Der elektronische Identitätsnachweis des zukünftigen Personalausweises

Marian Margraf

Bundesministerium des Innern
Alt-Moabit 101D, 10559 Berlin
marian.margraf@bmi.bund.de

Zusammenfassung

Personalausweise werden schon heute nicht nur zur Feststellung z.B. der Identität bei der Grenz- oder Personenkontrolle durch Polizei oder Zoll eingesetzt, sondern finden auch häufig im geschäftlichen Umfeld Anwendung. Die im Chip des zukünftigen elektronischen Personalasuweises 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 Vortrag geht auf die Hauptideen des elektronischen Identitätsnachweises ein, erläutert insbesondere die Unterschiede zur qualifizierten elektronischen Signatur und zeigt konkrete Einsatzszenarien.

1 Einleitung

Am 9. März 2005 beschloss das Bundeskabinett die Eckpunkte für eine gemeinsame eCard Strategie der Bundesregierung. Ziel dieser Strategie ist die flächendeckende Einführung von Chipkarten im Bereich der Bundesverwaltung, wesentlicher Stützpfeiler sind die elektronische Authentisierung und die qualifizierte elektronische Signatur, die auf Chipkarten in unterschiedlicher Ausprägung zum Einsatz kommen sollen. Für die eCard-Strategie sind folgende Projekte von Bedeutung:

- Elektronischer Personalausweis
- Elektronische Gesundheitskarte (eGK)
- Elektronische Steuererklärung (ELSTER)
- Elektronischer Einkommensnachweis (ELENA)

Aber auch bestehende Chipkarten, wie Signaturkarten (z.B. für fortgeschrittene und qualifizierte elektronische Signaturen gem. SigG), sollen unterstützt werden.

Mit dem in der Technischen Richtlinie TR-BSI-TR-03112 spezifizierten eCard-API-Framework hat das BSI einen einheitlichen technischen Rahmen zur Umsetzung der eCard-Strategie geschaffen, siehe auch [HuBa08]. Durch die eCard-API wird eine interoperable Nutzung von Signatur- und Authentisierungsanwendungen, die auf unterschiedlichen Chipkarten (kontaktbehaftet, kontaktlos) realisiert sein können, garantiert.

Der elektronische Personalausweis, der zum 1.11.2010 ausgegeben werden wird, unterstützt diese eCard-Strategie. Durch die flächendeckende Verfügbarkeit bei den Bürgerinnen und Bürgern (jährlich werden durschnittlich etwa acht Millionen Personalausweise ausgegeben), wird durch die auf dem Chip des Personalausweises zur Verfügung gestellten Funktionen des elektronischen Identitätsnachweises und der qualifizierten elektronischen Signatur eine sichere und auch rechtsverbindliche Kommunikation im Internet ermöglicht.

2 Der elektronische Personalausweis

Neben der Feststellung der Identität bei der Grenz- oder Personenkontrolle, z.B durch Polizei oder Zoll, werden vor allem Personalausweise auch regelmäßig im privatrechtlichen Umfeld angewendet. 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.

Dabei wird folgendes geprüft:

- die Echtheit des Dokuments, z.B. durch Begutachtung der Sicherheitsmerkmale und
- die Übereinstimmung von Dokument und Person, z.B. an Hand des auf dem Ausweis aufgedruckten Bildes und der im Dokument aufgedruckten Personendaten.

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 elektronischen Personalausweises 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 Gegenseitige Authentisierung mit der eID-Funktion

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). 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. 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 Abgrenzung zur qualifizierten elektronischen 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 elektronische 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 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:

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

Schritte	**klassische Kontoeröffnung**	**Kontoeröffnung online**
1. Schritt = Identitätsnachweis (eID-Funktion)		
Die Bank weist Ihre Identität nach	Der Kunde betritt die Geschäftsräume einer Bank.	Bank legt Berechtigungszertifikat vor, das vom elektronischen Personalausweis überprüft wird.
Der Kunde weist seine Identität nach	Der vom Kunden vorgelegte Personalausweis wird vom Bankangestellten geprüft.	Der elektronische Personalausweis übersendet verschlüsselt ausgewählte eID-Daten.
2. Schritt = Unterschrift (QES-Funktion)		
Vertragsvorbereitung	Bankangestellte und Kunde handeln die Vertragsbedingungen aus und nehmen alle erforderlichen Daten in den Vertragstext auf.	Der Kunde wählt im geführten Dialog die gewünschten Vertragsinhalte, liest die AGB und ergänzt in den Browsermasken weitere erforderliche Sachdaten.
Abschluss eines Vertrages zur Kontoführung	Der Kunde und der Bankangestellte unterschreiben einen Kontoführungsvertrag.	Unter Verwendung der QES-Funktion des Personalausweises und der QES eines Angestellten der Bank wird ein Vertrag über die Kontoführung signiert.

