Elektronische Reise- und Ausweisdokumente

Prof. Dr. Claudia Eckert
Fraunhofer Institut für Sichere Informationstechnologie (FhI-SIT)
TU Darmstadt,
Lehrstuhl für Sicherheit in der Informationstechnik
28. Juli 2008

Inhaltsverzeichnis

1 Elektronische Pässe

Mit den neuen Ausweis- und Reisedokumenten, dem elektronischen Reisepass (ePass) und auch dem elektronischen Personalausweis (ePA) wird in Deutschland flächendeckend eine Infrastruktur eingeführt, die jeden Bundesbürger mit einer elektronisch prüfbaren Identität versorgt. Während der Reisepass der hoheitlichen Personenkontrolle (Grenzkontrolle) vorbehalten ist, wird der elektronische Personalausweis neben dieser hoheitlichen Aufgabe auch eine Authentisierungsfunktion anbieten, die so genannte eID, die es erlauben soll, den Personalausweis in digitalen (Geschäfts)-Prozessen zur Identifizierung zu verwenden. Beispiele für solche Prozesse sind Online-Authentisierungen beim eBusiness oder auch eGovernment-Anwendungen.

Im Folgenden werden die wichtigsten Sicherheitsmechanismen dieser elektronischen Reise- und Ausweisdokumente vorgestellt. Abschnitt 1.1 diskutiert die Eigenschaften des elektronischen Reisepasses, dem ePass, der bereits seit 2005 in Deutschland im Einsatz ist. In Abschnitt 1.2 gehen wir auf den aktuellen Stand der Technologie-Diskussion im Zusammenhang mit dem deutschen elektronischen Personalausweis ein, dessen Einführung für 2010 angekündigt ist.

1.1 Der elektronische Reisepass (ePass)

Ausgangspunkt der Entwicklung elektronischer Reisedokumente war am 13. Dezember 2004 der Beschluss des Rats der Europäischen Union, die Pässe der Mitgliedsstaaten gemäß dem Standard, der von der ICAO[1] spezifiziert wurde, mit maschinenlesbaren Personenkennzeichen, zu denen auch biometrischen Daten des Inhabers gehören, auszustatten. In Deutschland wurde diese EU-Richtlinie mit dem Beschluss des Bundeskabinetts vom 22.6.2005 umgesetzt, in dem die Einführung des elektronischen Reisepasses zum 1.11.2005 beschlos-

[1] International Civil Aviation Organisation

sen wurde. Wesentliches Merkmal des neuen Reisepasses ist ein RFID-Chip, der in den Pass integriert ist (vgl. Abbildung 1). Mit dem Pass werden zwei wesentliche Ziele verfolgt, nämlich

1. die Fälschungssicherheit der Daten auf dem Pass zu erhöhen und
2. den Missbrauch von Pässen zu erschweren, d.h. zu erschweren, dass echte Pässe von ähnlich aussehenden Personen (engl. *look-alike fraud*) missbraucht werden.

Zur Erreichung dieser Ziele enthält der ePass verschiedene Sicherheitsmerkmale. Die engere Bindung des Passes an seinen rechtmäßigen Besitzer soll durch den Einsatz biometrischer Daten erreicht werden, während zur Erhöhung der Fälschungssicherheit klassische Mechanismen, wie Digitale Signatur, Hashfunktionen und verschiedene, spezifisch auf die Einsatzszenarien elektronischer Reisedokumente zugeschnittene Authentisierungsprotokolle zum Einsatz kommen.

Abbildung 1.1 zeigt den deutschen elektronischen Reisepass mit integriertem RFID-Chip. Deutsche Reisepässe werden von der Bundesdruckerei herausgegeben.

1.1.1 Daten auf dem ePass

ePass

Der elektronische Reisepass enthält personen- und dokumentenbezogene Daten, die teilweise auf dem Reisepass aufgedruckt, in der Maschinenlesbaren Zone (MRZ) codiert bzw. im RFID-Chip des Reisepasses abgespeichert sind. Die Daten zur Person umfassen Vorname, (Familien-)Name, Wohnort, Geburtsort, Geschlecht, Geburtsdatum, Körperhöhe, Augenfarbe, Passfoto, Unterschriftenprobe und zwei Fingerabdrücke. Die Daten, die zum Dokument gehören, sind die 9-stellige Seriennummer (Passnummer), der ausstellende Staat, der Dokumententyp und das Gültigkeitsdatum des Passes. Deutsche Reisepässe haben eine Gültigkeit von 10 Jahren. Die 9-stellige Passnummer besteht aus zwei Teilnummern: die vierstellige Behördennummer und die 5-stellige PassID.

RFID

Zentraler Bestandteil des elektronischen Reisepasses ist ein kontaktloser, passiver RFID-Chip. Es handelt sich hierbei um einen ISO/IEC 14443-konformen Chip [7] mit kryptographischem Koprozessor. In deutschen Reisepässen werden CC-zertifizierte Chips

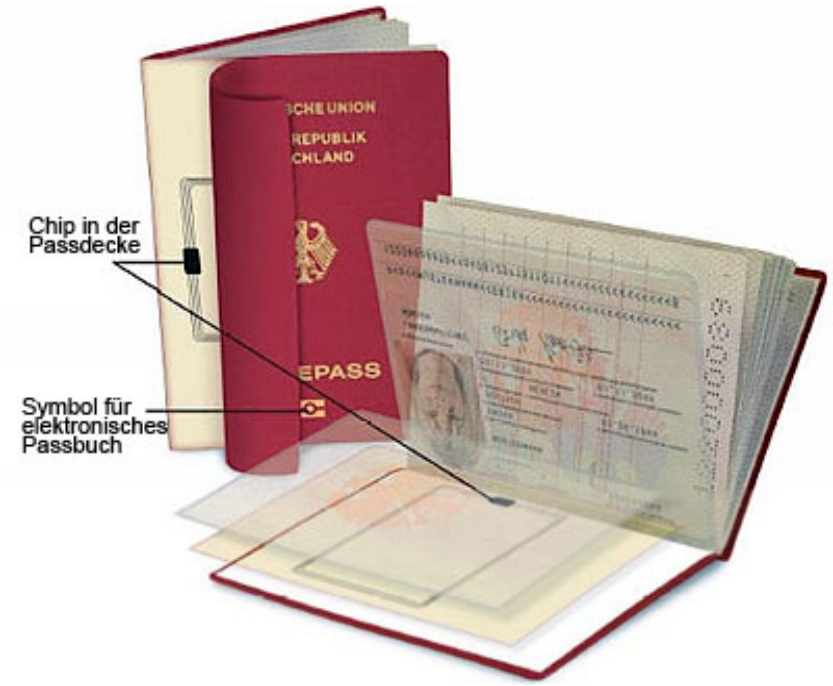

Abbildung 1.1: Der ePass mit integriertem RFID-Chip (Quelle: Bundesministerium des Inneren)

SmartMX von NXP der Firmen NXP Semiconductors mit Typ A (72 kB) und von Infineon Typ B (64 kB) eingesetzt. Die Hardware des SmartMX ist vom BSI nach EAL 5+ zertifiziert[1]. Der Infineon-Chip SLE66CLX641P / m1522-a11 wurde ebenfalls vom BSI zertifiziert und hat die Einstufung EAL 5, erweitert um die Komponenten ALC_DVS.2, AVA_MSU.3 und AVA_VLA.4[2] erhalten.

Die Signalisierungsreichweite der kontaktlosen Chips ist auf ca. 10 cm begrenzt. Damit und durch die integrierten Sicherheitsfunktionen unterscheidet sich der im ePass zum Einsatz kommende RFID-Chip erheblich von RFID-Chips gemäß ISO 15693 bzw. ISO 1800-6, die insbesondere in der Logistik verwendet werden. Diese RFID-Chips besitzen eine deutliche größere Signalisierungsreichweite, die zwischen einem und sieben Metern liegt.

Der Zugriff auf die Daten im Chip ist zumindest über eine einfache Zugriffskontrolle, der Basic Access Control (BAC) und optional auch über eine erweiterte Zugriffskontrolle, der Extended Access Control (EAC), abgesichert. PACE ist eine Entwicklung des BSI, das als Alternative zum BAC Protokoll einsetzbar ist (vgl. [3]). Das PACE-Verfahren (vgl. auch Abschnitt 1.2.2) soll in dem geplanten elektronischen Personalausweis eingesetzt werden. Auf die Zugriffskontrollmechanismen wird weiter unten noch genauer eingegangen.

Daten auf dem RFID-Chip

Die Daten auf dem Chip werden entsprechend der ICAO-Spezifikation für maschinenlesbare Reisedokumente (vgl. [5, 6]) in 16 Datengruppen und einem sogenannten Document Security Object aufgeteilt (vgl. Tabelle 1.1).

MRZ

Datengruppe 1 enthält die Daten, die auch in der maschinenlesbaren Zone (MRZ, Machine readable Zone) codiert abgelegt sind. Es handelt sich hierbei um den Namen, das Geschlecht und das Geburtsdatum des Passinhabers. Da diese Daten auch in der maschinenlesbaren Zone des Passes abgelegt sind, können sie optisch ausgelesen werden. Zum Auslesen der Daten aus der MRZ ist es erforderlich, dass der Pass auf ein optisches Lesegerät gelegt wird (vgl. Abbildung 1.2), während zum Auslesen der Daten aus der Datengruppe 1 des Chips eine Funkverbindung zum Chip aufgebaut werden

[1] Siehe http://www.bsi.bund.de/zertifiz/zert/reporte/0227a.pdf
[2] Siehe: http://www.bsi.bund.de/zertifiz/zert/reporte/0338b.pdf

Datengruppe	obligatorisch / optional	Inhalt	Zugriffskontrolle
DG1	obligatorisch	Daten aus der Maschinenlesbare Zone (MLZ)	BAC/PACE
DG2	obligatorisch	Gesichtsbild	BAC/PACE
DG3	optional	Fingerabdrücke	BAC/PACE + EAC
DG4	optional	Iris	BAC/PACE + EAC
...	optional		BAC/PACE
DG14	optional	Public Key für Chip Authentication	BAC/PACE
DG15	optional	Public Key für Active Authentication	BAC/PACE
DG16	optional	Im Notfall zu benachrichtigende Person	BAC/PACE
Document Security Object	obligatorisch	Hashwerte von allen Datengruppen; Signierte Hashwerte	BAC/PACE

Tabelle 1.1: Datenstruktur des ePass

muss.

Biometrische Daten

Datengruppen 2, 3 und 4 sind für die Speicherung biometrischer Merkmale vorgesehen. Datengruppe 2 enthält dabei das digitale Gesichtsbild (Foto) des Passinhabers, Datengruppe 3 den digitalen Fingerabdruck, während die Datengruppe 4 laut Spezifikation für das biometrische Merkmal Iris vorgesehen ist, was jedoch in den deutschen Pässen nicht verwendet wird. Die Datengruppen 3 und 4 sind optional. In Deutschland wird seit November 2007 auch der digitale Fingerabdruck (beide Zeigefinger) auf dem Chip gespeichert.

DSO

Weitere wichtige Datengruppen sind die Datengruppen 14 und 15, die öffentliche Schlüssel enthalten, die für die aktive Authentisierung des Chips gegenüber einem Lesegerät verwendet werden. Zur Prüfung der Unverfälschtheit der auf dem Chip abgelegten Daten dient das Document Security Object (DSO). Es enthält die mittels einer Signatur gesicherten, digitalen Hashwerte aller auf dem Chip gespeicherten

Abbildung 1.2: ePass und Lesegerät für die optisch auslesbare MRZ (Quelle: BSI)

Datengruppen. Die Daten auf dem Chip sind alle **nicht wiederholt beschreibbar**, so dass sich die Hashwerte im Document Security Object über die Lebenszeit des Reisepasses nicht ändern.

1.1.2 Sicherheitsmechanismen im ePass

Sicherheitsmechanismen

Der ePass sieht im Zusammenspiel mit einem Lesegerät unterschiedliche Sicherheitskontrollen vor.

- Mittels der *passiven Authentifizierung* kann ein Lesegerät die Integrität und Authentizität der Passdaten durch Vergleich ihres Hashs mit den ausgelesenen Daten aus dem Document Security Object prüfen. Damit soll die Fälschungssicherheit der Passdaten im Vergleich zum abgelösten nicht-elektronischen Pass erhöht werden.
- Die stärkere *aktive Authentifizierung*, bei der sich der Chip im Pass mittels eines asymmetrischen Challenge-Response-Protokolls gegenüber dem Lesegerät authentifiziert, dient darüber hinaus zur Erkennung geklonter Pässe, da der hier verwendete private Schlüssel nicht vom Lesegerät ausgelesen wird, sondern nur chip-intern und indirekt bei der Berechnung der Response einfließt.
- Der Zugriff auf die Daten im Chip ist mittels *Zugriffskontrollmechanismen* geschützt. Sie umfassen verpflichtend eine einfache Zugriffskontrolle, die Basic Access Control (BAC). Diese soll in deutschen elektronischen Personalausweisen durch eine verbesserte, passwortbasierte Kontrolle, das PACE-Verfahren, ersetzt werden.

- Für den Zugriff auf sensitive biometrische Daten, wie den Fingerabdruck, wird eine erweiterte Kontrolle, die Extended Access Control (EAC) gefordert. Sie fordert die Authentifikation des zugreifenden Lesegeräts mittels eines gültigen Zertifikats. Dieses Protokoll wird als *Terminal Authentifizierung* bezeichnet.
  Die Mitgliedsländer der EU haben sich verpflichtet, die erweiterte Zugriffskontrolle in ihren Lesegeräten zu verwenden, so dass der Zugriff auf alle Passdaten dieser verbesserten Kontrolle unterliegen wird.

Tabelle 1.2 fasst die Sicherheitsmechanismen und Protokolle, die auf dem ePass umgesetzt sind, sowie die damit verfolgten Schutzziele zusammen. Die Sicherheitsmechanismen werden nachfolgend erläutert.

