Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Informatik

Zeitaktualisierung des nPA mit einer Android-App

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor of Science [B. Sc.]

eingereicht von: Hera Khan
geboren am: 12.12.1991
geboren in: Berlin

Gutachter/innen: Prof. Dr. rer. nat. Jens-Peter Redlich
Prof. Dr. Johannes Köbler

eingereicht am: .....

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

nPA Neuer Personalausweis

EAC Extended Access Control

PACE Password Authenticated Connection Establishment

CA Chipauthentifizierung

PA Passive Authentifizierung

TA Terminalauthentifizierung Version

CAN Card Access Number

MRZ Machine Readable Zone

DS Document Signer

DV Document Verifier

CVCA Country Validating Certificate Authority

DVCA Document Verifying Certification Authority

CSCA Country Signing Certificate Authority

CHAT Certificate Holder Authorization Template

RFID Radio Frequency Identification

NFC Near Field Communication

APDU Application Protocol Data Units

CLA Class Byte

INS Instruction Code

FBZ Fehlbedienungszähler

PICC Proximity Integrated Circuit Card

PKI Public Key Infrastructure

BAC Basic Access Control

BSI Bundesamt für Sicherheit in der Informationstechnik

PKI Public Key Infrastructure

PUK PIN Unblocking Key

QES Qualifizierte Elektronische Signatur

1 Einleitung

Am 1. November 2010 wurde der neue Personalausweis (nPA) in Deutschland eingeführt. Er besitzt alle Merkmale eines Sichtausweises und enthält im Inneren zusätzlich einen Mikrochip[1]. Dieser soll einerseits dem Ausweisinhaber und eBusiness- oder eGovernment-Dienstleistern andererseits eine sichere gegenseitige Authentifizierung ermöglichen. Die Authentisierung kann auch über eine Internetverbindung erfolgen. Zudem erstellt er qualifizierten elektronischen Signaturen. Dazu sind auf dem Chip ausgewählte Daten des Ausweisinhabers gespeichert. Diese dürfen jedoch nur von berechtigten Diensten abgefragt werden. Dazu weist ein Terminal durch seinem Terminalzertifikat dem nPA) die Zugriffsrechte nach. Diese Terminalzertifikate (ausgenommen Zertifikate für Signaturterminals) besitzen eine kurze zeitliche Validität, damit ein Missbrauch begrenzt werden kann. Der nPA ist nicht in der Lage eine innere Uhr zu verwalten, da er keine eigene Stromversorgung hat. Damit ein kompromittiertes Terminal von dem nPA erkannt werden kann, verwaltet der Chip des nPAs eine untere Grenze für das aktuelle Datum. Diese wird durch den erfolgreichen Import bestimmter Zertifikate aktualisiert. Um zu untersuchen ob ein Terminal bereits unsicher geworden ist, vergleicht der nPA das Ausstellungsdatum des Terminalzertifikats nur mit seiner eigenen unteren Grenze für das Datum und prüft die Gültigkeit des Zertifikats. Wird ein nPA lange nicht benutzt, so veraltet seine untere Grenze für das Datum und kompromittierte Terminals können die auf dem nPA gespeicherten Dateien und Funktionen verwenden, obwohl der Außenwelt bereits länger bekannt ist, dass diese Terminals unsicher geworden sind.

1.1 Ziel der Arbeit

In dieser Arbeit wird eine Android-App vorgestellt, die die untere Grenze des Datums auf dem nPAs aktualisiert. Da Smartphones verbreitet sind, ist die App als Zeitaktualisierungsdienst für viele Benutzer mit geringem Aufwand verwendbar. Für die Aktualisierung benötigt der Ausweisinhaber lediglich die in dieser Arbeit vorgestellte App, ein vertrauenswürdiges Smartphone und

[1] Weil in den entsprechenden Dokumenten verkürzend von Chip anstatt Mikrochip die Rede ist, wird dies im weiteren in dieser Arbeit auch so verwendet.

eine entsprechende Zertifikatskette . Es wird gezeigt, dass die Zertifikatskette aus einer unsichere Quelle entnommen werden kann und keine besonderen Zugriffsrechte benötigt werden, um eine Zeitaktualisierung auf dem nPA durchzuführen. Damit wird vielen Nutzern eine sichere Möglichkeit dargestellt, um die Sicherheit der Authentifizierungsfunktion des nPA zu verbessern.

1.2 Aufbau der Arbeit

Kapitel 2 widmet sich dem nPA. In Kapitel 3 werden die elektronischen Funktionen und Dateien des neuen Personalausweises ausführlich beschrieben. Kapitel 4 beschreibt das Sicherheitskonzept und die verwendeten Protokolle. Die dabei verwendeten Passwörter werden in Kapitel 5 vorgestellt. Kapitel 6 kategorisiert die Terminals in vier verschiedene Terminaltypen. Des weiteren wird der Unterschied zwischen local und entfernten Terminals erklärt. In Kapitel 7 werden die in [BSI TR-03119] definierten Profile von Lesegeräteklassen dargestellt. Dabei werden die unterschiedlichen funktionalen und sicherheitsrelevanten Anforderungen an die Lesegerätklassen betrachtet. Kapitel 8 stellt kurz eine Technologie zur kontaktlosen Identifizierung, die Radio Frequency Identification, dar und geht auf dem NFC-Standard ein. Das Kommunikationsprotokoll nach [ISO 7816], das für die Kommunikation mit dem nPA verwendet wird, wird in Kapitel 9 vorgestellt. Kapitel 10 erklärt, wieso ein Zeitaktualisierungsdienst benötigt wird. Dazu wird veranschaulicht, wie ein kompromittiertes Terminal vom nPA erkannt wird. Kapitel 11 beschreibt die Funktionsweise eines Zeitaktualisierungsdienstes und stellt eine Android-App vor, die die untere Grenze für das Datum auf dem nPA aktualisiert. Außerdem wird ein Verfahren zum Herunterladen einer hoheitlichen Zertifikatskette erklärt, da eine solche Zertifikatskette zum Aktualisieren der unteren Grenze für das Datum benötigt wird. In Kapitel 12 werden die Ergebnisse zusammengefasst.

2 Der neue Personalausweis

Der neue Personalausweis ist ein Ausweisdokument[2] im td-1-Format[3] mit einem integrierten kontaktlosen Chip[4]. Dieser erlaubt eine elektronische Nutzung des Personalausweises[5].

Die physikalischen Sicherheitsmerkmale (z.B. Hologramme) und das Design der Karte sind nicht Gegenstand dieser Arbeit. Hier werden nur die elektronischen Funktionen des Ausweises betrachtet.

Der nPA besitzt einen kontaktlosen Chip und eine Antenne. Somit ist er in der Lage mittels induktiver Kopplung mit einem Kartenterminal[6] zu kommunizieren[7]. Diese Terminals können dabei sowohl als Lese- als auch als Schreibgeräte fungieren.

Abbildung 1: Muster des neuen Personalausweises (Quelle: http://der-neue-personalausweis.de)

3 Elektronische Funktionen des neuen Personalausweises

Zusätzlich zur Identifizierung per Sichtprüfung verfügt der neue Personalausweis über drei elektronische Funktionen: die eID-Funktion, die eSign-Funktion und

[2] [Elektronische Ausweisdokumente]
[3] [ICAO Doc 9303], Pt. 3 Vol. 2
[4] [ISO/IEC 14443]-4
[5] [BSI TR-03127], S.8
[6] Kapitel 6
[7] [ISO/IEC 14443]

die ePassport-Funktion[8].

Von diesen drei Funktionen ist lediglich die ePassport-Funktion verpflichtend vorhanden. Die eID-Funktion und die eSign-Funktion können nachträglich aktiviert werden. Um auf die Dateien der Anwendungen zugreifen zu können, muss eine erfolgreiche Authentifizierung des Terminals stattgefunden haben. Dies geschieht mittels der Terminalauthentifizierung nach PACE und vor der Chipauthentifizierung. Es wird zwischen dem local Terminal und dem entfernten Terminal unterschieden. Das local Terminal (Kartenleser) ist für die Interaktion mit dem Ausweisinhaber zuständig. Es zeigt dem Benutzer wichtige Informationen an ermöglicht es ihn gegenüber dem nPA durch PACE zu authentifizieren. Wohingegen das entfernte Terminal in der TA seine Berechtigung nachweist und für den eID-Dienst zuständig ist. Bei der Signaturanwendung vereint der Komfortleser das local Terminal (Nutzerinteraktion) mit dem entfernten Terminal (Berechtigungsnachweis) in einer Instanz. In dieser Arbeit wird "Terminal" kontextabhängig für das local (PACE) und das entfernte Terminal (Kommunikation nach PACE, z.B. TA und CA) verwendet. Diese drei Applikationen werden im Folgenden genauer erklärt.

3.1 Biometrieanwendung (ePassport-Funktion)

Durch die Biometrieanwendung kann der nPA als elektronischer Reisepass verwendet werden. Im Gegensatz zu dem ePass müssen in dieser Anwendung die Fingerabdrücke nicht gespeichert werden. Für die hoheitliche Nutzung sind die in der Tabelle 1 aufgeführten und in [ICAO Doc 9303],Pt. 3 Vol. 1 definierten Datengruppen gespeichert.[9]

Diese Dateien sind ausschließlich für authentifizierte Inspektionsterminals lesbar. Dazu wird der Nachweis entsprechender Rechte über die Terminalauthentifizierung[10] benötigt. Nach der initialen Personalisierung des Ausweises ist das Schreiben dieser Daten nicht mehr möglich.

[8] [BSI TR-03127]
[9] [BSI TR-03127], S.11
[10] Kapitel 4

Datei	Inhalt	Zugriffsrecht Lesen
EF.SOD	Hashwerte der Datengruppen DG1, DG2, DG3; Signatur über diese Hashwerte sowie das DS-Zertifikat	IS
DG1	Daten der maschinenlesbaren Zone (MRZ), wie auf dem Ausweiskörper aufgedruckt	IS
DG2	Digitales Gesichtsbild, identisch mit dem aufgedruckten Bild	IS
DG3	Zwei Fingerabdrücke (optional). Werden keine Fingerabdrücke gespeichert, enthält diese Datengruppe einen zufälligen Wert	IS + Read DG3
IS: authentisiertes Inspektionssystem (PACE mit CAN o. MRZ, TA2, CA2)		

Tabelle 1: Daten der Biometrieanwendung (Quelle: [BSI TR-03127])

3.2 eID-Anwendung (eID-Funktion)

Die eID-Funktion des Ausweises dient der elektronischen Authentifizierung des Ausweisinhabers gegenüber einer dritten Person oder einem Dienst. Möglich ist dies auch über eine Internetverbindung , z.B. im Rahmen von eBusiness und eGovernment Anwendungen.[11] Die sogenannte Offline-Authentifizierung ist ebenfalls möglich. Dies bezeichnet die elektronische Identifizierung des Inhabers an einen autonomen Betrieb aufgestellten Automaten oder Terminal ohne Datenkommunikationsanbindung. Die eID-Applikation enthält die in Tabelle 2 dargestellten Datengruppen.

Zugriff auf die vom Nutzer preisgegebenen Dateien erhalten nur erfolgreich authentifizierte Inspektions- und Authentifizierungsterminals.

3.3 Signaturanwendung (eSign-Funktion)

Die Signaturanwendung[12] ermöglicht das Leisten qualifizierter elektronischer Signaturen (QES) im Sinne des deutschen Signaturgesetzes[13].Für die optionale Nutzung der QES muss durch den Nutzer, nach der Auslieferung der Karte, ein Signaturschlüsselpaar erzeugt werden.[14] Dies erfolgt durch einen Zertifizierungsdienstanbieter. [15]

[11] [BSI TR-03127], S.13
[12] [BSI TR-03117]
[13] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)
[14] [BSI TR-03117]
[15] [BSI TR-03127], S.23

Datei	Inhalt	Zugriffsrechte		
		Lesen	**Schreiben**	**Interne Verwendung**
DG1	Dokumententyp	IS; AT + Read DG1	-	-
DG2	Ausgebender Staat(„D“ für Deutschland)	IS; AT + Read DG2	-	-
DG3	Ablaufdatum im Format JJJJMMTT	IS; AT + Read DG3	-	AT
DG4	Vorname(n)	IS; AT + Read DG4	-	-
DG5	Familienname	IS; AT + Read DG5	-	-
DG6	Ordensname/ Künstlername	IS; AT + Read DG6	-	-
DG7	Doktorgrad	IS; AT + Read DG7	-	-
DG8	Geburtsdatum im Format JJJJMMTT	IS; AT + Read DG8	-	-
DG9	Geburtsort als unformatierter Text	IS; AT + Read DG9	-	-
DG10-DG12	unbenutzt	-	-	-
DG13	Geburtsname	IS; AT + Read DG13	-	-
DG14-DG16	unbenutzt	-	-	-
DG17	Adresse	IS; AT + Read DG17	AT + Write DG17	-
DG18	Wohnort-ID	IS; AT + Read DG18	AT + Write DG18	AT + Community ID Verification
DG19-DG21	unbenutzt	-	-	-
	Vergleichsgeburtssdatum für Altersverifikation	-	-	AT + Age Verification
	Schlüssel für dienstanbieterspezifisches Sperrmerkmal	-	-	AT
	Schlüssel für dienst- und kartenspezifische Kennung	-	-	AT + Restricted Identification

IS: authentisiertes Inspektionssystem (PACE mit CAN o. MRZ, TA2, CA2)

AT: authentisiertes Authentisierungsterminal (PACE mit eID-PIN o. CAN mit Recht CAN allowed), TA2, CA2)

Tabelle 2: Daten der eID-Anwendung (Quelle: [BSI TR-03127])

3.4 Master File

Zusätzlich zu den oben beschriebenen Dateien wird ein Master File auf dem Chip gespeichert. Darin befinden sich die Systemdaten und Passwörter, die zur Abwicklung der Zugriffsprotokolle notwendig sind.

