funktion) realisiert eine gegenseitige Authentisierung zweier Kommunikationspartner über das Internet, so dass jede Partei weiß, mit wem sie kommuniziert.

Die qualifizierte elektronische Signatur (kurz QES) nach deutschem Signaturgesetz stellt das Äquivalent zur eigenhändigen Unterschrift im elektronischen Rechts- und Geschäftsprozess dar.

2.1. Der elektronische Identitätsnachweis

Nach der Definition aus dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist Authentisierung ein Vorgang oder Verfahren zur Überprüfung und Bestätigung einer Identität.

Geschieht dies auf Seiten des Dienstanbieters beim bisherigen Personalausweis durch Sichtprüfung der Sicherheitsmerkmale und Abgleich des Gesichtsbildes, müssen in der elektronischen Welt andere Mechanismen gefunden werden. Die Prüfung von Sicherheitsmerkmalen, d. h. das Überprüfen, ob ein echter Personalausweis vorliegt, kann durch geeignete kryptographische Echtheitsnachweise geschehen.

An Stelle der Überprüfung der Übereinstimmung körperlicher Merkmale (Abgleich des Gesichtsbildes) tritt in der elektronischen Welt die Eingabe einer geheimen PIN. Durch diesen Prozess beweist der Besitzer des Personalausweises auch Inhaber, d. h. rechtmäßiger Besitzer des Personalausweises zu sein.

Ein weiteres Ziel ist, dass sich nicht nur der Personalausweisinhaber gegenüber einem Dienstanbieter authentisiert, sondern auch der Dienstanbieter gegenüber dem Personalausweisinhaber; die Authentisierung soll also gegenseitig sein. Dies geschieht über so genannte Berechtigungszertifikate, die Dienstanbieter erhalten. In diesem ist neben Angaben zur Gültigkeit des Zertifikates, zum Inhaber des Zertifikates auch ein öffentlicher Schlüssel und die Kategorien der Daten, die der Dienstanbieter vom Chip des Personalausweises lesen darf, enthalten.

Diese Zertifikate erhalten Dienstanbieter von einer staatlichen Stelle, der Vergabestelle für Berechtigungszertifikate (VfB), die beim Bundesverwaltungsamt (BVA) betrieben wird. Dabei muss der Dienstanbieter ein berechtigtes Interesse nachweisen, personenbezogene Daten aus dem elektronischen Personalausweis auszulesen. Das berechtigte Interesse wird innerhalb einer Erforderlichkeitsprüfung festgestellt und stellt die Voraussetzung für die Vergabe von Berechtigungszertifikaten dar. Wesentliches Ziel dieses Verwaltungsaktes durch die VfB ist auch zu prüfen, welche der auf dem Chip des Ausweises gespeicherten Daten der Diensteanbieter auslesen darf. Beispielsweise erhalten Dienste, die eine Altersverifikation durchführen müssen, lediglich Zugriff auf das Datum, das beschreibt, ob der Inhaber ein gewisses Alter über- oder unterschritten hat. Andere Dienste, wie zum Beispiel Online-Versandhäuser, können darüber hinaus auch Zugriff auf Daten wie Name, Vorname und Wohnadresse erhalten.

2.2. Qualifizierte elektronische Signatur

Die elektronische Authentisierung mit der eID-Funktion des elektronischen Personalausweises soll die erforderliche Sicherheit und das Vertrauensverhältnis zwischen Anbietern und Nutzern elektronischer Dienste im Internet herstellen. Im Unterschied zum elektronischen Identitätsnachweis wird mit der eigenhändigen Unterschrift eine dauerhafte Zurechenbarkeit zu den unterzeichnenden Personen erreicht. Wird durch ein gesetzliches Schriftformerfordernis im Geschäftsverkehr bzw. Verwaltungsverfahren gemäß § 126 a Absatz 1 BGB bzw. einschlägiger Vorschriften des Verwaltungsverfahrensgesetzes ein dauerhaft zurechenbarer Beweis über die Abgabe einer Willenserklärung oder einer Handlung in der elektronischen Welt gefordert, bedarf es der qualifizierten elektronischen Signatur.

Eine wesentliche Rolle spielen dabei die Abschluss- und Warnfunktion der eigenhändigen Unterschrift als Bestätigung von übereinstimmenden Willenserklärungen. Diese dient insbesondere der Klarheit darüber, den Inhalt eines Rechtsgeschäfts verstanden und akzeptiert zu haben sowie im Streitfalle einen hinreichenden Beweis führen zu können. Dabei sollen die Vertragsparteien mit dem Akt der Unterzeichnung zugleich gewarnt werden, voreilig Verträge abzuschließen.