Schutzziel(e)	**Mechanismen**	**Protokolle**
Integrität	Hashfunktion, Signatur	Passive Authentifikation
Authentizität der Passdaten	digitale Signatur, Zertifikat, länderübergreifende PKI	Passive und Aktive Authentifikation
Vertraulichkeit der Daten	physischer Zugriff (MRZ-Daten), Verschlüsselung	Zugriffskontrolle (BAC/PACE, EAC), Secure Messaging
Missbrauch reduzieren	Biometrische Merkmale (Foto, Fingerabdruck), Chip-Schlüssel (Signatur)	Passive Authentifikation, Terminal Authentifikation

Tabelle 1.2: Sicherheitsmechanismen und -Protokolle des ePass

Passive Authentifizierung

Bei der passiven Authentifizierung prüft ein Lesegerät die Passdaten auf Integrität und Authentizität des Datenursprungs. Die Prüfung der Passdaten durch ein Lesegerät erfolgt 2-stufig und ist verbunden mit Maßnahmen zur Zugriffskontrolle, der sogenannten Basic Access Control (BAC), auf die Abschnitt 1.1.3 noch genauer eingeht.

Bei der der passiven Authentifizierung muss sich das Lesegerät nicht *Lesegeräte*

gegenüber dem Pass (genauer dem RFID-Chip im Pass) authentisieren. Es hat lediglich nachzuweisen, dass es die Daten aus der MRZ des Passes kennt. In der Regel erfordert dies einen optischen Zugriff auf die MRZ, aber natürlich können diese Daten auch durch einen Angreifer anderweitig beschafft werden. Die passive Authentisierung verhindert somit nicht, dass unautorisierte Lesegeräte versuchen können, die Daten aus dem Chip des Reisepasses auszulesen. Auch wenn die geringe Signalisierungsreichweite des Chips das einfache Auslesen erschwert. Zur Abwehr derartiger Angriffe müsste das zugreifende Lesegerät nachwesen, dass es authentisch ist. Zudem müsste es einen signierten Nachweis vorlegen, auf welche Daten es zugreifen darf. Dies wird durch das Protokoll der *Terminal-Authentifizierung erreicht*, auf das wir auf Seite 14 eingehen.

Integritätsprüfung

Passive Authentifikation zusammen mit der einfachen Zugriffskontrolle für den Datenzugriff (BAC) orientiert sich am herkömmlichen Schutzniveau für Daten in Reisepässen. Das heißt, zum Auslesen der Daten muss der herkömmliche Reisepass (willentlich) dem Passbeamten übergeben werden. Analoges gilt auch für den ePass, der in ein optisches Lesegerät eingelegt werden muss, damit dieses die Daten aus der MRZ des Passes auslesen kann. Aus den optisch gelesenen Daten der MRZ berechnet das Lesegerät einen Zugriffsschlüssel, der als Basis zum Aufbau eines sicheren Kommunikationskanals zwischen Lesegerät und RFID-Chip des Passes genutzt wird. Damit das Lesegerät die Daten der MRZ auf Integrität prüfen kann, benötigt es das Data Security Objekt (DSO), das auf dem RFID-Chip abgelegt ist. Diese Daten werden mittels Secure Messaging unter Verwendung eines gemeinsamen 112-Bit Sitzungsschlüssel vertraulich vom Pass zum Lesegerät übermittelt. Der gemeinsame Sitzungsschlüssel wird bei der Ausführung des BAC-Protokolls sowohl im Chip des Passes als auch im Lesegerät berechnet, indem Teilschlüssel zwischen dem Chip und dem Lesegerät mittels eines Challenge-Response-Protokolls vertraulich ausgetauscht werden. Bei deutschen Reisepässen wird als Verschlüsselungsverfahren für das Secure Messaging 3DES im CBC Modus verwendet.

Secure Messaging

Zur Integritätsprüfung berechnet das Lesegerät die SHA-1-Hashwerte der ausgelesenen Daten aus den Datengruppen auf den RFID-Chip und vergleicht sie mit den in dem Data Security Objekt abgelegten Hashwerten.

Bei der passiven Authentifikation kann das Lesegerät auch die In-

tegrität der Gesichtsbilddaten (Datengruppe 2) prüfen, während der Zugriff auf die Fingerabdrücke einer höheren Sicherheitsanforderung unterliegt. Hierfür ist obligatorisch die Extended Access Control (EAC) durchzuführen, die vom Lesegerät einen Nachweis erfordert, dass es zum Zugriff tatsächlich berechtigt ist.

Authentizitätsprüfung

Um die Authentizität der im Pass gespeicherten Daten überprüfen zu können, muss das Lesegerät die Signatur des vom Pass erhaltenen Data Security Objekts prüfen. Abbildung 1.3 veranschaulicht die dafür benötigten Komponenten.

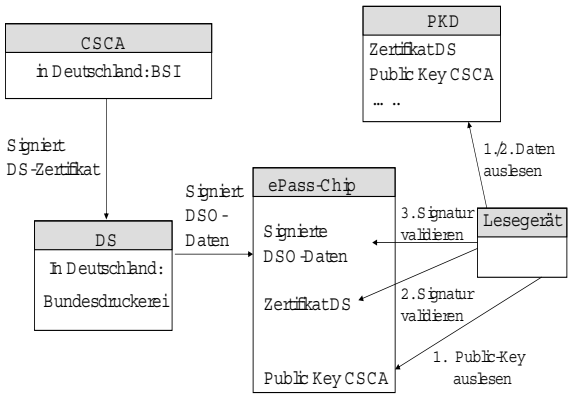

Abbildung 1.3: Prüfen der Authentizität der Passdaten durch ein Lesegerät

Die Daten im Data Security Object werden bei der Passerstellung vom Passaussteller signiert, so dass das Lesegerät das Zertifikat dieses Passausstellers benötigt, um die Signatur zu prüfen. In Deutschland ist diese Instanz die Bundesdruckerei. In der ICAO-Spezifikation für maschinenlesbare Reisedokumente ([5, 6, 3]) wird eine solche Instanz ein Document Signer (DS) genannt. Das Zertifikat eines Document Signers wird entweder auf dem Pass selbst abgelegt oder über das Public-Key Directory (PKD) der Standardisierungsorganisation ICAO veröffentlicht, so dass sich ein Lesegerät das erforderliche Zertifikat von dieser Stelle besorgen kann.

Das Zertifikat des Document Signers ist seinerseits digital signiert. Zur vollständigen Zertifikatsvalidierung benötigt das Lesegerät somit noch den öffentlichen Schlüssel derjenigen Instanz, die das Zertifikat des Document Signers signiert hat. Laut ICAO-Spezifikation muss es pro Land genau eine solche Instanz, die sogenannte Country Signing Certification Authority (CSCA) geben. In Deutschland ist dies das BSI. Der öffentliche Schlüssel der CSCA wird auf dem RFID-Chip des Reisepasses abgelegt und entweder im Public-Key Directory der ICAO veröffentlicht oder über diplomatische Wege den CSCA-Instanzen anderen Ländern bekannt gemacht. Der öffentliche Schlüssel der CSCA bildet den Vertrauensanker für die Zertifikatsvalidierung.

Zertifikat-Validierung

Beim Prüfen der Signatur des Document Security Objects ist somit eine 2-stufige Vertrauenskette durch ein Lesegerät zu validieren:

1. Validieren der Signatur der CSCA (also in Deutschland des BSI). Dazu sind die Schritte (1) und (2) aus Abbildung 1.3 auszuführen.
2. Validieren der Signatur des DS (also in Deutschland der Bundesdruckerei). Dazu ist der Schritt (3) aus der Abbildung auszuführen.

Signaturschlüssel

Da ein deutscher Reisepass eine Geltungsdauer von 10 Jahren besitzt, müssen die Signaturen eine entsprechend lange Gültigkeit (10 Jahre plus drei Monate) besitzen. Dies erfordert lange Signaturschlüssel. In Deutschland wird für das Signieren der Passdaten ein 224 Bit ECDSA-Schlüssel (Elliptic Curve DSA) des Passausstellers (Bundesdruckerei) verwendet. Der private Schlüssel besitzt nur eine kurze Gültigkeit von maximal drei Monaten. Dadurch wird sicher gestellt, dass derselbe private Schlüssel nur während je drei Monaten zur Zertifikatserstellung verwendet und anschließend durch einen neuen ersetzt wird. Damit will man erreichen, dass im Fall einer Schlüsselkompromittierung möglichst wenige Pässe betroffen sind. Die Zertifikate der Bundesdruckerei sind vom BSI als der deutschen CSCA-Instanz signiert. Hierfür wird ein 256-Bit ECDSA-Schlüssel verwendet. Der private Schlüssel der CSCA muss zwischen 3 und 5 Jahren gültig sein, während für den öffentlichen Schlüssel eine Gültigkeitsdauer von mindestens 13-15 Jahren gefordert wird. Um kompromittierte Schlüssel bekannt zu geben, muss jede CSCA re-

gelmäßig CRLs (Certificate Revokation Lists)[1] ausstellen und diese über diplomatische Kanäle oder über das ICAO Public-Key Directory publizieren.
In deutschen Pässen wird wie oben erwähnt zur Erstellung der digitalen Signaturen ECDSA verwendet. Die Spezifikation erlaubt auch die Verwendung von RSA oder alternativ von DSA und empfiehlt hierfür Schlüssellängen von 3072 Bit für die CSCA-Instanzen bzw. von 2048 Bit für Document Signer Instanzen.

Aktive Authentifizierung

Klonen

Allein durch passive Authentisierung der Passdaten kann ein Lesegerät nicht erkennen, ob der Pass vollständig gekloned wurde, und es sich damit nicht um einen authentischen Pass handelt. Die Daten in der MRZ auf der Datenseite des Passes sind zwar logisch mit den Daten in der Datengruppe 1 auf dem RFID-Chip verknüpft, so dass das Klonen eines Passes auch erfordert, dass die Datenseite des Passes kopiert wird. Dies ist schwierig, da die Datenseite durch zusätzliche physische Sicherheitsmerkmale, wie Hologramme, vor dem Kopieren geschützt wird. Dennoch ist ein Klone-Angriff nicht vollständig auszuschließen. Beim Klonen eines RFID-Chips werden die Chip-Daten ausgelesen und auf einen leeren Chip kopiert.

Abwehr

Zur Abwehr derartiger Angriffe wurde der Sicherheitsmechanismus der *Aktiven Authentifizierung* entwickelt. Bei der aktiven Authentifizierung muss der RFID-Chip des Passes dem Lesegerät beweisen, dass er den Chip-individuellen, geheimen Schlüssel kennt. Dieser Schlüssel muss deshalb im geschützten, nicht auslesbaren Speicher des RFID-Chips abgelegt sein. Ein solcher Schlüssel kann dann nur intern genutzt werden, so dass der Schlüssel nicht in einen geklonten Chip kopiert werden kann.
Zur aktiven Authenisierung gibt es zwei alternative Ansätze: die *Active Authentication* und die *Chip-Authentication*. Nachfolgend werden beide Protokolle kurz beschrieben. Da bei beiden Protokollen auf Daten des RFID-Chips lesend durch das Lesegerät zugegriffen wird, muss einer aktiven Authentisierung stets eine passive Authentisierung vorausgehen, in deren Verlauf zwischen Chip und Lesegerät ein gemeinsamer Sitzungsschlüssel etabliert wird.

[1] Rückruflisten für ungültige öffentliche Schlüssel

Active Authentication

AA

Die Basis einer Active Authentication (AA) bildet ein statisches Schlüsselpaar, dessen öffentlicher Bestandteil auf dem Chip in der Datengruppe 15 abgelegt ist. Der zugehörige private Schlüssel ist im geschützten Speicherbereich des Chips abgelegt. Zum Nachweis der Kenntnis des privaten Schlüssels wird ein asymmetrisches Challenge-Response-Protokoll zwischen Chip und Lesegerät abgewickelt. Dazu erzeugt das Lesegerät eine Random-Zahl, die vom Chip mit seinem geheimen Schlüssel signiert werden muss. Zur Signatur-Validierung liest das Lesegerät den zugehörigen Schlüssel aus der Datengruppe 15 aus, der mittels Secure Messaging zum Lesegerät übertragen wird. Die ICAO-Spezifikation erlaubt für die Active Authentication den Einsatz von RSA, DSA oder ECDSA. Die empfohlenen Schlüssellänge bei RSA/DAS-Schlüsseln beträgt 1024 Bit und bei ECDSA 160 Bit. Beim heutigen Stand der Technik sind das relativ kurze Schlüssel.

Challenge-Semantik

Ein mögliches Sicherheitsproblem bei der Verwendung von aktiver Authentifikation wird darin gesehen, dass der Chip keine Kenntnis darüber hat, ob die Random-Nachricht, die das Lesegerät sendet, eine Semantik trägt. Ein durchaus realistisches Szenario ist das folgende: Ein Lesegerät, das bei Grenz-Kontrollen offiziell eingesetzt wird, sendet spezielle Challenges an die elektronischen Pässe. Diese Challenges sind so formatiert, dass sie in geeigneter Form das Datum, die Uhrzeit und ggf. auch Ortsinformationen enthalten. Mit dem Signieren einer solchen Challenge durch einen ePass kann an Kontrollpunkten beispielsweise nachgehalten werden, wann und wo eine bestimmte Person eine Grenze überschritten hat. Da jedoch eine solche Challenge auch von einem gefälschten Lesegerät gesendet werden kann, könnte ein Pass dazu verleitet werden, einen beliebigen Wert zu signieren, z.B. falsche Orts- und Zeitangaben. Diese signierten Daten könnten zu einem späteren Zeitpunkt dazu verwendet werden, falsche Orts- und Aufenthaltsdaten über den Passinhaber zu verbreiten.

Als Alternative zu der Active Authentication (AA) der ICAO hat die EU die Chip-Authentifikation spezifiziert, die das Problem der Challenge-Semantik behebt und zusätzlich stärkere Sitzungsschlüssel für das Secure Messaging etabliert. In den deutschen Reisepässen kommt deshalb nicht das Verfahren der aktiven Authentisierung, sondern das Verfahren der Chip-Authentifikation zum Einsatz.