<table>
<tr><th colspan="2">Einsatzbereich</th><th>Anwendung</th><th>Visualisierung</th><th>Änderung</th></tr>
<tr><td rowspan="6">Hoheitliche Aufgaben</td><td rowspan="3">Ausweisbehörden</td><td>ePass</td><td rowspan="2">QS bei Ausgabe + Auskunftsbegehren</td><td>-</td></tr>
<tr><td>eID</td><td>Adresse, BKZf. PIN-Management</td></tr>
<tr><td>eSign</td><td>-</td><td>-</td></tr>
<tr><td rowspan="3">Kontrollbehörden</td><td>ePass</td><td rowspan="2">Identitätsfeststellung (inkl. Adresse)</td><td>-</td></tr>
<tr><td>eID</td><td>-</td></tr>
<tr><td>eSign</td><td>-</td><td>-</td></tr>
<tr><td rowspan="6">Nichthoheitliche Aufgaben</td><td rowspan="3">Online-Authentisierung</td><td>ePass</td><td>-</td><td>-</td></tr>
<tr><td>eID</td><td rowspan="2">Online-Identitätsnachweis (inkl. Altersverifikation) elektronische Signatur</td><td>-</td></tr>
<tr><td>eSign</td><td>Generieren des Schlüsselpaares, Zertifikatsspeicherung</td></tr>
<tr><td rowspan="3">Offline-Authentisierung</td><td>ePass</td><td>-</td><td>-</td></tr>
<tr><td>eID</td><td>Offline-Identitätsnachweis (inkl. Altersverifikation)</td><td>-</td></tr>
<tr><td>eSign</td><td>Offline-Signatur von Daten</td><td>-</td></tr>
<tr><td colspan="5">BKZf: Abkürzung für Behördenkennziffer; im vorliegenden Zusammenhang der amtliche Gemeindeschlüssel</td></tr>
</table>

Tabelle 3: Verwendung des nPAss (Quelle: [BSI TR-03128], S.13)

4 Schutzmechanismen des nPA

Die folgenden kyptografischen Protokolle[16] werden für die Authentifizierung der Chips und Terminals, zum Regeln der Zugriffskontrolle und zur Gewährleistung der Integrität und Vertraulichkeit der Kommunikation genutzt.

- PACE - Password Authenticated Connection Establishment[17]

[16] [BSI TR-03116] Teil 2
[17] [BSI TR-03110] Teil 2

- TA2 - Terminalauthentifizierung Version 2[18]
- PA - Passive Authentifizierung[19]
- CA2 - Chipauthentifizierung Version 2[20]

Die Ausführung dieser Protokolle in dieser Reihenfolge wird als General Authentication Procedure[21] bezeichnet. Mit der General Authentication Procedure ist der Zugriff auf die auf dem nPA gespeicherten Daten und Funktionen möglich. In [BSI TR-03116], Teil 2 und [IBSI TR-02102] werden die Anforderungen an die verwendeten Algorithmen und Schlüssellängen festgelegt. Weiterhin ist in [BSI TR-03111] die Kryptografie auf elliptischen Kurven definiert und [IBSI TR-02102] ist verbindlich für die Erzeugung von Zufallszahlen und Schlüsselmaterial.

4.1 Extended Access Control (EAC)

EAC ist ein Verfahren zur gegenseitigen Authentifizierung zwischen dem nPA und dem local Terminal. Durch die EAC sollen sensitive Daten des nPAs geschützt werden, indem geprüft wird ob das Terminal berechtigt ist, auf die Daten zuzugreifen. Außerdem wird die Echtheit des Chips nachgewiesen und eine starke Verschlüsselung und Integritätssicherung der übertragenen Daten wird erzwungen. Die EAC existiert in zwei Versionen. Der nPA unterstützt die zweite Version des EAC-Protokolls (EAC2), das nach dem Schema der General Authentication Procedure ausgeführt wird. Bevor ein Zugriff auf die Anwendungen des nPAs möglich ist, müssen in der General Authentication Procedure PACE, TA2, Passive Authentication und CA2 in dieser Reihenfolge erfolgreich durchgeführt werden. Im Folgenden ist mit TA und CA die jeweilige zweite Version des Protokolls gemeint. Als Nächstes werden die Schritte der General Authentication Procedure betrachtet.

[18] [BSI TR-03110] Teil 2
[19] [ICAO Doc 9303]
[20] [BSI TR-03110] Teil 2
[21] [BSI TR-03110] Teil 2

4.2 PACE - Password Authenticated Connection Establishment

Bei der EAC wird als Erstes PACE[22] durchgeführt, um einen verschlüsselten und integritätsgesicherten Kanal[23] zwischen dem Terminal und dem Chip auf der Grundlage eines schwachen geteilten Passworts zu etablieren. Mit dem gewählten Passwort[24] vergibt der Besitzer die Berechtigung, bestimmte Datengruppen des Ausweises zu lesen. Außerdem authentifiziert sich der Besitzer des Ausweises mit der Eingabe des Passworts, da nur er dieses Geheimnis kennt. Das Terminal ist bereits durch PACE in der Lage dem Chip mitzuteilen, welchen Terminaltyp er hat und welche Rechte von ihm während der Sitzung angestrebt werden.

PACE ist eine Alternative zur Basic Access Control (BAC), die z.B. beim elektronischen Reisepass verwendet wird und ihm ermöglicht, zu überprüfen, ob das Terminal berechtigt ist, auf weniger sensible Daten zuzugreifen.

Das PACE Protokoll basiert auf dem Diffie-Hellman-Schlüsselaustausch-Protokoll[25], bei dem sich der Chip und das Terminal mit einem schwachen, geteilten Geheimnis π authentifizieren. Dadurch ist kein man-in-the-middle-attack möglich. Mit PACE werden, trotz eines kurzen und damit schwachen Passwortes, starke Schlüssel generiert.

Protokollablauf

Bei PACE werden die folgenden Schritte sowohl auf dem Chip als auch durch dem Terminal ausgeführt. In Tabelle 4 ist der generische Protokollablauf von PACE[26]schematisch dargestellt.

1. Eine zufällig erzeugte Nonce s wird von dem nPA zu z=E(K_s,s) mit K_π=$KDF_\pi(\pi)$ verschlüsselt, wobei π das bei PACE übertragene Passwort (CAN, MRZ, eID-PIN, PUK) ist. Das Chiffrat z wird vom nPA an das Terminal gesendet.

[22] [BSI TR-03110] Teil 1, S.17
[23] Es werden zwei starke Sitzungsschlüssel während des PACE vereinbart.
[24] Kapitel 5
[25] [BSI 02101], S.52
[26] [ICAO 1]

Chip (PICC)		**Terminal (PCD)**
Domänenparameter D_{PICC}		
s zufällig		
z = E(K_π,s)	$\xrightarrow{D_{PICC},\ z}$	s = D(K_π,z)
	Datenaustausch für Map()	
$\widetilde{D}$=Map(D_{PICC},s)		$\widetilde{D}$=Map(D_{PICC},s)
wähle flüchtiges Schlüsselpaar ($\widetilde{SK_{PICC}}$, $\widetilde{PK_{PICC}}$,$\widetilde{D}$)		wähle flüchtiges Schlüsselpaar ($\widetilde{SK_{PCD}}$, $\widetilde{PK_{PCD}}$,$\widetilde{D}$)
prüfe: $\widetilde{PK_{PCD}} \neq \widetilde{PK_{PICC}}$	$\widetilde{PK_{PCD}}, \widetilde{PK_{PICC}}$	prüfe: $\widetilde{PK_{PCD}} \neq \widetilde{PK_{PICC}}$
K = KA($\widetilde{SK_{PICC}}$, $\widetilde{PK_{PCD}}$, $\widetilde{D}$)		K = KA($\widetilde{SK_{PCD}}$, $\widetilde{PK_{PICC}}$, $\widetilde{D}$)
T_{PICC}=MAC(KS_{MAC},$\widetilde{PK_{PCD}}$)	$\widetilde{T_{PCD}}, \widetilde{T_{PICC}}$	T_{PCD}=MAC(KS_{MAC},$\widetilde{PK_{PICC}}$)
verifiziere $\widetilde{T_{PCD}}$		verifiziere $\widetilde{T_{PICC}}$

Tabelle 4: vereinfachte Darstellung von PACE (Quelle: [ICAO 1], S.11)

2. Das Terminal verwendet das geteilte Geheimnis π,um aus dem Chiffretext z s=D(K_π,z) zu rekonstruieren.

3. Der nPA und das Terminal führen die folgenden Schritte aus:

   a) Zusätzliche Daten werden zum Mappen der Nonce ausgetauscht.

   b) Die ephemeralen Domänenparameter $\widetilde{D}$=Map(D_{PICC},s) werden aus der Nonce s und dem statischen Domänenparameter D_{PICC} berechnet.

   c) Eine anonyme Diffie-Hellman-Schlüsselvereinbarung wird zwischen beiden auf der Basis des ephemeralen Domänenparameter $\widetilde{D}$ durchgeführt, wodurch das gemeinsame Geheimnis K=KA($\widetilde{SK_{PICC}}$, $\widetilde{PK_{PCD}}$, $\widetilde{D}$)=KA($\widetilde{SK_{PCD}}$, $\widetilde{PK_{PICC}}$, $\widetilde{D}$) berechnet wird.

   d) Dabei sollen beide Parteien sicherstellen, dass sich $\widetilde{PK_{PICC}}$ und $\widetilde{PK_{PCD}}$ unterscheiden.

   e) Aus dem gemeinsamen Geheimnis K werden die Sitzungsschlüssel KS_{MAC}=KDF_{MAC}(K) und KS_{ENC}=KDF_{ENC}(K) abgeleitet.

   f) Mit K_{MAC} bilden beide eine Prüfsumme T_{PCD}=MAC(KS_{MAC},$\widetilde{PK_{PICC}}$) bzw. T_{PICC}=MAC(KS_{MAC},$\widetilde{PK_{PCD}}$) über den ephemeralen öffentlichen Schlüssel des anderen und schicken diese an die Gegenstelle. Diese verifiziert die Prüfsumme.

4.2.1 Secure Messaging

Nachdem PACE erfolgreich durchgeführt wurde, haben der nPA und das lokale Terminal sich gegenseitig authentifiziert und kommunizieren anschließend sicher per Secure Messaging[27] mit den ausgehandelten Sitzungsschlüsseln KS_{MAC} und KS_{ENC}. Secure Messaging bietet einen sicheren und authentifizierten Kanal zwischen dem Chip und dem Terminal, der durch PACE, (später nach) CA oder Basic Access Control aufgebaut werden kann. Die Sicherheitsstufe hängt von den dabei verwendeten Algorithmen ab.

4.3 TA - Terminalauthentifizierung

Der Nachweis der Zugriffsrechte eines Terminals bzw. eines Dienstanbieters wird mit der Terminalauthentifizierung[28] im Rahmen der General Authentication Procedure sichergestellt. Für den Zugriff auf alle Anwendungen des Chips ist ein Nachweis notwendig. Die Zugriffsrechte müssen für jeden neuen, durch Chipauthentifizierung aufgebauten, Kanal neu nachgewiesen werden und können über diesen hinaus nicht mehr ausgeübt werden. Die TA kann nur einmal während einer Sitzung durchgeführt werden.

Der Berechtigungsnachweis erfolgt über Terminalzertifikate[29], die während der TA an den nPA übermittelt werden. Terminalzertifikate werden durch eine Berechtigungs-PKI (auch EAC-PKI) vergeben. Anhand dieser Zertifikatskette erkennt der nPA den Typ[30] des Terminals, sowiso die maximalen Rechte des Terminals. Damit die TA in der General Authentication Procedure erfolgreich ist, muss der Terminaltyp aus dem Zertifikat mit dem Terminaltyp übereinstimmen, der in PACE angekündigt wurde und ein zulässiges Passwort[31] muss verwendet worden sein. Nur die während PACE beantragten und in der Zertifikatskette nachgewiesenen Zugriffsrechte werden eingeräumt.

Die Berechtigungs-PKI ist in drei Stufen gegliedert[32], welche in der folgenden Abbildung dargestellt sind:

[27] [BSI TR-03110] Teil 3, S. 73
[28] [BSI TR-03110]
[29] [BSI TR-03127], S.27
[30] Kapitel 9
[31] Kapitel 9
[32] [BSI TR-03128], S.16 und S.17

1. **Country Verifying Certification Authority (CVCA)**

   Den nationalen Vertrauensanker der gesamten Berechtigungs-PKI bildet die Country Verifying Certification Authority für den nPA. Die CVCA definiert die Bedingungen, unter denen ein Zugriff auf die in den Anwendungen gespeicherten Daten des nPA gewährt werden kann, über ihre Policy. Alle Teilnehmer sind zur Realisierung und Einhaltung dieser Policy verpflichtet. Welche in Zertifikaten die Zugriffsrechte der Document Verifier (DV) auf dem nPA festlegt. Die Document Verifier können aus ihren Zertifikaten entnehmen, für welche Anwendungen bzw. Daten sie Zugriffsrechte vergeben dürfen.

2. **Document Verifying Certification Authority (DVCA)**

   Eine DVCA verantwortet und betreut als organisatorische Einheit zusammengehörige Terminals, indem sie unter anderem deren Berechtigungszertifikate ausstellt. Die CVCA autorisiert eine DVCA zur Ausgabe von Zertifikaten für nationale Terminals. Eine DVCA darf nur Terminalzertifikate mit maximal den Rechten ausstellen, über die sie selbst durch ihr Document-Verifier-Zertifikat verfügt.

3. **Terminals**

   Die Terminals (Inspektionssysteme, Authentisierungsterminals und Signaturterminals) kommunizieren mit dem Chip des nPAs.

Die von der Berechtigungs-PKI ausgestellten Zertifikate sind CV-Zertifikate nach [ISO 7816], Teil 6 und [BSI TR-03110].