3 Technische Umsetzung der eID-Funktion

Grundidee der eID-Funktion ist, zwischen Chip des elektronischen 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).

Sowohl der elektronische Personalausweis als auch der Dienstanbieter, d.h. beide Kommunikationspartner, sind im Besitz eines Diffie-Hellman-Schlüsselpaares (je ein öffentlicher Schlüssel und ein privater geheimer Schlüssel). Auf dieser Basis erzeugen beide Kommunikationspartner ein gemeinsames Geheimnis, das nur diese beiden kennen. Auf dieser Basis werden kryptographische Schlüssel zur sicheren Übertragung der auf dem Chip des Ausweises gespeicherten personenbezogenen Daten, die der Dienstanbieter laut Berechtigungszertifikat auslesen darf, generiert.

Um zu erreichen, dass das beschriebene 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.

3.1 Authentisierung des Dienstanbieters

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 elektronischen Personalausweise ein Rootzertifikat des BSI gespeichert, mit dem die Gültigkeit der Berechtigungszertifikate 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, der öffentliche Diffie-Hellman-Schlüssel und die zugehörige Signatur, werden zum Chip des Personalausweises gesendet.

Der Chip

- prüft die Signatur 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.

[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 die Signatur mit dem dazugehörigen öffentlichen Schlüssel.

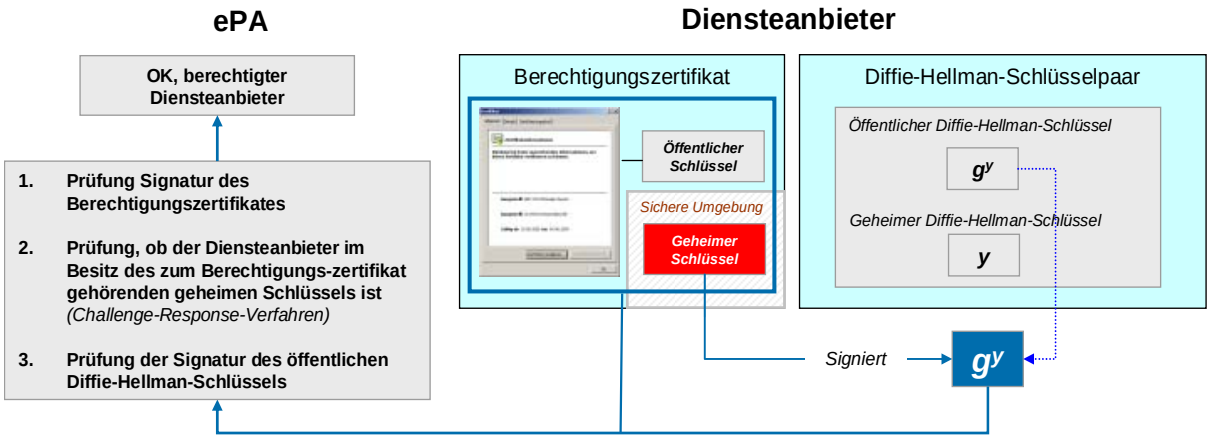

Abb. 1: Dienstanbieter weist seine Berechtigung und Identität nach

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

3.2 Authentisierung des Personalausweises

Der Chip des Personalausweises besitzt im Gegensatz zum Dienstanbieter 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 chipkarten-individuelles Schlüsselpaar würde Dienstanbieter ja 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.