Chip-Authentifikation

Chip-Schlüssel

Bei der Chip-Authentifikation handelt es sich um ein Diffie-Hellmann-Schlüsselaustauschprotokoll unter Nutzung klassischer Diffie-Hellman (DH) oder Elliptic Curve DH (ECDH)-Verfahren. Dadurch kann auf ein Challenge-Response Protokoll verzichtet werden und der Chip läuft nicht Gefahr, einen beliebigen Wert (die Challenge) zu signieren. Der benötigte statische, öffentliche DH-Schlüssel ist auf dem Chip in der Datengruppe 14 abgelegt. Der private Schlüssel ist wiederum im geschützten, nicht auslesbaren Speicher des Chips gespeichert. Auf der Seite des Lesegeräts benötigt das Protokoll einen flüchtigen (ephemeral) DH-Schlüssel, der vom Lesegerät speziell für die Abwicklung des Protokolls erzeugt wird. In deutschen Reisepässen wird zur Chip-Authentifikation das ECDH-Verfahren mit einem 224 Bit-Schlüssel verwendet.

Verschlüsselung

Zusätzlich zur aktiven Authentisierung eines RFID-Chips ermöglicht die Chip-Authentisierung auch den Aufbau eines stark verschlüsselten und integritätsgesicherten Kommunikationskanals für den Datenaustausch zwischen Chip und Lesegerät. In den Mitgliedsländern der EU ist der Einsatz der Chip-Authentisierung für die verwendeten Lesegeräte verpflichtend, so dass wann immer möglich (wenn der Chip dies unterstützt), eine starke Verschlüsselung beim Datenaustausch mittels Secure Messaging verwendet wird und nicht nur beim Zugriff auf Fingerabdruckdaten im Kontext der Extended Access Control.

Das nachfolgend skizzierte Ablaufprotokoll setzt voraus, dass zwischen dem RFID-Chip und dem Lesegerät bereits mittels passiver Authentifikation ein sicherer Kommunikationskanal mit einem gemeinsamen Sitzungsschlüssel etabliert wurde, so dass alle unten angegebenen Nachrichten vertraulich kommuniziert werden. Ist das Chip-Authentifikations-Protokoll nicht erfolgreich durchgeführt worden, so bleibt dieser Basisschutz für den Datenaustausch weiterhin bestehen. Das heißt, dass der mittels Basis Access Control vereinbarte 112 Bit Sitzungsschlüssel weiterhin für das Secure Messaging verwendet wird. Dagegen wird bei erfolgreicher Abwicklung des Protokolls der alte Sitzungsschlüssel durch den auf einer sicheren Basis ausgehandelten und damit stärkeren Schlüssel ersetzt.

Varianten

Das Chip-Authentisierungsprotokoll kann in zwei Versionen implementiert werden. Variante 1 sieht eine implizite Echtheitsprüfung des Chips vor, während die Variante 2 aktive Aktionen seitens des Chips

zum expliziten Echtheitsnachweis, also zum Nachweis, dass der Chip nicht geklont ist, fordert.

Protokollablauf:

1. Der Chip sendet seinen statischen DH-Public-Key und die zu dessen Erzeugung verwendeten DH-Parameter zum Lesegerät.
2. Das Lesegerät erzeugt ein anonymes, flüchtiges DH-Schlüsselpaar und sendet den öffentlichen Teil $PK_{Terminal}$ an den Chip zurück.
3. Beide Parteien berechnen nach dem DH-Verfahren den gemeinsamen Schlüssel K.
4. Beide leiten aus K einen gemeinsamen MAC-Schlüssel K_{MAC} und Verschlüsselungsschlüssel K_{Enc} ab.
5. In Version 2 des Protokolls (explizite Echtheitsprüfung) berechnet der Chip ein Authentifizierungstoken T=Hash$(PK_{Terminal}, K_{MAC})$. Mit dem Token, der lediglich ein MAC-Wert ist, weist der Chip explizit die Kenntnis des gemeinsamen Hash-Schlüssels K_{MAC} nach.
6. Wiederum nur in Version 2 prüft das Lesegerät das Token T.

Secure Messaging

Nach einer erfolgreichen Durchführung des Chip-Authentifizierungsprotokolls erfolgt die weitere Kommunikation zwischen Chip und Lesegerät mittels Secure Messaging und der Verwendung der **neuen** gemeinsamen Schlüssel K_{MAC} bzw. K_{Enc}.

Um tatsächlich von der Echtheit des Chips überzeugt zu sein, sollte laut Spezifikation das Lesegerät unmittelbar nach einer erfolgreichen Chip-Authentifizierung die Integrität der Chip-Daten anhand des Data Security Objekts prüfen. Wenn der Chip in der Lage ist, das Datenobjekt mit dem gemeinsamen Schlüssel K_{Enc} zu verschlüsseln und wenn die Daten korrekt sind, so wird der Chip als unverfälscht betrachtet.

Terminal Authentifizierung

Terminal Authentifikation

Sensitive Daten auf dem Chip, für die eine erweiterte Zugriffskontrolle (EAC) vorgeschrieben ist, erfordern auch eine Authentisierung des Lesegeräts (Terminal) gegenüber dem Chip. Die Authentizitätsprüfung von Lesegeräten erfolgt auf der Basis von Zertifikaten und einem asymmetrischen Challenge-Response Protokoll. Hierzu ist der Aufbau einer erweiterten, ländergrenzenübergreifend funktionie-

renden PKI erforderlich (vgl. Abschnitt 1.1.4).

Protokollablauf:

1. Das Lesegerät sendet eine Folge von Zertifikaten, die zur Validierung seiner Signatur erforderlich sind, zum Chip. Die Folge beginnt mit einem Zertifikat, dessen Signatur durch einen öffentlichen Schlüssel prüfbar ist[1], der auf dem Chip gespeichert ist. Das letzte Element der Zertifikat-Kette ist das Zertifikat des Lesegeräts.
2. Der Chip prüft die Zertifikate und extrahiert den öffentlichen Schlüssel des Lesegeräts.
3. Der Chip sendet eine Zufallszahl an das Lesegerät.
4. Das Lesegerät signiert die Zufallszahl zusammen mit der Chip-ID (auslesbar aus der MRZ des Chips).
5. Der Chip validiert die Signatur.

Nach einer erfolgreichen Terminal-Authentifikation kann das Lesegerät Daten auf dem Chip auslesen. Über das für das Lesegerät ausgestellte Zertifikat wird geregelt, welche Zugriffsberechtigungen das Lesegerät für die Daten des Chips besitzt. In Abschnitt 1.1.4 gehen wir auf die Ausstellung der Zertifikate und die länderübergreifende PKI noch genauer ein.

1.1.3 Zugriffskontrolle

Zur Vermeidung unautorisierter Lese-Zugriffe auf die Daten des RFID-Chips, sieht die ICAO-Spezifikation verpflichtend eine Zugriffskontrolle mit mindestens der Mechanismenstärke einer Basic Access Control (BAC) vor. Mit dieser Basis-Zugriffskontrolle soll verhindert werden, dass über drahtlose Verbindungen beliebige Lesegeräte die Passdaten unbemerkt, z.B. wenn der Passbesitzer den Pass in seiner Tasche bei sich trägt, auslesen können. Da BAC einige Mängel aufweist, wurde vom BSI eine Alternative, das PACE (Password Authenticated Connection Establishment) Protokoll entwickelt (siehe Abschnitt 1.2.2).

Für sensitive Daten im Chip, wie die biometrischen Merkmale der

[1] Da auf dem Chip das Zertifikat der Country Signing Certification Authority (CSCA) abgelegt ist, gibt es stets einen Vertrauensanker.

Fingerabdrücke des Passinhabers, wird eine stärkere Zugriffskontrolle, die erweiterte Kontrolle, Extended Access Control (EAC), benötigt. Durch sie wird geprüft, ob das zugreifende Lesegerät berechtigt ist, auf die sensitiven Daten zuzugreifen. Die erweiterte Zugriffskontrolle wird in den deutschen Reisepässen umgesetzt.

Basic Access Control

BAC

Der Zugriff auf die Daten des RFID-Chips ist zumindest über Basic Access Control geschützt. Das Ziel ist, dass mit diesem Protokoll die Zugriffsmechanismen, die heute für nicht-elektronische Reisedokumente verwendet werden, nachgebildet werden, indem das Lesegerät physischen Zugriff auf den ePass haben muss. Diese Anforderung wird dadurch technisch umgesetzt, dass das Lesegerät die Daten aus der MRZ optisch auslesen muss. Die ausgelesenen Daten sind die 9-stellige Passnummer, das Geburtsdatum und das Ablaufdatum. Aus diesen Daten berechnet das Lesegerät den 56-Bit Zugriffsschlüssel (Access Key) K, indem ein SHA-1-Hashwert der Daten berechnet wird. In nachfolgenden Schritten weisen der ePass und das Lesegerät sich wechselseitig die Kenntnis dieses Access-Keys K nach und tauschen dabei Informationen zur Berechnung eines gemeinsamen Session-Keys $K_{session}$ aus. Für die nachfolgende verschlüsselte Kommunikation zwischen ePass und Lesegerät wird dann nur noch der dynamisch berechnete Sitzungsschlüssel $K_{session}$ verwendet. Der statische Schlüssel K dient nur als Initialisierungsschlüssel. Er ist aber ein bevorzugtes Angriffziel, da er der Sicherheitsanker für die weiteren dynamisch erzeugten Schlüssel ist. Die Abwicklung eines BAC-Ablaufs erfordert ca. 1 Sekunde Berechnungszeit.

Access Key

Protokollablauf:

1. Der RFID-Chip wählt eine Zufallszahl r_{chip} und eine 56-Bit Schlüsselhälfte K_{chip}. Die Zufallszahl r_{chip} wird an das Lesegerät übermittelt.
2. Das Lesegerät wählt eine Zufallszahl r_{reader} und eine 56-Bit Schlüsselhälfte K_{reader}.
3. Das Lesegerät berechnet einen Kryptotext $C1$:

$$C1 = E((r_{reader} \mid r_{chip} \mid K_{reader}), K)$$

Der Kryptotext C1 wird an den Chip übermittelt.

4. Der Chip entschlüsselt den Kryptotext C1 unter Einsatz des auf dem Chip abgelegten Schlüssels K:

$$D(C1, K) = \text{r‘}_{reader} \mid \text{r‘}_{chip} \mid \text{K‘}_{reader}$$

Der Chip prüft die Korrektheit der Daten: $\text{r‘}_{chip} = r_{chip}$.

5. Der Chip übermittelt dem Lesegerät nun seinerseits seinen Teil des Schlüssels, sowie den Nachweis, dass er über den gemeinsamen Schlüssel K verfügt, indem er einen Kryptotext $C2$ berechnet und diesen an das Lesegerät übermittelt:

$$C2 = E((r_{chip} \mid \text{r‘}_{reader} \mid K_{chip}), K).$$

6. Das Lesegerät entschlüsselt $C2$ mit

$$D(C2, K) = r_{chip} \mid \text{r‘}_{reader} \mid K_{chip}$$

und überprüft die Korrektheit von $\text{r‘}_{reader} = r_{reader}$.

Sitzungsschlüssel

Nach der Authentifikation berechnen beide Partner einen gemeinsamen 112 Bit 3DES-CBC Sitzungs-Schlüssel und einen gemeinsamen Integritätsschlüssel. Dazu werden die in dem obigen Protokoll ausgetauschten Schlüsselbestandteile konkateniert:

$$K_{session} = K_{reader} \;||\; K_{chip}.$$

Wie aus dem Protokollablauf ersichtlich, ist es für die Schritte 3-6 notwendig, dass das initiale Geheimnis K nicht gebrochen ist. Dies spielt bei der Bewertung der BAC in Abschnitt 1.1.5 eine entscheidende Rolle.

Extended Access Control

EAC

Die erweiterte Zugriffskontrolle, Extended Access Control (EAC) bietet einen stärken Zugriffsschutz als der BAC-basierte Schutz. Laut ICAO Spezifikation muss zumindest der Zugriff auf die Fingerabdruckdaten im Pass durch die Extended Access Control abgesichert werden. Hierbei erhalten nur berechtigte und authentische Lesegeräte Zugriff auf diese Daten. EAC erfordert, dass das zugreifende Lesegerät eine Terminal-Authentifizierung (siehe Abschnitt 1.1.2)

durchführt. Dabei muss das Lesegerät ein Zugriffszertifikat[1], das die Zugriffsrechte für den Pass definiert, sowie eine Kette von Zertifikaten vorweisen, mit deren Hilfe der Pass in der Lage ist, das Zugriffszertifikat des Lesegerätes zu validieren. Hierfür ist eine länderübergreifende PKI erforderlich.

1.1.4 Länderübergreifende PKI

PKI

Die elektronischen Reisedokumente werden vom Aussteller unterschrieben und zur Prüfung werden Signatur-Zertifikate der Unterzeichner benötigt. Elektronische Reisepässe bzw. Personalausweise erfordern eine Public Key Infrastruktur. Abbildung 1.4 veranschaulicht die generelle Struktur einer nationalen PKI. Sie ermöglicht eine Validierung von Zertifikaten von nationalen Lesegeräten. Im internatonalen Grenzverkehr müssen auch ausländische Lesegeräte Zertifikate erhalten, die der Reisepass prüfen kann. Darauf gehen wir dann nachfolgend noch kurz ein.

