Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann

Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis

Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen

Dieser Artikel gibt einen Überblick über die Ziele und die Funktion der Sicherheitsmechanismen, wie sie voraussichtlich im deutschen elektronischen Personalausweis zur Anwendung kommen.

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

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI), derzeit nationaler Experte bei der European Network and Information Security Agency (ENISA)
E-Mail: Ingo.Naumann@enisa.europa.eu

Einleitung

Neben den bereits seit Oktober 2005 ausgegebenen elektronischen Reisepässen plant die Bundesregierung auch die nächste Generation des Personalausweises, den *elektronischen Personalausweis*, mit einem kontaktlosen Chip (RF-Chip) nach ISO 14443 [9] auszustatten, um die Fälschungssicherheit zu erhöhen und neue Funktionalitäten zu unterstützen.

Der im Dokument integrierte Chip bietet neben der Aufnahme biometrischer Merkmale die Möglichkeit, den Personalausweis zu einer gegenseitigen „Online-Authentisierung" zu nutzen. Durch diese Authentisierung wird es berechtigten *eBusiness*- und *eGovernment*-Dienstleistern ermöglicht, auf sichere Art und Weise auf bestimmte im Chip gespeicherte Daten unter der Kontrolle des Inhabers zuzugreifen.

Eine weitere, optionale Anwendung des elektronischen Personalausweises ist die Signaturfunktion wie sie bereits heute auf separaten Signaturkarten zu finden ist. Diese Anwendung wird erst vom Karteninhaber nachträglich bei Bedarf aktiviert.

Daneben bleibt der neue Personalausweis auch ein Sichtausweis mit physikalischen Sicherheitsmerkmalen auf dem bekannten Niveau.

Die drei Anwendungen des elektronischen Personalausweises

Auf dem Chip des elektronischen Personalausweises stehen drei Anwendungen zur Verfügung, und zwar:

- die ePass-Anwendung, welche die Daten der maschinenlesbaren Zone (MRZ) und die biometrischen Daten enthält;
- die Authentisierungsfunktion (auch electronic identity, eID), welche den Zugriff auf personen- und dokumentenbezogene, aber nicht auf biometrische Daten ermöglicht;
- die fortgeschrittene/qualifizierte elektronische Signatur.

Während die ePass-Anwendung ausschließlich für die Verwendung seitens hoheitlicher Kontrollbehörden vorgesehen ist, bekommt der Inhaber des Personalausweises mit den beiden zusätzlichen Funktionen die Möglichkeit, kommerzielle (*eBusiness*) und behördliche (*eGovernment*) Dienste elektronisch über Netze zu nutzen.

Die Authentisierungsfunktion und die qualifizierte elektronische Signatur bilden elektronisch die Anwendungen ab, die heute schon im geschäftlichen Umfeld mit Hilfe des herkömmlichen Personalausweises eingesetzt werden.

Dieser Artikel konzentriert sich auf die Darstellung der neuen Authentisierungsfunktion, wie sie in [1],[2],[6] spezifiziert wird.[1]

1 Zur Nutzung der qualifizierten elektronischen Signatur auf einer kontaktlosen Karte und das Nach-

Die Sicherheitsmechanismen, die beim elektronischen Personalausweis Verwendung finden, basieren auf den vom ePass bekannten Protokollen der *Extended Access Control* (EAC). Diese sind ausführlich in [11] beschrieben. Eine Neuentwicklung des BSI im Zuge der Einführung des elektronischen Personalausweises ist das Protokoll *Password Authenticated Connection Establishment* (PACE), das – als neues Protokoll von EAC – hier dargestellt wird.

Sicherheitsziele

Der innerhalb des Kartenkörpers eingebaute kontaktlose Chip benutzt eine induktive Kopplung mit einer Spule für die Energie- und Datenübertragung. Mit dieser Technologie können in einer Entfernung von bis zu ca. 20 cm vom Lesegerät Daten sowohl gelesen als auch geschrieben werden. Das Mithören dieser Kommunikation ist prinzipiell auch aus größerer Entfernung möglich ([11]), daher sind – wie beim ePass – sowohl Zugriffsschutz- als auch Verschlüsselungsmechanismen für die Kommunikation über die Luftschnittstelle erforderlich. Im Falle der Online-Authentisierung über ein nicht geschütztes Netzwerk (Internet) ist auch diese Kommunikation zu schützen.