Der Chip des nPAs ist nicht in der Lage, Rückruflisten für Zertifikate zu verarbeiten, weshalb Terminalzertifikate, ausgenommen Zertifikate für bestätigte Signaturterminals, nur mit einer kurzen Laufzeit ausgestellt werden.[33] Die Gültigkeitsdauer der Zertifikate ist je nach Verwendungszweck und Betriebsart unterschiedlich und erstreckt sich von 2 Tagen (Lesen der eID-Daten oder Pseudonym) bis zu einem Monat (Verifikation von Alter/Wohnort, Nachladen der QES). Bedingt durch das Fehlen einer Stromquelle enthält der Chip keine eigene Uhr. Dennoch soll der Ausweis die Gültigkeit der Zertifikate prüfen können. Dazu speichert der Chip eine untere Grenze für das aktuelle Datum. Diese

[33] [BSI TR-03128], S. 37

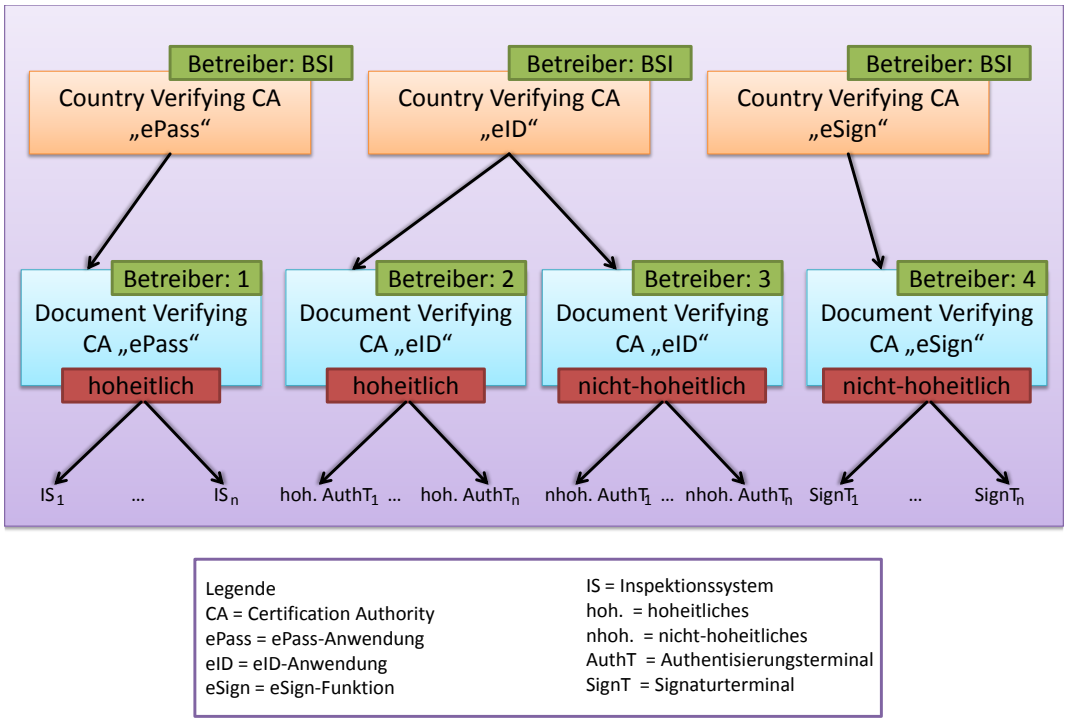

Abbildung 2: Anwendungsorientierte Grundstruktur der EAC-PKI (Quelle: [BSI TR-03128], S.19)

leitet er aus den Ausstellungsdaten der CVCA-, DV- und Terminalzertifikate von hoheitlichen nationalen Inspektionssystemen und hoheitlichen nationalen Authentisierungsterminals her.

Protokollablauf

Das TA-Protokoll ist ein Challenge-Response-Protokoll zum authentifizieren des Terminals. In Abbildung 5 ist der vereinfachte Ablauf dargestellt. Alle Nachrichten werden, durch die in PACE vereinbarten Schlüssel verschlüsselt, per Secure Messaging übertragen.

1. Das Terminal schickt eine Zertifikatskette an den nPA, in der seine Berechtigung und der öffentliche Schlüssel des CVCA s vermerkt sind.

2. Der Chip des nPAs prüft die einzelnen Zertifikate, um sicher zu stellen, dass das Terminalzertifikat von einer vertrauenswürdigen Instanz ausgestellt wurde. Der Ausweis entnimmt der Zertifikatskette den öffentlichen Schlüssel des Terminals $\widetilde{PK_{PCD}}$.

Chip (PICC)		**Terminal (PCD)**
Verifikation Extraktion von PK_{PCD}	$\underleftarrow{Zertifikatskette}$	
	$\underleftarrow{Comp(\widetilde{PK_{PCD}}), A_{PCD}}$	erzeuge ein Diffie-Hellman-Schlüsselpaar $(\widetilde{SK_{PCD}},\widetilde{PK_{PCD}}, D_{PICC})$
r_{PICC} zufällig	$\underrightarrow{r_{PICC}}$	
	$\underleftarrow{s_{PCD}}$	s_{PCD}=Sign(SK_{PCD},ID_{PICC}|| r_{PICC}||Comp($\widetilde{PK_{PCD}}$)||A_{PCD})
Verify(PK_{PCD},s_{PCD},ID_{PICC}|| r_{PICC}||Comp($\widetilde{PK_{PCD}}$)||A_{PCD})		

Tabelle 5: vereinfachte Darstellung von den TA Protokoll (Quelle: [BSI TR-03110] Teil 2, S.20)

3. Das Terminal generiert ein ephemerales Diffie-Hellman-Schlüsselpaar $(\widetilde{SK_{PCD}},\widetilde{PK_{PCD}}, D_{PICC})$ und sendet den komprimierten öffentlichen Schlüssel Comp($\widetilde{PK_{PCD}}$) an den nPA. Unter Umständen schickt das Terminal Zusatzdaten A_{PCD}.

4. Der nPA schickt eine zufällige Challenge r_{PICC}.

5. Aus dem in PACE übertragenen öffentlichen Schlüssel des nPAswird eine Kennnummer ID_{PICC}=Comp($\widetilde{PK_{PICC}}$) berechnet. Das Terminal schickt die Signatur s_{PCD}=Sign(SK_{PCD},ID_{PICC}\|\| r_{PICC}\|\|Comp($\widetilde{PK_{PCD}}$)\|\|A_{PCD}), welche durch den privaten Schlüssel seines Terminalzertifikats erstellt wurde.

6. Der nPA verifiziert die Signatur mit dem im 2. Schritt extrahierten öffentlichen Schlüssel des Terminals.

   Verify(PK_{PCD},s_{PCD},ID_{PICC}\|\| r_{PICC}\|\|Comp($\widetilde{PK_{PCD}}$)\|\|A_{PCD})=true

Nachdem die TA erfolgreich durchgeführt wurde, erlaubt der nPA durch die Berechtigung des Terminals und mit Chat beschränkten Zugriff auf seine sensiblen Daten. Der in Schritt 3 übermittelte ephemerale public Key des Terminals wird nach erfolgreicher TA in der CA verwendet. Die TA verbindet also PACE (Schritt 4) und CA.

4.4 passive Authentisierung

Nachdem das Terminal durch die TA seine Echtheit nachgewiesen hat, wird durch die passive Authentisierung[34] der Echtheitsnachweis der auf dem Chip gespeicherten Daten durchgeführt. Während der Personalisierung beim Ausweishersteller werden die in der Biometrieanwendung gespeicherten Daten und der öffentliche Schlüssel des Chips digital signiert. Die Authentizität der Signatur wird über die Dokumenten-PKI[35] nachgewiesen, die in zwei Stufen gegliedert ist:

- Country Signing Certification Authority (CSCA), Wurzelinstanz betrieben von der BSI
- Document Signer (DS), betrieben von dem Ausweishersteller

Die Zertifikate der Wurzelinstanz sind vom BSI erhältlich und das DS-Zertifikat ist auf dem Chip des nPAs gespeichert.

Um die Daten mit der passiven Authentifizierung zu verifizieren führt ein Terminal folgende Schritte[36] aus:

1. Das Terminal liest die EF-SOD-Datei aus der Biometrieanwendung, die die Hashwerte der Datengruppen DG1, DG2, DG3, eine Signatur über diese Hashwerte und das DS-Zertifikat enthält.
2. Es sucht die zugehörigen Zertifikate (CSCA-Zertifikat und DS-Zertifikat) und prüft sektorindividuelle Rückruflisten.
3. Das DS-Zertifikat und die Signatur über die Hashwerte in EF-SOD werden verifiziert.
4. Das Terminal liest relevante Datengruppen, berechnet deren Hashwerte und vergleicht sie mit denen in der EF-SOD-Datei.

Die passive Authentifizierung erkennt nachträgliche Veränderungen der Datengruppen des nPAs, weist jedoch nicht die Echtheit des Chips nach. Dazu muss zusätzlich zur passiven Authentisierung die CA durchgeführt werden.

[34] [BSI TR-03110]
[35] [ICAO Doc 9303] Part 1 und Part 3
[36] [BSI TR-03110] Teil 1, S.6

4.5 Chipauthentisierung

Mit der Chipauthentisierung[37] weist der Chip nach, dass er den privaten Schlüssel besitzt, der zum öffentlichen Schlüssel in der EF.CardSecurity im Master File passt.[38] Dadurch wird, in Verbindung mit der passiven Authentisierung, die Echtheit des Chips und der auf dem Chip gespeicherten Daten nachgewiesen. Außerdem wird durch die CA ein neuer Secure-Messaging-Kanal zwischen dem Chip und dem Dienstanbieter aufgebaut. Bei der CA handelt es sich um ein Diffie-Hellmann-Protokoll.

Protokollablauf

Für die CA werden die folgenden Schritte[39] vom Chip des nPAs und dem Terminal ausgeführt (Tabelle 6). Das in der CA verwendete flüchtige Schlüsselpaar des Terminals ($\widetilde{SK_{PCD}}$,$\widetilde{PK_{PCD}}$, D_{PICC}) wurde vorher während der TA generiert.

Chip (PICC)		**Terminal (PCD)**
statisches Schlüsselpaar (SK_{PICC},PK_{PICC},D_{PICC})	$\xrightarrow{PK_{PICC}, D_{PICC}}$	
	$\xleftarrow{\widetilde{PK_{PCD}}}$	
K=KA(SK_{PICC},$\widetilde{PK_{PCD}}$,D_{PICC})		K=KA($\widetilde{SK_{PCD}}$,PK_{PICC},D_{PICC})
r_{PICC} zufällig		
[T_{PICC}=MAC(K_{MAC},$\widetilde{PK_{PCD}}$)]	$\xrightarrow{T_{PICC}, r_{PICC}}$	Verifiziere(r_{PICC})

Tabelle 6: vereinfachte Darstellung von den CA Protokoll

1. Der Ausweis sendet seinen statischen öffentlichen Diffie-Hellmann-Schlüssel PK_{PICC} und die Domainparameter D_{PICC} an das Terminal.
2. Das Terminal sendet seinen flüchtigen öffentlichen Schlüssel $\widetilde{PK_{PCD}}$ zum Chip des nPAs.
3. Der Ausweis komprimiert den öffentlichen Schlüssel des Terminals zu Comp($\widetilde{PK_{PCD}}$) und vergleicht ihn mit dem während der TA übertragenen komprimierten öffentlichen Schlüssel.

[37] [BSI TR-03110] Teil 2, S.18
[38] [BSI TR-03127], S.10
[39] [BSI TR-03110] Part 2, S.19

4. Das Terminal und der nPA berechnen das gemeinsame Geheimnis: K=KA(SK_{PICC},$\widetilde{PK_{PCD}}$,D_{PICC})=KA($\widetilde{SK_{PCD}}$,PK_{PICC},D_{PICC})

5. Der nPA leitet aus einer zufällig erzeugten Nonce r_{PICC} und dem gemeinsamen Geheimnis K die Sitzungsschlüssel K_{MAC}=KDF_{MAC}(K,r_{PICC}) und K_{ENC}=KDF_{ENC}(K,r_{PICC}) für Secure Messaging ab und sendet r_{PICC} und den Authentifizierungstoken T_{PICC}=MAC(K_{MAC},$\widetilde{PK_{PCD}}$) an das Terminal.

6. Das Terminal berechnet ebenfalls die Schlüssel K_{MAC}=KDF_{MAC}(K,r_{PICC}) und K_{ENC}=KDF_{ENC}(K,r_{PICC}) für das Secure Messaging aus K und r_{PICC} und verifiziert den Authentifizierungstoken T_{PICC}.

Die Authentizität von PK_{PICC} hat das Terminal vorher mittels dem Verfahren passive Authentifizierung verifiziert. Nachdem die CA erfolgreich durchgeführt wurde, werden die in der CA etablierten Schlüssel K_{MAC} und K_{ENC} zur Initialisierung eines neuen Secure-Messaging-Kanals verwendet und die in PACE ausgehandelten Sitzungsschlüssel werden ungültig. Erst jetzt kann das Terminal gemäß der vergebenen Zugriffsrechte auf den nPA zugreifen.

5 Passwörter

Um die elektronischen Funktionen des nPAsverwenden zu können, muss sich der Benutzer vorab mit einem Passwort authentisieren. Dieses ist abhängig von der Anwendung und den benötigten Berechtigungen. Für die Authentifizierung sind die folgenden Passwörter vorgesehen[40]

5.1 CAN-Card Access Number

Die Card Access Number ist eine sechsstellige, zufällige Dezimalzahl, die sichtbar rechts unten auf der Vorderseite des Ausweises aufgedruckt ist. Sie hat keine Bindung an den Besitzer und kann nicht aus anderen personen- oder dokumentenbezogenen Daten berechnet werden. Auch eine dynamische Generierung der CAN auf dem Dokument ist erlaubt.[41] Die falsche Eingabe der CAN kann nicht

[40] [BSI TR-03127], S.17 und S.18
[41] [BSI TR-03110] 2.1, S.10

zur Sperrung des Ausweises führen.

Die CAN wird verwendet, wenn ein sicherer Kanal ohne Authentifizierung des Ausweisinhabers zwischen Terminal und nPA benötigt wird:

- Hoheitliche Kontrollen (z.B. Grenz- oder Personenkontrolle)
- Änderungsdienst/Visualisierung in der Ausweisbehörde
- Verbindungsaufbau zur Signaturanwendung
- Freischalten des dritten Eingabeversuchs der eID-PIN

5.2 MRZ-maschienenlesbare Zone

Die maschinenlesbare Zone kann an hoheitlichen Terminals alternativ zur CAN als Passwort für PACE verwendet werden, um bereits vorhandene Durchzugsleser für den elektronischen Reisepass auch mit dem nPA nutzen zu können. Die dreizeilige MRZ befindet sich unten auf der Rückseite des nPAs.

5.3 eID-PIN

Die eID-PIN ist ein sechsstelliges in der Regel dezimales Passwort, das nur dem Ausweisinhaber bekannt sein soll. Dieser authentisiert[42] sich mit der eID-PIN, um die eID-Funktion des nPAs freizuschalten und damit die auf der Anwendung gespeicherten Daten auch im nicht hoheitlichen Kontext preiszugeben.

Der Ausweis wird zunächst mit einer zufällig erzeugten, fünfstelligen Transport-PIN ausgeliefert, die dem Inhaber nach dem Erhalt des nPAs durch den PIN-Brief mitgeteilt wird.[43] Diese Transport-PIN kann noch nicht zum Authentifizieren des Nutzers verwendet werden, sondern wird durch den Inhaber auf eine operationelle, nur ihm bekannte, sechsstellige eID-PIN geändert[44].