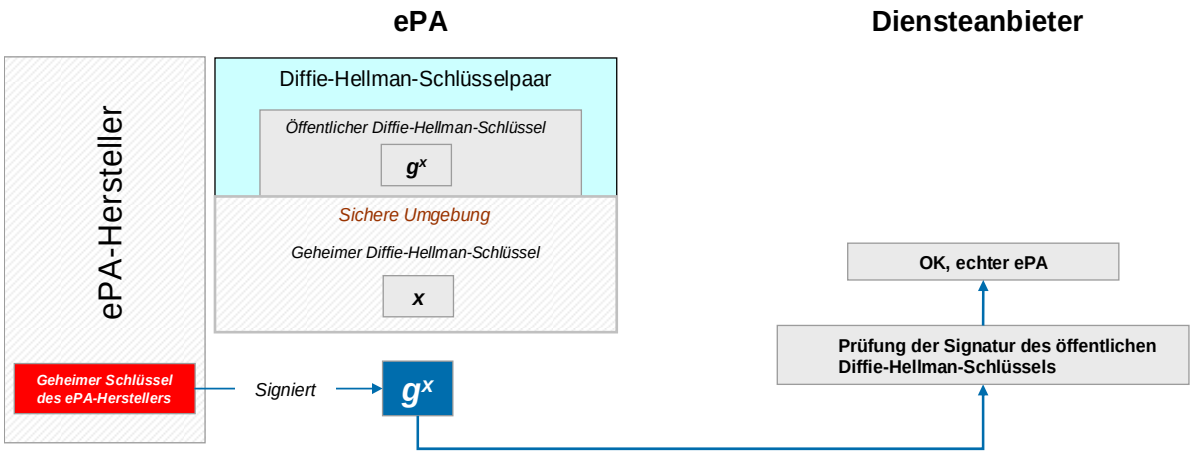

Abb. 2: Ausweisinhaber weist seine Identität nach

Eine Kommunikation mit dem Chip des elektronischen 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 zwiechen kontaktlosem Chip des Ausweises und lokalem Lesegerät, so dass weder personenbezogene Daten noch die PIN von Dritten mitgelesen werden können. Eine genaue Beschreibung dieses Verfahrens findet sich in [Kueg08].

3.3 Übermittlung der Identitätsdaten aus dem Personalausweis

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

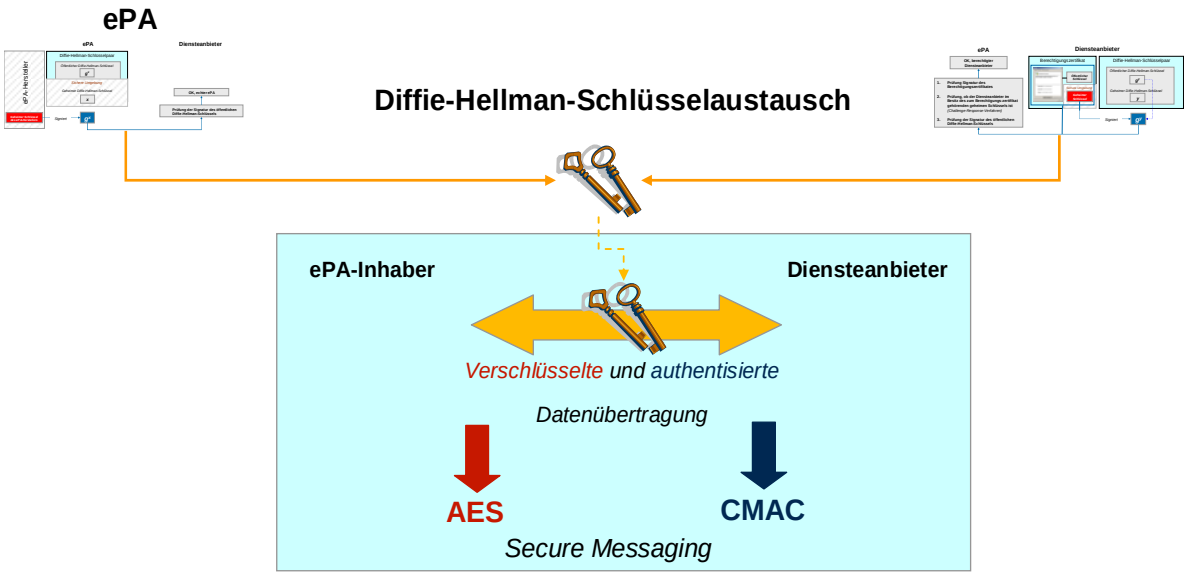

Abb. 3: Verschlüsselte und authentisierte Datenübertragung

Die verschlüsselte Datenübertragung erfolgt mit dem symmetrischen Verschlüsselungsalgorithmus AES (*Advanced Encryption Standard*). Authentisiert wird die Datenübertragung durch die Verwendung von CMAC (Cipher Message Authentication Code), womit die Vertraulichkeit und Authentizität der zu übertragenden elektronischen Daten gewährleistet wird. Dies dient letztendlich der Sicherung vor unbemerkter Manipulation der personenbezogenen Ausweisdaten.