Neben dem Schutz der Daten während eines (berechtigten) Auslesevorgangs vor Abhören und Verfälschen muss auch ein unberechtigtes Auslesen verhindert werden. Weiter muss die Authentizität und Integrität sowohl der gespeicherten Daten als auch des Chips selbst gesichert werden.

Ein weiteres Ziel ist es, dass der Inhaber möglichst genau auswählen kann, welche Daten ein Dienstanbieter auslesen darf und welche nicht (Datensparsamkeit). Die letztliche Freigabe der Daten muss immer durch den Nutzer erfolgen. Da im Online-Bereich nicht durch Vergleich des Gesichtsbildes mit der Person sichergestellt werden kann, dass der Nutzer tatsächlich der Inhaber des Ausweises ist, muss diese Personenbindung auf anderem Wege sichergestellt werden.

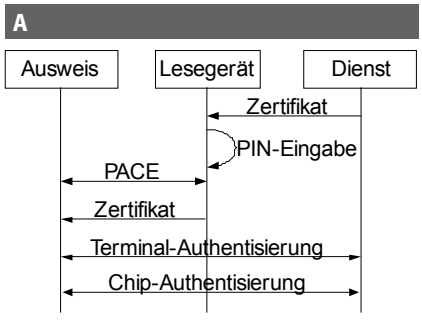
Zusätzlich muss der elektronische Personalausweis es dem Inhaber ermöglichen festzustellen, mit welchem Dienstanbieter er kommuniziert, um z.B. Phishing-Attacken zu erschweren.

Neben den gespeicherten Daten ist auch die Information über den Aufenthaltsort des Inhabers bzw. des Ausweises schützenswert, d.h. das unbemerkte Wiedererkennen eines elektronischen Personalausweises (*Tracking*) muss verhindert werden.

Diese Sicherheitsanforderungen an den elektronischen Personalauweis werden durch mehrere, aufeinander aufbauende, kryptographische Protoktolle erfüllt, die im Folgenden dargestellt werden.

Sicherheitsmechanismen

Neben den vom ePass bekannten Verfahren *Extended Access Control* (EAC, bestehend aus Chip-Authentisierung und Terminal-Authentisierung) sowie der Passiven Authentisierung ([7]) wird für den elektronischen Personalausweis auch das neu entwickelte Protokoll *Password Authenticated Connection Establishment* (PACE) verwendet.



Password Authenticated Connection Establishment – PACE

► Verbindungsaufbau ...

Der ePass verwendet für den Aufbau einer verschlüsselten Verbindung zwischen Chip und Lesegerät das von der *International Civil Aviation Organization* (ICAO) normierte *Basic Access Control* (BAC, [7]). Dieses Protokoll verwendet einen Teil der Daten aus der maschinenlesbaren Zone, um daraus einen symmetrischen Schlüssel abzuleiten. Basierend auf diesem Schlüssel findet eine gegenseitige Authentisierung zwischen Chip und Lesegerät statt. Nur wenn das Lesegerät die notwendigen Daten kennt (in der Regel durch optisches Lesen der MRZ), kann es auf die restlichen Daten zugreifen. Wie in [11] beschrieben, hängt die Stärke der BAC-Verschlüsselung von der Entropie der verwendeten MRZ-Felder ab[2].

Für den elektronischen Personalausweis ist *Basic Access Control* nicht geeignet: Die Einwilligung des Inhabers zum Lesen der Passdaten erfolgt beim ePass durch Übergabe des Reisepasses und optischen Zugriff auf die MRZ. Beim Personalausweis soll es dem Inhaber ermöglicht werden, durch Eingabe einer geheimen PIN in einen Vorgang einzuwilligen. BAC mit einer PIN als Passwort ist nicht möglich, da die dann mit BAC ausgehandelten Sitzungsschlüssel zu schwach wären.