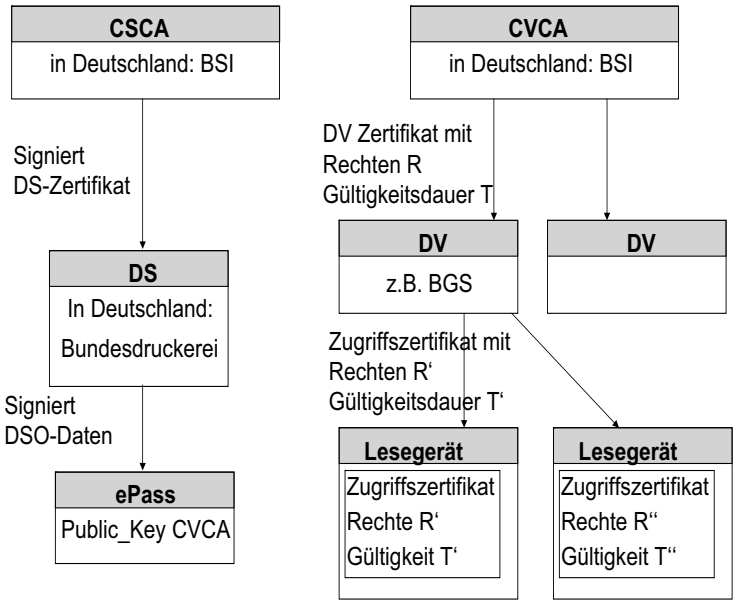

Abbildung 1.4: Nationale PKI mit Zertifikaten für Lesegeräte

[1] Bem.: Im Zusammenhang mit dem elektronischen Personalausweis werden derartige Zertifikate idR als Berechtigungszertifikat bezeichnet.

Signer-Instanzen

Die zur Prüfung elektronischer Reisepässe aufzubauende PKI muss international interoperabel sein. Jedes teilnehmende Land baut hierfür eine zweistufige PKI auf. Die Wurzel-Instanz dieser länderspezifischen PKI ist die CSCA (Country Signing Certification Authority). Auf der zweiten Ebene sind die Document Signer (DS), das sind die Passaussteller, angesiedelt. In Deutschland wird, wie bereits weiter vorne erwähnt, die CSCA vom BSI betrieben. Die CSCA signiert ausschließlich die Zertifikate für die Document Signer, in Deutschland ist dies aktuell ausschließlich die Bundesdruckerei, die zum Signieren der Passdaten berechtigt sind. Die deutschen Reisepässe sind 10 Jahre gültig. Laut Spezifikation müssen die jeweils verwendeten öffentlichen Schlüssel der CSCA 13-15 Jahre gültig sein, um auf jeden Fall die Gültigkeitsdauer der Pässe abzudecken. Die Document Signer müssen spätestens nach 3 Monaten ihre Schlüssel wechseln, um den Schaden bei einer Kompromittierung möglichst klein zu halten.

Verifier-Instanzen

Für das Verfahren der Terminal-Authentisierung muss die PKI um Verifier-Instanzen und Zertifikate erweitert werden. Nicht nur Pässe und Passaussteller benötigen hierbei ein Zertifikat, das prüfbar sein muss, sondern auch jedes Lesegerät im In- und Ausland, das seine Authentizität gegenüber einem beliebigen Reisepass nachweisen muss, benötigt ein Zertifikat, das vom Chip des Reisepasses validierbar ist.
Die Zertifikate für Lesegeräte werden von den Document Verifier-Instanzen (DV) ausgestellt. Jede DV-Instanz verwaltet eine Menge von Lesegeräten. In Deutschland ist eine solche DV-Instanz zum Beispiel der Bundesgrenzschutz (BGS), der Lesegeräte verwaltet, die bei der Grenzkontrolle zum Einsatz kommen. Document Verifier Instanzen müssen von der nationalen CVCA autorisiert sein, Zertifikate für Lesegeräte auszustellen. Jedes Land ist deshalb verpflichtet, eine vertrauenswürdige Instanz einzurichten, die *Country Verifying CA* (CVCA). Sie hat die Aufgabe, Document Verifier-Zertifikate für Document Verifier-Instanzen (DV) auszustellen.

Die CVCA kann die gleiche Komponente wie die CSCA sein, muss aber für die unterschiedlichen Aufgaben (Signieren, Validieren) unterschiedliche Schlüssel verwenden. In Deutschland werden sowohl CSCA- als auch CVCA-Aufgaben durch das BSI wahrgenommen. Der öffentliche Schlüssel der CVCA wird auf dem Chip des Reisepasses gespeichert; er dient als Vertrauensanker für Zertifikatsvalidierungspfade.

Zugriffszertifikat

Die von der CVCA ausgestellten Verifier-Zertifikate sind Zugriffszertifikate, sie beinhalten Zugriffsrechte auf Daten auf dem Chip. Um Missbrauch zu beschränken, sollten die Zertifikate nur eine kurze Gültigkeitsdauer besitzen. Die Festlegung der Gültigkeitsdauer der Zertifikate und der Umfang der vergebenen Zugriffsrechte obliegt der nationalen CVCA. Bei der Ausstellung eines Terminal-Zertifikats durch einen Document Verifier legt der DV für das Terminal die Zugriffsberechtigungen fest. Hierbei kann es sich jedoch höchstens um eine weitere Einschränkung der Rechtemenge handeln, die die CVCA-Instanz in dem entsprechenden Zugriffszertifikat bereits an den DV vergeben hat. Auch die Gültigkeitsdauer des Terminal-Zertifikats kann höchstens so lang sein, wie die des DV-Zertifikats.

Validierung

Bei der Terminal-Authentisierung muss das Lesegerät ein gültiges Zertifikat vorweisen und zur Validierung eine Zertifikatskette an den Chip übermitteln, die so enden muss, dass die Validierung mit dem auf dem Chip gespeicherten öffentlichen Schlüssel der nationalen Wurzel-Instanz starten kann. Um die Gültigkeit von Zertifikaten zu prüfen, benötigt der Chip eine aktuelle Zeit bzw. ein aktuelles Datum. Da er selber über keine lokale Uhr verfügt, nutzt er die effektive Zeit, die in einem Zertifikat steht, das er zuletzt validiert hat; d.h. Gültigkeitsprüfungen werden vom Chip nur vergröbert durchgeführt.

Grenzüberschreitende Prüfung

Bei ausländischen Lesegeräten muss ebenfalls gewährleistet werden, dass das Lesegerät ein validierbares Zertifikat besitzt. Dazu muss der DV dieses Lesegeräts im Vorfeld ein Zugriffszertifikat bei der zuständigen nationalen Wurzelinstanz CVCA des zu prüfenden Reisepasses beantragen. Diese CVCA erstellt ein Zugriffszertifikat (oder lehnt es aus staatlichen Interessen ab) und räumt damit dem ausländischen Document Verifier bzw. den von diesen kontrollierten Lesegeräten Leserechte an Daten auf den Reisepässen der Bürger des Landes, das die CVCA repräsentiert, ein. Derartige Zugriffszertifikate werden u.a. über diplomatische Kanäle verteilt.

1.1.5 Sicherheit des ePasses

Im Verlauf der Einführung des ePasses wurden eine Vielzahl von Sicherheitsbedenken beim Umgang mit dem Pass geäußert. Nachfolgend werden einige Problembereiche angesprochen und diskutiert. Hauptkritikpunkte betreffen das mangelhafte Sicherheitslevel der Basic Access Control, die Gefahr des unerlaubten Mitlesens

von Kommunikationsbeziehungen, die Möglichkeit, Aufenthalts- und Bewegungsprofile von Passbesitzern zu erstellen (z.B. durch nicht autorisiert betriebene Lesegeräte, die an Türen angebracht sind), sowie die Beeinträchtigung der Privatsphäre durch das unberechtigte Auslesen biometrischer Daten aus dem Reisepass. Wir gehen auf diese Punkte im Folgenden kurz ein.

Sicherheit von BAC

Zugriffsschlüssel

Obwohl der Sitzungsschlüssel mit 112-Bit eine zwar bei heutiger Technologie noch zufriedenstellende Schlüsselstärke aufweist, kann der Schlüssel kompromittiert werden. Zudem ist der Pass 10 Jahre lang gültig. Welche Anforderungen an die Schlüssellänge in 10 Jahren zu stellen sind, ist noch offen, da die Bundesnetzagentur keine Vorgaben für so lange Zeiträume macht. Eine Kompromittierung des Sitzungsschlüssels ist aber bereits bei heutiger Technologie möglich, da die beiden 56-Bit Teilschlüssel zur Übertragung nur mit dem Zugriffsschlüssel K verschlüsselt werden. Da dieser Schlüssel lediglich aus wenigen Daten (Passnummer, Geburtsdatum, Ablaufdatum) aus der MRZ berechnet wird, besitzt er nur eine geringe Entropie. Hinzu kommt, dass dies ein statischer Schlüssel ist, der bei jedem Protokolllauf für jedes Lesegerät der gleiche ist.

Brute-Force

Aufgrund der geringen Entropie des Schlüssels K besteht die Möglichkeit von Brute-Force Angriffen. Die Stärke des Schlüssels K entspricht etwa einem 56 Bit Schlüssel und ist damit einem DES-Schlüssel vergleichbar. Dies ergibt sich aus den Daten, die zur Schlüsselberechnung eingehen: die 9-stellige Passnummer (also 10^9 Möglichkeiten), das Geburtsdatum mit ca. $365 \cdot 10^2$ Möglichkeiten und das Ablaufdatum mit $365 \cdot 10$ Möglichkeiten, da der Pass einen Gültigkeit von 10 Jahren besitzt. Damit ergibt sich ein Suchraum von $365^2 \cdot 10^{12}$, was ungefähr dem Suchraum von 2^{56} entspricht.

Schlüsselraum

Dieser Suchraum von 2^{56} kann jedoch deutlich reduziert werden, wenn Informationen, wie zum Beispiel das exakte Geburtsdatum des Passinhabers, bekannt sind. Auch ergeben sich Schwächen daraus, dass die zur Schlüsselableitung verwendeten Daten des Passes nicht zufällig und gleichverteilt sind. So besteht die 9-stellige Passnummer in Deutschland aus einer 4-stelligen Behördennummer und einer 5-stellligen PassID. Ist die Behördenkennung bekannt, reduziert sich der unbekannte Raum der Passnummern auf 10^5. Auch das Geburtsdatum kann z.B. mit Kenntnis des Passfotos geschätzt und damit auch

dieser Suchraum eingeengt werden. Das Ablaufdatum des Passes ist abhängig von dem Ausstellungsdatum. Da an Feiertagen und Wochenenden normalerweise keine Pässe ausgestellt werden, reduziert sich die Zahl der Ausgabetage auf ca. 253 pro Jahr und damit auch dieser Suchraum. Auf diese Weise ist eine Reduktion des Raums auf 2^{30} möglich. Ein Angriff ist mit herkömmlicher Hardware innerhalb weniger Stunden möglich.
Sind die Daten der MRZ überwiegend bekannt, so kann der Suchraum sogar auf 2^{20} begrenzt werden. Anzumerken ist, dass bei der Durchführung der Brute-Force Angriffe der Angreifer Zugriff auf den Pass haben muss, um die Daten abzugleichen. Auch wenn Brute-Force Angriffe auf die Daten praktisch durchführbar sind, muss man sich klar darüber sein, dass es sich bei den Daten um solche personenbezogene Daten handelt, die i.d.R. auch auf anderem Wege leicht zu beschaffen sind. Dennoch bedeuten diese Angriffsmöglichkeiten eine Gefährdung der Privatsphäre. Aufgrund der Schwächen von BAC wird in Europa beim Zugriff auf **alle** Daten die Verwendung der Extended Access Control gefordert.

Auslesen der Passdaten

aktiv

Mit der Kenntnis des Zugriffsschlüssels K kann ein Lesegerät versuchen, einen aktiven Leseangriff auf den Pass durchzuführen, ohne im physischen Besitz des Passes zu sein. Zum aktiven Auslesen muss sich der Pass aber in der Nähe des Gerätes befinden, da es sich bei dem in den Pässen verwendeten RFID-Chips um ISO 14443-konforme Chips handelt, die eine deutlich geringe Signalisierungsreichweite als die in der Logistik üblicherweise eingesetzten Chips besitzen. Analysen und Studien, wie die MARS-Studie des BSI (vgl. [4]) oder die Untersuchungen der Gruppe von D. Wagner (vgl. [8]) haben gezeigt, dass unter der Voraussetzung, dass die Daten der MRZ bekannt sind, ein aktives Auslesen eines ISO 14443-konformen Chips nur in einer Reichweite bis zu 25cm möglich ist.

passiv

Die oben zitierte BSI-Studie hat zudem gezeigt, dass ein passives Mitlesen (engl. *skimming*) der verschlüsselt übertragenen Daten in einer Entfernung bis zu 2m möglich ist. Da die Daten mit einem 112 Bit Schlüssel mittels 3DES-CBC verschlüsselt sind, haben einzelne Bitfehler in einem übertragenen 64-bit Block eine direkte Auswirkung auch auf den unmittelbar folgenden Block. Der Angreifer müsste,

auch wenn ihm der verwendete Sitzungsschlüssel bekannt wäre, die möglichen Bitfehler manuell korrigieren. Derartige Angriffe sind möglich, aber auch relativ aufwändig.

Profilbildung

dynamische UID

Bei jeder Interaktion zwischen ePass und einem Lesegerät fordert die ICAO-Spezifikation die Übermittlung einer UID (Universal Identifier) des Chips. Dies wird zur Durchführung eines Collision Avoidance Protokolls bei der drahtlosen Kommunikation benötigt. Falls ein ePass hierbei stehts die gleiche UID überträgt, könnte die Gefahr einer Profilbildung bestehen. Deshalb empfiehlt die ICAO-Spezifikation die Erzeugung dynamischer UIDs, so dass bei jeder Kontaktaufnahme eine Random-ID erzeugt und verwendet wird. Dynamische UIDs kommen in deutschen Reisepässen zum Einsatz. Zusammen mit der geringen Reichweite von 10 bis max. 25cm eines ISO 14443-konformen Chips und den Zugriffskontrollen basierend auf BAC oder EAC scheint die Bedrohung der Profilbildung relativ gering.

