Institut für Informatik der Freien Universität Berlin

Der neue Personalausweis

– Seminar Chipkartentechnologien –

Simon Hohberg, B.Sc

Matrikelnummer: 4284530

Betreuer: Dipl.-Inf. Kristian Beilke

Berlin, 16. Mai 2014

Zusammenfassung

Der neue Personalausweis ist eines der großen Projekte der Bundesregierung im Bereich der Informationssicherheit. Neben der klassischen Verwendung des neuen Personalausweises als Ausweis- und Reisedokument, sollte eine sichere und vertrauenswürdige zentrale Quelle von personenbezogenen Daten im Bereich eGovernment und eBusiness geschaffen werden. Bei der Entwicklung wurde großen Wert auf Datenschutz und Sicherheit gelegt, was durch die Verwendung der Protokolle PACE, Chip Authentication und Terminal Authentication sichergestellt wird. Dennoch gab es einige Meldungen in den Medien, die behaupteten, dass der neue Personalausweis unischer sei. Dies wird der tatsächlichen Sicherheit des neuen Personalausweises jedoch nicht gerecht. Zweifel sind allerdings angebracht, ob der neue Personalausweis tatsächlich jemals eine starke Verbreitung im eBusiness-Bereich finden wird.

Inhaltsverzeichnis

1 Einführung

Diese Seminararbeit gibt einen Überblck über die Entwicklung des neuen Personalausweis. Es wird aufgezeigt warum und mit welchem Ziel der neue Personalausweis entwickelt wurde, welche Protokolle und kryptographischen Mechanismen zur Absicherung der Daten verwendet werden und wie diese funktionieren. Neben dem neuen Personalausweis wird auch auf den elektronischen Personalausweis eingegangen, da die Entwicklung beider Ausweisdokumente stark mit einander verknüpft ist.

In Deutschland besitzt jeder Bürger, der älter als 16 Jahre alt ist einen Personalausweis oder Reisepass. Dies ist durch das Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PerAuswG) geregelt: „Deutsche [...] sind verpflichtet, einen Ausweis zu besitzen, sobald sie 16 Jahre alt sind [...].“. Dabei dient der Personalausweis innländisch zur Identifikation des Bürgers durch die staatlichen Behörden. Dem gegenüber steht der Reisepass, welcher als Reisedokument international zur Identifikation verwendet wird. Obwohl der Personalausweis ursprünglich ein nationales Dokument ist, wird er mitlerweile auch außerhalb Deutschlands in einigen Ländern akzeptiert, was ihn neben dem Reisepass zu einem, wenn auch in begrenztem Maße, weiteren Reisedokument macht. Hinsichtlich der Fälschungssicherheit bedeutet dies, dass der Personalausweis dem Reisepass in Bezug auf die Sicherheitsmerkmale in nichts nachstehen darf, da sonst die Sicherheit im Reiseverkehr durch den Personalausweis beeinträchtigt werden würde.

1.1 Motivation

Die Geschichte des Personalausweises lässt beobachten, dass zur Erhöhung der Fälschungssicherheit nach und nach immer mehr personenbezogene Merkmale auf diesen aufgebracht wurden und technische Maßnahmen getroffen wurden, die das Fälschen erschweren.[1] Durch Einbeziehung einer größeren Anzahl von Merkmalen wird das Ausweisdokument stärker an seinen rechtmäßigen Besitzer gebunden, so dass es erschwert wird, dass eine andere Person das selbe Dokument missbräuchlich verwenden kann.

Die Biometrie hat in den letzten Jahren große Fortschritte gemacht, so dass es nur eine Frage der Zeit war bis auch in Ausweisdokumenten biometrische Merkmale integriert würden. Der Anlass zur Einführung biometrischer Merkmale in Reisedokumente zur weiteren Erhöhung der Fälschungssicherheit war durch die terroristischen Anschläge vom 11. September 2001 gegeben bei dem gefälschte Reisedokumente verwendet wurden.[9] So wurde durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 Änderungen am PerAuswG vorgenommen, die es erlauben biometrische Daten im Personalausweis zu verwenden. Schließlich wurde am 29. Dezember 2004 durch den europäischen Rat die EG-Verordnung 2252/2004 erlassen, die vorsieht EU weit Pässe und Reisedokumente mit biometrischen Daten (Gesichtsbild und Fingerabdrücke) auszustatten. Dieser Richtlinie folgend wurde am 1. November 2005 in Deutschland ein neuer Reisepass – der so genannte ePass – mit integriertem Chip eingeführt, der zunächst nur ein digitales Foto beinhaltete und ab 2007 zusätzlich Fingerabdrücke speicherte. Obwohl in der Verordnung Personalausweise explizit ausgenommen sind [8], entschied man sich biometrische Daten auch in den Personalausweis zu integrieren und damit den so genannten neuen

Personalausweis (nPa) zu entwickeln und schließlich am 1. November 2010 einzuführen. Diese Entscheidung folgt der Tatsache, dass der Personalausweis teilweise als Passersatz dient und damit das gleiche Sicherheitsniveau wie ein solcher erfüllen muss (vergl. [7]).

Grundsätzlich gelten Personalausweis und Reisepass als fälschungssicher[7] und werden daher als besonders vertrauenswürdig betrachtet. Neben der Nutzung durch den Staat, spielen die Ausweisdokumente ebenso eine wichtige Rolle im geschäftlichen Bereich, z.B. zum Abschluss von Verträgen, Abholen von Paketen etc. Durch die Verlagerung vieler Geschäftsbereiche in das Internet (eBusiness) spielt der Nachweis der Identität im Internet eine immer stärkere Rolle. Um die Identität eines Kunden über das Internet zu verifizieren sind umständliche Verfahren nötig, die meistens auf den Briefverkehr zurückfallen. Hinzu kommt, dass ein Internetnutzer nicht nur eine, sondern vielmehr eine Vielzahl an Identitäten besitzt, da Dienstanbieter bei der Datenerhebung nicht kooperieren und somit jeder eigene Daten mit unterschiedlichen Verfahren erhebt. Daher scheint die Idee einer staatlich garantierten elektronischen Identität, die durch jeden Dienstanbieter genutzt werden kann und ein hohes Maß an Sicherheit bietet, durchaus attraktiv. Die Entwicklung des nPa bot die Gelegenheit diese vielversprechende Funktionalität umzusetzen.

2 Überblick über den neuen Personalausweis

2.1 Äußere Eigenschaften

Auffälligste Änderung beim nPa ist das Format, welches vom ID-2 auf das Scheckkartenformat ID-1 geändert wurde und ihn dadurch in der Größe Kreditkarten und dem Führerschein angleicht. In Bezug auf die aufgedruckten Daten ändert sich kaum etwas, wie in Abbildung 1 zu sehen ist. Neu ist die Wiedereinführung des Ordens- oder Künstlernamens auf der Rückseite, sowie, dass die maschinenlesbare Zone (Machine Readable Zone, MRZ) nicht mehr auf der Vorder- sondern der Rückseite zu finden ist.

Die maschinenlesbare Zone ist eine Sequenz von Zeichen, die die wichtigsten Daten und zusätzliche Prüfziffern in einer Weise kodiert, so dass diese leicht automatisiert optisch erfasst werden können. Der genaue Inhalt und Aufbau wird durch die Internationl Civil Aviation Organization (ICAO) spezifiziert.