Während BAC ausschließlich auf symmetrischer Kryptographie basiert, verwendet PACE zusätzlich asymmetrische Kryptographie. Die Basis stellt dabei das Diffie-Hellman-Verfahren zum Aushandeln eines gemeinsamen Geheimnisses zwischen Chip und Lesegerät dar. Dabei erzeugen Chip und Lesegerät bei jeder Authentisierung jeweils ein eigenes flüchtiges Schlüsselpaar („*ephemeral key pair*“) und tauschen die öffentlichen Schlüssel aus. Aus dem eigenen privaten Schlüssel und dem öffentlichen Schlüssel des jeweils anderen kann nur ein gemeinsames Geheimnis berechnet werden. Da beide Parteien jeweils ein flüchtiges Schlüsselpaar verwendet haben, ist das gemeinsame Geheimnis nicht authentisiert, es besteht also die Möglichkeit einer *Man-in-the-Middle*-Attacke bzw. eines unberechtigten Zugriffs.

► ... und PIN-Abfrage

Zur Authentisierung des gemeinsamen Geheimnisses und insbesondere des Lesegeräts wird ein Passwort (PIN) verwendet. Bei PACE wird das Passwort zur (symmetrischen) Verschlüsselung einer durch den Chip gewählten Zufallszahl genutzt[3]. Damit das Lesegerät die Zufallszahl entschlüsseln kann, benötigt es das korrekte Passwort – andernfalls entschlüsselt das Lesegerät eine falsche Zufallszahl und die Authentisierung – und damit das PACE-Protokoll – schlägt fehl. Dabei dient je nach Anwendungsfall wahlweise ein aus der MRZ abgeleiteter Schlüssel (analog zu BAC), eine auf der Karte aufgedruckte

laden eines qualifizierten Zertifikates unter Verwendung der Authentisierungsfunktion wird vom BSI eine separate Richtlinie erstellt [3].

2 Um die Entropie der Schlüssel zu erhöhen, werden bei den ePässen der zweiten Stufe (seit 1. November 2007) Teile der nun alphanumerischen Seriennummer pseudozufällig gewählt.

3 Die Stärke des Passworts und die Stärke der Chiffre sind dabei unerheblich; es muss nur sichergestellt werden, dass ein Chiffretext mit jedem möglichen Schlüssel entschlüsselt werden kann.

Karten-PIN oder eine geheime Benutzer-PIN (eID-PIN) als Passwort. Für die Online-Authentisierung wird im Allgemeinen die geheime eID-PIN genutzt. Dadurch wird die Authentisierung nicht nur an den Ausweis, sondern auch direkt an den Inhaber gebunden (Nachweis von Besitz und Wissen).

Für die hoheitliche Personenkontrolle, z.B. durch die Polizei, ist es notwendig, dass die Daten auch ohne PIN-Eingabe durch den Inhaber ausgelesen werden können. In diesem Fall wird für den Verbindungsaufbau die MRZ oder die aufgedruckte Karten-PIN genutzt. Dabei muss der Status des hoheitlichen Lesegerätes durch entsprechende Zertifikate in der nachfolgenden Terminal-Authentisierung nachgewiesen werden.

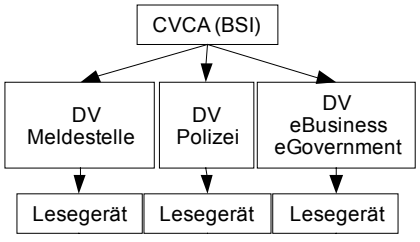
Aus dem gemeinsamen Geheimnis werden dann symmetrische Schlüssel für die verschlüsselte und authentisierte Kommunikation zwischen Chip und Lesegerät abgeleitet (*Secure Messaging*).

Die asymmetrischen Algorithmen, die für PACE und auch die anderen Protokolle genutzt werden, basieren auf elliptischen Kurven (ECDH, ECDSA) nach [5]. Dadurch sind relativ kurze Schlüssellängen möglich (224 Bit, siehe auch [4]). Für das *Secure Messaging* wird der moderne symmetrische Verschlüsselungsalgorithmus AES (*Advanced Encryption Standard*) verwendet. Dadurch wird sowohl für die asymmetrischen Protokolle als auch die symmetrisch verschlüsselte Datenübertragung ein sehr hohes Sicherheitsniveau erreicht.

Rechtevergabe mit Terminal-Authentsierung

Die Terminal-Authentisierung dient der Autorisierung der Lesegeräte – bzw. im Falle der Online-Authentisierung des Dienstanbieters – und der Festlegung der Leserechte unter Nutzung einer Public Key-Infrastruktur, der EAC-PKI. Diese PKI besteht aus der Wurzelinstanz *Country Verifying Certification Authority* (CVCA) sowie mehreren *Document Verifier* (DV), die wiederum die Schlüsselpaare der einzelnen Lesegeräte oder Dienstanbieter signieren.