Zertifizierung

Zertifizierung

Zur Sicherstellung der internationalen Interoperabilität der elektronischen Reisepässe und der dazugehörigen Lesegeräte hat das BSI eine technische Richtlinie im Sinne von Prüfkriterien entwickelt. Neutrale Prüfstellen, die vom BSI hierzu lizensiert sein müssen, können eine Konformitätsprüfung auf Grundlage der in der technischen Richtlinie definierten Prüfspezifikationen durchführen. Die Prüfung wird von der zuständigen Bestätigungsstelle des BSI überwacht und nach erfolgreichem Abschluss mit einem Konformitätsbescheid und einem Zertifikat[1] bestätigt. Im Zusammenhang mit dem Reisepass sind verschiedene technische Richtlinien von Bedeutung. Dazu gehören die Richtlinie zur Produktionsdatenerfassung, zur Produkt-Qualitätsprüfung oder aber auch die Prüfkriterien für elektronische Reisedokumente. Nach diesen technischen Richtlinien wurden beispielsweise Zertifikate an die Bundesdruckerei GmbH für das VISOTEC Expert 500 ePass-Lesegerät, an NXP Semiconductors GmbH für den ePass RFID-Chip, für die Bundesdruckerei für den Elektronischen Reisepass der Bundesrepublik Deutschland oder aber auch für Sagem für den Fingerabdruckscanner vergeben.

[1] Es handelt sich hierbei nicht um X509-Zertifikate, sondern Zertifikate im Sinne von Prüfsiegeln.

Die Konformitätsprüfung erfolgte gemäß Teil 4 der TR 03105 und wurde von der vom BSI akkreditierten Prüfstelle Cetecom ICT Services GmbH, Saarbrücken, durchgeführt. Dabei wurde überprüft, ob eine stabile RFID-Kommunikation zwischen Lesegerät und einem standardkonformen ePass gewährleistet ist.

1.2 Der elektronische Personalausweis (ePA)

ePA

Das Bundeskabinett hat am 23.7. 2008 dem Entwurf des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften zugestimmt. Der elektronische Personalausweis soll ab November 2010 an die deutschen Bürger ausgegeben werden und den bisherigen Personalausweis ablösen. Der elektronische Personalausweis (ePA) wird im Vergleich zum jetzigen Ausweis auf Scheckkartenformat ID-1 verkleinert. Abbildung 1.5 zeigt eine mögliche Ausprägung des zukünftigen ePA. Wie der Reisepass, so wird auch der ePA mit einem kontaktlosen, ISO 14443-konformen RFID-Chip [7] ausgestattet werden [2]. Seine Gültigkeitsdauer wird für Personen ab der Vollendung des 24ten Lebensjahres 10 Jahren sein; bei Personen unter 24 Jahren wird er eine Gültigkeit von 6 Jahren haben.

Seit dem 2.6.2008 liegt ein vom Bundesministerium des Innern veröffentlichtes Grobkonzept zur Einführung des elektronischen Personalausweises in Deutschland[1] zur Kommentierung vor.

1.2.1 Funktionen des ePA

Biometrie

Der elektronische Personalausweis ist so ausgelegt, dass er als Passersatz auch für hoheitliche Personenkontrollen, wie z.B. durch die Polizei, verwendet werden kann. Dazu werden, wie bereits bei den heutigen Ausweisen, körperliche Merkmale, wie Lichtbild, Größe, Augenfarbe, Alter optisch sichtbar aufgebracht, so dass eine Identitätsprüfung durch Inaugenscheinnahme und Vergleich möglich ist. Für einen elektronischen Abgleich wird der Ausweis die **ePass-Anwendung** unterstützen. Analog zur Personenkontrolle mittels des elektronischen Reisepasses werden bei dieser Anwendung die Daten der MRZ sowie die auf dem Chip des elektronischen Personalausweises gespeicherten biometrischen Daten benötigt. Verpflichtend ist

ePass

[1] siehe http://www.bmi.bund.de

Abbildung 1.5: Mögliche Ausprägung des ePA (Quelle: Grobkonzept des ePA, BMI)

hierfür das Gesichtsbild (wie beim Reisepass) bei der Ausweisausstellung im Ausweis digitalisiert abzuspeichern. Anders als jedoch beim Reisepass kann der Benutzer selber entscheiden, ob er auch seinen Fingerabdruck auf den Chip des Personalausweises ablegen möchte.

Zwei wichtige Funktionen charakterisieren den neuen Personalausweis und unterscheiden ihn damit auch vom elektronischen Reisepass. Es handelt sich um die eID Funktion zum Nachweis der digitalen Identität und die Option der Verwendung fortgeschrittener oder qualifizierter Signaturen.

eID-Funktion

eID

Der elektronische Personalausweis wird die so genannte eID-Funktion anbieten. Mit ihr wird es möglich sein, Daten, die auf dem RFID-Chip des Ausweises abgelegt sind, zur Online-Authentifizierung zu verwenden. Der Personalausweis liefert damit digitale Identitätsnachweise, so dass der Passinhaber im Geschäftsverkehr mit Verwaltung und Privatwirtschaft, beispielsweise beim Online-Shopping, Online-Banking oder Online-Auktionen, einfach und sicher identifiziert werden kann. Um die eID-Funktion des Passes nutzen zu können, muss sie aktiviert sein. Die eID Funktion soll jederzeit aktiviert und wieder deaktiviert werden können. Ein aktivieren und deaktivieren der eID Funktion ist jedoch nur durch die Personalausweisbehörde zulässig. Diese muss dafür ein spezifisches Berechtigungszertifikat

(s.u.) besitzen. Für Jugendliche unter 16 Jahren ist die eID-Funktion deaktiviert und kann erst ab dem 16. Lebensjahr durch die Behörde freigeschaltet werden.

Datenfelder

Für die eID Funktion sind folgende Datenfelder vorgesehen:

- Vornamen, Familienname,
- Doktorgrad,
- Tag und Ort der Geburt, sowie Angabe, ob ein bestimmtes Alter über- bzw. unterschritten ist (wie beispielsweise 18 Jahre)
- gegenwärtige Anschrift, sowie Angabe, ob Wohnort mit einem bestimmten Wohnort übereinstimmt
- Dokumentenart (Personalausweis),
- ausstellendes Land, Abkürzung D für Bundesrepublik Deutschland,
- Möglichkeit zur Abfrage der Gültigkeit des ePA
- Dienste- und anbieterspezifische Kennzeichen für die Erstellung von Pseudonymen.

Bei der Beantragung des neuen Ausweises kann der Benutzer explizit untersagen, dass bestimmte Datenfelder zum Auslesen verfügbar sind. Die biometrischen Daten stehen **ausschließlich für hoheitliche Kontrollen** zur Verfügung. Das heißt, dass eBusiness oder eGovernment-Anwendungen **keinen Zugriff** auf biometrische Daten im Ausweis mittels der eID Funktion erhalten. Der Zugriff auf die Daten im Ausweis erfordert vom zugreifenden Service einen Nachweis, dass er authentisch und zum Zugriff berechtigt ist. Diensteanbieter benötigen deshalb Berechtigungszertifikate (Zugriffszertifikate), die von dazu autorisierten, staatlichen Stellen auszustellen sind. Der Vorgang entspricht dem weiter oben beschriebenen Vorgang der Ausstellung von Zugriffszertifikaten für Lesegeräte für den elektronischen Reisepass. Wir gehen weiter unten auf das Konzept des Berechtigungszertifikats noch etwas genauer ein.

PIN

Anders als beim Zugriff auf Daten im Chip des elektronischen Reisepasses durch Lesegeräte soll der Besitzer des Personalausweises die Kontrolle darüber behalten, welcher Online-Dienstanbieter Zugriff auf welche Daten im Personalausweis erhält. Dazu ist vorgesehen, dass dem Benutzer angezeigt wird, welcher Diensteanbieter auf wel-

che Datenfelder im Ausweis zugreifen möchte. Der Benutzer kann explizit die Zugriffe auf einzelne Datenfelder für den Zugriff verbieten oder erlauben (ankreuzen von entsprechenden Datenfeldern). Bevor ein Zugriff dann tatsächlich erfolgen kann, muss der Benutzer noch explizit die Erlaubnis dazu erteilen. Dazu muss er seine 6-stellige Benutzer-PIN verwenden, die er bei der Beantragung des Personalausweises per PIN/PUK-Brief zugesandt bekommt. Mit der Eingabe seiner 6-stelligen Benutzer-PIN bestätigt der Benutzer, dass der Zugriff auf seinen ePA erfolgen darf. Durch die Verknüpfung von Besitz (der Ausweis) und Wissen (PIN) beim Zugriff auf die Daten im Chip soll zudem die Sicherheit erhöht werden, dass Jemand, der im Besitz des Ausweises ist, unter der digitalen Identität des Ausweisinhabers im Online-Business aktiv wird.
Eine Änderung der PIN ist vorgesehen. Der Passbesitzer kann seine PIN selber ändern; dazu ist wie üblich die Kenntnis der alten PIN notwendig. Wurde die PIN vergessen, so kann nur die Personalausweisbehörde nach eindeutiger Identifizierung des Ausweisinhabers die PIN ändern. Die PUK dient nur zum Zurücksetzen des Fehlbedienungszählers, der für die Benutzer-PIN im Chip geführt wird und nach dreimaliger Falscheingabe zum Blockieren der PIN führt.

Sperrung

Der versiegelte PIN-Brief, der per Post zugestellt werden soll, enthält auch das Nutzer-spezifische Sperrkennwort, mit dem der Nutzer bei Verlust seines Ausweises den Ausweis sperren lassen kann. Geplant ist eine rund um die Uhr erreichbare Telefon-Hotline, damit Bürger bei einem Verlust oder Diebstahl ihren Ausweis sperren lassen können. Laut BMI soll der gesperrte Ausweis auf eine Sperrliste gesetzt werden, die von jedem Diensteanbieter heruntergeladen werden kann. Mit Hilfe der Sperrliste kann jeder Dienstanbieter prüfen, ob eine Authentisierung mit einem als verloren oder gestohlen gemeldeten elektronischen Personalausweis versucht wird.

Erforderliche Komponenten

Um die eID Funktion für Online-Transaktionen nutzen zu können, benötigt ein Ausweisinhaber sowohl Hardware- als auch Software-Komponenten. Laut BMI sind folgende Komponenten gefordert:

- Funktionsfähiger Arbeitsplatzrechner mit (virenfreiem) Betriebssystem,
- (zertifiziertes) Kartenlesegerät für kontaktlose Chipkarten. Die entsprechenden Kartenleser sollen durch das BSI zertifiziert wer-

den, wobei, laut BMI, bei der Zertifizierung neben den Sicherheitsaspekten auch die Benutzerfreundlichkeit eine wichtige Rolle spielen soll.

- eine Software zur Kommunikation zwischen Arbeitsplatzrechner und Kartenlesegerät,
- ein Internetzugang.

Qualifizierte Signatur

Signatur

Ist bei Geschäftstransaktionen oder Verwaltungsabläufen eine eigenhändige Unterschrift erforderlich, so wird im eBusiness oder eGovernment eine elektronische Signatur als Äquivalent verlangt. Deshalb wird der elektronische Personalausweis optional die fortgeschrittene oder qualifizierte Signatur als optionale Anwendung unterstützen. Das bedeutet, dass der ePA für die Aufnahme eines qualifizierten Signaturzertifikates gemäß Signaturgesetz vorbereitet ist. Der Ausweisbesitzer entscheidet selber, ob er ein Zertifikat in den Chip des Ausweises nachladen möchte. Weiterhin kann der Ausweisinhaber dasjenige Trustcenter auswählen, von dem er sich ein Zertifikat ausstellen lassen möchte. Das Nachladen von Zertifikaten wird gebührenpflichtig sein.

Schutzziele

Schutzziele

Analog zum ePass gehören die Integrität der Ausweisdaten, die Authentizität, die Zugriffskontrolle und die vertrauliche Kommunikation zu den Schutzzielen des ePA. Anders als beim ePass werden jedoch bei der Online-Authentisierung Ausweisdaten nicht nur über kurze Distanzen drahtlos zwischen Chip und Lesegerät übertragen, sondern über das ungesicherte Internet, so dass die Kommunikationsverbindung stark abgesichert werden muss. Zudem sind im Sinne der mehrseitigen Sicherheit bei einer Online-Authentisierung die Sicherheitsanforderungen beider beteiligter Parteien zu berücksichtigen:

1. Der Online-Dienstanbieter muss in der Lage sein zu überprüfen, ob der Nutzer des Passes auch der berechtigte Inhaber des Ausweises ist. Bei der ePass-Anwendung erfolgt dies durch den kontrollierenden Grenzbeamten, der den Ausweis kontrolliert und das Gesichtsbild auf dem Ausweis mit der Person direkt vergleicht bzw. einen Rechner bedient, der den Vergleich durchführt. Beim ePA wurde dafür die Benutzer-PIN zusammen mit dem bereits

erwähnten PACE-Verfahren (siehe Abschnitt 1.2.2) entwickelt.

2. Der Inhaber des Personalausweises sollte die Kontrolle darüber haben, welche Dienstanbieter auf welche Daten auf seinem Ausweis zugreifen dürfen. Zudem ist analog wie beim ePass zu verhindern, dass Bewegungs- und Aufenthaltsprofile des Ausweisinhabers erstellt werden können, um die Privatsphäre nicht zu gefährden.

Zur Erfüllung der Sicherheitsanforderungen kommen die Verfahren PACE (Password Authenticated Connection Establishment) und EAC zur Zugriffskontrolle sowie Terminal- und Chip-Authentifizierung zur Authentisierung der Teilnehmer zum Einsatz. Anwendungen dürfen nicht auf den ePA nachgeladen werden.