Außerdem ist auf der Vorderseite nun eine Card Access Number (CAN) abgebildet. Dies ist eine Zufallszahl, die für die Absicherung des Zugangs zu den Daten auf dem integrieten Chip eine wichtige Rolle spielt.

2.2 Integrierter Chip

Die eigentliche Neuerung beim nPa ist der integrierte Chip. Dieser ermöglicht das kontaktlose Auslesen von auf dem Chip gespeicherten Daten. Die Daten, die so elektronisch ausgelesen werden können, entsprechen den auf den Chip gedruckten Daten mit Ausnahme von Augenfarbe, ausstellende Behörde, Ausstellungsdatum, Ausweisnummer, CAN, Körpergröße und Unterschrift. Zusätzlich lassen sich von hoheitlichen Stellen die biome-

Vorderseite

1	Familienname, Vorname	5	Staatsangehörigkeit
2	Seriennummer	6	letzter Tag der Gültigkeitsdauer
3	Chip	7	Tag und Ort der Geburt
4	Zugangsnummer (CAN)	8	Lichtbild

Rückseite

9	Anschrift
10	Logo
11	Ordens- bzw. Künstlername
12	Maschinenlesbare Zone (enthält keine zusätzlichen Angaben zur Person)

Abbildung 1: Aufgedruckte Daten [5]

trischen Daten auslesen, welche eine digitale Version des Bildes und – wenn vorhanden – Fingerabdrücke beinhalten. Bei der Beantragung kann der Bürger entscheiden, ob er Fingerabdrücke für den nPa abgeben möchte oder nicht.

Der integrierte kontaktlose Chip ist ISO/IEC 14443 konform und wird per Induktion vom Lesegerät mit Strom versorgt. Die internationale Normenreihe ISO/IEC 14443 beschreibt die physikalischen Eigenschaften und die Kommunikation auf der Bitübertragungsschicht des Chips. Die darüberliegende Kommunikation verläuft nach ISO/IEC 7816 Teil 4. Diese legt unter anderem fest, dass bei der Kommunikation Application Data Units (APDUs) als Kommando-Antwort-Paare ausgetauscht werden. Desweiteren wird die verschlüsselte Kommunikation (Secure Messaging), sowie die Struktur von Anwendungen und Daten, Dateiorganisation und Zugriffsrechte spezifiziert. Wiederum eine Abstraktionsschicht darüber folgt der nPa der ISO 24737 Teil 3 zur Bereitstellung von Schnittstellen für externe Applikationen (Service Access Layer).

Der nPa bietet drei verschiedene Anwendungen, die teilweise ausschließlich hoheitlichen Stellen zur Verfügung stehen und teilweise auch durch nicht hoheitliche Stellen verwendet werden können.

Zunächst ist hier die ePass-Anwendung zu nennen, welche der ausschlaggebende Grund für die Einführung des nPa war (siehe Kapitel 1.1). Diese Anwendung entspricht der Funktionalität im ePass zum Auslesen der biometrischen Daten und kann ausschließlich von hoheitlichen Stellen verwendet werden.

Neben der ePass-Anwendung gibt es die eID-Anwendung (oder auch Online-Ausweisfunktion

genannt). Diese erfüllt den Zweck den nPa zu einem universellen Identitätsanbieter im Internet zu machen und kann auch durch nicht-hoheitliche Stellen genutzt werden. Das heißt, jeder Internet-Dienstanbieter kann unter gewissen Voraussetzungen und unter Einhaltung gewisser Rahmenbedingungen Nutzer dieser Funktion werden und Daten mit der Zustimmung des Ausweisinhabers über das Internet vom nPa auslesen.

Als dritte Anwendung bietet der nPa die Möglichkeit qualifizierte elektronische Signaturen zu erstellen. Diese Funktion kann genau wie die eID-Anwendung durch nicht-hoheitliche Stellen verwendet werden und erlaubt es über das Internet Verträge durch Signatur abzuschließen, wobei die elektronische Signatur nach §126a BGB rechtlich einer Unterschrift des Ausweisinhabers gleichkommt, sofern das nicht vom jeweils zutreffenden Gesetz ausgeschlossen ist. Standardmäßig kann diese Funktion jedoch nicht genutzt werden, da zunächst ein Zertifikat zur Erstellung einer solchen Signatur erworben und auf den nPa geladen werden muss wodurch weitere Kosten entstehen.

2.3 Lesegeräte

Zur Kommunikation mit dem nPa wird ein Lesegerät für kontaktlose Chipkarten benötigt. Dabei werden drei Klassen im Kontext des nPa unterschieden: Basis-, Standard- und Komfortkartenleser. Während der Basiskartenleser ein reines Lesegerät ist, besitzen Standard- und Komfortkartenleser ein PIN-Pad. Bei der Verwendung eines Basiskartenleser wird die für PACE (siehe Kapitel 4.3) benötigte PIN am PC über die Tastatur eingegeben. Bei Standard- und Komfortkartenlesern wird dies über das PIN-Pad vorgenommen. Ein Komfortkartenleser bietet außerdem ein Display und die Möglichkeit qualifizierte elektronische Signaturen mit dem nPa zu erstellen.

3 Protokolle der ICAO für Reisedokumente

Die International Civil Aviation Organization (ICAO), eine Organisation der Vereinten Nationen, hat unter Anderem die Aufgabe Standards für maschinenlesbare Dokumente zu entwickeln und festzulegen welche Mechanismen und Protokolle zum Schutz der Daten unterstützt werden müssen. Die drei wichtigsten Mechanismen sind passive Authentisierung, aktive Authentisierung und Access Control. Die ICAO schreibt lediglich die Verwendung von passiver Authentisierung als verfplichtend vor, alle anderen Mechanismen sind im internationalen Kontext optional (vergl. [2]).

3.1 Access Control

Access Control beschreibt eine Gruppe von Protokollen zur Zugriffskontrolle. Es soll verhindert werden auf den Chip zuzugreifen ohne direkten Zugriff zu dem Dokument zu haben in dem dieser integriert ist – so genanntes Skimming.

3.1.1 Basic Access Control

Um Zugriff auf die Daten im Chip zu erhalten, muss das Terminal bei der Basic Access Control nachweisen, dass es einen aus der MRZ abgeleiteten symmetrischen Schlüssel kennt.

Das Basic Access Control Protokol ist insofern problematisch, da die Anzahl der möglichen Schlüssel, die von den Daten der MRZ abgeleitet werden können, nicht groß genug ist, um aktuellen Sicherheitsstandards zu genügen.[13] Zur Ableitung der Schlüssel werden die Dokumentnummer, das Geburtsdatum und das Ablaufdatum des Dokuments verwendet, was in etwa zu einer Schlüsselstärke von 56 Bit bzw. 73 Bit führt, je nachdem ob die Dokumentnummer nur aus Zahlen oder auch aus Buchstaben besteht.[12] Die Schlüsselstärke wird teilweise außerdem zusätzlich dadurch reduziert, dass die Dokumentnummern nicht wirklich zufällig sind oder die Dokumentnummer mit dem Ablaufdatum korreliert. Das BSI empfiehlt hingegen mindestens eine Schlüsselstärke von 100 Bit für eine ideale Blockchiffre.[4] Für AES bedeutet dies eine Mindestschlüssellänge von 128 Bit.