Der neue Personalausweis ist als sichere Signaturerstellungseinheit nach dem deutschen Signaturgesetz ausgestaltet, so dass Personalausweisinhaber jederzeit bei Bedarf ein qualifiziertes elektronisches Zertifikat auf den Chip des Personalausweises von einem Trust-Center laden lassen können.

2.3. Beispiel für die Anwendung von eID-Funktion und QES

Das nachfolgende, vereinfacht dargestellte Beispiel, soll die Übertragung der heutigen Funktionen des Personalausweises in die elektronische Welt darstellen.

Möchte ein Bankkunde ein Konto eröffnen, muss dieser heute in der Regel unter Vorlage eines gültigen Ausweisdokuments zum Identitätsnachweis persönlich erscheinen. Gemäß § 4 Abs. 4 GWG kann die Identität bei natürlichen Personen »... anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird...« geprüft werden. Mit dem Betreten der Bank vertraut der Bankkunde auf die Handlungsvollmacht der Bankmitarbeiter. Damit findet eine gegenseitige Authentisierung zwischen Kunde und Bank statt. Die Authentisierung ist dabei lediglich eine Momentaufnahme. Erst mit dem anschließenden Vertragsschluss zwischen Bank und Kunde erhält die Willenserklärung Beweiskraft. Mit Verabschiedung des PAuswG wird § 6 Abs. 2 Nr. 2 Satz 1 des GWG in der Weise ergänzt, dass die persönliche Vorlage eines Personalausweises durch die Nutzung des elektronischen Identitätsnachweises ersetzt werden kann.

Dank dieser Gesetzesänderung könnte der Prozess künftig online wie folgt abgebildet werden:

Schritte	Kontoeröffnung klassisch	Kontoeröffnung online
1. Schritt = Identitätsnachweis (eID-Funktion)		
Bank weist ihre Identität nach	Der Kunde betritt die Geschäftsräume einer Bank	Personalausweis prüft Berechtigungszertifikat der Bank
Kunde weist seine Identität nach	Personalausweis wird vom Bankangestellten geprüft.	Bank prüft elektronisch Sicherheitsmerkmale, Chip übersendet (verschlüsselt) die benötigten Daten
2. Schritt = Unterschrift (QES-Funktion)		
Abschluss des Vertrages zur Kontoführung	Der Kunde und der Bankangestellte unterschreiben den Kontoführungsvertrag.	Mit der QES-Funktion des Personalausweises und der QES eines Angestellten der Bank wird ein Vertrag über die Kontoführung signiert.

Tab.1: Vergleich klassischer und elektronischer Kontoeröffnung mit dem Personalausweis.

3. Technische Umsetzung des elektronischen Identitätsnachweises

Grundidee der eID-Funktion ist, zwischen Chip des neuen Personalausweises und Dienstanbieter einen authentisierten Diffie-Hellman-Schlüsselaustausch ablaufen zu lassen. Damit werden zwei Ziele erreicht:

- Beide Kommunikationspartner wissen, mit wem sie kommunizieren (Authentizität).
- Zwischen den Kommunikationspartnern wird ein gemeinsames Geheimnis ausgetauscht, so dass ein verschlüsselter und authentischer Kanal aufgebaut werden kann (Schlüsselaustausch).

Um zu erreichen, dass das Diffie-Hellman-Verfahren auch authentisiert ist, müssen die öffentlichen Schlüssel dem jeweiligen Kommunikationspartner zugeordnet werden können. Dies geschieht, wie im Folgenden beschrieben, über elektronische Signaturen und, um eine Bindung zwischen Inhaber und Ausweis zu garantieren, der Nutzung der nur dem Inhaber des Ausweises bekannten geheimen PIN.

Genaue Beschreibungen der kryptographischen Protokolle finden sich in der Technischen Richtlinie TR 03110, siehe [5], Anforderungen an die Mindestschlüssellänge der jeweiligen Verfahren in der Technischen Richtlinie TR 02102, siehe [6].