1.2.2 PACE (Password Authenticated Connection Establishment)

PACE ist ein kryptographisches Protokoll, das zum Ziel hat, die Verwendung klassischer PIN-basierter Authentisierungstechniken auch für kontaklose Karten, wie dem ePass oder dem ePA, zu ermöglichen. Das PACE-Verfahren besteht im Kern aus einem Diffie-Hellmann-Schlüsselaustauschprotokoll, wobei die ausgetauschten Schlüssel mittels (einfacher) Passworte (PINs) abgesichert werden. Auch bei BAC wird ein Passwort verwendet. Dies ist der immer gleiche Zwischenschlüssel, der aus den Daten der MRZ berechnet wird und damit jedem Lesegerät mit optischem Zugriff direkt zugänglich ist. PACE unterstützt demgegenüber mehrere, falls die Geräte es zulassen sogar dynamische Passworte bzw. PINs zur Authentisierung. PACE unterscheidet 2 Klassen von PINs:

Karten-PIN

- Karten-PIN (CardPIN): Die Karten-PIN ist keine geheime PIN, sondern kann eine statische oder dynamische PIN sein. Eine dynamische PIN wird von der Karte auf dem Karten-Display angezeigt (falls ein solches vorhanden ist). Eine statische PIN ist eine Nummer, die auf das Dokument (den Pass) aufgedruckt ist. Diese Nummer kann maschinell auslesbar sein. Sie dient zur Simulation des Steckvorgangs kontaktbehafteter Karten. Analog zur BAC-Prüfung erfordert das Auslesen dieser PIN den optischen Zugriff auf den Pass.

eID

- Nutzer-Pin (eID): Die Nutzer-PIN ist eine geheime PIN, die nur der Pass- bzw. Ausweis-Besitzer und sein Chip kennen sollten. Analog zur PIN-basierten Authentisierung bei der Verwendung von Smartcards, kann der Kartenbesitzer unter Eingabe der PIN am Lesegerät nachweisen, dass er der berechtigte Nutzer ist. Die PIN wird dem Nutzer wie üblich mittels PIN-Brief auf dem Postweg übermittelt.

Verzögertes Blockieren

Die Karten-PIN ist eine nicht-blockierende PIN, während mit Benutzer-PINs, die beim ePA 6 Ziffern lang sind, ein Fehlbedienungszähler verknüpft ist. Entsprechend sind mittels ePINs geschützte Karten anfällig gegen Denial of Service-Angriffe, die bei den kontaktlosen Karten eine physische Nähe (ca. 10 cm) zur Karte erfordern. Zur Abschwächung derartiger Angriffe verwendet PACE das Konzept des verzögerten Blockierens. Nach Ablauf der maximalen Zahl an Fehlbedienungen (beim ePA sind das 2 Versuche) wird die Karte zunächst suspendiert und der Benutzer muss als nächstes die korrekte Karten-PIN eingeben, so dass ein Angreifer physischen Zugriff auf den Ausweis haben müsste. Erst wenn nach korrekter Eingabe einer Karten-PIN erneut eine falsche Benutzer-PIN eingegeben wird, erfolgt die Sperrung der PIN. Vom Nutzer nicht bemerkbare DoS-Angriffe sind auf solche Weise natürlich nicht abzuschwächen.

Protokollablauf (vergröbert)

Basis

Im Gegensatz zu der oben beschriebenen Chip-Authentisierung, bei der ein statisches DH-Schlüsselpaar, das auf dem ePass-Chip abgelegt ist, verwendet wird, generieren bei der PACE-Authentisierung sowohl der Chip als auch das Lesegerät dynamisch flüchtige (ephemeral) DH-Schlüsselpaare, basierend auf den auf dem Chip abgelegten DH-Parametern, den sogenannten Domänen-Parametern. Die Authentizität der öffentlichen DH-Schlüssel wird über den Nachweis der Kenntnis des gemeinsamen Geheimnisses, der PIN, sichergestellt. Beim ePA kommen zur Abwicklung des PACE-Protokolls die Verfahren ECDH und ECDSA mit 224 Bit-Schlüssel zum Einsatz.

Protokoll

1. Der Chip wählt eine Zufallszahl s und verschlüsselt diese mit einem aus der PIN π abgeleiteten Schlüssel $K_\pi : C = E(s, K_\pi)$.
2. Der Chip überträgt den Kryptotext C und seine DH-Parameter zum Lesegerät.
3. Das Lesegerät muss die PIN π besitzen, entweder durch direktes

Extrahieren aus der lesbaren Zone des Ausweises, falls es sich um eine statische Karten-PIN handelt, oder der Benutzer muss seine geheime PIN am Lesegerät eingeben.

4. Das Lesegerät leitet seinerseits den Schlüssel K_π aus der PIN ab und entschlüsselt den erhaltenen Kryptotext: $s = D(C, K_\pi)$.
5. Chip und Lesegerät erzeugen jeweils flüchtige DH-Schlüsselpaare basierend auf den neu berechneten DH-Parametern, die das Ergebnis einer Abbildungsfunktion sind, die auf die ursprünglichen Domänen-Parameter des Chips angewendet wird und in die die Kenntnis der verschlüsselt ausgetauschten Zufallszahl s eingeht.
6. Beide Partner tauschen ihre jeweiligen öffentlichen DH-Schlüssel aus.
7. Beide Partner berechnen den gemeinsamen, geheimen DH-Schlüssel K und leiten davon einen gemeinsamen Integritäts- K_{MAC} und Sitzungsschlüssel K_{Enc} ab.
8. Beide Partner erzeugen jeweils ein Authentisierungstoken. Dies ist ein MAC basierend auf dem Integritätsschlüssel K_{MAC} und dem öffentlichen DH-Schlüssel des Partners.
9. Beide prüfen den MAC und verwenden danach die neuen Schlüssel für das nachfolgende Secure Messaging.

PIN-Klassen

Die bei PACE verwendete PIN ist im Fall einer Online-Authentisierung bei E-Business oder E-Government eine 6-stellige Benutzer-PIN, um die Personenbindung zum Ausweis durchzuführen. Wird jedoch nur ein sicherer Kanal zwischen einem bestimmten Ausweis und einem Lesegerät benötigt, wie dies bei hoheitlichen Kontrollen erforderlich ist, so wird lediglich eine Karten-PIN benötigt. Diese kann als 6-stellige PIN auf der Karte aufgedruckt oder in der MRZ abgelegt sein. Dies ist dann natürlich keine geheime PIN mehr, was aber für die hoheitliche Personenkontrolle auch nicht notwendig ist, da hierbei der Besitz des Ausweises nachgewiesen wird und die Nutzeridentität unmittelbar prüfbar ist.

1.2.3 ePA bei der Online-Authentisierung

In diesem Abschnitt gehen wir etwas genauer auf die Nutzung der eID-Funktion des Ausweises beim der Online-Authentisierung ein.

Berechtigungszertifikat

Berechtigungszertifikat

Will ein Online-Dienstanbieter auf Daten im Personalausweis zugreifen, muss er ein Berechtigungszertifikat[1] besitzen. Ein solches Zertifikat wird von einer staatlichen Stelle auf Antrag des Diensteanbieters ausgestellt. Der Antrag muss Angaben über Name und Anschrift des Dienstanbieters, Nachweis des berechtigten Interesses an den personenbezogenen Daten, Zweckbindung der Daten, Angabe über die eingesetzte Krypto Hard- und Software, eine Datenschutzerklärung der zuständigen Datenschutzaufsichtsbehörde, sowie eine Darlegung enthalten, dass geeignete, (zertifizierte) Software beim Diensteanbieter zum Einsatz kommt. Die staatliche Stelle hat bei der Anfrage die Zulässigkeit des Dienstanbieters, sowie die Plausibilität der angefragten Datenzugriffe in Bezug auf den intendierten Verwendungszweck zu prüfen. Ist die Prüfung erfolgreich verlaufen, wird der Diensteanbieter aufgefordert, ein Schlüsselpaar mit einer zertifizierten Krypto-Soft- und Hardware zu erstellen. Als nächstes muss der Diensteanbieter seinen öffentlichen Schlüssel, sowie ein SSL/TLS Zertifikat auf sicherem Weg an die staatliche Stelle übermitteln. Die staatliche Stelle generiert aus den Daten das Berechtigungszertifikat für den Diensteanbieter.

Das Berechtigungszertifikat enthält u.a. folgende Angaben:

- Name, Anschrift und E-Mail Adresse des Diensteanbieters,
- Berechtigung zum Zugriff auf Datenfelder im ePA, z.B. Vor- und Nachname, Alter,
- Anbieterspezifische Kennung, die von der ausgegebenen Stelle vergeben wird; dies wird vom ePA zur Erzeugung von Pseudonymen (s.u.) benötigt,
- Zweck der Datenübermittlung,
- Angabe der zuständigen Datenschutzaufsichtsbehörde,
- Ablaufdatum des Zertifikats.

Die Berechtigungszertifikate haben eine Gültigkeit von 1-3 Tagen, da der ePA nicht in der Lage ist, Sperrlisten zu prüfen. Demgegenüber wird die Berechtigung zur Erhebung von Authentisierungsdaten ei-

[1] Das Berechtigungszertifikat entspricht dem Konzept des Zugriffszertifikats beim elektronischen Reisepass.

nem Diensteanbieter für einen Zeitraum von bis zu drei Jahren erteilt. Folgezertifikate sollen im Rahmen dieser Gültigkeitsdauer bei der staatlichen Stelle online abrufbar sein.

Anhand eines generischen Szenarios werden zunächst der allgemeine Ablauf und dann die dabei verwendeten Konzepte und Protokolle beschrieben.

Allgemeiner Ablauf

Abbildung 1.6 verdeutlicht den allgemeinen Ablauf bei einer Online-Authentisierung mittels des ePA und zeigt die dabei involvierten Parteien.

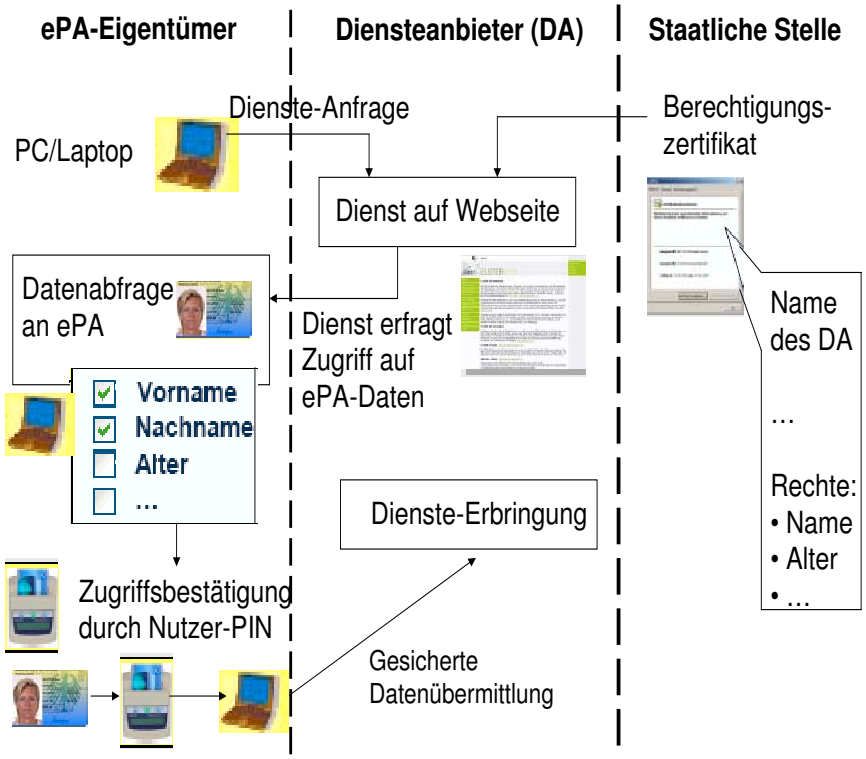

Abbildung 1.6: Nachweis der digitalen Identität mit dem ePA

Diensteanfrage

Der Ausweisinhaber stellt über den Web-Browser seines Rechners eine Anfrage an einen Online-Diensteanbieter *Online_Games* zur Nutzung eines Online Dienstes, z.B. zum Online-Erwerb eines Spiels *Game_X*, das erst ab 18 zu kaufen ist. Falls der Diensteanbieter im Vorfeld bereits ein Berechtigungszertifikat für seinen Dienst bei einer staatlichen Stelle, wie oben beschrieben, beantragt und erhalten hatte, wird er dieses Zertifikat an den Browser des Anfragers übermitteln. In dem Berechtigungszertifikat sind die Berechtigungen, die die staatliche Stelle dem Diensteanbieter *Online_Games* zur Durchführung des Dienstes *Game_X* prinzipiell erteilt hat, aufgelistet. In diesem speziellen Beispiel ist die Altersangabe von Bedeutung, so dass der Diensteanbieter beispielsweise die Berechtigung erlangt, eine Altersabfrage an den ePA zu stellen. Der ePA sieht dafür eine spezielle Funktion vor, so dass bei einer solchen Anfrage keine genauen Geburtsdaten übermittelt werden, sondern lediglich, wie in dem Beispiel erforderlich, die Anfrage z.B. auf Volljährigkeit mit ja oder nein beantwortet wird.
In dem in Abbildung 1.6 skizzierten Szenario ist dargestellt, dass das Berechtigungszertifikat des Diensteanbieters den Zugriff auf die Namensfelder sowie das Alter prinzipiell ermöglicht.

kontrollierbare Datenfreigabe

Der Diensteanbieter übermittelt sein Berechtigungszertifikat an den Browser bzw. das Lesegerät des anfragenden Nutzers. Die ePA-Spezifikation fordert, dass dem Nutzer die wesentlichen Daten, die im Berechtigungszertifikat enthalten sind, optisch angezeigt werden. Der Nutzer ist damit in der Lage zu prüfen, für welchen Diensteanbieter und welchen Dienst das Zertifikat ausgestellt wurde, sowie welche Berechtigungen dem Dienstanbieter durch den Zertifikatsaussteller eingeräumt wurden. Die in dem Zertifikat festgelegten Zugriffsrechte können nun vom Benutzer explizit weiter eingeschränkt werden. Dieser Vorgang ist bei jeder Online-Authentisierung individuell durchzuführen. Im Beispiel des Online-Game-Kaufs könnte es beispielsweise sein, dass der Ausweiseigentümer lediglich die Altersabfrage zulassen, sonst aber keine persönlichen Daten übermitteln möchte. In dem in Abbildung 1.6 skizzierten Szenario verweigert der Benutzer demgegenüber explizit den Zugriff auf das Alter, in dem er die Berechtigung entfernt (Haken wird entfernt).
Der Ausweisinhaber autorisiert den Zugriff auf die Daten in seinem Ausweis durch die Eingabe seiner 6-stelligen Benutzer-PIN. Durch die Eingabe der 6-stelligen PIN gibt der Benutzer somit explizit sei-

ne Einwilligung zu einem Auslesevorgang und das Lesegerät kann prüfen, ob der Benutzer die PIN kennt und damit der rechtmäßige Inhaber des Personalausweises ist (falls die PIN nicht weitergegeben oder anderweitig offen gelegt wurde).