Der Dienstanbieter kann im Ergebnis der Übermittlung sicher sein, dass die an ihn übermittelten Daten aus einem echten Personalausweis stammen. Aufgrund der Trennung Besitz (elektronischer 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.

3.4 Sperrung elektronischer Personalausweise

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 stark (aus dem selben Grund werden, wie in Abschnitt 3.2 beschrieben, die Ausweischips auch nit mit einem eindeutigen Schlüsselpaar ausgestattet). Daher werden diensteanbieterspezifische Sperrlisten erzeugt, d.h. jeder

Ausweis übersendet während des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Dienstanbieter, den dieser gegen eine diensteanbieterspezifische Sperrliste abgleicht. Die zentrale Sperrliste, aus der diensteanbieterspezifische Listen berechnet werden, wird zukünftig bei der Vergabestelle für Berechtigungszertifikate (VfB) betrieben.

Der Prozess wird wie folgt umgesetzt:

Im Rahmen der Produktion berechnet der Ausweishersteller das kartenspezifische Sperrkennwort eines jeden Ausweischips auf Basis des öffentlichen Schlüssels des Sperrlistenbetreibers und eines geheimen Sperrschlüssels des Chips.

Dieses Sperrkennwort teilt der Hersteller dem Ausweisinhaber im PIN/ PUK-Brief mit, damit der Inhaber unter Angabe dieses Sperrkennworts eine unverzügliche Sperrung der eID-Funktion beim Sperrlistenbetreiber (z. B. per Telefon) veranlassen kann. Darüber hinaus erhält die ausstellende Personalausweisbehörde dieses Sperrkennwort zur Speicherung im Personalausweisregister, so dass dem Sperrlistenbetreiber das Sperrkennwort auch durch die ausstellende Personalausweisbehörde übermittelt werden kann, wenn der Ausweisinhaber den Verlust bei der Behörde anzeigt.