3.1. PACE (PIN-Eingabe)

Eine Kommunikation mit dem Chip des neuen Personalausweises kann nur dann stattfinden, wenn der Ausweisinhaber vorab seine geheime, nur ihm bekannte PIN eingegeben hat und damit einwilligt, seine Identität nachzuweisen. Dadurch wird eine sogenannte Zwei-Faktor-Authentisierung umgesetzt, die auf Besitz (Personalausweis) und Wissen (PIN) basiert.

Das zur Eingabe der PIN verwendete Protokoll PACE (Password Authenticated Connection Establishment) sorgt gleichzeitig für eine verschlüsselte Verbindung zwischen kontaktlosem Chip des Ausweises und lokalem Lesegerät, so dass weder personenbezogene Daten noch die PIN von Dritten mitgelesen werden können. Ein Sicherheitsbeweis dieses Protokolls findet sich in [1].

3.2. EAC (Terminal- und Chip-Authentisierung)

3.2.1. Terminal Authentisierung (Authentisierung des Diensteanbieters)

Zunächst ist der Dienstanbieter, wie bereits beschrieben, im Besitz eines Berechtigungszertifikats, das u. a. Name des Dienstanbieters und einen öffentlichen Schlüssel beinhaltet. Der zu diesem öffentlichen Schlüssel zugehörige geheime Schlüssel muss in einem sicheren Speicherbereich der Systemumgebung beim Dienstanbieter abgelegt werden. Weiter ist auf den Chips der neuen Personalausweise ein Rootzertifikat des BSI gespeichert, mit dem die Gültigkeit der Berechtigungszertifikate (über eine Zertifikatskette) überprüft werden kann.

Für den Verbindungsaufbau mit einem Ausweis erzeugt der Dienstanbieter ein variables Diffie-Hellman-Schlüsselpaar. Der öffentliche (Diffie-Hellman)-Schlüssel wird vom Dienstanbieter mit dem geheimen Schlüssel signiert, der zum Schlüsselpaar des Berechtigungszertifikats gehört. Diese Daten, d. h. das Berechtigungszertifikat (und die weiteren Zertifikate bis zum Rootzertifikat), der öffentliche Diffie-Hellman-Schlüssel und die zugehörige Signatur, werden zum Chip des Personalausweises gesendet.

Der Chip
- prüft die kryptographische Gültigkeit des Berechtigungszertifikates,
- prüft, ob der Dienstanbieter im Besitz des geheimen Schlüssels ist (durch ein Challenge-Response-Verfahren[1]) und
- prüft die Signatur des o. g. öffentlichen (Diffie-Hellman)-Schlüssels.

Danach weiß der Personalausweisinhaber, mit welchem Dienstanbieter er kommuniziert und dass dieser die Berechtigung erhalten hat, Daten aus dem Personalausweis anzufragen.

3.2.2. Chip-Authentisierung (Nachweis der Echtheit des Ausweises)

Der Chip des Personalausweises besitzt ein statisches Diffie-Hellman-Schlüsselpaar. Der geheime (Diffie-Hellman-)Schlüssel befindet sich in einem sicheren Speicherbereich im Chip des elektronischen Personalausweises, so dass er weder ausgelesen noch kopiert werden kann.

Der zugehörige öffentliche (Diffie-Hellman-)Schlüssel wird mit dem geheimen Schlüssel des Ausweisherstellers im Zuge der Personalisierung des Ausweises signiert. Für diesen Zweck erhält der Ausweishersteller vom BSI ein Zertifikat mit den entsprechenden Schlüsseln, d. h. auch für diese Zertifikate bildet das BSI die Root und autorisiert den Ausweishersteller zur Erstellung hoheitlicher Dokumente.

Diese Signatur wird vom Dienstanbieter durch Prüfung der Zertifikatskette bis zum Rootzertifikat verifiziert, so dass der Dienstanbieter nach erfolgreicher Prüfung weiß, dass er mit einem echten Personalausweis kommuniziert.

Um das Tracking eines elektronischen Personalausweises zu verhindern, werden Personalausweise, die während eines bestimmten Zeitraumes ausgestellt werden (z. B. im Zeitraum von drei Monaten) mit dem selben Diffie-Hellman-Schlüsselpaar ausgestattet. Ein chipkartenindividuelles Schlüsselpaar würde Dienstanbieter in die Lage versetzen, Personalausweise zu erkennen, ohne dass personenbezogene Daten überhaupt übermittelt werden. Die Sicherheit ist von dieser Lösung nicht betroffen. Im Gegensatz zu vielen anderen Lösungen authentisiert sich der Ausweisinhaber nicht über ein eindeutiges Schlüsselpaar, wie zum Beispiel in einem Challenge-Response-Protokoll, sondern, wie im folgenden Abschnitt beschrieben, über Teile der im Chip gespeicherten Daten. Das Diffie-Hellman-Schlüsselpaar dient den Dienstanbietern lediglich dazu, festzustellen, dass ein echter Personalausweis vorliegt.