3.2 Passive Authentisierung

Die passive Authentisierung dient der Überprüfung der Integrität der Daten. Dazu enhält der Chip signierte Hashwerte aller auf dem Chip gespeicherten Daten, sowie den zur Überprüfung nötigen öffentlichen Schlüssel, der wiederum von einer vertrauenswürdigen Stelle signiert worden ist. Dadurch ist es möglich festzustellen, ob die gespeicherten Daten vertrauenswürdig sind und nicht im Nachhinein geändert wurden.

3.3 Aktive Authentisierung

Bei der aktiven Authentisierung verfügt der Chip über ein Schlüsselelpaar, das verwendet wird um über ein Challenge-Response-Verfahren sicherzustellen, dass es sich bei dem Chip nicht um einen Klon handelt. Der Chip weist nach, dass er tatsächlich über den privaten Schlüssel passend zu einem öffentlichen Schlüssel, der durch eine vertrauenswürdige Stelle signiert wurde, besitzt. Dazu schickt das Terminal eine belliebige Challenge an den Chip. Dieser erstellt mit dem privaten Schlüssel des hinterlegten Schlüsselpaars die Signatur für die erhaltene Challenge und sendet diese als Antwort zurück an das Terminal. Das Terminal kann nun mit Hilfe des vertrauenswürdigen öffentlichen Schlüssels des Chips diese Signatur überprüfen.

Dieser Mechanismus besitzt jedoch Probleme im Hinblick auf den Datenschutz, da das Terminal eine beliebige Challenge übermitteln kann, ist es möglich z.B. einen Zeitstempel und GPS-Koordinaten als Challenge zu wählen. Mit der signierten Challenge kann nun nachvollzogen werden wann sich der Chip an welchem Ort befunden hat.

4 Kryptographie

Die Kryptographie spielt beim nPa eine sehr wichtige Rolle, da der Anspruch an die Sicherheit insbesondere auch bei der eID-Funktion sehr hoch sind. Für das Verständnis der Protokolle PACE, Chip Authentication und Terminal Authentication ist das Wissen um den Diffie-Hellman-Schlüsselaustausch immanent. Desweiteren ist es nötig zu wissen wie die Zertifikate, die zum Auslesen des nPa benötigt werden, organisiert sind.

4.1 Diffie-Hellman-Schlüsselaustausch

Der Diffie-Hellman(DH)-Schlüsselaustausch wurde von Whitfield Diffie und Martin E. Hellman entwickelt und 1976 veröffentlicht.[19] Das in ihrer Veröffentlichung beschriebene Protokoll ermöglicht es zwei Kommunikationspartnern sich über einen unsicheren Kanal auf ein gemeinsames Geheimnis zu einigen. Dieses Geheimnis kann dann als symmetrischer Schlüssel für eine verschlüsselte Kommunikation verwendet werden.

Beim DH-Schlüsselaustausch wird eine mathematischen Gruppe $\mathbb{Z}_p^*$ verwendet, die durch alle Zahlen koprim (Gleichung 1) zu der ganzen Zahl $p \geq 1$ modulo p gebildet wird. Als Verknüpfung der Gruppenelemente wird die Multiplikation verwendet. Zur Generierung von Schlüsseln einigen sich die Kommunikationspartner neben der verwendeten Gruppe außerdem auf einen Generator für diese Gruppe. Ein Generator (auch primitive Wurzel) einer Gruppe ist eine Zahl g für die Gleichung 2 erfüllt ist. D.h. k ist der diskrete Logarithmus von x zur Basis g modulo p. Die verwendeten Zahlen p und g, also welche Gruppe und welcher Generator verwendet werden, können öffentlich gemacht werden, da deren Kenntnis nicht sicherheitskritisch ist.

$$ggT\,(x,p) = 1 \mod p \tag{1}$$

$$g\,Generator \Leftrightarrow \forall x \in \mathbb{Z}_p^*\, \exists k : g^k \equiv x \mod p \tag{2}$$

Der eigentliche Schlüsselaustausch besteht darin, dass beide Kommunikationspartner jeweils eine geheime Zufallszahl (geheime Schlüssel) a und b wählen und die öffentlichen Schlüssel u (Gleichung 3) bzw. v (Gleichung 4) berechnen. Nun tauschen sie die berechneten Werte u und v aus und können so mit Hilfe ihrer geheimen Schlüssel den geteilten geheimen Schlüssel k wie in Gleichung 5 bzw. Gleichung 6 berechnen.

$$u \equiv g^a \mod p \tag{3}$$

$$v \equiv g^b \mod p \tag{4}$$

$$k \equiv v^a \equiv \left(g^b\right)^a \equiv g^{b \cdot a} \mod p \tag{5}$$

$$k \equiv u^b \equiv (g^a)^b \equiv g^{a \cdot b} \mod p \tag{6}$$

Ein Angreifer, der die Kommunikation abhört, kennt zwar p, g sowie $u \equiv g^a$ und $v \equiv g^b$, um jedoch das gemeinsame Geheimnis k der Belauschten zu berechnen, müsste der Angreifer eine der geheimen Zufallszahlen a oder b berechnen. Dies ist als diskretes

Logarithmus-Problem bekannt. Es wird davon ausgegangen, dass es nicht möglich ist dieses Problem effizient zu lösen.[17]

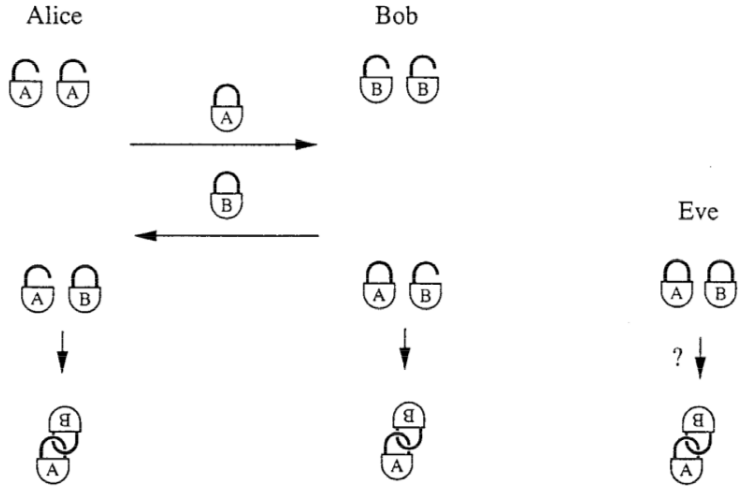

Abbildung 2: Mechanische Analogie des Diffie-Hellman Schlüsselaustauschs [18]

In [18] verdeutlichen die Autoren dieses Problem mit einer mechanischen Analogie. Wie in Abbildung 2 zu sehen, werden die geheimen Zufallszahlen als offene Schlösser und die übertragenen öffentlichen Schlüssel als geschlossene Schlösser dargestellt. Es ist einfach ein offenes Schloss zu schließen – von einem geheimen Schlüssel den öffentlichen Schlüssel zu berechnen – aber sehr schwer ein geschlossenes Schloss zu öffnen – von einem öffentlichen Schlüssel den geheimen Schlüssel zu berechnen. Alice und Bob können daher leicht eine Kombination ihrer Schlösser herstellen. Für Eve ist dies hingegen sehr schwer, da er nur im Besitz der geschlossenen Schlösser (öffentlichen Schlüssel) ist.