Abbildung 2 | Die EAC-PKI



Beim ePass wird dieses Protokoll zur Autorisierung zum Zugriff auf die Fingerabdruckdaten verwendet. Eine Autorisierung des Lesegerätes zum Auslesen der MRZ-Daten und des Geschichtsbildes ist beim ePass hingegen nicht notwendig, da diese Daten auch auf der Datenseite des Passes aufgedruckt sind und die Einwilligung zum Auslesen des Passes durch die Übergabe an z.B. einen Grenzbeamten gegeben wird.

Anders ist die Situation beim elektronischen Personalausweis. Dieser wird auch zur Online-Authentisierung genutzt, also in der Kommunikation mit *a priori* nicht vertrauenswürdigen Gegenstellen. Es wäre denkbar, dass ein nicht-seriöser Anbieter die für den Verbindungsaufbau notwendigen Daten (MRZ oder aufgedruckte Karten-PIN) z.B. durch Phishing erhält und anschließend unbemerkt Zugriff auf das Gesichtsbild nimmt. Um dieses zu verhindern, werden beim elektronischen Personalausweis *alle* Daten durch die Terminal-Authentisierung vor unbefugtem Auslesen geschützt.

Die Leserechte für die Authentisierungsfunktion lassen sich über die Zertifikate der Teminal-Authentisierung detailliert festlegen, so kann z.B. das Leserecht für den Nachnamen unabhängig vom Leserecht für den/die Vornamen vergeben werden. Die in den Zertifikaten vorgegebenen Rechte können durch den Nutzer vor der Eingabe seiner PIN weiter eingeschränkt werden, so dass dieser die volle Kontrolle darüber behält, welche Daten ein Dienstanbieter auslesen darf.

Der Chip bindet die durch die Terminal-Authentisierung gewonnenen Leserechte an die Sitzungsschlüssel, die durch die nachfolgende Chip-Authentisierung ausgehandelt werden. Dadurch ist sichergestellt, dass die Daten nur in einem stark gesicherten Ende-zu-Ende-Kanal zwischen Chip und Dienstanbieter übertragen werden, der nur durch den authentisierten Dienstanbieter aufgebaut werden kann. Eine *Man-in-the-Middle*-Attacke, bei dem die Daten nicht durch den Anbieter sondern durch einen Dritten ausgelesen werden, wird so verhindert.

Fälschungssicherheit

► **Passive Authentisierung**

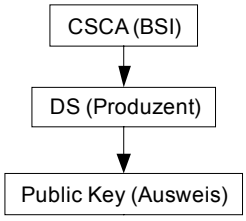
Wie in [11] beschrieben wird die Integrität und Authentizität der Daten der ePass-Anwendung durch digitale Signaturen (Passive Authentisierung) geschützt. Dazu wird eine PKI genutzt, bestehend aus der Wurzelinstanz *Country Signing Certification Authority* (CSCA, betrieben vom BSI) sowie mindestens einem *Document Signer* (DS, betrieben vom Ausweishersteller). Für die Daten der Authentisierungsfunktion ergeben sich bei dieser Vorgehensweise zwei Probleme:

1. Die Authentisierungsfunktion ist auch zur Authentisierung gegenüber einem Dienstanbieter über ein Netzwerk vorgesehen. Werden die Daten der Authentisierungsfunktion signiert an diesen übertragen, so kann er diese Daten einschließlich einer „hoheitlichen Echtheitsgarantie" weitergeben. Er kann gegenüber einem Dritten nachweisen, dass es sich um authentische Daten des Ausweisinhabers handelt. Dies ist aus Datenschutzgründen nicht wünschenswert.[4]
2. Teil der Daten der Authentisierungsfunktion ist die Wohnadresse des Ausweisinhabers. Dieses Datum kann bei einer Adressänderung durch die ausstellende Behörde geändert werden. Zum Signieren der geänderten Adresse wäre der Zugriff der ausstellenden Behörde auf den privaten Schlüssel des *Document Signers* (DS) notwendig. Dieser Schlüssel ist abgesichert in einer sicheren Signaturerstellungseinheit beim Ausweishersteller gespeichert, d.h. für die Meldestellen besteht kein Zugriff auf diesen Schlüssel.

