Sicherheitsaspekte beim Chipkarten-basierten Identitätsnachweis

Detlef Hühnlein · Johannes Schmölz · Tobias Wich · Moritz Horsch

ecsec GmbH, Sudetenstraße 16, 96247 Michelau, vorname.nachname@ecsec.de

Abstract Mit der Einführung des neuen Personalausweises wurde insbesondere auch der elektronische Identitätsnachweis gemäß § 18 PAuswG ermöglicht, mit dem Ausweisinhaber ihre Identität gegenüber öffentlichen und nicht-öffentlichen Stellen elektronisch nachweisen können. In analoger Weise können auch andere Chipkarten, wie z.B. die elektronische Gesundheitskarte oder Bank- und Signaturkarten für die sichere Authentisierung und den Chipkarten-basierten Identitätsnachweis genutzt werden. Damit hierbei jeweils dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit vorgesehen werden können, sollen in diesem Beitrag die typischen Bedrohungen, Risiken und Sicherheitsaspekte für den Chipkarten-basierten Identitätsnachweis in systematischer Weise betrachtet werden.

1. Einleitung

Gemäß § 18 Abs. 1 Satz 1 PAuswG kann der Personalausweisinhaber, der mindestens 16 Jahre alt ist, seinen Personalausweis (nPA) dazu verwenden, seine Identität gegenüber öffentlichen und nicht-öffentlichen Stellen elektronisch nachzuweisen (vgl. [1, 2, 3]), sofern diese einen entsprechenden Zugang hierfür eröffnen. Als Beispiele können Online-Shops und Bürgerportale von Kommunen und Städten genannt werden. Hierbei werden Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises ausgelesen (§ 18 Abs. 2 PAuswG).

Voraussetzung hierfür ist insbesondere, dass

1. bestimmte Attribute[1] des Ausweisinhabers auf dem Chip des Ausweises gespeichert sind und
2. mittels geeigneter technischer Protokolle ausgelesen werden können.

Wie in [5] gezeigt und in Abschnitt 2 näher erläutert, kann deshalb ein an § 18 PAuswG angelehnter Identitätsnachweis, auch auf Basis anderer Chipkarten, wie z.B. der elektronischen Gesundheitskarte (eGK) oder anderer Signaturkarten, realisiert werden. Betrachtet man die spezifischen Bedrohungen für den elektronischen Identitätsnachweis gemäß § 18 PAuswG näher, so zeigt sich, dass die hierbei relevanten Bedrohungen in der Regel auch beim Identitätsnachweis mit anderen Chipkarten zu berücksichtigen sind. Werden umgekehrt geeignete Sicherheitsmaßnahmen ergriffen, die den nicht bereits systembedingt abgewehrten Bedrohungen entgegenwirken, so kann auch beim Identitätsnachweis mit anderen Chipkarten ein vergleichbares Sicherheitsniveau wie beim Personalausweis-basierten Verfahren erreicht werden.

Der folgende Beitrag stellt in Abschnitt 2 ein abstraktes Modell für den Chipkarten-basierten Identitätsnachweis vor, das am Beispiel des nPA und der eGK näher erläutert wird und als Referenz für die weiteren Betrachtungen dient. Abschnitt 3 enthält eine systematische Bedrohungs- und Risikoanalyse für ein System zum Chipkarten-basierten Identitätsnachweis und diskutiert Sicherheitsmaßnahmen, die diesen Bedrohungen entgegenwirken können. Hierbei wird unterschieden zwischen grundlegenden und grundsätzlich empfehlenswerten Maßnahmen und solchen Maßnahmen, die bei bestimmten Systemausprägungen zusätzlich zu berücksichtigen sind. Abschnitt 4 fasst schließlich die wesentlichen Aspekte dieses Beitrags zusammen und liefert einen Ausblick auf zukünftige Entwicklungen.

[1] Begriffsbestimmungen im Umfeld des Identitätsmanagements finden sich in [4].