Das Berechnen der geheimen Schlüssel ist nach aktuellem Stand zwar kaum möglich, allerdings verhindert der DH-Schlüsselaustausch nicht, dass sich ein Angreifer zwischen die beiden Kommunikationspartner schaltet (Man-in-the-Middle). Der Angreifer fängt die Nachrichten beider Seiten ab, erzeugt sich ein eigenes Schlüsselpaar und ersetzt die übertragenen öffentlichen Schlüssel durch seinen eigenen öffentlichen Schlüssel. Effektiv haben die eigentlichen Kommunikationspartner also einen DH-Schlüsselaustausch mit dem Angreifer gemacht. Dieser kann nun alle Nachrichten mitlesen und auch verändern. Um diesen Angriff zu verhindern werden die Nachrichten mit Hilfe von digitalen Signaturen authentifiziert.

4.2 Public Key Infrastruktur

Zur Kontrolle des Zugriffs auf die Daten im nPa wurde die Extended Access Control (EAC) Public Key Infrastruktur (PKI) aufgebaut. Damit der nPa das Auslesen von Daten zulässt, muss diesem nachgewiesen werden, dass der Auslesende im Besitz eines gültigen Berechtigungszertifikat ist. Ein solches Berechtigungszertifikat wird für einen

bestimmten Verwendungszweck und eine bestimmte Menge von Attributen, die mit diesem Zertifikat ausgelesen werden dürfen, ausgestellt. Beim Auslesen der Daten soll dem Bürger dieses Zertifikat zur Kontrolle angezeigt werden. Da sichergestellt sein muss, dass ein Berechtigungszertifikat vertrauenswürdig ist bzw. nicht von einer beliebigen Person ausgestellt werden kann, werden diese mit einem Zertifikat signiert, das entweder selbst vertrauenswürdig ist oder wiederum von einem Zertifikat signiert wurde usw. Dadurch ergibt sich eine Kette von Zertifikaten, die jedoch schließlich in einem dem nPa bekannten, vertrauenswürdigen Zertifikat münden muss.

Im Allgemeinen besteht diese Kette aus drei Zertifikaten: dem bereits erwähnten Berechtigungszertifikat, dem Document Verifier (DV) Zertifikat und dem Country Verifying Certification Authority (CVCA) Zertifikat.

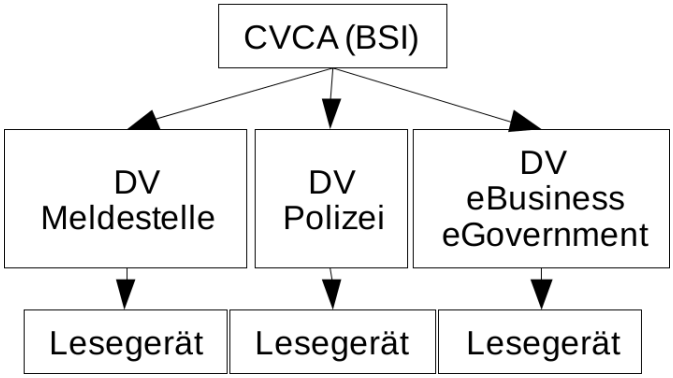

Abbildung 3: Extended Access Control Public Key Infrastruktur [14]

In Abbildung 3 ist die Hierarchie dieser Zertifikate abgebildet. Das CVCA Zertifikat stellt das Wurzelzertifikat dar und ist dem nPa bekannt, da es bei der Herstellung im nPa hinterlegt wird. Ausgehend von diesem Zertifikat werden die DV Zertifikate für bestimmte Bereiche wie Polizei oder online Dienstanbieter ausgestellt und durch die CVCA signiert. Die DV Zertifikate stellen dann wiederum die Berechtigungszertifikate aus und signieren diese.

Berechtigungszertifikate zur Nutzung der Online-Ausweisfunktion werden von der Vergabestelle für Berechtigungszertifikate ausgestellt.

Um die Authentizität des nPa überprüfbar zu machen, werden die von der Chipkarte verwendeten öffentlichen Schlüssel signiert. Für diese Signaturen gibt es wiederum eine eigene PKI, die in Abbildung 4 zu sehen ist. An oberster Stelle steht hier die Country Signing Certification Authority (CSCA), die die Zertifikate der Hersteller signiert. Bei der Herstellung wird dann jeder nPa mit diesem signierten Hersteller-Zertifikat signiert.

4.3 PACE

Password Authenticated Connection Establishment (PACE) ist ein Protokol aus der Familie der Access Control Protokolle (siehe Kapitel 3.1). PACE wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und befindet sich in der

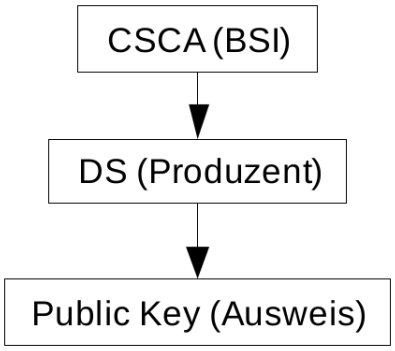

Abbildung 4: Signer Public Key Infrastruktur [14]

Standardisierung als ISO/IEC JTC1/SC17/WG3. Die ICAO sieht vor PACE als Supplemental Access Control zu verwenden um das unsichere Basic Access Control (siehe Kapitel 3.1.1) zu ersetzen.[11]

Das Ziel von PACE ist die Authorisierung des Zugriffs eines Terminals (Proximity Coupling Device (PCD)) auf die kontaklose Chipkarte (Proximity Integrated Circuit Card (PICC)) mit Hilfe eines Passworts. Der Begriff Terminal ist hier nicht ausschließlich als Lesegerät zu verstehen, sondern vielmehr als eine Software, die die verschiedenen Protokolle durchführt, um den Zugriff auf die Daten der Chipkarte zu ermöglichen. Abgeleitet von dem schwachen Passwort soll außerdem eine verschlüsselte Verbindung mit starken Schlüsseln aufgebaut werden, so dass nach der Durchführung von PACE ein sicherer Kanal zwischen Chipkarte und Terminal aufgebaut ist. Um dies zu erreichen wird ein DH-Schlüsselaustausch durchgeführt (siehe Kapitel 4.1).

4.3.1 Passwörter

Für den nPa gibt es drei verschiedene Passwörter. Je nachdem welches Passwort mit PACE verwendet wird, können unterschiedliche Anwendungen genutzt werden. Zunächst gibt es die persönliche Identifikationsnummer (PIN), die nur dem Ausweisinhaber bekannt sein sollte. Diese kann durch den Ausweisinhaber oder das Bürgeramt geändert werden. Desweiteren gibt es die Card Access Number (CAN), eine auf den Ausweis gedruckte Zufallszahl. Schließlich kann auch wie bei BAC ein von der MRZ abgeleitetes Passwort verwendet werden. Vor jeder Durchführung von PACE wählt das Terminal aus, welches der Passwörter verwendet werden soll.