Das Erraten der eID-PIN durch Ausprobieren soll durch einen Fehlbedienungszähler (FBZ) auf dem Chip verhindert werden. Die Anzahl der Fehlversuche ist auf drei begrenzt. Nach der dritten falschen Eingabe der eID-Pin, sperrt der nPA die eID-Funktion, bis die eID-PIN mit dem PUK freigeschaltet wird. Da

[42] Authentifizierung durch Besitz und Wissen
[43] [BSI TR-03127], S. 33
[44] [BSI TR-03127], S. 33

die Gefahr eines Denial-of-Service-Angriffs über die kontaktlose Schnittstelle besteht, muss die auf dem nPA aufgedruckte CAN zunächst erfolgreich eingegeben werden, um den dritten Eingabeversuch der eID-PIN freizuschalten. Nach jeder erfolgreichen Eingabe der eID-PIN wird der FBZ auf Null zurückgesetzt. Dieser Ablauf ist in Abbildung 3 dargestellt. Nach der Eingabe der eID-PIN in entsprechender Client-Software kann sie gewechselt werden.[45] Es besteht jedoch auch die Möglichkeit, die eID-PIN in einer Ausweisbehörde neu zu setzen, falls man sie vergessen hat. Dazu sind (bestimmte) Terminals mit dem Recht der Neusetzung der eID-PIN ausgestattet und weisen diesen Recht bei der Terminalauthentifizierung nach[46].

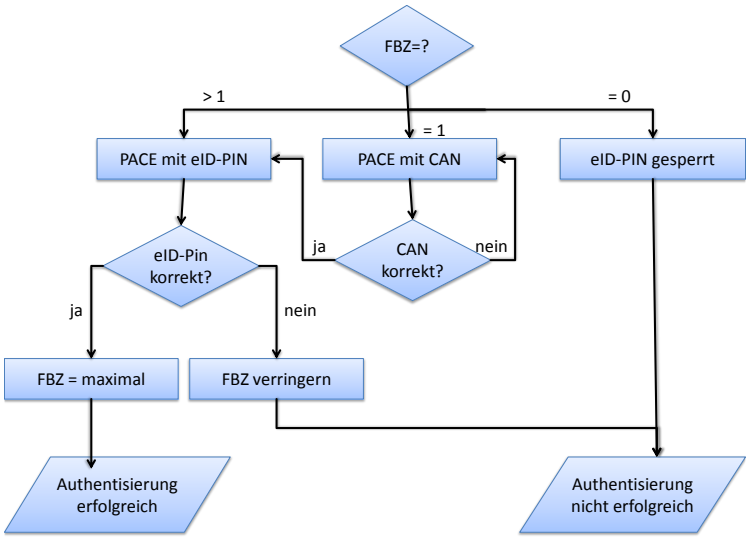

Abbildung 3: Eingabe der eID-PIN (Quelle: [BSI TR-03127])

5.4 Signatur-PIN

Die auf dem Chip des nPAs gespeicherte, sechsstellige dezimale Signatur-PIN dient zum Erzeugen qualifizierter elektronischer Signaturen[47] (Signaturanwendung des nPAs). Die Signatur-PIN muss erst durch den Inhaber gesetzt werden und ist bei der Auslieferung des Ausweises noch nicht auf den nPA gespeichert. Der Fehlbedienungszähler der Signatur-PIN sperrt die PIN nach drei Fehleingaben. Um die Signatur-PIN neu zu setzen, reicht die Eingabe der aktuellen Signatur-PIN. Falls noch keine qualifizierte elektronische Signatur vorhanden ist

[45] [BSI TR-03127], S.24
[46] [BSI TR-03127], S.35
[47] [BSI TR-03117]

oder diese terminiert ist, kann nach der Authentisierung als bestätigtes Signaturterminal[48] mit dem Recht "generate qualified electronic signature" ebenfalls die Signatur-PIN neu gesetzt werden.

5.5 PUK - Pin Unblocking Key

Die PUK ist eine zehnstellige, zufällig erzeugte Dezimalzahl, die ebenfalls mit dem PIN-Brief an den Auweisinhaber geschickt wird. Nach dreimaliger Falscheingabe wird sowohl die eID-PIN als auch die Signatur-PIN gesperrt. Beide können mit der PUK jeweils maximal zehn mal entsperrt werden. Dabei wird der jeweilige Rücksetzzähler runter gezählt.

6 Terminals

Der Zugriff zum Auslesen der Daten des Ausweises kann durch vier verschiedene Terminaltypen[49] erfolgen. Dabei werden im Allgemeinen die Schritte[50] aus Tabelle 7 durchgeführt.

6.1 Inspektionssysteme

Hoheitliche Stellen können Inspektionssysteme zur Kontrolle der Ausweisdaten, z.B. für eine Grenzkontrolle, verwenden. Ein Inspektionssystem kann nur verwendet werden, um die in der Biometriefunktion gespeicherten MRZ-Daten (Datengruppe1), das Lichtbild (Datengruppe2), die Fingerabdrücke (Datengruppe 3) und die Daten der eID-Funktion zu lesen. Ein Inspektionssystem kann keinen Schreibzugriff auf den Chip oder Zugriff auf die Signaturanwendung besitzen.

6.2 Authentisierungsterminal

Ein Authentifizierungsterminal ist berechtigt, Teile der in der eID-Anwendung gespeicherten Daten und Funktionen zu nutzen. Durch Rechte, die während der Authentisierung vergeben werden, wird festgelegt, auf welche Daten der

[48] Kapitel 6
[49] [BSI TR-03127], S.21-S.24
[50] [BSI TR-03127], S.20

Chip	Terminal
Lesen der Datei EF.CardAccess	
	Eingabe/Lesen PACE-Passwort (eID-PIN/CAN/MRZ)
PACE	
Übertragen der Zertifikatskette Terminalauthentisierung	
Lesen der Datei EF.CardSecurity	
	Passive Authentisierung EF.CardSecurity
Chipauthentisierung	
Authentisierungsterminal (optional): Abfrage der Dokumentengültigkeit Authentisierungsterminal (optional): Lesen des Sperrmerkmals	
	Authentisierungsterminal (optional): Sperrlistenabfrage – nur möglich, wenn Ausweis noch gültig
Inspektionssystem: Lesen des EF.SOD	
	Inspektionssystem: Prüfen der Signatur der Datei EF.SOD (Passive Authentisierung)
Optional: Auslesen der freigegebenen Daten Ausüben der speziellen Rechte	
	Inspektionssystem: Vergleichen der Hashwerte der ausgelesenen Datengruppen mit den in der Datei EF.SOD gespeicherten Werten

Tabelle 7: Zugriff auf die Daten des nPAs (Quelle: [BSI TR-03127], S.20)

Zugriff beschränkt wird.

Vor dem Lesen der Daten durch das Authentifizierungsterminal kann überprüft werden, ob der Ausweis gültig ist (d.h. der Ausweis nicht abgelaufen ist oder z.B. als gestohlen gemeldet wurde). Dafür können die Funktionen Abfrage der Dokumentengültigkeit und Lesen des Sperrmerkmals[51] verwendet werden.

6.2.1 Online-Authentifizierung

Ein Spezialfall eines Zugriffs durch ein Authentisierungsterminal ist die Online-Authentifizierung[52] (Authentifizierung gegenüber einem Dienstanbieter). Das

[51] [BSI TR-03110]
[52] [BSI TR-03127], S. 25

Authentisierungsterminal ist dabei nicht zwingend örtlich zusammenhängend, sondern besteht aus einem lokalen Terminal, das aus Lesegerät und lokalem Rechner besteht, und dem entfernten Terminal (der Dienstanbieter). Damit die Online-Authentifizierung stattfinden kann, muss zwischen dem lokalen und dem entfernten Terminal eine Verbindung bestehen.

<table>
<tr><th>Chip</th><th>Lokales Terminal</th><th>Dienstanbieter</th></tr>
<tr><td></td><td colspan="2">Übertragen des Dienstanbieterzertifikats</td></tr>
<tr><td></td><td>Präsentation des Zertifikats
Einschränken der Zugriffsrechte durch Benutzer
Eingabe der eID-PIN</td><td></td></tr>
<tr><td colspan="2">Lesen der Datei EF.CardAccess
PACE mit eID-PIN als Passwort</td><td></td></tr>
<tr><td colspan="3">Übertragen der vollständigen Zertifikatskette
Terminalauthentisierung</td></tr>
<tr><td colspan="3">Lesen der Datei EF.CardSecurity</td></tr>
<tr><td></td><td></td><td>Passive
Authentisierung</td></tr>
<tr><td colspan="3">Chipauthentisierung</td></tr>
<tr><td colspan="3">Lesen des Sperrmerkmals,
Abfrage der Dokumentengültigkeit</td></tr>
<tr><td></td><td></td><td>Sperrlistenabfrage</td></tr>
<tr><td colspan="3">Auslesen der freigegebenen Daten,
Ausüben der speziellen Rechte</td></tr>
</table>

Tabelle 8: Schritte der Online-Authentisierung (Quelle: [BSI TR-03127], S. 25)

Eine Online-Authentifizierung besteht aus den in Tabelle 8 dargestellten Schritten. Das lokale Terminal präsentiert dem Benutzer das Zertifikat des Dienstanbieters, Informationen über den Dienstanbieter und den Verwendungszweck der Kommunikation im zweiten Schritt der Online-Authentifizierung. Die folgenden Daten müssen angezeigt werden:

- Name des Dienstanbieters
- erwünschte Zugriffsrechte

Auf Aufforderung des Benutzers müssen weiterhin angezeigt werden:

- Zweck der Datenübermittlung
- Anschrift und Email-Adresse des Dienstanbieters

- Hinweis auf die zuständige Datenschutzbehörde
- Gültigkeitszeitraum des Zertifikats

Die vom Dienstanbieter verlangten Zugriffsrechte können durch den Benutzer eingeschränkt werden. Zu Beginn von PACE werden die eigeschränkten Rechte an den Chip übertragen. Nach PACE wird die Kommunikation zwischen Chip und lokalen Terminal vertraulich und integritätssicher ausgeführt. Nach erfolgreicher Chipauthentifizierung wird ein gesicherter Kanal zwischen Chip und Dienstanbieter aufgebaut.

Die Umsetzung der Online-Authentisierung ist schematisch in Abbildung 4 dargestellt.

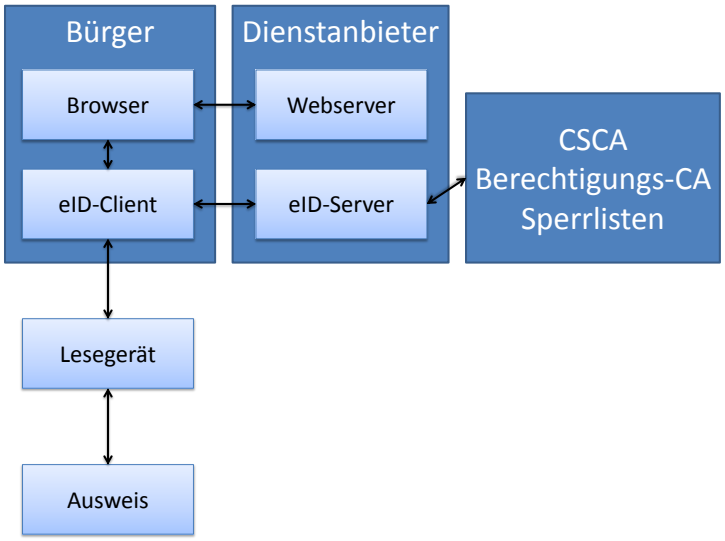

Abbildung 4: Kommunikationsbeziehungen der Online-Authentisierung (Quelle: [BSI TR-03127], S.25)

6.3 Bestätigtes Signaturterminal

Mit der CAN als Passwort kann ein bestätigtes Signaturterminal verwendet werden, um eine qualifizierte Signatur zu löschen oder eine neue Signatur-PIN zu setzen. Wird die eID-PIN als PACE-Passwort benutzt, kann eine Signatur-PIN und das Signatur-Schlüsselpaar gelöscht werden.[53]

[53] [BSI TR-03117]

6.4 Nicht authentisiertes Terminal

Der Ausweisinhaber kann für administrative Zwecke (z.B. das Zurücksetzen eines Fehlbedienungszählers), Ändern der eID-PIN nicht authentisierte Terminals verwenden. Dabei wird beim Verbindungsaufbau mit PACE kein Certificate Holder Authorization Template (CHAT) übergeben und es werden keine Terminal- und Chipauthentifizierung durchgeführt.

Terminaltyp		**PACE-Passwort**	**Mögliche Terminalrechte**
Inspektionssystem (hoheitlich national bzw. hoheitlich ausländisch)	General Authentication Procedure	CAN; MRZ	• Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild) der Biometrieanwendung • Lesezugriff auf DG3 (Fingerabdrücke) der Biometrieanwendung und Daten der eID-Anwendung je nach nachgewiesenen Rechten
	Nur eAT: Standard ePassport Inspection Procedure	CAN; MRZ	Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild) der Biometrieanwendung
	Nur eAT: Advanced ePassport Inspection Procedure	CAN; MRZ	Lesezugriff auf DG1 (MRZ), DG2 (Gesichtsbild), DG3 (Fingerabdrücke) der Biometrieanwendung
Authentisierungsterminal (hoheitlich national bzw. nicht-hoheitlich/ausländisch)		eID-PIN; CAN falls Recht CAN allowed nachgewiesen	Lese-/Schreibzugriff auf die Datengruppen der eID-Anwendung gemäß authentisierten Rechten Spezielle Rechte: • Erzeugung eines Signaturschlüsselpaares • eID-PIN setzen, eID-Anwendung An-/Ausschalten • Pseudonym • Altersverifikation • Wohnortabfrage
Bestätigtes Signaturterminal		CAN	• Erzeugung qualifizierter Signaturen mitzusätzlicher Eingabe der Signatur-PIN • Setzen einer neuen Signatur-PIN mit zusätzlicher Eingabe der alten Signatur-PIN
		eID-PIN	• Anlegen der Signatur-PIN • Terminieren des Schlüssels für qualifizierte Signaturen und der Signatur-PIN
Nicht authentisiertes Terminal		eID-PIN	Setzen einer neuen eID-PIN
		PUK	Zurücksetzen der Fehlbedienungszähler von eID-PIN/Signatur-PIN

Tabelle 9: Übersicht über die Terminaltypen (Quelle: [BSI TR-03127], S. 21)

7 Kartenleser nach [BSI TR-03119]

Damit der Ausweisinhaber einen Missbrauch des nPAs ausschließen kann, werden von der BSI zertifizierte Kartenleser nach [BSI TR-03119] zur Kommunikation mit dem Chip des nPAs vorgeschlagen. Um die Dateien des nPAs zu schützen und Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen, wurden hohe Anforderungen an diese Leser gestellt.