3.2.3 Authentisierung des Inhabers

Nach beiderseits erfolgreichem Austausch der signierten, öffentlichen Diffie-Hellman-Schlüssel (Diffie-Hellman-Schlüsselaustausch) kann jede Seite mit dem eigenen geheimen Diffie-Hellman-Schlüssel und dem öffentlichen Diffie-Hellman-Schlüssel der

1 Dieses Verfahren dient der Authentisierung und dem Nachweis, dass der Diensteanbieter im Besitz des ihm zugeteilten geheimen Schlüssels ist. Der Ausweischip erzeugt eine Zufallszahl und sendet diese an den Diensteanbieter. Dieser signiert diese Zufallszahl mit dem geheimen Schlüssel, der zum Schlüsselpaar des Berechtigungszertifikats gehört. Der Ausweischip prüft entsprechend die Signatur mit dem dazugehörigen öffentlichen Schlüssel.

Gegenseite das gleiche kryptographische Geheimnis erzeugen. Aus diesem Geheimnis werden kryptographische Schlüssel zur Authentisierung und Verschlüsselung der zu übertragenden personenbezogenen Daten abgeleitet (Secure Messaging).

Die verschlüsselte Datenübertragung erfolgt mit dem symmetrischen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) im CBC-Mode. Authentisiert wird die Datenübertragung durch die Verwendung von AES-CMAC (Cipher Message Authentication Code), womit die Vertraulichkeit und Authentizität der zu übertragenden elektronischen Daten gewährleistet wird.

Der Dienstanbieter kann im Ergebnis der Übermittlung sicher sein, dass die an ihn übermittelten Daten aus einem echten Personalausweis stammen. Aufgrund der Trennung Besitz (Personalausweis) und Wissen (PIN) kann der Dienstanbieter davon ausgehen, dass der Personalausweisinhaber diesen willentlich selbst verwendet. Damit hat sich schließlich auch der Personalausweisinhaber gegenüber dem Dienstanbieter authentisiert.

Umgekehrt hatte sich der Dienstanbieter bereits zuvor über sein Berechtigungszertifikat gegenüber dem Personalausweisinhaber authentisiert. Zusätzlich weiß der Personalausweisinhaber dank der verschlüsselten Kommunikation, dass nur der berechtigte Dienstanbieter seine ausgewählten personenbezogenen Daten erhält.

3.3. Sperrmanagement

3.3.1. Sperrung von Personalausweisen

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, können diese gesperrt werden. Dazu muss ein eindeutiges, ausweisindividuelles Merkmal während des elektronischen Identitätsnachweises zum Diensteanbieter gesendet werden, damit Personalausweise, die sich in einer Sperrliste befinden, vom Dienstanbieter als gesperrte Ausweise erkannt werden können.

Auf der anderen Seite soll ein Tracking des Ausweises verhindert werden. Ein eindeutiges Sperrmerkmal unterläuft diese Anforderung allerdings (aus dem selben Grund werden, wie Abschnitt 3.2.3 beschrieben, die Ausweischips auch nicht mit einem eindeutigen Schlüsselpaar ausgestattet). Eine Lösung dieses »Widerspruchs« ist die Verwendung von diensteanbieterspezifischen Sperrlisten, d. h. jeder Ausweis übersendet während des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Dienstanbieter, den dieser gegen seine diensteanbieterspezifische Sperrliste abgleicht. Die zentrale Sperrliste, aus der diensteanbieterspezifische Listen berechnet werden, wird beim Bundesverwaltungsamt betrieben. Der genaue Prozess ist wieder in [5] beschrieben.

Ein Tracking von Ausweisen über ein globales Personalausweismerkmal ist somit ausgeschlossen.

3.3.2. Sperrung von Berechtigungszertifikaten der Dienstanbieter

Da der Chip des Personalausweises nur über begrenzte Ressourcen verfügt, ist es nicht möglich, Berechtigungszertifikate vom Dienstanbieter, deren Berechtigung zurückgezogen wurde, über eine Rückrufliste zu sperren. Daher ist hierfür ein anderer Mechanismus vorgesehen, der allerdings das gleiche Sicherheitsniveau garantiert.