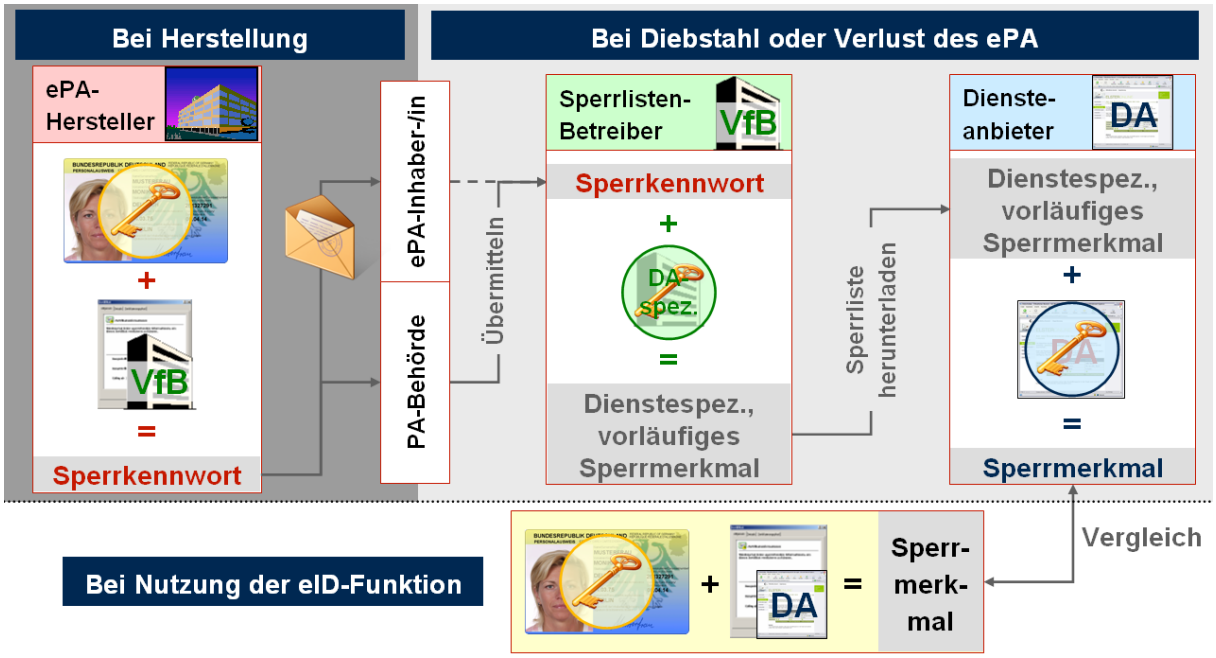

Abb. 4: Prozess Sperrmanagement für abhanden gekommene Personalausweise

Aus dem übermittelten Sperrkennwort und einem diensteanbieterspezifischen, geheimen Schlüssel berechnet dann der Sperrlistenbetreiber ein dienstespezifisches, vorläufiges Sperrmerkmal. Jeder Dienstanbieter kann die für ihn berechneten diensteanbieterspezifischen vorläufigen Sperrmerkmale über öffentliche Netze vom Sperrlistenbetreiber herunterladen.

Um überprüfen zu können, ob ein verwendeter Personalausweis gesperrt ist, muss der Dienstanbieter zunächst aus dem vorläufigen Sperrmerkmal und einem nur ihm bekannten zweiten geheimen Schlüssel das (endgültige) dienste- und kartenspezifische Sperrmerkmal berechnen.

Wird die eID-Funktion genutzt (Freigabe der Daten durch Eingabe der geheimen PIN), berechnet der Chip des Personalausweises automatisch aus seinem geheimen Sperrschlüssel und dem öffentlichen Sperrschlüssel des Dienstanbieters, welches im Berechtigungszertifikat enthalten ist, das dienste- und kartenspezifische Sperrmerkmal. Mit diesem kann der Dienstanbieter dann mittels seiner individuellen Sperrliste überprüfen, ob der Ausweis gesperrt wurde.

Wichtig ist, dass die dienste- und kartenspezifischen Sperrmerkmale, wie der Name schon sagt, für jeden Diensteanbieter verschieden sind und von zwei Diensteanbietern auch nicht ineinander umgerechnet werden können. Dadurch wird gewährleistet, dass zwei Diensteanbieter nicht in der Lage sind, Daten eines Ausweisinhabers miteinander abzugleichen.

3.5 Sperrung von Berechtigungszertifikaten der Dienstanbieter

Da der Chip des elektronischen Personalausweises nur über einen begrenzten Speicherplatz 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. 1 bis 2 Tage). Die Gültigkeit der öffentlichen Schlüssel ist im Berechtigungszertifikat enthalten. Der Chip des Ausweises speichert lediglich den Gültigkeitsbeginn des Berechtigungszertifikats, welches als letztes akzeptiert wurde. Wird ein Berechtigungszertifikat vorgelegt, dessen Gültigkeitszeitraum vor diesem gespeicherten Zeitpunkt liegt, wird dieser zurückgewiesen. Ein Entzug der Berechtigung für einen Dienstanbieter kann damit durch das Nicht-Ausstellen weiterer Berechtigungszertifikate geschehen.

Im Übrigen ist vorgesehen, nicht für jedes neues Berechtigungszertifikat eines Dienstanbieters ein neues Schlüsselpaar zu verlangen. Berechtigungen werden für drei Jahre ausgesprochen. Für diesen Zeitraum werden die öffentlichen Schlüssel lediglich rezertifiziert, d.h. der Dienstanbieter erhält unter einmaliger Anmeldung seines öffentlichen Schlüssels beim Trust-Center automatisch vor Ablauf seines Zertifikats ein neues, in dem lediglich der Gültigkeitszeitraum aktualisiert wurde; der öffentliche Schlüssel bleibt – wie die übrigen Felder im Zertifikat – gleich.

Literatur

[BKMN08] Jens Bender, Dennis Kügler, Marian Margraf und Ingo Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD, Datenschutz und Datensicherheit, 32(3): 850–864, 2008.

[HuBa08] Detlef Hühnlein und Manuel Bach. Die Standards des eCard-API-Frameworks. In: DUD, Datenschutz und Datensicherheit, 32(6): 379-382, 2008.

[Kueg08] Dennis Kügler. Technische Richtlinie TR03110, Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.0. Report, BSI, 2008.

[ICAO06] ICAO. Doc9303, Machine Readable Travel Documents, Part 1- Machine Readable Passport – Volume 2 Specifications for Electronically Enabled Passports withBiometric Identification Capabilities. Report, International Civil AviationOrganization, 2006.

[RoHS08] Alexander Roßnagel, Gerrit Hornung und Christoph Schnabel. Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicherSicht. DuD, Datenschutz und Datensicherheit, 32(3): 850–864, 2008.