4.3.2 Protokollablauf

In Abbildung 5 ist der Ablauf des PACE Protokolls vereinfacht dargestellt. Dieses kann in vier Schritte aufgeteilt werden:

Im ersten Schritt generiert die Chipkarte eine Zufallszahl, genannt Nonce (number used once), verschlüsselt diese symmetrisch mit dem Passwort und sendet das Ergebnis an das Terminal. Das Terminal kann nun aus dem Kryptogram die gleiche Nonce wieder

herstellen, da sowohl Chipkarte als auch Terminal im Besitz des selben Passworts sind. Wurde das Passwort auf der Seite des Terminals falsch eingegeben, führt die Entschlüsselung des Kryptogramms zu einer anderen Nonce, so dass das Protokoll an späterer Stelle fehl schlägt.

Im zweiten Schritt führen beide Seiten ein Mapping der verwendeten Domänenparameter durch. Vor der eigentlichen Durchführung von PACE teilt das Terminal der Chipkarte mit welche mathematische Gruppe für den in PACE durchgeführten DH-Schlüsselaustausch verwendet werden soll. Diese Information wird Domänenparameter genannt. Das Mapping dieser Parameter ändert den für die Gruppe verwendeten Generator, so dass bei jeder Durchführung ein anderer Generator verwendet wird.

Als drittes führen nun Terminal und Chipkarte einen DH-Schlüsselaustausch durch. D.h. jede Seite erzeugt sich ein Schlüsselpaar mit der vereinbarten Gruppe und dem gemappten Generator. Sie tauschen ihre öffentlichen Schlüssel aus und können daraus ihr gemeinsames Geheimnis berechnen. Von diesem Geheimnis leiten schließlich beide einen symmetrischen Schlüssel zur Erzeugung von Signaturen und einen für die Verschlüsselung ab.

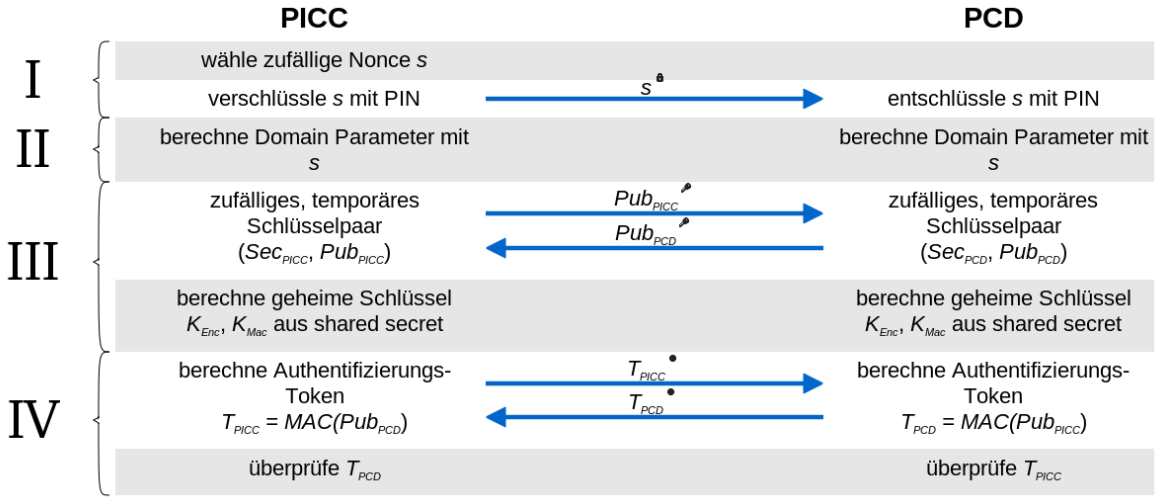

Abbildung 5: Vereinfachter Ablauf des PACE Protokolls

Im vierten und letzen Schritt verifizieren Terminal und Chipkarte, dass kein Man-in-the-Middle-Angriff stattgefunden hat und dass PACE erfolgreich durchgeführt wurde. Dies geschieht dadurch, dass beide den öffentlichen Schlüssel des jeweils Anderen signieren und diesen Token an die andere Seite schicken, welche die Signatur überprüft. Sollte das auf Terminalseite eingegebene Passwort falsch gewesen sein, so wird dies in diesem letzten Schritt dazu führen, dass die Chipkarte den vom Terminal übertragenen Token nicht verifizieren kann und damit den Zugriff ablehnt.

In [15] zeigen die Autoren, dass das PACE Protokoll nach gängigen Sicherheitsmodellen, im Sinne eines zu großen Aufwands gegenüber dem Nutzen, sicher ist, unter der Annahme, dass eine perfekte Hash-Funktion und perfekte Verschlüsselung verwendet werden.

4.4 EAC

Während das PACE Protokoll eine Neu-Entwicklung im Zuge der Entwicklung des nPa ist, wurde Extended Access Control (EAC) bereits für den biometrischen Pass entwickelt. Da biometrische Daten als besonders schützenswert angesehen werden, wurde entschieden, die bestehenden schwachen Protokolle, die ein elektronisches Reisedokument schützen sollten, durch EAC zu erweitern und die biometrischen Daten so effektiv zu schützen. Wie der Name schon sagt, bildet EAC eine Erweiterung zu der Familie der Access Control Protokollen. D.h. der Durchführung von EAC geht eine erfolgreiche Ausführung von BAC bzw. PACE voraus, sodass beide Kommunikationspartner bereits verschlüsselt kommunizieren.

EAC ist ein Oberbegriff für die beiden Protokolle Terminal Authentication (TA) und Chip Authentication (CA). Da die beiden Protokolle in kryptographischer Hinsicht ineinander greifen, macht es keinen Sinn diese einzeln zu betrachten.

In der ersten Version ist bei EAC vorgesehen CA vor TA durchzuführen. Dies kann allerdings zur Identifikation von Ausweisen ausgenutzt werden ohne dass das Terminal im Besitz eines Berechtigungszertifikats ist. Die Identifikation ist möglich, da der nPa bei CA ein statisches Schlüsselpaar verwendet. Aufgrund dieses Sicherheitsproblems wurde in der zweiten Version die Reihenfolge der Protokolle umgedreht. Folglich muss das Terminal zuerst nachweisen, dass es berechtigt ist Daten auszulesen bevor der Ausweis seine Echtheit nachweist. Im folgenden wird EAC in der zweiten Version betrachtet.

4.4.1 Terminal Authentication

Terminal Authentication dient dazu die Berechtigung des Auslesenden zu überprüfen. Dabei kann der Zugriff auch auf einen Teil der Daten beschränkt werden, je nachdem für welche Menge an Attributen das Zertifikat des Auslesenden ausgestellt ist.

Abbildung 6 zeigt vereinfacht den Ablauf des TA Protokolls: Zunächst überträgt das Terminal eine Kette von Zertifikaten. Diese Kette beginnt mit einem Zertifikat, das durch die dem nPa bekannten CVCA signiert ist und endet mit dem Berechtigungszertifikat des Auslesenden (siehe dazu Kapitel 4.2). Alternativ kann die Kette auch mit einem neuen CVCA Zertifikat beginnen. Dann muss dieses jedoch durch die alte CVCA, die dem nPa bekannt ist, signiert sein. Dies kann der Fall sein, wenn einmal ein neues Wurzelzertifikat vewendet werden soll.