Um diese Probleme zu umgehen, wird die Integrität und Authentizität der Daten der Authentisierungsfunktion implizit durch die Chip-Authentisierung gesichert.

4 Ist eine nicht abstreitbare Authentisierung gewünscht, bietet sich die Verwendung der fortgeschrittenen/qualifizierten elektronischen Signatur an.

Abbildung 3 | Die Signer-PKI



► **Chip-Authentisierung**
Die Chip-Authentisierung dient zum einen dem Nachweis, dass es sich bei dem Chip um einen echten Chip (und nicht etwa um eine Fälschung oder einen Klon) handelt, zum anderen wird ein sicherer Kanal zwischen Chip und Lesegerät, bzw. Dienstanbieter bei der Online-Authentisierung, aufgebaut.

Die Chip-Authentisierung basiert auf dem Diffie-Hellman-Schlüsselaustausch, wobei das Lesegerät ein flüchtiges (*ephemeral*) Schlüsselpaar und der Chip ein statisches Paar nutzt. Der öffentliche Schlüssel des Chips wird während des Herstellungsprozesses signiert (Passive Authentisierung). Durch die Verwendung des signierten Schlüssels wird die Echtheit des Chips nachgewiesen, gleichzeitig wird ein stark verschlüsselter und authentisierter Ende-zu-Ende-Kanal zwischen Chip und (im Falle der Online-Authentisierung) Dienstanbieter aufgebaut.

Da die Daten auf dem Chip (nach der Personalisierung während der Herstellung) nur durch eine Ausweisbehörde geschrieben werden können, ist die Authentizität der Daten auf dem Chip gesichert. Durch die Chip-Authentisierung wird neben der Authentizität des Chips auch die Integrität und Authentizität der in dem gesicherten Kanal übertragenen Daten sichergestellt. Eine explizite Signatur der Daten ist daher nicht notwendig und, wie oben beschrieben, auch nicht wünschenswert.

Die Korrektheit der Protokolle der EAC wurde durch das BSI in formalen Analysen nachgewiesen. Ein Sicherheitsbeweis für das PACE-Protokoll wurde durch das BSI erstellt und wird zur Zeit zur Veröffentlichung vorbereitet.

Zusammenfassend erhalten wir durch die verschiedenen kryptographischen Protokolle Schutz vor verschiedenen Angriffen:

- **PACE schützt vor Zugriff „im Vorbeigehen" und baut einen verschlüsselten integritätsgesicherten Kanal zwischen Karte und Lesegerät auf.**
- **PACE ermöglicht zusätzlich die Eingabe/Verifikation einer PIN, dadurch Bindung der Authentisierung an die Person und Schutz vor unbefugter Nutzung des elektronischen Personalausweises.**
- **Die Terminal-Authentisierung stellt sicher, dass das Lesegerät/der Dienstanbieter nur berechtigte Zugriffe durchführen kann. Die Leserechte können für die verschiedenen Datenfelder separat vergeben werden.**
- **Die Chip-Authentisierung baut einen sicheren Ende-zu-Ende-Kanal zwischen Chip und Dienstanbieter auf. Weiter wird durch die Chip-Authentisierung in Verbindung mit der Passiven Authentisierung die Echtheit des Chips nachgewiesen.**
- **Die Integrität und Authentizität der ausgelesenen Daten wird implizit über den Echtheitsnachweis des Chips gesichert.**

Tracking

Neben der Gefahr des unbemerkten Auslesens besteht bei einer kontaktlosen Schnittstelle prinzipiell auch die Möglichkeit, die Bewegungen des Besitzers durch das Auslesen eindeutiger Kartenmerkmale unbemerkt zu verfolgen (*Tracking*). Um dies zu verhindern, werden verschiedene Mechanismen eingesetzt: Analog zum ePass verwendet der elektronische Personalausweis eine variable Chip-UID (mit der sich der Chip gegenüber einem Lesegerät meldet), vergleiche [11].

Ebenso kann auf alle anderen identifizierenden Daten nur nach erfolgreicher Durchführung von PACE und Terminal-Authentisierung zugegriffen werden.