Nach [BSI TR-03119] sind die wichtigsten Anforderungen an einen Chipkartenleser eine fehlerfreie, störungsfreie und zuverlässige Funktionsweise, sowie die Integrität der Chipkarten, weswegen detaillierte Anforderungen und weitere Funktionen nötig sind, um die Interoperabilität kontaktloser und kontaktbehafteter Chipkartenleser zu gewährleisten. Um die Integrität und Vertraulichkeit der Kommunikation sicherzustellen, muss außerdem die Informationssicherheit berücksichtigt werden.[54] Chipkartenleserhersteller können die Leser nach [BSI TR-03119] zertifizieren lassen. Für die Erteilung eines solchen Zertifikats[55] ist eine erfolgreiche Konformitätsbewertung[56] von einer unabhängigen Bewertungseinrichtung nötig. Die Zertifizierungsstelle beim BSI überwacht die Konformitätsbewertung und vergibt die Zertifikate auf der Grundlage der resultierenden Prüfberichte.

Um Smartcard-Leser bewerten und beurteilen zu können, haben alle Leser[57] die gleichen Grundeigenschaften, verfügen jedoch abhängig von der Anwendung über zusätzliche Funktionen und die dafür benötigte Hardware. In [BSI TR-03119] sind die folgenden drei Leser beschrieben.

7.1 Basisleser

Der Basisleser kann sowohl durch den Besitzer für den Heimgebrauch eingesetzt werden, als auch als ein Baustein integrierter Geräte, wie Smartphones und Notebooks, verwendet werden. Er wird für die folgenden Dienste eingesetzt:

- E-Government-Dienstleistungen wie Authentifizierungsdienst oder Rentenversicherung

[54] [BSI TR-03119], S. 5
[55] [BSI TR-03119], S. 6
[56] [BSI TR-03110], S.21-23
[57] [BSI TR-03119], S.7 und 8

Abbildung 5: Beispiel für Basisleser (unten), Standardleser (rechts) und Komfortleser (links) (Quelle http://www.reiner-sct.com/ccsdata/attImage.png?attachmentId=79491))

- Alterskontrolle
- elektronisches Kaufen von Fahrausweisen
- Identitätsnachweis und Nachweis des Wohnsitzes für Internet-Shopping

Der Basisleser unterstützt die Übertragung der Daten zwischen dem nPA und dem jeweiligen Anwendungsserver über das Internet.

7.2 Standardleser

Höheren Qualitätsanforderungen können Standardleser gerecht werden, die mindestens über ein Pinpad verfügen und damit die sichere Eingabe von Passwörtern gewährleisten.

Zusätzlich zu den Anwendungen für einen Basisleser, kann der Standardleser für die eID-Funktion im Internet mit höherer Sicherheitsanforderung verwendet werden.

7.3 Komfortleser

Aufgrund seiner Vielseitigkeit und der bequemen Nutzungsmodi kann der Komfortleser für eine Vielzahl von Anwendungen eingesetzt werden. Dieser verfügt mindestens über ein Pinpad für eine sichere Geheimzahleingabe und ein Display zur Anzeige von 2x16 alpha-numerischen Zeichen. Der Komfortleser unterstützt alle Anwendung der eID-Karte, einschließlich der qualifizierten elektronischen Signatur. Neben dem Personalausweis werden auch kontaktbehaftete klassische Signaturkarten oder Gesundheitskarten unterstützt. Die Unterstützung für Bankanwendungen oder andere Anwendungen ist ebenfalls möglich.

Während die Basisgeräte die kostengünstige Variante für die Anwendung mit eingeschränkter Sicherheitsstufe für Heimnutzer darstellen, sind die Standard- und Komfortleser darüber hinaus für Anwendungen mit erweiterten Sicherheitsfunktionen ausgelegt. Die Tabelle 9 gibt eine Übersicht über die Anforderungen an die drei Lesegeräte.

	Basisleser	**Standard-leser**	**Komfort-leser**
Schnittstelle zum Host-Rechner	X	X	X
kontaktlose Schnittstelle ([ISO/IEC 14443])	X	X	X
kontaktbehaftete Schnittstelle [ISO 7816])	O	O	X
PIN-Pad (sichere PIN-Eingabe) mit PACE-Unterstützung	O	X	X
Display (mindestens 2x16 alphanumerische Zeichen)	O	O	X
Qualifizierte Signatur mit kontaktbehafteten Karten	O	O	X
Qualifizierte Signatur mit kontaktlosen Karten [BSI TR-03117]) (z.B. nPA)	O	O	X
Firmwareupdate	O	X	X
X = verpflichtend O = optional			

Tabelle 10: Übersicht der Chipkartenleser-Kategorien (Quelle: [BSI TR-03119], S.7)

8 RFID und NFC

Eine Technologie zur kontaktlosen Identifizierung ist die Radio Frequency Identification (RFID). RFID-Systeme bestehen aus zwei Komponenten: einem Transponder (auch als Tag bezeichnet) und einem Lesegerät. Der Transponder

wird in ein Objekt integriert (z.B. in einer Chipkarte) und fungiert als ein Datenträger, auf dem eine Identifikationsnummer und weitere Daten über den Transponder und das Objekt, mit dem er verbunden ist, gespeichert sind. Der Transponder kann kontaktlos über eine Funktechnologie gelesen werden. Das Lesegerät dient zum Auslesen und Schreiben von Daten auf dem Transponder.

RFID-Geräte unterscheiden sich stark in den verwendeten Frequenzbereichen und der Sendestärke der Lesegeräte[58]. BSI unterteilt die daraus resultierenden Transpondertypen auf die in der Tabelle 11 aufgeführten Kategorien.

Parameter	**Niedrig-frequenz**	**Hoch-frequenz**	**Ultrahoch-frequenz**	**Mikrowelle**
Frequenz	125 – 134 kHz	13,56 MHz	868 bzw. 915 MHz	2,45 bzw. 5,8 GHz
Leseabstand	bis 1,2 m	bis 1,2 m	bis 4 m	bis zu 15 m (in Einzelfällen bis zu 1 km)
Lesege-schwindigkeit	langsam	je nach ISO-Standard*	schnell	sehr schnell (aktive Transponder)
Heutige ISO-Standards	11784/85 und 14223	14443, 15693 und 18000	14443, 15693 und 18000	18000
Beispielhafte Anwendungen	Zutrittskontrolle, Routenkontrolle, Wegfahrsperren, Wäschereinigung, Gasablesungß	Wäschereinigung, Asset Management, Ticketing, Tracking und Tracing, Pulkerfassung	Palettenerfassung, Container-Tracking	Straßenmaut, Container-Tracking
unter 1 s bis 5 s bei ISO 14443 (5 s für 32 kByte), mittel (0,5 m/s Vorbeibewegung bei ISO 15693)				

Tabelle 11: Kenngrößen von RFID Technologien (Quelle: [RFID-Systeme], S.25)

Weiterhin unterscheiden sich die Transponder durch ihre Energieversorgung und Datenübertragung. Man unterscheidet zwischen aktiven und passiven Transpondern, sowie deren Mischformen. Aktive Tags verfügen über eine eigene Energiequelle (z.B. eine Batterie). Dagegen werden passive Tags durch die Lesegeräte über Funkwellen mit Energie versorgt.

Die ISO übernimmt die Aufgabe der internationalen Normierung und legt z.B. Standards für Frequenzen, Übertragungsgeschwindigkeiten und Kodierungen fest. So ist im [ISO/IEC 14443] der Standard, auf dem viele kontaktlose Smartcards und auch der nPA basieren, definiert. Im [ISO 7816] Part 4 ist ein Anwendungsprotokoll zum Kommunizieren mit Smartcards beschrieben.

Near Field Communication[59] (NFC) ist ein Standard zur kontaktlosen Da-

[58] [RFID-Systeme]
[59] [ECMA 340]

tenübertragung über eine Entfernung von bis zu 10 cm per Funk, der mit [ISO/IEC 14443]-4 weitgehend kompatibel ist. Smartphones die über NFC-Technologie verfügen, können in der Lage sein mit kontaktlosen Smartcards (z.B. mit dem nPA) zu kommunizieren.

9 Kommunikationsprotokoll nach [ISO 7816]

Die im Rahmen dieser Arbeit entwickelte Android-App wickelt die Kommunikation mit dem nPA nach [ISO 7816] ab. Bei diesem Request-Response-Protokoll findet die Kommunikation zwischen den beteiligten Parteien über Kommunikationseinheiten, die sogenannten Application Protocol Data Units (APDUs), statt. Das Smartphone, auf dem die App ausgeführt wird, steuert dabei die Kommunikation. Es sendet Command APDUs an den Chip des nPA. Dieser arbeitet den Befehl ab und antwortet auf jeder Command APDU mit einer Response APDU.

9.1 Command APDU

Eine Command APDU (Tabelle 12) besteht aus einem 2 Byte langen Header und einem optionalen Body mit variabler Länger.

Header				**Body**		
CLA	INS	P1	P2	Lc	Data field	Le

Tabelle 12: Aufbau einer Command APDU (Quelle: [ISO 7816]-4)

Das Class Byte (CLA) gibt die Befehlsklasse der APDU an und signalisiert mit den ersten beiden Bits ob Secure Messaging aktiv ist. Der Instruction Code (INS) ist der Befehl, welcher durch den nPA ausgeführt werden soll. P1 und P2 sind Parameter des Befehls. Die Anzahl der Bytes aus dem Data Field wird in Lc notiert. Le ist die maximale Anzahl der Bytes im Datenfeld aus der erwarteten Response APDU. Wenn die Le Null ist, ist damit die maximale Anzahl an Datenbytes gemeint. Der nPA unterstützt erweiterte Lc- und Le-Felder und ermöglicht damit, dass mehr als 256 Byte lange Datenfelder (extended length APDUs) übertragen werden können.

9.2 Response APDU

Response APDUs bestehen aus einem optionalen Body variabler Länger und einem 2 Byte langen Trailer.

Body	**Trailer**	
Data field	SW1	SW2

Tabelle 13: Aufbau einer Response APDU (Quelle: [ISO 7816]-4)

Der Trailer kodiert den Status des nPAs nachdem der Befehl der Command APDU ausgeführt wurde. Der Code "0x9000" bedeutet hierbei, dass der Befehl erfolgreich abgearbeitet wurde.

10 Problem: Ungültige Terminalzertifikate

Da der nPA keine eigene Stromversorgung besitzt und deshalb auch keine innere Uhr verwalten kann, werden Terminals, ausgenommen Signaturterminals, mit Zertifikaten ausgestattet, die eine kurze Gültigkeitsdauer besitzen. Das soll einen Missbrauch von Terminalzertifikaten begrenzen. Grundsätzlich kann ein kompromittiertes Terminal von einem nPA jedoch nicht erkannt werden. Damit eine Kontrolle der Zertifikate durch den Chip möglich ist, verwaltet der Chip ein angenähertes aktuelles Datum. Das Datum wird durch den erfolgreichen Import bestimmter[60] vorgelegter Zertifikate aktualisiert. Berücksichtigt werden:

- CVCA -und DV-Zertifikate
- Terminalzertifikate von hoheitlichen nationalen Inspektionssystemen und hoheitlichen nationalen Authentisierungsterminals

Damit der nPA die Gültigkeit des Terminals überprüfen kann, wird an dem Chip des nPAs während der TA eine Zertifikatskette, die mit einem auf dem Chip gespeicherten Vertrauensanker beginnt, übergeben. Diese Vertrauensanker sind mehr oder weniger aktuelle öffentliche Schlüssel eines vom nPA vertrautem CVCAs. Bei der Produktion des nPAs wurden ein oder mehrere Vertrauensanker sicher auf dem Chip gespeichert. Da eine CVCA ihre Schlüsselpaare über die Zeit verändert, werden CVCA -Linkzertifikate verwendet, diese werden mit dem

[60] [BSI TR-03127] Teil 3, S.28

bis zu diesem Zeitpunkt aktuellem CVCA -Schlüssel signiert. Der Chip aktualisiert die internen Vertrauensanker entsprechend dem empfangenen, gültigen Linkzertifikat.

Der nPA akzeptiert abgelaufene CVCA -Zertifikate, jedoch nicht abgelaufene DV- oder Terminalzertifikate. Um festzustellen, ob ein Zertifikat abgelaufen ist, verwendet der Chip seine aktuelle untere Grenze für das Datum. Um das aktuelle Datum anzunähern[61], verwendet der nPA das jüngste Ausstellungsdatum eines gültigen CVCA -Linkzertifikats, eines DV-Zertifikats oder eines entsprechenden Terminalzertifikats. Nur wenn der Chip der DV, die das Terminalzertifikat verwaltet, vertraut, wird das Datum durch das Terminalzertifikat aktualisiert. Ein Terminal kann ein CVCA -Linkzertifikat, ein DV-Zertifikat oder ein Terminalzertifikat an den Chip senden, um die innere aktuelle Zeit und den Vertrauensanker des Chips zu aktualisieren, ohne die TA fortzusetzen. D.h. das Terminal muss nicht nachweisen, dass es den passenden privaten Schlüssel besitzt, um die Zeit des nPAs zu aktualisieren. Um festzustellen ob ein Zertifikat abgelaufen ist, vergleicht der nPA nur das Ausstellungsdatum des Zertifikats mit seiner eigenen unteren Grenze für das Datum und prüft die Gültigkeit des Zertifikats. Wenn ein Ausweis also lange nicht benutzt wurde und die untere Grenze für das Datum im Chip des nPAs bereits sehr alt ist, können komprimierte Terminals die auf dem nPA gespeicherten Dateien lesen, schreiben und sogar Signaturen mit dem Ausweis erstellen, obwohl der Außenwelt bereits länger bekannt ist, dass diese Terminals unsicher geworden sind.

Um eine Zeitaktualisierung durchzuführen, wird nur eine entsprechende Zertifikatskette, jedoch nicht ihr privater Schlüssel benötigt. Deswegen kann mithilfe eines vertrauenswürdigen Geräts eine Aktualisierung des inneren Datums durchgeführt werden, wenn man über entsprechende Zertifikate verfügt.