Wurde die Zertifikatskette erfolgreich durch den nPa verifiziert, extrahiert dieser den öffentlichen Schlüssel aus dem Berechtigungszertifikat. Daraufhin erzeugt das Terminal eine neues Schlüsselpaar und sendet den neuen öffentlichen Schlüssel an die Chipkarte.

Als nächstes erfolgt die eigentliche Authentisierung des Terminals. Dieses muss nun nachweisen, dass es tatsächlich im Besitz des privaten Schlüssel zu dem übertragenen Berechtigungszertifikat ist. Dazu erzeugt der nPa eine Challenge genannte Zufallszahl und sendet diese an das Terminal. Mit dem privaten Schlüssel des Berechtigungszertifikats erzeugt das Terminal nun eine Signatur über die erhaltene Challenge und den zuvor neu erzeugten öffentlichen Schlüssel. Diese Signatur wird an die Chipkarte übertragen und mit dem im Berechtigungszertifikat enthaltenen öffentlichen Schlüssel geprüft.

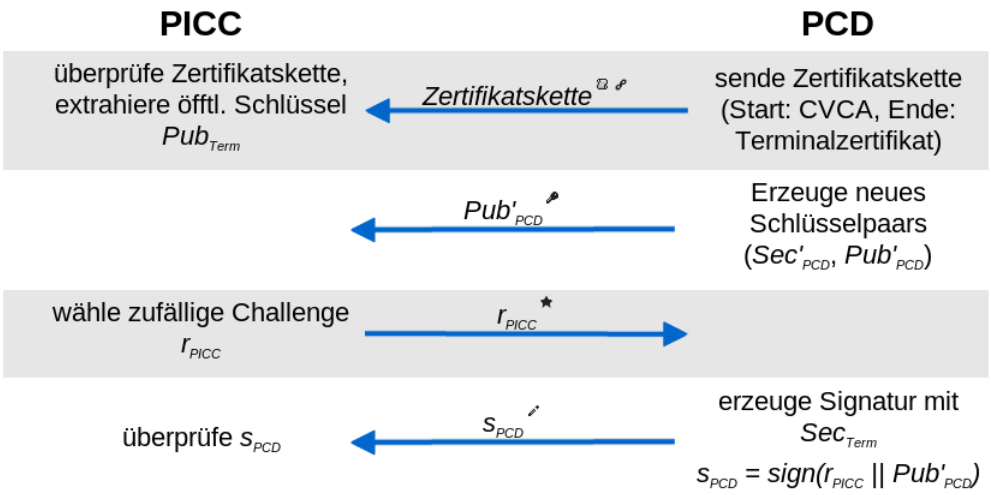

Abbildung 6: Vereinfachter Ablauf der Terminal Authentication

Dadurch, dass die Signatur auch über den neuen öffentlichen Schlüssel erstellt wird, kann gleichzeitig sichergestellt werden, dass bei der Übertragung des neuen öffentlichen Schlüssels kein Man-in-the-Middle-Angriff stattgefunden hat.

Das hier vom Terminal erzeugte Schlüsselpaar wird bei CA zur Durchführung eines erneuten DH-Schlüsselaustauschs verwendet.

4.4.2 Chip Authentication

Während beim elektronisch Pass die passive Authentisierung verwendet wird, um zu zeigen, dass die enthaltenen Daten vertrauenswürdig sind, wird beim nPa die CA für diesen Zweck genutzt. Diese Entscheidung beruht auf der Überlegung, dass es für einen Dienstanbieter, der Daten vom nPa ausgelesen hat, nicht möglich sein soll Dritten zu beweisen, dass diese vom nPa stammen. Da bei der passiven Authentisierung Signaturen für die Daten verwendet werden, wäre dies möglich. Die CA verwendet jedoch keine Signaturen, sondern setzt auf einen impliziten Nachweis für die Vertrauenswürdigkeit der Daten in dem der nPa seine Echtheit nachweist.[14]

Der Ausweis befindet sich im Besitz eines statischen Schlüsselpaars, dessen öffentlicher Schlüssel, wie in Abbildung 7 zu sehen, als erstes an das Terminal übertragen wird. Im zweiten Schritt sendet das Terminal erneut den in TA erzeugten und auch schon übertragenen öffentlichen Schlüssel an die Chipkarte. Diese überprüft nocheinmal, ob es sich bei diesem Schlüssel noch um den gleichen wie in TA handelt. Bei diesem Schlüsselaustausch handelt es sich wieder um einen DH-Schlüsselaustausch, so dass beide Seiten nun ein geteiltes Geheimnis basierend auf den ausgetauschten Schlüsseln berechnen können.

Da in TA bereits sichergestellt wurde, dass der öffentliche Schlüssel des Terminals nicht abgefangen und ersetzt wurde, muss nun nur der öffentliche Schlüssel des nPa verifiziert werden. Dazu erzeugt die Chipkarte als erstes eine Nonce und erzeugt symmetrische Schlüssel für die Signatur und Verschlüsselung in Abhängigkeit von dem gemeinsamen

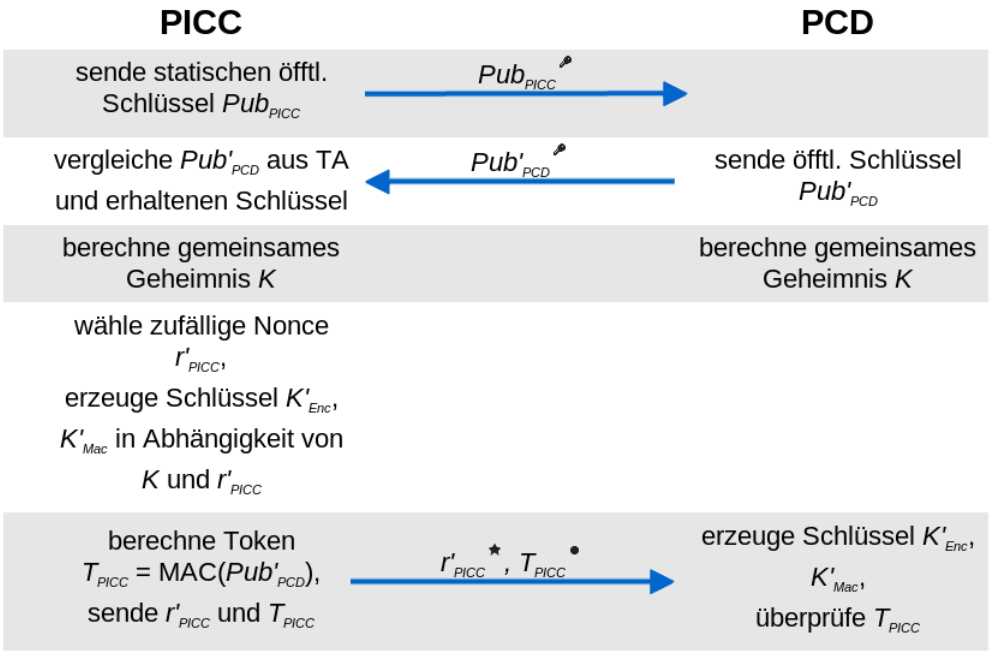

Abbildung 7: Vereinfachter Ablauf der Chip Authentication

Geheimnis und der Nonce. Außerdem berechnet der nPa die Signatur für den öffentlichen Schlüssel des Terminals. Nonce und Signatur werden schließlich an das Terminal gesendet. Das Terminal kann mit der erhaltenen Nonce ebenfalls die Schlüssel für Signatur und Verschlüsselung ableiten und damit die erhaltene Signatur überprüfen.