PINs

► **Authentisierungs-PIN**
Der Zugriff auf die Authentisierungsfunktion zur Nutzung für *eGovernment* oder *eBusiness* erfolgt über eine geheime sechsstellige PIN. Dadurch wird bei der Authentisierung nicht nur der Besitz des Personalausweises nachgewiesen, sondern durch den Nachweis des Wissens „PIN" wird die Authentisierung an den Inhaber gebunden.[5] Eine eingegebene PIN wird nicht an den Chip übertragen, d.h. sie ist durch einen Angreifer nicht durch Abhören zu erlangen. Stattdessen wird die richtige Eingabe der PIN durch den erfolgreichen Ablauf der PACE-Authentisierung nachgewiesen.

Wie bei Kartenanwendungen üblich, ist diese PIN durch einen Fehlbedienungszähler geschützt, der die Authentisierungsfunktion nach dreimaliger Falscheingabe sperrt. Im Vergleich zu anderen Kartenanwendungen (z.B. Bankkarte) wird die Länge der PIN von üblicherweise vier Ziffern auf sechs Ziffern erhöht. Dies entspricht den Vorgaben der qualifizierten elektronischen Signatur. Ein Entsperren der PIN ist durch einen PUK möglich.

Wird die Signaturfunktion genutzt, wird für diese eine weitere geheime Signatur-PIN genutzt.

► **Karten-PIN**
Ist nur der Aufbau eines sicheren PACE-Kanals zu einer bestimmten Karte gewünscht, so wird hierzu statt der geheimen PIN eine aufgedruckte sechsstellige Karten-PIN (oder die MRZ) genutzt. Hier wird nur der Besitz der Karte, nicht aber die Identität des Benutzers nachgewiesen. Dies wird beispielsweise für die hoheitliche Kontrolle genutzt, bei der die Identität des Benutzers direkt (z.B. über das Gesichtsbild) überprüft wird.

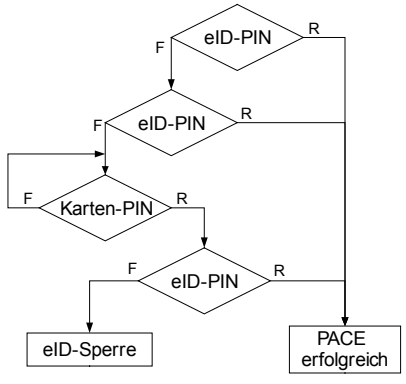
Im optimalen Fall würde die Karten-PIN vom elektronischen Personalausweis beim Verbindungsaufbau zufällig gewählt und auf einem Display auf dem Personalausweis angezeigt. Alternativ kann die Karten-PIN während des Herstellungsprozesses der Karte zufällig erzeugt und aufgedruckt werden.

Denial of Service

Durch die kontaktlose Schnittstelle besteht die Gefahr eines *Denial-of-Service*-Angriffs auf die geheime PIN, indem ein Angreifer „im Vorübergehen" drei Verbindungsversuche mit falschen PINs durchführt und dadurch die Karte sperrt. Um dies zu verhindern, muß spätestens nach zwei Fehlversuchen der Besitz der Karte durch die korrekte Eingabe der aufgedruckten Karten-PIN nachgewiesen werden.

5 Natürlich ist Voraussetzung, dass der Inhaber seine geheime PIN tatsächlich geheim hält.

Abbildung 4 | Eingabe eID-PIN (F=Falsche Eingabe, R=Richtige Eingabe)



Spezialfälle Altersverifikation und Gültigkeitsabfrage

Der elektronische Personalausweis dient auch zur elektronischen Altersverifikation gegenüber beispielsweise einem Verkaufsautomaten oder Internetdiensten (z.B. Online-Videotheken mit Altersfreigabe nach FSK). Dies ließe sich über das Auslesen des Geburtsdatums realisieren, allerdings würden in dem Fall wesentlich mehr Informationen als nur die Bestätigung eines bestimmten Mindest- oder Höchstalters freigegeben.

Stattdessen stellt der Service-Provider eine Anfrage an den Personalausweis, ob der Inhaber nach einem bestimmten Datum geboren ist. Diese Frage wird vom Personalausweis nur mit „Ja" oder „Nein" beantwortet. Um ein Bestimmen des Alters durch mehrere aufeinanderfolgende Altersverifikationen zu verhindern, ist pro Authentisierungsablauf nur eine Abfrage möglich. Das Recht zur Altersabfrage wird durch spezielle Zugriffsrechte in den Zertifikaten der Terminal-Authentisierung signalisiert.