11 Zeitaktualisierungsdienst

Der Zeitaktualisierungsdienst[62] soll die auf dem Chip des Ausweises gespeicherte untere Grenze für das Datum aktualisieren, damit alte, abgelaufene Zertifikate vom nPA erkannt und nicht mehr akzeptiert werden.

[61] [BSI TR-03127] Teil 3, S.29
[62] [Mobiler Chipkartenleser]

Da noch kein offizieller Zeitaktualisierungsdienst existiert, wird anhand dieser Arbeit eine Android-App vorgestellt, die die untere Grenze für das Datum des nPAs aktualisiert. Um dies zu ermöglichen, übergibt die App hoheitliche Zertifikate an den Chip des nPAs. Solche Zertifikate, insbesondere deren private Schlüssel, sind nicht öffentlich zugänglich. Es kann jedoch auch eine Zertifikatskette aus einer unsicheren Quelle an den nPA übergeben werden, ohne im Besitz des dazugehörigen privaten Terminalschlüssels zu sein. Diese Zertifikatskette wird während der TA, noch bevor das Terminal nachweist, dass es im Besitz des privaten Schlüssels ist, übergeben und validiert. Die untere Grenze für das Datum wird auf dem nPA nur aktualisiert, wenn die Zertifikatskette hoheitlich ist und auf einem Vertrauensanker des Ausweises aufsetzt.

Um ein Zeitupdate durchführen zu können, werden vom Terminal keine besonderen Rechte benötigt. Das PACE-Protokoll kann mit allen für PACE zulässigen Passwörtern, insbesondere mit der CAN aufgebaut werden. Die in der Arbeit betrachtete App führt PACE mit der CAN durch.

Es existieren bereits einige Apps, die mit dem Personalausweis kommunizieren können sollen. Manche befinden sich noch im Entwicklungsstatus. Einige Beispiele sind die PersoApp, die vom Darmstädter Forschungsinstitut CASED entwickelt wird, das Open-eID-Projekt vom Frauenhofer FOKUS-Institut, sowie die Open-eCard-App und Androsmex. In dieser Arbeit wird auf Androsmex aufgesetzt. Bevor wir Androsmex betrachten, wird erklärt wie bei unserem Versuchsaufbau die Zertifikatskette beschafft wurde.

11.1 Herunterladen der Zertifikatskette

Wie bereits erwähnt werden keine offiziellen Quellen zum Herunterladen einer hoheitlichen Zertifikatskette angeboten. In dieser Arbeit wird eine Möglichkeit beschrieben, um an hoheitliche Zertifikate[63] zu gelangen.

Für unsere Versuchsdurchführung wurden ein nPA, ein Standardleser, die AusweisApp2 , USBPcap und Wireshark verwendet. Um eine Zertifikatskette herunterzuladen, wurde der Dienst der Ausweis Auskunft des Bundes[64] verwendet. Während die Zertifikatskette an den Standardleser (mit dem nPA) geschickt

[63] Den privaten Schlüssel der Zertifikatskette erhält der Benutzer nicht auf diesem Weg. Dieser wird jedoch nicht für unseren Zweck benötigt.
[64] [Selbstauskunft]

wurde, wurde der Datenverkehr zu dem Standardleser mit USBPcap[65] in einer Pcap-Datei aufgezeichnet. Anschließend wurde diese Dabei verwendet, um die Zertifikatskette zu extrahieren. Auf diese Weise wird die Zertifikatskette abgefangen, bevor sie in Secure Messaging durch den Standardleser verschlüsselt an den nPA übertragen wurde. Abbildung 6 zeigt eine Pcap-Datei aus unserer Versuchsdurchführung. In Abbildung 6 ist unten die erste APDU markiert, die während der TA an den nPA geschickt wurde.

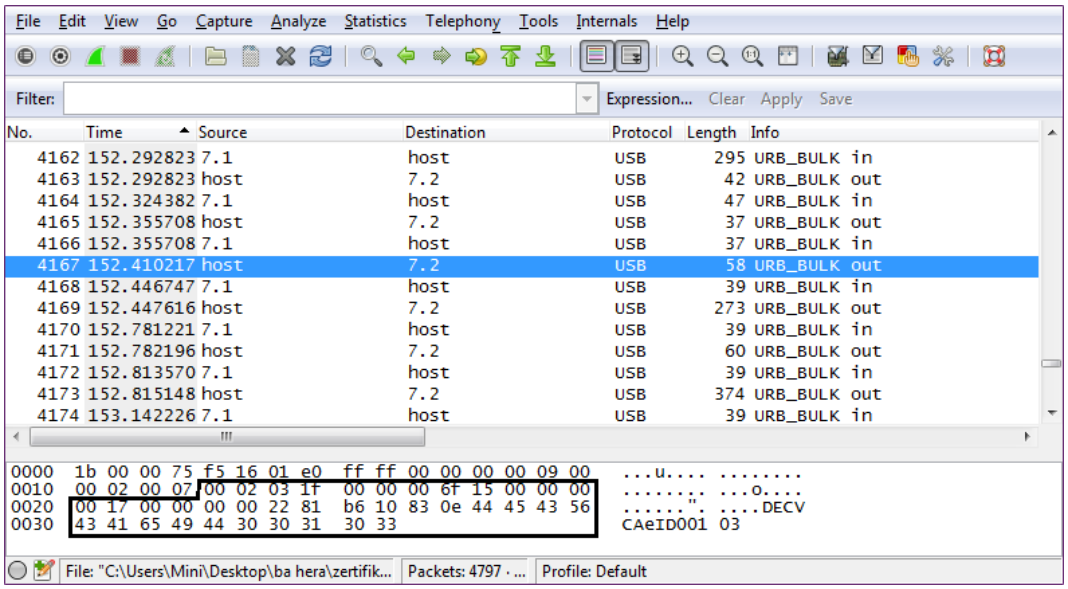

Abbildung 6: Ausschnitt einer Pcap-Datei die eine Zertifikatskette enthält

Aus dieser Pcap-Datei haben wir die folgenden APDUs extrahiert, die während der TA geschickt werden müssen, um die Zertifikatskette zu übertragen.

Mit dieser APDU überträgt das Terminal sein DVZertifikat an den nPA:

002a00bee77f4e81a05f290100420e4445435643416549443030313033 7f494f0

60a04007f000702020202038641041f27ad823f8ad678dc9b5b5c11f8fffac5c6e

fd4517a6a4dc394de52547fc8bb31bf485816b3b3c157f7500ad60eb7e034a88e

164dadb1ee7210284071a456425f20104445445665494444505354303030333

37f4c12060904007f000703010202530540051 3ff875f25060104010101075f240

60105000201055f3740076661078637bbbd2dcde9260598dfac72d58d72743de

b2677a99193de94c3b6907110cf4bfc4d1c5b5dd77b72116d9297c67c351fe78

[65] [Anleitung: USBPcap]

fcc8ee25c1f1c500b95

Und wiederum mit dieser APDU überträgt das Terminal seinen öffentlichen Schlüssel an den nPA:

002281b6128310444544566549444450535430303033333

Mit dieser APDU überträgt das Terminal den Rest der Zertifikatskette an den nPA:

002a00be00014a7f4e8201025f2901004210444544566549444450535430303033

337f494f060a04007f000702020202038641049636 0c557ed7e67db285ff5055c74c

7ebb3b5ad6614b2a57159ec2e339148bf6a64ad215fdc69491171a9e8a316548b4

4e477fb65902d9e017b127848f9512415f20104445474f5653454c42535430303136

307f4c12060904007f000703010202530500051 3fb045f25060104010200055f2406

010401020006655e732d060904007f000703010301802091732d82e0877be9ac8d9

49ebf0615b1288fcf4c06220ee49ce0c1b862887482732d060904007f000703010302

80205104bf997c7f95f1e538a9d8cd27353ae0c36dea5cba541a2ac3b462c032e8f05

f3740286a35dcc3ca4222ec9c3d0326b6227e673dc2b3d7f3ef8d33b8a7a21ee3128

b6a0765f21c897d8bfbbb3e107e6629cd9c973f1fd56ed59a55729782137778cf

Eine so gewonnene Zertifikatskette kann an einen anderen nPA übertragen werden und löst eine Aktualisierung der unteren Grenze für das Datum auf dem nPA aus, falls sie mit einem Vertrauensanker des nPAs startet und aktueller ist als das auf seinem Chip gespeicherte Datum.

11.2 Androsmex

Androsmex ist eine Android-App, die das PACE-Protokoll implementiert. Die Kommunikation wird per NFC durchgeführt. Wenn ein Nutzer Androsmex aufruft, sieht er die in Abbildung 7 (links) abgebildeten Elemente. Hier wurde noch kein Ausweis erkannt. Wenn das Smartphone einen Ausweis erkennt und diese Information an Androsmex weiterleitet, erscheint im grauen Bereich

der App eine Tag-ID. Nachdem der Ausweis auf RF-Level[66] erkannt wurde, kann die weitere Kommunikation in der [ISO 7816] Sicherheit erfolgen. Um PACE auszuführen, nachdem ein Ausweis erkannt wurde, muss in das erste Feld das PACE Passwort eingetragen werden und danach der Button "Start PACE" betätigt werden. Dazu kann die PIN (anfangs eingestellt) oder die CAN verwendet werden. Wenn das PACE-Passwort falsch eingegeben wurde, erscheint im grauen Feld der Text "PACE failed!" (Abbildung 7 mitte), ansonsten erscheint "PACE established!" (Abbildung 7 rechts) und der PACE-Kanal wird aufgebaut.

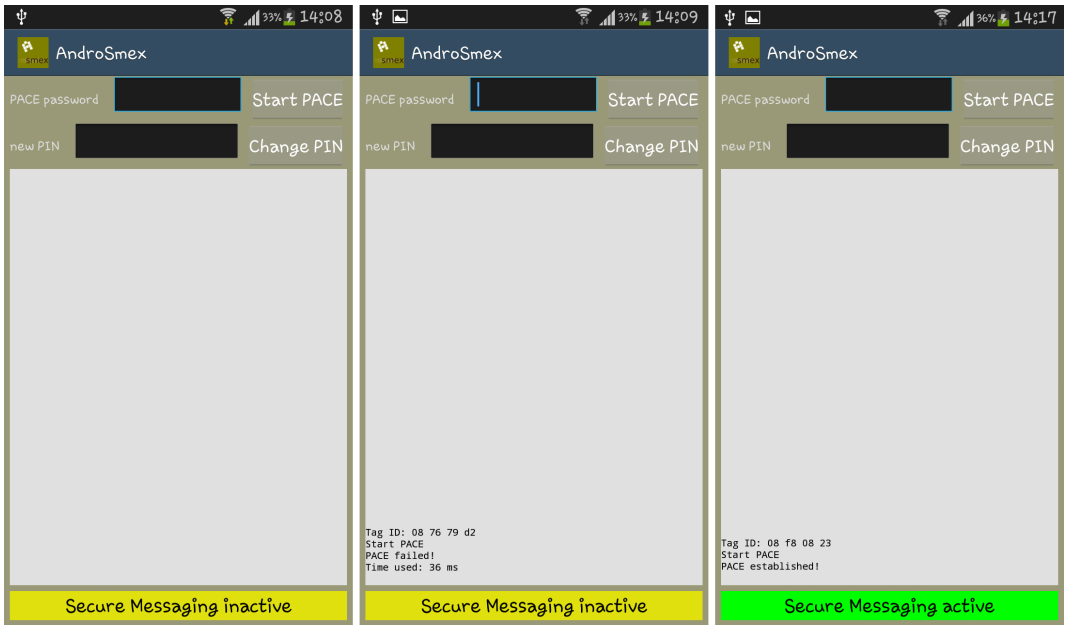

Abbildung 7: Androsmex vor PACE (links), nach fehlgeschlagenem PACE (mitte)und nach erfolgreichem PACE (rechts)

Nachdem ein sicherer PACE-Kanal über die NFC-Schnittstelle etabliert wurde, kann in das zweite Feld eine neue PIN eingegeben werden. Wenn danach der Button "Change PIN" verwendet wird, wird die PIN neu gesetzt. Diese Funktion ist für unseren Zweck irrelevant. Wir wollen direkt nachdem PACE erfolgreich durchgeführt wurde, das TA Protokoll anstoßen und eine aktuelle hoheitliche Zertifikatskette an den nPA übertragen. Da wir keine besonderen Rechte benötigen, können wir PACE mit der CAN durchführen. Die CAN soll in der App gespeichert werden können, damit der Benutzer automatisch durch das Antippen eines Buttons eine Zertifikatskette an seinen nPA übertragen kann.

Animamea ist eine Javaimplementation der Protokolle PACE, TA und CA, die auf Androsmex aufsetzt. Im Rahmen dieser Arbeit wird Animamea verwendet,

[66] [ISO/IEC 14443]

um den Anfang der TA in Androsmex zu implementieren. In dieser Arbeit wird die erweiterte Androsmex-App Androsmex2 genannt.

11.3 Androsmex2

Androsmex2 kann zusätzlich zu PACE auch TA mit dem nPA durchführen. Diese App bietet, anders als Androsmex, nicht die Möglichkeit, die eID-PIN zu ändern, da Androsmex2 nur mit der CAN verwendet werden soll.