Die vom Diensteanbieter angefragten und vom Benutzer freigegebenen Daten werden aus dem ePA ausgelesen und an den Diensteanbieter zur Durchführung des Dienstes übermittelt.

Pseudonyme

Pseudonyme

Das Telemediengesetz schreibt vor, dass ein Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Verwendung eines Pseudonyms zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist. Laut Bundesdatenschutzgesetz bedeutet eine Pseudonymisierung, dass der Name und andere Identifikationsmerkmale ersetzt wird durch ein Kennzeichen, das den Zweck hat, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Der ePA sieht zwei miteinander zu kombinierende Konzepte vor, um die Forderung nach Pseudomisierung zu erfüllen. Dies ist zum einen die anbieterspezifische, zufällige Kennung, die in dem Berechtigungszertifikat für den Diensteanbieter abgelegt wird. Zum anderen ist es die Anwendung *Restricted Identification*, die auf dem ePA implementiert werden soll. Bei der Authentisierung eines ePA-Inhabers mittels Pseudonym werden beide Konzepte kombiniert. Mittels der Restricted Identification-Anwendung wird aus einem personalausweisindividuellen, geheimen Schlüssel und der Kennung des Diensteanbieters ein bereichsspezifisches Kennzeichen berechnet. Dieses wird als Pseudonym dem Diensteanbieter übermittelt. Da unterschiedliche Diensteanbieter verschiedene Kennnummern besitzen, werden stets unterschiedliche Pseudonyme berechnet. Auf diese Weise soll verhindert werden, dass diensteanbieterübergreifend Nutzerprofile erstellt werden.

Anhand der bereichsspezifischen Kennung können Diensteanbieter zudem einen registrierten Nutzer wieder erkennen. D.h. die Restricted ID-Funktion des ePA erlaubt es, einen Personalausweis eindeutig wiederzuerkennen, ohne dass damit Ausweisdaten oder Daten über den Ausweisbesitzer gespeichert werden müssen[1].

[1] Bem.: Die Verwendung der Seriennummer des Personalausweises in kommerziellen Anwendungen ist gesetzlich unzulässig.

Verwendete Protokolle

Abbildung 1.7 verdeutlicht die Protokolle, die bei einer Online-Authentisierung mittels des ePA verwendet werden.

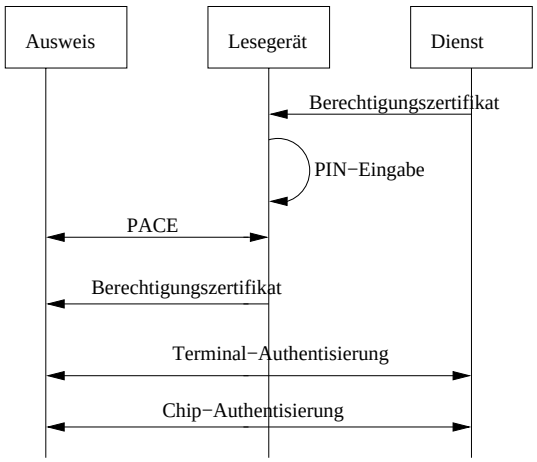

Abbildung 1.7: Online-Authentisierung mit dem ePA (Abbildung aus [1])

Entsprechend dem oben beschriebenen Ablauf, übersendet der Diensteanbieter sein Berechtigungszertifikat und der Ausweisinhaber bestätigt den Zugriff auf seinen Ausweis durch die Eingabe seiner Benutzer-PIN. Es ist nun zu prüfen, ob der Benutzer eine korrekte PIN eingegeben hat. Ist dies der Fall, so wird ein sicherer Kanal zwischen dem Ausweis und dem Lesegerät aufgebaut.

PACE

Zur Prüfung der Korrektheit der PIN und zum Aufbau einer verschlüsselten Verbindung zwischen Personalausweis und Lesegerät wird PACE verwendet. Nach der Eingabe der geheimen Benutzer-PIN am Lesegerät durch den Benutzer wird mittels PACE aus den öffentlichen DH-Schlüsseln der Partner (Ausweis-Chip und Lesegerät) ein gemeinsames Geheimnis berechnet. Aus diesem Geheimnis werden anschließend der Integritäts- und Sitzungsschlüssel für das Secure Messaging zwischen den Partnern abgeleitet. Zum verschlüsselten Datentransfer zwischen Chip und Lesegerät soll laut derzeitigen Stand der ePA das AES-Verfahren verwenden. Nachdem über PACE gemeinsame Sitzungsschlüssel ausgehandelt wurden, überträgt das Lesegerät das Berechtigungszertifikat des Diensteanbieters zum Ausweis.

dynamische UIDs

Um Tracking-Angriffe zu erschweren, verwendet auch der ePA dy-

namische UIDs beim Aufbau einer Kommunikationsverbindung zu einem Lesegerät.

Authentisierung des Diensteanbieters

Als nächsten Schritt führen der Chip des Ausweises und der Dienstanbieter ein Terminal-Authentisierungs-Protokoll (siehe Seite 14) durch, wobei hier der Diensteanbieter den Part des Terminals übernimmt und das Lesegerät lediglich als Gateway zwischen Chip und Dienstanbieter fungiert. Durch das Challenge-Response-Protokoll, das bei der Terminal-Authentisierung[1] abgewickelt wird, weist der Diensteanbieter durch die Erstellung einer Signatur die Kenntnis seines privaten Schlüssels nach, der zu dem öffentlichen Schlüssel passen muss, der im Berechtigungszertifikat enthalten ist. Der Chip prüft die Signatur, jedoch ist er nicht in der Lage, Sperrlisten abzufragen, um zu prüfen, ob das Berechtigungszertifikat noch gültig ist. Deshalb haben derartige Zertifikate nur eine sehr kurze Gültigkeit von max. 3 Tagen.

Chip-Authentisierung

Wird der Diensteanbieter vom Chip als authentisch erkannt, führen Chip und Diensteanbieter eine Chip-Authentisierung durch (siehe Seite 13). Basierend auf den dabei ausgetauschten DH-Werten berechnen der Chip und der Diensteanbieter ein gemeinsames MAC-Geheimnis sowie einen gemeinsamen, geheimen Sitzungsschlüssel K. Der Diensteanbieter kann anhand des vom Personalausweisaussteller signierten, im Chip abgelegten, öffentlichen Schlüssels des Chips dessen Authentizität prüfen.
Der Chip verschlüsselt die zu übertragenen Daten mit diesem Sitzungsschlüssel K und überträgt sie zum Diensteanbieter. Die Leserechte an den Chip-Daten sind durch das Konzept implizit an diesen Schlüssel gebunden, da die Daten mit diesem Schlüssel verschlüsselt und zum Service übermittelt werden. Der angeschlossene Rechner des Ausweisbesitzers fungiert hierbei nach jetzigem Kenntnisstand nur als Gateway. Die verwendeten Schlüssel sollten dem Browser des Nutzers entsprechend nicht bekannt sein.

Anders als beim ePass erfolgt die Integritätsprüfung der Daten des Chips bei der eID Anwendung nicht unter Rückgriff auf die signierten Hashwerte im Document Security Object, sondern implizit über die Chip-Authentisierung[2].

---

[1] Der Autorin ist unklar, auf welche Weise die Chip-ID an den Diensteanbieter übermittelt wird; im ursprünglichen Protokoll liest das Lesegerät diese ID aus der MRZ des Ausweises, dies ist im Online-Szenario so nicht möglich.

[2] Bem.: Dies entspricht nicht den Empfehlungen der Spezifikationsdokumente zum ePass, die empfehlen, nach einer Chip-Authentisierung noch zusätzlich eine explizite Echtheits-

Schlüssel- und Zertifikatsmanagement
Die für die Nutzung der eID-Funktion notwendige PKI ist analog zu der PKI des elektronischen Reisepasses geplant. Das BSI ist wiederum die Wurzelinstanz, die ein Zertifikat für den Personalausweishersteller ausgibt und dieses mit dem Root-Schlüssel signiert. Der Ausweishersteller seinerseits signiert für jeden Personalausweis das Ausweis-individuelle, statische Diffie-Hellman Schlüsselpaar, das bei der Herstellung des ePA im Chip abgelegt wird.
Das BSI ist zudem die Wurzelinstanz für auszustellende Berechtigungszertifikate. Das Root-Zertifikat wird im Chip des ePA abgelegt. Die Wurzelinstanz autorisiert weitere staatliche Stellen zur Ausstellung von Berechtigungszertifikaten für Dienstanbieter. Ein Berechtigungszertifikat signiert ein variables DH-Schlüsselpaar des Diensteanbieters.

Bei der Online-Authentisierung wird während der Terminal-Authentisierung das Berechtigungszertifikat dem Chip vorgelegt. Dieser prüft die Echtheit des Zertifikats unter Nutzung des auf dem Chip abgelegten öffentlichen Schlüssels der Root-Instanz als Vertrauensanker für den Zertifikatsvalidierungspfad.

1.2.4 Anwendungsszenarien

Der ePA kann überall dort zum Einsatz kommen, wo heute die Vorlage eines gültigen Personalausweises, also das persönliche Erscheinen, benötigt wird, wie zum Beispiel bei Antragsprozessen, oder der Einsichtnahme in laufende Verfahren, in Daten beim Finanzamt, Rentenstatus etc. Zurzeit werden unterschiedliche Einsatzszenarien für die Authentisierungsfunktion des ePA diskutiert. Hierzu gehören Anwendungen im Bereich des eCommerce ebenso wie im Bereich des Jugendschutzes (z.B. Altersabfrage bei der Ausleihe von Videofilmen) oder dem eGovernment. Neben authentisierten Downloads (z. B. die elektronische Ausleihe von Büchern) ist auch ein authentischer Upload möglich, z.B. in der Erwachsenenbildung. Das vom BMI veröffentlichte Grobkonzept zum elektronischen Personalausweis führt einige Beispiele aus den Bereichen eBusiness, eGovernment, zur Automatisierung von Geschäftsprozessen und zum Einsatz der qualifizierten Signatur auf.

Online Banking

Im Bereich des eBusiness wird eine besondere Akzeptanz der eID-

prüfung der Chip-Daten durchzuführen.

Funktion durch Bürger beim Online Banking erwartet. Durch die bei der eID integrierte Authentisierung des Diensteanbieters mittels der Terminal-Authentisierung könnte die Abwehr von Phishing-Angriffen verbessert werden, da die Bank sich mit einem Berechtigungszertifikat ausweisen muss. Für den Nutzer ergibt sich zudem eine höhere Sicherheit, da zur Autorisierung von Banktransaktionen nicht nur die Kenntnis von PIN und TAN erforderlich ist, sondern auch noch die Benutzer-PIN, die zur Durchführung der eID Funktion erforderlich ist. Als konkreten neuen Anwendungsfall, der durch die eID möglich wird, nennt das Dokument die Konto-Eröffnung via Online-Banking. Herkömmlicherweise ist hierzu das persönliche Erscheinen in der Bankfiliale, das Vorzeigen des Personalausweises zur Identifizierung und das Ausfüllen eines Antrags erforderlich. Unter Nutzung des ePA authentifiziert sich der Benutzer gegenüber der Bank, nachdem deren Berechtigungszertifikat geprüft wurde. Die Bank soll durch Validierung des signierten öffentlichen Chip-Schlüssels und über die Chip-Authentisierung die Echtheit des Chips auf dem Personalausweis und darüber auch die Echtheit der Ausweisdaten prüfen können. Über die Eingabe der Benutzer-PIN wird die Zugehörigkeit der agierenden Person zum Ausweis bestätigt. Zur Konto-Eröffnung könnten die erforderlichen Daten direkt aus dem ePA entnommen werden.

Online-Versand

Beim Online-Versand- und Auktionshandel wird häufig die Identität des privaten Käufers oder Verkäufers nur durch die Zustellung der Zugangsdaten via ungeschützter E-Mails oder ungeschützter Web-Formulare übermittelt. Eine Aussage über die Seriosität des Händlers steht dem Kunden in der Regel nicht zur Verfügung. Laut BMI bietet der ePA mit seiner eID-Funktion den Vorteil, dass durch die Vorlage eines von staatlicher Stelle ausgestellten Berechtigungszertifikats des Händlers ein höheres Vertrauen in die Seriösität des Händlers etabliert, der Verbraucherschutz im Online-Handel gestärkt und durch die digitale Identität der Käufer ein Identitätsbetrug bei Auktionen und bei Bestellungen erheblich erschwert werden kann.

Jugendschutz

Der Zugang zu altersbeschränkten Internetangeboten, aber auch der Zugang zu alterbeschränkten Waren und Dienstleistungen, wie z.B. Genussmitteln an Automaten, wird häufig nur unzureichend, z.B. nur durch eine Alterserklärung, geschützt und ist leicht zu umgehen. Um Jugendschutzauflagen des Gesetzgebers einzuhalten, kann sich ein Diensteanbieter durch die Verwendung entsprechender Berechtigungszertifikate durch den ePA bestätigen lassen, dass der

Ausweisbesitzer eine bestimmte Altersgrenze erreicht hat.

Online-Anmeldungen

Im Zusammenhang mit eGovernment-Anwendungen sind sicherlich Online-An- und Ummeldungen, die bei der Nutzung der eID Funktion kein persönliches Erscheinen mehr erforderlich machen, interessant. So finden jährlich in Deutschland rund 40 Millionen Meldevorgänge im Kfz-Wesen statt, wofür bisher idR das persönliche Erscheinen bei der Kfz-Zulassungsbehörde der zuständigen Kommune bzw. des Landkreises für die An- oder Abmeldung, Stilllegung etc. erforderlich ist. Gemäß BMI soll für die An- bzw. Ummeldung oder die Fortschreibung der Meldedaten nach der elektronischen Identifizierung ein bereits weitgehend vorausgefülltes Meldeformular zur Verfügung gestellt und von den Meldepflichtigen online ausgefüllt, ggf. elektronisch signiert und über eine gesicherte Verbindung an das Melderegister übermittelt werden. Im Zusammenhang mit KfZ-Meldungen ist geplant, den ePA für den elektronischen Identitätsnachweis gegenüber einem Fachverfahren einzusetzen, das Kfz-Zulassungsbehörden und Versicherungen integriert.