Nach der erfolgreichen Durchführung von CA bis hier, werden nun nicht mehr die Schlüssel aus PACE zur Absicherung der Kommunikation, sondern die in CA erstellten Schlüssel verwendet.

Für die im nPa enthaltenen Daten wird zwar keine passive Authentisierung durchgeführt, für den öffentlichen Schlüssel des nPa jedoch schon. Dies ist nötig um sicherzugehen, dass der Ausweis tatsächlich echt ist. Erst nach der erfolgreichen passiven Authentisierung des öffentlichen Schlüssels des Ausweises ist CA erfolgreich abgeschlossen.

5 Online-Ausweisfunktion

Die Online-Ausweisfunktion des nPa ist eine besonders interessant Funktion, da dadurch nicht nur staatliche Stellen die elektronischen Daten nutzen können, sondern auch jeder Dienstanbieter. Dennoch muss gewährleistet sein, dass die Daten nicht unrechtmäßig ausgelesen werden können. Es soll also nicht möglich sein, ohne die Zustimmung des Bürgers seine Daten zu verwenden. Außerdem soll transparent sein, welche Daten verwendet werden und wofür, wobei immer nur die Daten ausgelesen werden sollen die tatsächlich benötigt werden (Datensparsamkeit).

Diese Anforderungen werden größtenteils durch das Design der bereits erläuterten Pro-

tokolle garantiert. So muss zum Auslesen des Ausweises im Zuge der Online-Ausweisfunktion immer die PIN des Inhabers eingegeben werden. Durch diese Eingabe stimmt der Bürger dem Auslesen explizit zu. Diese PIN kann auch nur dreimal falsch eingegeben werden, was vor Brute-Force-Attacken gegen die PIN schützt. Die Datensparsamkeit wird dadurch erzielt, dass Berechtigungszertifikate auf gewisse Attribute, je nach Zweck, eingeschränkt sind. Zusätzlich bietet der nPa Funktionen wie die Altersverifikation und Wohnortabfrage, bei denen nicht das Geburtsdatum bzw. die Adresse ausgelesen wird, sondern ein Referenzdatum bzw. eine Referenz-Gemeinde-ID an den Ausweis übertragen wird und dieser mit der Information antwortet, ob der Ausweisinhaber älter als das gegebene Datum ist bzw. in der übertragenen Gemeinde wohnhaft ist.

5.1 Infrastruktur

In den vorangegangenen Kapiteln wurde bisher nur abstrakt von einem Terminal gesproche, das die Software zum Auslesen enthält. Für den behördlichen Anwendungsfall trifft dies auch zu. Für die Online-Ausweisfunktion ist jedoch eine komplexere Infrastruktur nötig.

Der entscheidende Punkt im Hinblick auf die Sicherheit beim Auslesen der Daten aus dem nPa ist das Berechtigungszertifikat. Dieses muss an einem sicheren Ort abgelegt werden, aber gleichzeitig beim Auslesevorgang an den Ausweis übertragen werden. Grundsätzlich kann aus sicherheitstechnischer Sicht dem PC des Ausweisinhabers nicht vertraut werden, da dieser frei darin ist mit seinem PC zu tun, was er möchte. Die Daten vom Ausweis sollten daher verschlüsselt an den Dienstanbieter übertragen werden, damit diese nicht zwischendurch abgegriffen werden können.

Daher wird die Software zum Auslesen in zwei Komponenten unterteilt: eID-Server und eID-Client. Der eID-Server implementiert die Logik für das eigentliche Auslesen der Daten und ist im Besitz des Berechtigungszertifikats. Dienstanbieter und eID-Server sind mit einander vertraut. D.h. möchte ein Dienstanbieter die Online-Ausweisfunktion nutzen, benötigt er einen eID-Server, der das Auslesen übernimmt und die Daten an ihn überträgt. Entweder betreibt er dazu einen eigenen eID-Server oder mietet sich einen bei einem eID-Server-Anbieter.

Damit der eID-Server mit dem Ausweis bei dem Bürger kommunizieren kann, benötigt der eID-Server eine Software auf dem PC des Bürgers. Diese wird eID-Client genannt und kommuniziert über ein Lesegerät mit dem Ausweis. Dieser Aufbau ist in Abbildung 8 zu sehen.

5.2 Ablauf

Damit die besprochenen Protokolle trotz dieser Aufspaltung der Software funktionieren, müssen eID-Client und eID-Server Hand in Hand arbeiten. Das bedeutet, dass beide in Verbindung miteinander stehen und verschiedene Nachrichten austauschen.

Zuerst baut der eID-Client eine sichere Verbindung mit dem Ausweis auf, in dem er die PIN vom Bürger abfragt und PACE durchführt. Für die TA sendet der eID-Server die benötigte Zertifikatskette an den eID-Client. Zusätzlich sendet er auch den in

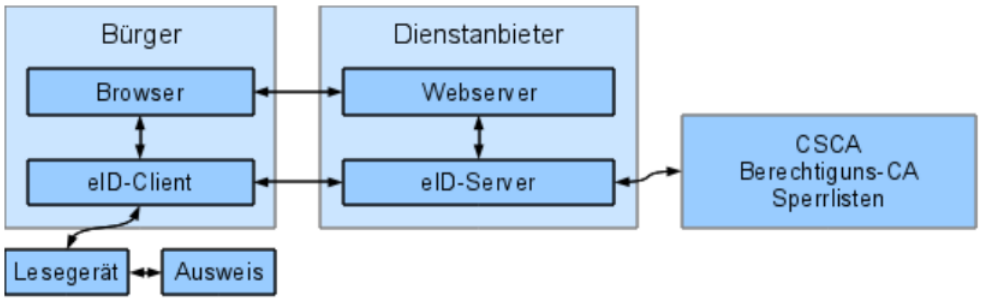

Abbildung 8: Infrastruktur bei der Online-Ausweisfunktion [3]

TA verwendeten öffentlichen Schlüssel. Beides verwendet der eID-Client, um den ersten Schritte von TA durchzuführen. Als nächstes erhält der eID-Client vom Ausweis die Challenge, die er an den eID-Server weiterleitet, damit dieser die benötigte Signatur mit dem privaten Schlüssel des Berechtigungszertifikats erstellen kann. Diese Signature sendet der eID-Server zurück an den eID-Client und dieser weiter an den nPa.

In der CA leitet nun zuerst der eID-Client, den vom Ausweis erhaltenen öffentlichen Schlüssel an den eID-Server weiter und sendet dem Ausweis erneut den öffentlichen Schlüssel des eID-Servers. eID-Server und Ausweis haben damit einen DH-Schlüsselaustausch abgeschlossen. Als letztes leitet der eID-Client die vom Ausweis erzeugte Signatur an den eID-Server weiter, damit er diese prüfen kann.