Berechtigungszertifikate werden für eine sehr kurze Zeit ausgestellt (i. d. R. ein bis zwei Tage). Die Gültigkeit der Schlüssel ist im Berechtigungszertifikat enthalten. Der Chip des Ausweises speichert lediglich den Gültigkeitsbeginn des hoheitlichen Zertifikates, welches als letztes akzeptiert wurde. Wird ein Berechtigungszertifikat vorgelegt, dessen Gültigkeitszeitraum vor diesem gespeicherten Zeitpunkt liegt, wird dieses zurückgewiesen. Ein Entzug der Berechtigung für einen Dienstanbieter kann damit durch das Nicht-Ausstellen weiterer Berechtigungszertifikate geschehen.

4. Infrastruktur

Die Nutzung der eID-Funktion im E-Government und E-Business setzt eine reibungslos funktionierende Infrastruktur voraus, wie z. B. die für Zertifikate und deren Sperrung benötigte Public Key Infrastruktur, an der eine Reihe von Behörden und Institutionen beteiligt sind. Dazu gehört insbesondere das BSI als Betreiber der Root-CAs, das BVA mit der VfB und dem Sperrdienst, TrustCenter, die die eigentliche technische Ausstellung der Berechtigungszertifikate übernehmen, die Bundesdruckerei GmbH als Hersteller der neuen Ausweise und die Hotline, die einfache Fragen zu den neuen Funktionen des Ausweises beantwortet und Sperrmeldungen abhanden gekommener Ausweise annimmt.

Wesentliche Komponenten für eine erfolgreiche Etablierung der eID-Funktion im privatwirtschaftlichen Umfeld sind zum einen der sogenannte Bürgerclient, eine Software, mit denen Bürgerinnen und Bürger den Chip des Ausweises erst nutzen können und zum Zweiten der sogenannte eID-Server, der es Diensteanbietern ermöglicht, die Nutzung der eID-Funktion einfach in ihre bereits existierenden IT-Systeme zu integrieren.

4.1. AusweisApp

Mit der AusweisApp stellt die Bundesregierung allen Bürgerinnen und Bürgern eine Softwarekomponente zur Nutzung der elektronischen Funktionen des neuen Personalausweises kostenfrei zur Verfügung. Kern dieser Software ist das eCard-API-Framework, das eine interoperable Nutzung von Signatur-, Authentisierungs- und Verschlüsselungsanwendungen, die auf unterschiedlichen Chipkarten (kontaktbehaftet, kontaktlos) realisiert sein können, garantiert, vergleiche [4]. Damit wird es zukünftig möglich sein, nicht nur den neuen Personalausweis zu nutzen, sondern auch bereits im Feld befindliche Lösungen sowie zukünftige Karten schnell und kostengünstig zu integrieren.

Die AusweisApp wird derzeit für alle gängigen Betriebssysteme, wie z. B. Windows XP, Vista und 7, Mac OS X und einige Linuxversionen (OpenSuse, Ubuntu, Debian) bereit gestellt und unterstützt die am häufigsten auf diesen Systemen genutzten Internetbrowser, sowie, zur Signatur und Verschlüsselung, alle gängigen E-Mail-Programme.

Weitere Informationen zum Bürgerclient finden sich auf den Internetseiten des Kompetenzzentrums »Neuer Personalausweis« unter www.ccepa.de.

4.2. eID-Server

Wie bereits oben beschrieben, soll der eID-Server die Integration der elektronischen Funktionen des neuen Personalausweises und aller weiteren, vom Bürgerclient unterstützten Karten, in die bereits bestehenden IT-Systeme der Diensteanbieter vereinfachen. Der eID-Server übernimmt dabei die gesamte Kommunikation mit der beim Bürger genutzten Karte. Die Kommunikation zur VfB zum Erhalt von Berechtigungszertifikaten und zum Sperrlistenbetreiber (dem BVA) zum Erhalt seiner Sperrlisten wird ebenfalls vom eID-Server übernommen. Ein Diensteanbieter muss somit nur noch eine sichere Verbindung zwischen seinem Web-Server und einem eID-Server etablieren (über ihm bereits bekannte Protokolle wie z. B. SSL oder SAML).

Spezifiziert ist der eID-Server in [9], weitere Informationen finden sich unter www.ccepa.de.