Elena

Laut BMI stellen rund 3 Millionen Arbeitgeber in Deutschland jedes Jahr etwa 60 Millionen Bescheinigungen, Einkommensnachweise und Auskünfte für ihre Angestellten in Papierform aus. Die Bundesregierung plant, diese Bescheinigungen automatisiert elektronisch in einer zentralen Speicherstelle zu erfassen. Unter Nutzung des ePA zusammen mit einer qualifizierten Signatur plant das BMI die Abläufe zu vereinfachen und zu beschleunigen. Dazu sollen die zum Datenabruf berechtigen Mitarbeiter der Arbeitsagenturen oder Kommunalbehörden den Datenabruf mit ihrer qualifizierten Signatur unterschreiben. Durch das ELENA-Verfahren soll auf die Ausstellung von papiergebundenen Einkommensnachweisen verzichtet werden.

Zugangskontrolle

Der ePA soll laut BMI auch in anderen Szenarien, als im Online-Umfeld, zum Einsatz kommen können. Zu denken ist hierbei zum Beispiel an die Zugangs- und Zutrittskontrolle von Gebäuden, Werkstätten, Labors etc. Mit dem ePA könnten manuelle Zugangskontrollen automatisiert werden.

Konkrete Einsatzszenarien für den ePA werden ab Sommer 2008 an der TU Darmstadt in einem gemeinsamen Pilotprojekt der TU Darmstadt und des Fraunhofer Instituts für Sichere Informationstechnologie entwickelt und erprobt.

1.2.5 Sicherheit des ePA

Da bislang lediglich das Grobkonzept sowie einige eher allgemein gehaltene Veröffentlichungen über den ePA frei verfügbar sind, kann an dieser Stelle keine detaillierte Sicherheitsanalyse erfolgen. Nachfolgend werden einige technische Punkte diskutiert und es wird auch auf den Bereich des Datenschutzes eingegangen, da hierzu bereits ein rechtswissenschaftliches Gutachten von Kollegen Rossnagel aus Kassel vorliegt.

Sicherheitsanforderungen
Das BMI hat ein Sicherheitsrahmenkonzept definiert, das die Anforderungen an ein Sicherheitskonzept für den ePA über dessen gesamten Lebenszyklus abdeckt, also von der Beantragung bis zur Vernichtung. Das Rahmenkonzept soll sowohl Vorgaben für die Ausweishersteller als auch Empfehlungen für die Personalausweisbehörden enthalten. Wesentliche Anforderungen sind (teilweise aus dem Grobkonzept zitiert):

1. Es muss ausgeschlossen werden, dass der ePA physisch so manipuliert wird, dass eine andere Person die Identität des Ausweisinhabers annehmen kann. Darüber hinaus muss auch eine Manipulation des Chips ausgeschlossen werden, damit eine andere Person nicht auf elektronischem Weg die Identität des Inhabers annehmen kann.
2. Jede Form von gefälschten oder manipulierten elektronischen Personalausweisen bzw. Teilen davon müssen erkannt werden können.
3. Das Abhören der Kommunikation zwischen Diensteanbieter und ePA muss ausgeschlossen werden können. Die Verschlüsselung muss auf geeignete kryptographische Verfahren zurückgreifen, die ausreichende Schlüssellängen aufweisen.
4. Lesegeräte für den PA müssen so sicher sein, dass ein Eingriff durch Dritte in den Kommunikationsprozess mit dem ePA ausgeschlossen werden kann.
5. Der Zugriff auf die personenbezogenen Daten im elektronischen Personalausweis darf nur mit Einwilligung des Benutzers oder über hoheitliche Berechtigungszertifikate möglich sein.

Erfüllung der Anforderungen
Nachfolgend wird diskutiert, welche Maßnahmen in dem bestehenden Sicherheitskonzept nach Ansicht der Autorin beitragen können, die oben gestellten Anforderungen zu erfüllen. Dabei werden auch einige, nach Ansicht der Autorin noch offene Punkte diskutiert.

1. Kopierschutzmaßnahmen, Anti-Kloning und Abwehrmaßnahmen gegen Identitätsdiebstahl:
   Es wird gefordert, dass auch der ePA mit optischen Sicherheitsmerkmalen wie Sicherheitsdruck oder Laserbeschriftung ausgestattet wird, die mindestens die im bisherigen Personalausweis realisierten Sicherheitsfunktionen umfassen. Damit soll erreicht werden, dass der ePA mindestens ebenso schwer zu kopieren ist, wie der herkömmliche PA.
   Durch den Einsatz der Chip-Authentisierung kann erkannt werden, ob ein Chip geklont wurde. Der öffentliche DH-Schlüssel des Chips wird signiert im Chip abgelegt, so dass dessen Modifikation erkannt werden kann. Da bei der Online-Authentisierung das Security-Object zur Integritätsprüfung nicht zur Verfügung steht, ist eine explizite Integritätsprüfung der Daten im Chip jedoch nicht möglich.
   Zur Abwehr von Identitätsdiebstählen insbesondere beim Online-Authentisieren dient die 2-Faktor-Authentisierung, die die Kenntnis der Benutzer-PIN erfordert. Über den Fehlbedienzähler wird verhindert, dass eine PIN durch Brute-Force Angriffe geraten wird. Nicht verhindert werden können Denial-of-Service Angriffe, bei denen ein Angreifer die kontaktlose Schnittstelle des Chips nutzt, um als Lesegerät einen Verbindungsaufbau zu provozieren. Durch die mehrmalige Eingabe falscher PINs kann er dafür sorgen, dass die Karte gesperrt wird. Das Konzept des verzögerten Blockierens hilft nicht gegen eine unbemerkte DoS-Attacke.
   Eine weitere Abwehrmaßnahme gegen Identitätsdiebstahl stellen die Sperrlisten dar. Sie sollen für Diensteanbieter Informationen über verlorene oder abhanden gekommene Ausweise verfügbar machen. Ob ein Diensteanbieter sich dieser Listen bedienen wird, bleibt abzuwarten.
2. Abwehrmaßnahmen gegen Chip-Manipulationen:
   Die Anti-Kloning-Maßnahme der Chip-Authentisierung wehrt keine Manipulationsversuche ab. Die Spezifikation des BMI legt

fest, dass nur Personalausweisbehörden die Daten auf dem Chip überschreiben dürfen, wofür sie ein spezielles Berechtigungszertifikat vorweisen müssen. Inwieweit diese Kontrolle unumgehbar ist, wird man erst durch intensive Sicherheitsanalysen feststellen können.

3. Vertrauliche Kommunikation:
   Durch die Abwicklung des Terminal-Authentisierungs- und Chip-Authentisierungsprotokolls werden geheime Sitzungsschlüssel zwischen dem Dienstanbieter und dem Chip etabliert. Zur Verschlüsselung soll das kryptographisch starke Verfahren AES verwendet werden und die Schlüssellänge soll mindestens 128 Bit betragen, was beim heutigen Stand der Technik eine ausreichende Länge ist.
   Sollen der Rechner des Nutzers und der Diensteanbieter nach der erfolgreichen Online-Authentisierung sicher weitere Daten, die nicht die ePA Daten sind, austauschen, so muss ein sicherer Kanal hierfür zwischen Browser und Diensteanbieter so etabliert werden, dass beide Seiten von der Authentizität überzeugt sind. Der Aufbau einer SSL/TLS Verbindung ist hierfür naheliegend; erfordert jedoch eine erneute Authentisierung und Aushandlung von Sitzungsschlüsseln. Ein Zusammenspiel mit der Online-Authentisierung ist in dem Grobkonzept nicht beschrieben.
4. Die für die Online-Authentisierung zu verwendenden Kartenlesegeräte für kontaktlose Chipkarten sollen durch das BSI zertifiziert werden. Dem Grobkonzept des BMI ist jedoch nicht zu entnehmen, welchen Anforderungen die Lesegeräte für eine erfolgreiche Zertifizierung genügen müssen.
5. Unberechtiger Datenzugriff
   Alle Stellen, die Zugriff auf die Daten im Ausweis erhalten möchten, benötigen ein Berechtigungszertifikat. Hoheitliche Stellen, die zur Durchführung einer Personenkontrolle auch auf biometrische Daten zugreifen müssen, benötigen ein Berechtigungszertifikat, das diesen Zugriff gestattet. Zudem müssen sie beim Zugriff den Nachweis der Kenntnis der auf dem Ausweis aufgedruckten KartenPIN nachweisen. Öffentliche Stellen und Nicht-Öffentliche Stellen benötigen ein Berechtigungszertifikat für den elektronischen Identitätsnachweis, der nicht die biometrischen Daten umfasst. Ein Zugriff soll dann nur auf die Daten möglich

sein, die der Benutzer explizit autorisiert und per PIN bestätigt. Hierfür ist wesentlich, dass zum einen die Anzeige-Funktion zum Setzen der Zugriffsrechte korrekt arbeitet und die Daten korrekt an den Chip übermittelt werden. Wie dies gewährleistet werden soll, ist aus dem Grobkonzept nicht zu entnehmen.
Weiterhin ist wesentlich, dass der Chip selber die Zugriffe korrekt gemäß der festgelegten Berechtigungen durchführt. Eine Common Criteria Zertifizierung des im ePA enthaltenen RFID-Chips analog zum ePass-Chip ist unabdingbar.

Auch wenn das vorliegende Sicherheitsgrobkonzept noch einige offene Punkte enthält, scheint es doch gut zu sein. Eine genauere Sicherheitsanalyse kann aber natürlich erst erfolgen, wenn alle Details offen gelegt sind. Wichtig ist natürlich auch, dass vor der Einführung des elektronischen Personalausweises umfangreiche Tests mit Personalausweisbehörden, Behörden (eGovernment) und Unternehmen (eBusiness) sowie Nutzern durchgeführt werden. Laut des vorliegenden Grobkonzeptes sind Technologieerprobungen im Rahmen von Pilotierungsprojekten, sowie Feldtests vorgesehen. Im Rahmen der Pilotierungen sollen die geplanten Chipkarten, Lesegeräte, Software, eCard-API, eGovernment- und eBusiness-Dienste sowie deren Kompatibilität untereinander getestet werden.

Abschließend gehen wir noch auf die Datenschutzaspekte ein, wobei hier die rechtlichen Anforderungen im Vordergrund stehen.

Datenschutz

Opt out

In [9] findet sich eine Zusammenfassung eines Gutachtens zu Datenschutzaspekten der Authentisierungsfunktion des ePA. Zur Nutzung der Authentisierungsfunktion des ePA wird die Nutzer-PIN benötigt, die der Nutzer per PIN-Brief erhält. Der Nutzer hat die freie Wahl, die Authentisierungsfunktion zu nutzen. Entscheidet er sich dagegen, so kann er beim Abholen des Passes den verschlossenen PIN-Brief der Behörde übergeben. Obwohl dies ein Opt-out-Konzept ist, haben die Autoren in [9] keine datenschutzrechtlichen Bedenken, da der Staat verpflichtet ist, seine Bürger umfassend über die Möglichkeiten des Nicht-Nutzens der Funktion zu informieren.

Unterrichtung

Gemäß §4 Abs. I BDSG darf ein Dienstleister oder eine Behörde nur dann Authentisierungsdaten erheben, wenn der Betroffene unterrichtet wird, wer der Empfänger ist und welchen Verwendungszweck er

mit den Daten verbindet. Die entsprechenden Informationen sind in geeigneter Weise optisch darzustellen. Bei ePA sollen die erforderlichen Informationen im Zugriffszertifikat des Dienstleisters enthalten sein. Dieses Zertifikat soll durch eine staatliche bzw. staatlich kontrollierte Stelle ausgestellt werden.

Plausibilität

Erforderlich ist, dass der Zertifikatsaussteller in einer Vorprüfung die Angaben des zu zertifizierenden Dienstleisters prüft. Zur Zeit wird lediglich über eine Plausibilitätsprüfung nachgedacht; eine echte Erforderlichkeitsprüfung erscheint zu aufwändig. Obwohl eine Plausibilitätsprüfung relativ schwach ist, sind die datenschutzrechtlichen Bedenken eher gering, da es in der Regel um die Frage gehen wird, ob der Dienstleister für seinen Dienst die eindeutige Identifizierung des Ausweisinhabers erfordert oder lediglich einige, anonymisierende Attribute. Im Gegenzug eröffnet die Vorlage eines Zugriffszertifikats dem Ausweisinhaber die Möglichkeit, die Identität des Dienstleisters zu prüfen, und kann als Grundlage für Rechtsverfolgung und -durchsetzung dienen.

Literaturverzeichnis

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

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

[3] BSI. Technische Richtlinie TR03110, Advanced Security Mechanisms for Machine Readable Travel Documents, Extended Access Control (EAQ, Version 2.0). Report, BSI, 2007.

[4] BSI. Messung der Abstrahleigenschaften von RFID-Systemen (MARS). Report, BSI, zur Veröffentlichung anstehend 2007.

[5] ICAO. Doc 9303, Machine Readable Travel Documents, Part 1 - Machine Readable Passport - Volume 1 Passports with Machine Readable Data Stored in Optical Character Recognition Format. Report, International Civil Aviation Organization, 2006.

[6] ICAO. Doc 9303, Machine Readable Travel Documents, Part 1 - Machine Readable Passport - Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capabilities. Report, International Civil Aviation Organization, 2006.

[7] ISO/IEC14443. Identification cards: Contactless integrated circuit cards, Proximity cards. Report, ISO.

[8] Ari Juels, David Molnar, and David Wagner. Security and Privacy Issues in E-passports. Report 2005/095, Cryptology ePrint Archive, March 2005.

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