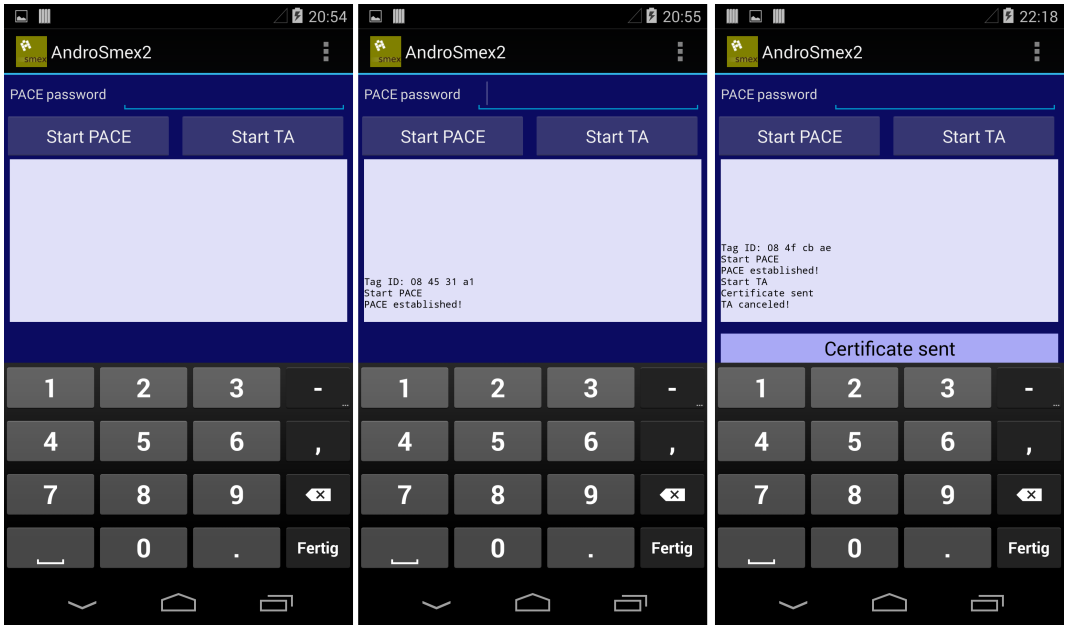

Abbildung 8: Androsmex2 vor PACE (links), nach erfolgreichem PACE (mitte)und nach abgebrochener TA (rechts)

Wird Androsmex2 aufgerufen, sieht man die in Abbildung 8 (links) abgebildeten Elemente. In dem Textfeld kann der Benutzer die CAN seines nPAs eingeben. Wenn das Smatphone einen Ausweis auf RF-Level[67] erkennt, kann "Start PACE" betätigt werden, wodurch das Smartphone PACE (mit der CAN aus dem Textfeld) mit dem nPA ausführt. Wenn die CAN falsch eingegeben wurde, erscheint im hellblauen Feld der Text "PACE failed!", ansonsten erscheint "PACE established!" (Abbildung 8 Mitte) und der PACE-Kanal wird aufgebaut. Um anschließend TA auszuführen muss der Benutzer "Start TA" betätigen. Androsmex2 sendet die Zertifikatskette an den nPA und bricht dann die TA ab (Abbildung 8 rechts). Wenn die Zertifikatskette mit einem Vertrauensanker des nPAs startet, löst sie eine Aktualisierung der unteren Grenze für das Datum auf dem nPA aus.

[67] [ISO/IEC 14443]

```
12-06 17:02:22.344: CommandAPDU (Plain)
12-06 17:02:22.344: 00 a4 02 0c 02 01 1c
12-06 17:02:22.384: ResponseAPDU (Plain)
12-06 17:02:22.384: 90 00
12-06 17:02:22.384: CommandAPDU (Plain)
12-06 17:02:22.384: 00 b0 00 00 08
12-06 17:02:22.394: ResponseAPDU (Plain)
12-06 17:02:22.394: 31 81 b3 30 0d 06 08 04 90 00
12-06 17:02:22.394: CommandAPDU (Plain)
12-06 17:02:22.394: 00 b0 00 00 b6
12-06 17:02:22.444: ResponseAPDU (Plain)
12-06 17:02:22.444: 31 81 b3 30 0d 06 08 04 00 7f 00 07 02 02 02 02
12-06 17:02:22.444: 01 02 30 12 06 0a 04 00 7f 00 07 02 02 03 02 02
12-06 17:02:22.444: 02 01 02 02 01 41 30 12 06 0a 04 00 7f 00 07 02
12-06 17:02:22.444: 02 03 02 02 02 01 02 02 01 45 30 12 06 0a 04 00
12-06 17:02:22.444: 7f 00 07 02 02 04 02 02 02 01 02 02 01 0d 30 1c
12-06 17:02:22.444: 06 09 04 00 7f 00 07 02 02 03 02 30 0c 06 07 04
12-06 17:02:22.444: 00 7f 00 07 01 02 02 01 0d 02 01 41 30 1c 06 09
12-06 17:02:22.444: 04 00 7f 00 07 02 02 03 02 30 0c 06 07 04 00 7f
12-06 17:02:22.444: 00 07 01 02 02 01 0d 02 01 45 30 2a 06 08 04 00
12-06 17:02:22.444: 7f 00 07 02 02 06 16 1e 68 74 74 70 3a 2f 2f 62
12-06 17:02:22.444: 73 69 2e 62 75 6e 64 2e 64 65 2f 63 69 66 2f 6e
12-06 17:02:22.444: 70 61 2e 78 6d 6c 90 00
12-06 17:02:22.804: Start PACE
12-06 17:02:22.804: CommandAPDU (Plain)
12-06 17:02:22.804: 00 22 c1 a4 27 80 0a 04 00 7f 00 07 02 02 04 02
12-06 17:02:22.804: 02 83 01 02 7f 4c 12 06 09 04 00 7f 00 07 03 01
12-06 17:02:22.804: 02 02 53 05 00 00 00 01 10 84 01 0d
12-06 17:02:22.874: ResponseAPDU (Plain)
12-06 17:02:22.874: 90 00
12-06 17:02:22.874: CommandAPDU (Plain)
12-06 17:02:22.874: 10 86 00 00 02 7c 00 ff
12-06 17:02:22.954: ResponseAPDU (Plain)
12-06 17:02:22.954: 7c 12 80 10 73 1a 61 eb 07 49 6f 12 b3 eb d2 76
12-06 17:02:22.954: 09 af 9c 6b 90 00
12-06 17:02:23.234: CommandAPDU (Plain)
12-06 17:02:23.234: 10 86 00 00 45 7c 43 81 41 04 8f 0b 22 9b ea 8f
12-06 17:02:23.234: c7 92 8e 5e 72 67 9b 6a 59 68 be 7b 59 aa 82 31
12-06 17:02:23.234: ce 8c 22 ef 5d d5 26 18 bf e2 5a 88 ac 8e ad 58
12-06 17:02:23.234: 2d a9 02 2b 85 b4 57 6c 4b 39 2c fc 5b e8 b4 6d
12-06 17:02:23.234: 48 4c c7 3c 1c f0 ba 36 65 d8 ff
12-06 17:02:23.594: ResponseAPDU (Plain)
12-06 17:02:23.594: 7c 43 82 41 04 4f 86 4a b0 7e d3 a5 2b 05 56 32
12-06 17:02:23.594: 3f bc 0d 17 78 11 62 56 8f 36 93 55 71 ae a6 97
12-06 17:02:23.594: ad c4 e7 70 1a 21 77 cb 4c 51 dd 21 32 7e fa d9
12-06 17:02:23.594: b6 4d 6a 08 b6 63 f3 e8 15 28 ed 82 f1 0c eb cc
12-06 17:02:23.594: 7a 93 3c d5 25 90 00
12-06 17:02:24.234: CommandAPDU (Plain)
12-06 17:02:24.234: 10 86 00 00 45 7c 43 83 41 04 8e e5 42 89 ea 55
12-06 17:02:24.234: e8 4d 5a 1d a7 74 61 a3 bd d5 88 51 93 40 f3 39
12-06 17:02:24.234: 83 17 51 44 65 36 7b 1f 4d 05 36 4e ee d1 9e 1e
12-06 17:02:24.234: 8d 57 91 6e f4 dc 5c 98 9b f2 62 8a 4f 8e 08 e9
12-06 17:02:24.234: 32 65 a8 d1 2f cc 43 19 ff 85 ff
12-06 17:02:24.534: ResponseAPDU (Plain)
12-06 17:02:24.534: 7c 43 84 41 04 35 54 81 74 2a 03 9e fc dd 85 26
12-06 17:02:24.534: 41 44 ce f4 b2 1d bc 82 ba 6a e4 0d b7 b9 82 cc
12-06 17:02:24.534: 1a 2d 08 21 21 29 80 c8 62 c2 02 67 0b dd 83 9a
12-06 17:02:24.534: 23 58 76 d7 d2 d0 96 44 6f 7e 19 0a 19 2c b6 02
12-06 17:02:24.534: 3f 88 41 d9 35 90 00
12-06 17:02:24.794: CommandAPDU (Plain)
12-06 17:02:24.794: 00 86 00 00 0c 7c 0a 85 08 6c d2 0d c5 83 d8 15
12-06 17:02:24.794: 94 ff
12-06 17:02:24.944: ResponseAPDU (Plain)
12-06 17:02:24.944: 7c 2a 86 08 cf 7f 51 a2 a9 9d 9b 93 87 0e 44 45
12-06 17:02:24.944: 43 56 43 41 65 49 44 30 30 31 30 33 88 0e 44 45
12-06 17:02:24.944: 43 56 43 41 65 49 44 30 30 31 30 32 90 00
12-06 17:02:24.944: PACE established!
12-06 17:02:25.814: Start TA
12-06 17:02:25.814: CommandAPDU (Plain)
12-06 17:02:25.814: 00 22 81 b6 10 83 0e 44 45 43 56 43 41 65 49 44
12-06 17:02:25.814: 30 30 31 30 33
12-06 17:02:25.824: CommandAPDU (SM)
12-06 17:02:25.824: 0c 22 81 b6 2d 87 21 01 65 bd a2 78 81 3f 3b 27
12-06 17:02:25.824: e7 c5 f9 36 67 3f c5 84 7b f8 f2 b0 dd 04 6f cc
12-06 17:02:25.824: 3a 59 94 ff 2f 0c 04 3b 8e 08 0b 91 d0 45 a0 e2
12-06 17:02:25.824: f9 70 00
12-06 17:02:25.914: ResponseAPDU (SM)
12-06 17:02:25.914: 99 02 90 00 8e 08 59 9c 72 2f d4 19 5a c6 90 00
12-06 17:02:25.914: ResponseAPDU (Plain)
12-06 17:02:25.914: 90 00
12-06 17:02:25.914: CommandAPDU (Plain)
12-06 17:02:25.914: 00 2a 00 be e7 7f 4e 81 a0 5f 29 01 00 42 0e 44
12-06 17:02:25.914: 45 43 56 43 41 65 49 44 30 30 31 30 33 7f 49 4f
12-06 17:02:25.914: 06 0a 04 00 7f 00 07 02 02 02 02 03 86 41 04 1f
12-06 17:02:25.914: 27 ad 82 3f 8a d6 78 dc 9b 5b 5c 11 f8 ff fa c5
12-06 17:02:25.914: c6 ef d4 51 7a 6a 4d c3 94 de 52 54 7f c8 bb 31
12-06 17:02:25.914: bf 48 58 16 b3 b3 c1 57 f7 50 0a d6 0e b7 e0 34
12-06 17:02:25.914: a8 8e 16 4d ad b1 ee 72 10 28 40 71 a4 56 42 5f
12-06 17:02:25.914: 20 10 44 45 44 56 65 49 44 44 50 53 54 30 30 30
12-06 17:02:25.914: 33 33 7f 4c 12 06 09 04 00 7f 00 07 03 01 02 02
12-06 17:02:25.914: 53 05 40 05 13 ff 87 5f 25 06 01 04 01 01 01 07
12-06 17:02:25.914: 5f 24 06 01 05 00 02 01 05 5f 37 40 07 66 61 07
12-06 17:02:25.914: 86 37 bb bd 2d cd e9 26 05 98 df ac 72 d5 8d 72
12-06 17:02:25.914: 74 3d eb 26 77 a9 91 93 de 94 c3 b6 90 71 10 cf
12-06 17:02:25.914: 4b fc 4d 1c 5b 5d d7 7b 72 11 6d 92 97 c6 7c 35
12-06 17:02:25.914: 1f e7 8f cc 8e e2 5c 1f 1c 50 0b 95
12-06 17:02:25.924: CommandAPDU (SM)
12-06 17:02:25.924: 0c 2a 00 be fe 87 81 f1 01 84 11 b5 e6 7e 20 32
12-06 17:02:25.924: 21 59 85 f2 0a 51 a9 3e 36 01 f6 6f 06 87 62 c9
12-06 17:02:25.924: c9 a1 32 fd 62 0f fd e8 6d 01 ae 15 c3 86 d5 0d
12-06 17:02:25.924: e1 db 87 79 71 28 a7 47 a6 d0 66 8b 0c 8b 35 0c
12-06 17:02:25.924: d6 d3 73 49 8a b2 f9 d0 b2 8e 6d cb 95 0f a4 01
12-06 17:02:25.924: ac bd 65 da 79 a9 e5 fa 32 e6 64 94 b6 b2 9b ed
12-06 17:02:25.924: 36 21 cd 74 93 b2 9a e5 ba c0 3e 93 7e 13 94 f3
12-06 17:02:25.924: 3c b5 f9 96 c6 71 28 92 ce d1 96 0a de 5f 2f 7b
12-06 17:02:25.924: ac 27 41 a4 59 81 0e a8 f3 a3 82 ea 29 4b 1a b0
12-06 17:02:25.924: 16 8d a0 4d 2f 1f b9 c1 44 cd 04 a6 72 60 c3 58
12-06 17:02:25.924: f3 5b 60 aa d8 ad b5 c9 3e 8f 13 fb 01 6d bd d1
12-06 17:02:25.924: 41 6b 90 5c 33 4a dc a8 48 e6 0a 24 28 21 32 9f
12-06 17:02:25.924: 60 3e f8 2a 37 7a 84 e1 56 c6 94 ee 59 30 fe aa
12-06 17:02:25.924: 6c 1d 7c fa 8c 0d c9 e4 fa e8 30 13 a3 44 f9 33
12-06 17:02:25.924: 58 f0 ef 89 bb 8a e8 47 72 8b 92 23 08 61 60 31
12-06 17:02:25.924: f4 a2 89 5e af f6 16 ab 02 8e 08 6a dc c0 bd d5
12-06 17:02:25.924: bd a8 d5 00
12-06 17:02:26.304: ResponseAPDU (SM)
12-06 17:02:26.304: 99 02 90 00 8e 08 d1 d4 56 db 04 d4 c8 14 90 00
12-06 17:02:26.304: ResponseAPDU (Plain)
12-06 17:02:26.304: 90 00
12-06 17:02:26.304: CommandAPDU (Plain)
12-06 17:02:26.304: 00 22 81 b6 12 83 10 44 45 44 56 65 49 44 44 50
12-06 17:02:26.304: 53 54 30 30 30 33 33
12-06 17:02:26.304: CommandAPDU (SM)
12-06 17:02:26.304: 0c 22 81 b6 2d 87 21 01 6f f4 12 db db 74 36 a5
12-06 17:02:26.304: 31 a0 e0 e8 0c f3 5c 2f b9 c1 23 48 af 34 df 1e
12-06 17:02:26.304: 11 1c 27 ff b7 60 3e dd 8e 08 11 95 48 5f bf c2
12-06 17:02:26.304: 1e 24 00
12-06 17:02:26.364: ResponseAPDU (SM)
12-06 17:02:26.364: 99 02 90 00 8e 08 a2 50 20 2a b6 60 43 fb 90 00
12-06 17:02:26.364: ResponseAPDU (Plain)
12-06 17:02:26.364: 90 00
12-06 17:02:26.364: CommandAPDU (Plain)
12-06 17:02:26.364: 00 2a 00 be 00 01 4a 7f 4e 82 01 02 5f 29 01 00
12-06 17:02:26.364: 42 10 44 45 44 56 65 49 44 44 50 53 54 30 30 30
12-06 17:02:26.364: 33 33 7f 49 4f 06 0a 04 00 7f 00 07 02 02 02 02
12-06 17:02:26.364: 03 86 41 04 96 36 0c 55 7e d7 e6 7d b2 85 ff 50
12-06 17:02:26.364: 55 c7 4c 7e bb 3b 5a d6 61 4b 2a 57 15 9e c2 e3
12-06 17:02:26.364: 39 14 8b f6 a6 4a d2 15 fd c6 94 91 17 1a 9e 8a
12-06 17:02:26.364: 31 65 48 b4 4e 47 7f b6 59 02 d9 e0 17 b1 27 84
12-06 17:02:26.364: 8f 95 12 41 5f 20 10 44 45 47 4f 56 53 45 4c 42
12-06 17:02:26.364: 53 54 30 30 31 36 30 7f 4c 12 06 09 04 00 7f 00
12-06 17:02:26.364: 07 03 01 02 02 53 05 00 05 13 fb 04 5f 25 06 01
12-06 17:02:26.364: 04 01 02 00 05 5f 24 06 01 04 01 02 00 06 65 5e
12-06 17:02:26.364: 73 2d 06 09 04 00 7f 00 07 03 01 03 01 80 20 91
12-06 17:02:26.364: 73 2d 82 e0 87 7b e9 ac 8d 94 9e bf 06 15 b1 28
12-06 17:02:26.364: 8f cf 4c 06 22 0e e4 9c e0 c1 b8 62 88 74 82 73
12-06 17:02:26.364: 2d 06 09 04 00 7f 00 07 03 01 03 02 80 20 51 04
12-06 17:02:26.364: bf 99 7c 7f 95 f1 e5 38 a9 d8 cd 27 35 3a e0 c3
12-06 17:02:26.364: 6d ea 5c ba 54 1a 2a c3 b4 62 c0 32 e8 f0 5f 37
12-06 17:02:26.364: 40 28 6a 35 dc c3 ca 42 22 ec 9c 3d 03 26 b6 22
12-06 17:02:26.364: 7e 67 3d c2 b3 d7 f3 ef 8d 33 b8 a7 a2 1e e3 12
12-06 17:02:26.364: 8b 6a 07 65 f2 1c 89 7d 8b fb bb 3e 10 7e 66 29
12-06 17:02:26.364: cd 9c 97 3f 1f d5 6e d5 9a 55 72 97 82 13 77 78
12-06 17:02:26.364: cf
12-06 17:02:26.364: CommandAPDU (SM)
12-06 17:02:26.364: 0c 2a 00 be 00 01 5f 87 82 01 51 01 2e 57 83 ce
12-06 17:02:26.364: cd 08 2e d9 02 7d c8 20 63 68 42 6e b9 b5 04 6d
12-06 17:02:26.364: 05 b9 23 fd bf 4b 61 b5 31 f4 25 62 27 df 24 1a
12-06 17:02:26.364: e1 3b 75 fa 5a 10 72 73 54 89 c1 a2 b4 64 dd 51
12-06 17:02:26.364: ea f4 a4 04 91 51 14 9c da cc 1a 3b fa ff 00 15
12-06 17:02:26.364: 37 ca 2e f3 f5 fd 99 61 a6 5b ad 22 6d 92 10 cf
12-06 17:02:26.364: a7 9d e5 7b 01 8f 32 8b ee 7b dd 04 55 fe 6c 81
12-06 17:02:26.364: f3 91 81 0c 64 70 e8 b4 06 18 cd ea 76 6f b6 b1
12-06 17:02:26.364: 4e 8c f2 a6 8f 19 39 62 fd b1 75 58 a0 6c 03 00
12-06 17:02:26.364: 4c 18 e0 4e a8 1e 94 18 a2 8d 9b 34 b8 ba 3d 89
12-06 17:02:26.364: 81 36 80 75 f7 15 5d 4e 28 69 8e c8 ff b4 15 db
12-06 17:02:26.364: a5 dd 75 6f a2 29 01 a1 09 f5 e1 21 3b 84 f5 aa
12-06 17:02:26.364: 5b 8c 13 3b 9c 67 0a c7 87 23 13 3a e9 93 7b d9
12-06 17:02:26.364: 9e ed a5 2c 87 8c 47 a4 05 86 5a 33 1c 74 fe 61
12-06 17:02:26.364: a2 b0 70 e6 e8 75 2a 0f f1 d3 d0 1b 10 9e db 01
12-06 17:02:26.364: 74 d1 b3 18 99 60 67 2d 2a 9c cf 47 74 d9 a4 62
12-06 17:02:26.364: a5 e8 32 86 db b7 61 69 58 01 c1 7a 7a 04 52 91
12-06 17:02:26.364: 49 2a de fd a7 b3 d5 39 7a b6 13 f5 46 5c 12 84
12-06 17:02:26.364: e0 b4 fd b6 f7 f4 41 f0 c7 b4 77 97 5f 46 4c 38
12-06 17:02:26.364: f8 cd cc 5e 31 ed 78 e7 fe 49 19 ac 9a 0a ef 2a
12-06 17:02:26.364: cc d3 10 ec 6a 01 03 fe d8 30 60 d9 9e 72 53 cb
12-06 17:02:26.364: fa ff db 82 f4 ed 3b d2 40 7c 0b 18 8e 08 e2 e7
12-06 17:02:26.364: 7f 1a f5 d5 87 3f 00
12-06 17:02:26.754: ResponseAPDU (SM)
12-06 17:02:26.754: 99 02 90 00 8e 08 6f 3b e6 08 b9 8c fd 75 90 00
12-06 17:02:26.754: ResponseAPDU (Plain)
12-06 17:02:26.754: 90 00
12-06 17:02:26.754: Certificate sent
12-06 17:02:26.754: TA canceled!
```