Auf ähnliche Weise kann auch das Ablaufdatum des Ausweises getestet werden.

Restricted Identification

Ein interessanter Anwendungsfall für die Online-Authentisierung ist das „Wiedererkennen" eines bereits registrierten Nutzers/Kunden. Dazu können grundsätzlich die persönlichen Daten (Name, Vorname, etc.) der Authentisierungsfunktion genutzt werden. Diese Daten alleine identifizieren den Inhaber aber u.U. nicht eindeutig, das Hinzuziehen weiterer Merkmale wie z.B. Geburtsdatum ist aber aus Gründen der Datensparsamkeit nicht wünschenswert. Eine Verwendung der Seriennummer des Personalausweises im kommerziellen Bereich ist nach Gesetzeslage nicht zulässig.

Daher bietet der elektronische Personalausweis die Möglichkeit der *Restricted Identification*. Ziel dieses Mechanismus ist es, dem Serviceanbieter die Möglichkeit zu bieten, einen elektronischen Personalausweis eindeutig wiederzuerkennen, ohne weitere Daten über den Ausweis oder den Inhaber zu erfahren. Weiterhin soll verhindert werden, dass mehrere Anbieter ihre Daten verbinden können, diese „Sektorspezifische Kennung" soll nicht zwischen verschiedenen Dienstanbietern übertragbar sein.

Dazu wird ein interner geheimer Schlüssel des Personalausweises und ein eindeutiges Kennzeichen des Serviceanbieters vom Chip zu einer Kennung zusammengeführt, die den Ausweis eindeutig gegenüber dem Anbieter identifiziert. Das Kennzeichen des Anbieters ist Bestandteil des Anbieterzertifikates der Terminal-Authentisierung, kann also von diesem nicht frei gewählt werden, sondern wird von der zertifizierenden Instanz zugewiesen. Die Kennungen, die verschiedene Anbieter vom gleichen Ausweis erhalten, können nicht ineinander umgerechnet werden.

Eine andere Anwendung der *Restricted Identification* ist die pseudonyme Anmeldung bei einem Dienstanbieter. Dabei erhält der Anbieter nicht die Identität des Ausweisinhabers, kann diesen aber bei einer späteren erneuten Authentisierung wiedererkennen.

Fazit

Mit dem elektronischen Personalausweis wird eine sichere Basis für *eBusiness*- und *eGovernment*-Dienste geschaffen. Ein Bürger hat die Möglichkeit, sich gegenüber einem Dienstanbieter sicher zu identifizieren. Da sich auch der Anbieter gleichzeitig über die Terminal-Authentisierung gegenüber dem Bürger sicher identifizieren muss, bietet die Anwendung des elektronischen Personalausweises auch einen wirksamen Schutz gegen Phishing und ähnliche Angriffe. Bei der Entwicklung der kryptographischen Protokolle wurde großer Wert auf eine datenschutzfreundliche Gestaltung gelegt. Neben der Datensparsamkeit war ein weiterer wichtiger Aspekt beim Design der Authentisierungsfunktion, dass ein Dienstanbieter gegenüber einem Dritten keine Beweise für eine gelungene Authentisierung vorlegen kann. Der elektronische Personalausweis erfüllt weiterhin seine Funktion als Ausweisdokument für die hoheitliche Kontrolle, wobei die Fälschungssicherheit durch die Integration des Chips und der damit verbundenen Verwendung kryptographischer Verfahren zur Echtheitsüberprüfung weiter erhöht wird.

Literatur

[1] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 2.0

[2] BSI: Technische Spezifikationen des deutschen elektronischen Personalausweises, Chipkartenspezifikationen

[3] BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit

[4] BSI: Technische Richtlinie TR-20102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen.

[5] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC) based on ISO 15946

[6] CEN/TC 224 WG15: Identification card systems – European Citizen Card

[7] ICAO: Doc 9303, Machine Readable Travel Documents

[8] ICAO: Supplement – 9303, Release 6, September 2007

[9] ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards

[10] ISO/IEC 7816: Identification cards – Integrated circuit cards

[11] Kügler, D.; Naumann, I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass, DuD – Datenschutz und Datensicherheit, März 2007, Seiten 176-180