4.3. Wissens- und Kommunikationsplattform

Auf der Wissens- und Kommunikationsplattform sollen sich sowohl Bürgerinnen und Bürger, als auch Diensteanbieter umfassend über alle Themen rund um den neuen Personalausweis informieren. Für Diskussionen, auch zu kritischen Fragen, steht zusätzlich ein moderiertes Internetforum zur Verfügung. Das Internetangebot findet man unter www.personalausweisportal.de.

5. Nutzungsmöglichkeiten in Bibliotheken

Ein wesentlicher Vorteil des elektronischen Identitätsnachweises ist die Nutzung einer sicheren Chipkarte auch ohne vorherige Registrierung für einen bestimmten Dienst. Dies lässt sich am Beispiel einer Online-Bibliothek einfach erläutern: Für einen Zugriff auf ein beschränktes Internetportal, auf dem z. B. elektronische Zeitschriften und Lehrbücher nur für Mitarbeiterinnen, Mitarbeiter und Studierende der jeweiligen Hochschule bereitgestellt werden, müssen sich heute die Nutzer vorab für diesen Dienst anmelden. In der Regel wird dazu ein amtlicher Ausweis bzw. ein Mitarbeiterausweis oder die Studienbescheinigung benötigt. (Dieses Vorgehen ähnelt dem Verfahren zum Erhalt eines herkömmlichen Bibliotheksausweises.) Nach dem erfolgreichen Registrierungsprozess vergibt die Bibliothek dann login und Passwort (in wenigen Bibliotheken auch eine sichere Chipkarte), der Nutzer ist erst danach in der Lage, sich mit diesen Daten an dem Portal anzumelden und den Dienst zu nutzen. Dies lässt sich zukünftig deutlich einfacher und

sicherer mit dem neuen Personalausweis gestalten. Ähnliches gilt für viele Prozesse an Hochschulen, wie z. B. Anmeldungen zu Prüfungen, Einsicht in Prüfungsergebnisse usw.

So wie Nutzer heute mit Hilfe des Personalausweises ihre Identität gegenüber einem Vertreter der Bibliothek nachweisen, können sie dies zukünftig unter Nutzung des elektronischen Identitätsnachweises ohne persönliches Erscheinen in der Bibliothek an ihrem Heim-PC. Mit einem entsprechenden Berechtigungszertifikat können die für die Anwendung notwendigen Daten, wie z. B. Name, Vorname, Adresse, aus dem Chip des Ausweises ausgelesen werden. Diese Daten können dann mit einer hochschulinternen Datenbank abgeglichen werden, um eine Mitgliedschaft der betreffenden Person zu der Hochschule zu verifizieren und gegebenenfalls den Status (d. h. Professor, wissenschaftlicher Mitarbeiter, Studierender) feststellen zu können. Abhängig von dem Ergebnis können dann spezielle Zugriffsrechte innerhalb des Portals freigegeben werden.

Literatur

[1] Jens Bender, Dennis Kügler, Marian Margraf & Ingo Naumann (2008). Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD, Datenschutz und Datensicherheit, 32(3): 850–864.

[2] Jens Bender (2009). Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[3] Jens Bender, Marc Fischlin und Dennis Kügler (2009). Security Analysis of the PACE Key-Agreement Protocol. Information Security Conference (ISC) 2009, Lecture Notes in Computer Science, Volume 5735, pp. 33-48, Springer-Verlag.

[4] Detlef Hühnlein & Manuel Bach (2008). Die Standards des eCard-API-Frameworks. DUD, Datenschutz und Datensicherheit, 32(6): 379-382.

[5] Dennis Kügler (2009). 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), Version 2.02. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[6] Marian Margraf (2008). Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

[7] Marian Margraf (2009). Der elektronische Identitätsnachweis des zukünftigen Personalausweises. in: 19. SIT-SmartCard Workshop (Fraunhofer-Institut für Sichere Informationstechnologie), Darmstadt 3./4. Februar 2009, pp. 3-14.

[8] Alexander Roßnagel, Gerrit Hornung & Christoph Schnabel (2008). Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht. DuD, Datenschutz und Datensicherheit, 32(3): 850–864.

[9] BSI (2009). Technische Richtlinie TR-03130, eID-Server, Version 1.0. Report, Bundesamt für Sicherheit in der Informationstechnik (BSI).

Technische Richtlinien des BSI finden Sie auf www.bsi.bund.de.