Tabelle 14: Dieser Trace wurde aufgenommen, als die aus Abbildung 6 extrahierte Zertifikatskette an einen nPA geschickt wurde.

12 Proof of Concept

Um die App zu testen, haben wir anfangs noch APDUs aus zwei erfolgreichen Beispielen, die in [Worked Example for EAC] detailliert beschrieben werden, verwendet. Um jedoch die untere Grenze für das Datum aktualisieren zu können, müssen neue hoheitliche Zertifikate an den nPA übertragen werden. In Kapitel 11.1 wird eine Möglichkeit beschrieben um eine solche Zertifikatskette herunterzuladen. Der Trace in Tabelle 14 wurde aufgenommen, als die aus Abbildung 6 extrahierte Zertifikatskette an den nPA geschickt wurde.
Aus dem Trace geht hervor, dass die Zertifikatskette komplett an den nPA geschickt wurde. Anschließend wurde die TA abgebrochen. Wie bereits erklärt wurde damit die untere Grenze für das Datum auf dem nPA aktualisiert, falls die übergebene Zertifikatskette mit einem Vertrauensanker des nPAs startet.

13 Fazit

In dieser Arbeit wurde die Android-App Androsmex2 vorgestellt. Androsmex2 kann die untere Grenze für das aktuelle Datum auf einem nPA erhöhen. Dafür schickt Adrosmex2 über die NFC-Schnittstelle des Smartphones eine neue hoheitliche Zertifikatskette an den nPA. Es wurde besprochen, dass nur der erfolgreiche Import von Terminalzertifikaten von hoheitlichen nationalen Inspektionssystemen und hoheitlichen nationalen Authentisierungsterminals die untere Grenze für das aktuelle Datum erhöhen kann. Solche Zertifikatsketten werden nicht offiziell zum Herunterladen zur Verfügung gestellt. Der Ausweisinhaber benötigt jedoch nicht den privaten Schlüssel der Zertifikatskette, um die untere Grenze für das aktuelle Datum aktualisieren zu können. Weiterhin wurde eine Möglichkeit vorgestellt, um eine hoheitliche Zertifikatskette herunterzuladen. Dazu werden die AusweisApp, ein Standardleser, Wireshark, USBPcap und ein nPA benötigt. Der Ausweisinhaber verbindet seinen nPA über die PC/SC-Schnittstelle des Standardleser mit einem entfernten Dienst (in unserem Ausweis Auskunft des Bundes) und führt die eID-Funktion aus. Dabei wird eine aktuelle hoheitliche Zertifikatskette an den nPA übertragen. Diese Übertragung speichert er mit USBPcap auf dem verwendeten PC und extrahiert anschließend die Zertifikatskette mithilfe von Wireshark. Danach

kann diese Zertifikatskette an andere nPAs übertragen werden und löst eine Zeitaktualisierung aus, falls sie mit einem Vertrauensanker des nPAs startet und aktueller ist als das auf dem Chip gespeicherte Datum.

Da vom nPA keine Information über die Zeitaktualisierung weitergegeben wird, konnte beim Testen von Androsmex2 nicht sichergestellt werden, dass die untere Grenze für das Datum tatsächlich erhöht wird, nachdem eine hoheitliche Zertifikatskette vollständig an einen nPA übertragen wurde. Dass die vollständige Zertifikatskette erfolgreich an den nPA übertragen werden konnte, wurde bereits gezeigt.

Literaturverzeichnis

[BSI TR-03119] Technical Guideline BSI TR-03119.Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control. Version 1.3. URL:https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03119/BSI-TR-03119_V1_pdf.pdf;jsessionid=C5823E55FAF0C56DFBFF847F18E48393.2_cid368?__blob=publicationFile (besucht am 7.12.2014).

[Elektronische Ausweisdokumente] Elektronische Ausweisdokumente - Grundlagen und Praxisbeispiele. Hanser, München, 2009.

[ICAO Doc 9303] International Civil Aviation Organisation. Machine Readable Travel Documents. Doc 9303. URL:http://www.icao.int/publications/pages/publication.aspx?docnum=9303 (besucht am 7.12.2014).

[ISO/IEC 14443] ISO 14443-4: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol. URL:http://wg8.de/wg8n1344_17n3269_Ballot_FCD14443-4.pdf(besucht am 7.12.2014)

[BSI TR-03127] Technische Richtlinie 03127. Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel. Version 1.15. URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03127/BSI-TR-03127_pdf.pdf?__blob=publicationFile (besucht am 7.12.2014).

[BSI TR-03117] Technical Guideline 03117. eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit. Version 1.0. URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03117/BSI-TR-03117_pdf.pdf?__blob=publicationFile (besucht am 7.12.2014).

[BSI TR-03128] Technische Richtlinie 03128. EAC-PKI'n für den elektronischen Personalausweis. Version 1.1. URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03128/BSI_TR-03128.pdf?__blob=publicationFile (besucht am 7.12.2014).

[BSI TR-03116] Technische Richtlinie 03116. Kryptographische Vorgaben für Projekte der Bundesregierung. URL:https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html (besucht am 7.12.2014).

[BSI TR-03110] Technical Guideline 03110. Advanced Security Mechanisms for Machine Readable Travel Documents. URL:https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html (besucht am 7.12.2014).

[IBSI TR-02102] Technische Richtlinie 02102. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. URL:https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html (besucht am 7.12.2014).

[BSI TR-03111] Technische Richtlinie 03111.Elliptische-Kurven-Kryptographie (ECC). URL:https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03111/index_htm.html (besucht am 7.12.2014).

[BSI 02101] Bestätigung von Produkten für qualifizierte elektronische Signaturen (BSI.02101.TE.06.2008). URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Signaturbestaetigung/02101_pdf.pdf?__blob=publicationFile (besucht am 7.12.2014).

[ICAO 1] ICAO: Supplemental Access Control for Machine Readable Travel Documents, Technical Report. Version 1.01. URL:http://www.icao.int/security/mrtd/downloads/technical%20reports/technical%20report.pdf (besucht am 7.12.2014).

[ISO 7816] ISO 7816 - Identification cards. URL:http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx (besucht am 7.12.2014).

[BSI: Certificate Policy] BSI: Certificate Policy für die „eID-Anwendung“ des ePA. Version 1.29. URL:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CVCA/Certificate_Policy_eID.pdf?__blob=publicationFile (besucht am 7.12.2014).

[RFID-Systeme] BSI: Risiken und Chancen des Einsatzes von RFID-Systemen. URL:http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_barrierefrei_pdf.pdf?__blob=publicationFile (besucht am 7.12.2014).

[ECMA 340] Standard ECMA-340. Near Field Communication - Interface and Protocol (NFCIP-1). URL:http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf (besucht am 7.12.2014).

[Selbstauskunft] https://www.buergerserviceportal.de/bund/ausweisapp/bspx_selbstauskunft (besucht am 7.12.2014).

[Anleitung: USBPcap] http://desowin.org/usbpcap/tour.html (besucht am 7.12.2014).

[Worked Example for EAC] BSI: Worked Example for Extended Access Control (EAC). Version 1.0. URL:https://www.dropbox.com/s/3rtcses45bk3txv/BSI_EAC_Worked-Example_V1.0.pdf (besucht am 7.12.2014).

[Mobiler Chipkartenleser] Frank Morgner (10.5.2012). Mobiler Chipkartenleser für den neuen Personalausweis. Sicherheitsanalyse und Erweiterung des „Systems nPA“. Diplomarbeit. Berlin: Humboldt-Universität zu Berlin. URL:http://sar.informatik.hu-berlin.de/research/publications/#SAR-PR-2011-04 (besucht am 7.12.2014).

Selbständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig verfasst und noch nicht für andere Prüfungen eingereicht habe. Sämtliche Quellen einschließlich Internetquellen, die unverändert oder abgewandelt wiedergegeben werden, insbesondere Quellen für Texte, Grafiken, Tabellen und Bilder, sind als solche kenntlich gemacht. Mir ist bekannt, dass bei Verstößen gegen diese Grundsätze ein Verfahren wegen Täuschungsversuchs bzw. Täuschung eingeleitet wird.

Berlin, den 9. Dezember 2014 .....