Nach Beendigung der CA haben Ausweis und eID-Server einen sicheren Kanal aufgebaut, in dem sie ein DH-Schlüsselaustausch durchgeführt haben und können nun direkt verschlüsselt kommunizieren. Ab hier leitet der eID-Client jegliche Kommunikation zwischen Ausweis und eID-Server nur noch weiter.

Auf den ersten Blick erscheint es, als ob der eID-Client eine kritische Software ist. Allerdings muss auf Grund des Designs der Protokolle diesem nicht vertraut werden, da ein Man-in-the-Middle-Angriff nicht möglich ist.

6 Kritik

Ein sicherheitskritisches Projekt wie der nPa ist natürlich ein interessantes Ziel für potentielle Angriffe. So hat sich z. B. der Chaos Computer Club (CCC) mit den Sicherheitsmechanismen des nPa beschäftigt und kritisch untersucht. Dabei identifizierten sie die PIN-Eingabe als Schwachstelle, sofern ein Basiskartenleser verwendet wird. In diesem Fall wird die PIN über die normale PC-Tastatur eingegeben, was es einer auf dem PC laufenden Schadsoftware möglich macht diese abzugreifen, so dass ein Angreifer Kenntnis von der PIN erlangen kann. Nun kann ein Angreifer einen Relay-Angriff durchführen. Ist der Ausweis im Lesegerät eingelegt, kann der Angreifer mit der gestohlenen PIN die Online-Ausweisfunktion nutzen in dem er die Pakete, die normalerweise lokal an den Ausweis gesendet werden, über den Rechner des Opfers an den Ausweis sendet.[10]

Ein weiteres Sicherheitsproblem, das in Verbindung mit der Online-Ausweisfunktion bestand, betraf die offizielle Implementierung des eID-Clients. Diese besaß eien Update-

funktion, die die Updates nicht auf ihre Authentizität überprüft hat, so dass es möglich war die Software durch ein gefälschtes Update zu kompromittieren.

Neben der Software wird auch kritisiert, dass es in Zukunft möglich sein könnte, den Chip im nPa durch neue ausgefeilte Techniken zu klonen. Im Bereich der Smartcards stellt dies eine gängige Art des Angriffs dar. Hier spielt das Verhältnis von Kosten und Nutzen eine wichtige Rolle. Lässt sich der Ausweis nur mit großem Aufwand klonen, stellt dies keine Gefahr dar.

Alle Sicherheitsmechanismen müssen auch im Hinblick auf zukünftige Entwicklungen betrachtet werden, da der nPa eine nicht zu verachtende Dauer von zehn Jahren (für über 24 Jährige) gültig ist, was im Bereich der Informationstechnik eine große Zeitspanne darstellt.

Schließlich werden die hohen Kosten für die Entwicklung des nPa kritisiert. Diese betragen für Entwicklung und Einführung des nPa etwa 18,5 Mio. Euro und für Promotion (Verteilung kostenloser Basiskartenleser) etwa 24 Mio. Euro wie aus der Antwort auf eine kleine Anfrage der Partei DIE LINKE im Jahr 2010 hervorgeht.[6]

7 Fazit

Trotz der umfangreichen Sicherheitsmechanismen und ausgereiften Protokollen hat der nPa viel Kritik hinsichtlich der Sicherheit erhalten. Diese Kritik wurde nicht ganz zu unrecht geäußert, denn die Kryptographie ist ein Gebiet voll Unsicherheit. Wie lange kann ein Verschlüsselungsalgorithmus als sicher angesehen werden? Was wenn sich herausstellt, dass ein mathematisches Problem auf dem ein Verschlüsselungsalgorithmus beruht doch einfacher als gedacht gelöst werden kann? Gerade im Hinblick auf die Gültigkeitsdauer des nPa, die bei über 24 Jährigen bei 10 Jahren liegt, scheint es fragwürdig, ob der nPa über diese Zeitspanne sicher bleibt.

Handwerklich lässt sich den Entwicklern des nPa und den entwickelten Protokollen wenig vorwerfen, vielmehr ist es eine grundsätzliche Frage, ob es sinnvoll ist eine solche kritische Funktionalität überhaupt umzusetzen.

Schließlich bleiben die Hohen Kosten für die Entwicklung des nPa die einer niedrigen Akzeptanz gegenüber stehen. Drei Jahre nach Einführugn des nPa haben lediglich 28% der Bürger, die einen nPa beantragten, die Online-Ausweisfunktion aktiviert.[16] Möglicherweise wird es in Zukunft ein größeres Angebot an Serviceanbietern geben, die die Nutzung des nPa unterstützen und evtl. wird dies zu einer größeren Akzeptanz und Nutzung führen. Bisher kann das Projekt eines nPa als universeller Identitätsnachweis im eBusiness-Bereich jedoch nicht als erfolgreich angesehen werden.

Literatur

[1] Andreas Reisen. *Der Passexpedient: Geschichte der Reisepässe und Ausweisdokumente - vom Mittelalter bis zum Personalausweis im Scheckkartenformat.* Nomos, 2012.

[2] BSI. Advanced Security Mechanisms for Machine Readable Travel Documents (Technical Guideline TR-03110-1). Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2012.

[3] BSI. Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel (Technical Guideline TR-03127). Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2012.

[4] BSI. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2014.

[5] bsi-fuer-buerger.de. Vorder- und Rückseite Personalausweis, November 2013. `https://www.bsi-fuer-buerger.de/SharedDocs/Bilder/DE/BSIFB/Personalausweis/Vorder_und_Rueckseite_Personalausweis.jpg`.

[6] Deutsche Bundesregierung. Sicherheitsrisiken und Kosten des neuen Personalausweises (Drucksache 17/3932), November 2010.

[7] Dipl.-Ing. Christian Engel. Auf dem Weg zum elektronischen Personalausweis. *Datenschutz und Datensicherheit*, 30:207–210, 2006.

[8] Europäischer Rat. Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, Dezember 2004.

[9] FBI. PENTTBOM.

[10] Frank Morgner und Dominik Oepen. "Die gesamte Technik ist sicher Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis, Dezember 2010.

[11] ICAO. Technical Advisory Group on Machine Readable Travel Documents. Technical report, International Civil Aviation Organization, 2009.

[12] ICAO. Supplemental Access Control for Machine Readable Travel Documents. Technical report, International Civil Aviation Organization, 2010.

[13] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, Ronny Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. *1st Int. Workshop on Security*, 1:152–167, 2006.

[14] Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. *Datenschutz und Datensicherheit*, 3:173–177, 2008.

[15] Jens Bender, Marc Fischlin, Dennis Kügler. Security Analysis of the PACE Key-Agreement Protocol. Cryptology ePrint Archive, Report 2009/624, 2009. `http://eprint.iacr.org/`.

[16] Jens Fromm, Petra Hoepner, Jonas Pattberg, Christian Welzel. 3 Jahre Online-Ausweisfunktion - Lessons Learned, Oktober 2013.

[17] Ueli M. Maurer. Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms. *Advances in Cryptology - CRYPTO '94*, 1994.

[18] Ueli M. Maurer, Stefan Wolf. The Diffie-Hellman Protocol. *Designs, Codes and Cryptography*, 19:147–171, 2000.

[19] Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory. 22*, 6:644–654, 1976.

Abbildungsverzeichnis