2. Der Chipkarten-basierte Identitätsnachweis

In diesem Abschnitt sollen die wesentlichen Aspekte des an § 18 PAuswG angelehnten Chipkarten-basierten Identitätsnachweis vorgestellt werden. Hierfür wird in Abschnitt 2.1 ein abstraktes Referenzmodell eingeführt, das als Grundlage für die spätere Bedrohungsanalyse dient. In Abschnitt 2.2 erfolgt eine vergleichende Betrachtung zwischen dem neuen Personalausweis und alternativen Chipkarten, wie z.B. der elektronischen Gesundheitskarte oder anderer Signaturkarten, hinsichtlich des Chipkarten-basierten Identitätsnachweises.

2.1 Abstraktes Referenzmodell

Den Betrachtungen in diesem Beitrag soll ein abstraktes Referenzmodell zu Grunde gelegt werden.

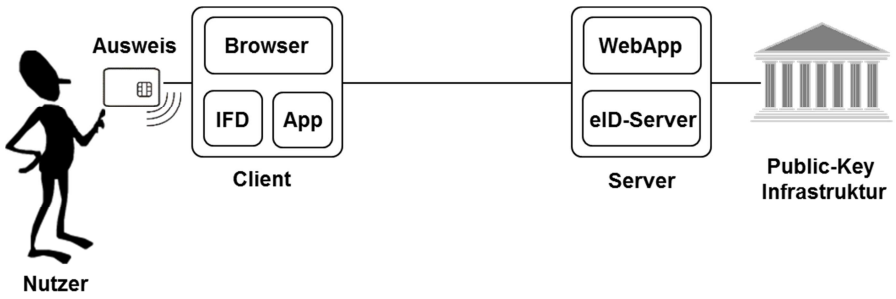

Abb. 1. Systemarchitektur für den Chipkarten-basierten Identitätsnachweis

Wie in Abbildung 1 illustriert, umfasst das System für den Chipkarten-basierten Identitätsnachweis die folgenden Komponenten:

- *Nutzer* – verwendet seinen Chipkarten-basierten Ausweis und ein geeignetes Client-System, um seine Identität gegenüber einem Dienst nachzuweisen. Der Dienst wird von einem Server-System bereitgestellt.
- *Ausweis* – enthält ein geeignetes elektronisches Speicher- und Verarbeitungsmedium (Chip), auf dem bestimmte Identitätsattribute des Nutzers gespeichert sind.
- *Client* – interagiert und vermittelt zwischen dem Nutzer und seinem Ausweis sowie dem Server-System. Das Client-System umfasst typischer Weise einen Browser, ein Chipkartenterminal (IFD, Interface Device), und eine geeignete eID-Applikation [6, 7] (App).
- *Server* – kommuniziert über das Client-System mit dem Nutzer und dem Ausweis, um den Chipkarten-basierten Identitätsnachweis durchzuführen und die

im Chip gespeicherten Identitätsattribute auszulesen. Das Server-System besteht aus einer Web-Applikation (WebApp), die den Dienst bereitstellt und den Identitätsnachweis veranlasst, und einem für den entsprechenden Ausweis geeigneten Authentisierungsdienst (eID-Server), der die erforderliche Funktionalität für den Chipkarten-basierten Identitätsnachweis bereitstellt.
- *Public-Key Infrastruktur* – außerdem existieren entsprechende Vertrauensinfrastrukturen für die Verwaltung von Zertifikaten und Sperrinformationen.

2.2 Vergleich des nPA mit alternativen Chipkarten

Vergleicht man den nPA hinsichtlich des Chipkarten-basierten Identitätsnachweises mit anderen Chipkarten der eCard-Strategie der Bundesregierung [8, 9], wie z.B. der eGK oder weiteren Signaturkarten, so sind unter anderem die folgenden Gemeinsamkeiten und Unterschiede hervorzuheben:

2.2.1 Gemeinsamkeiten

Beim Vergleich des nPA mit alternativen Chipkarten im Hinblick auf den Chipkarten-basierten Identitätsnachweis sind die folgenden Gemeinsamkeiten festzustellen:

- *Chipkarte gemäß ISO/IEC 7816-4* – sowohl der nPA als auch die alternativen Chipkarten (eGK, Signaturkarten etc.) können mit Chipkartenkommandos gemäß ISO/IEC 7816 [10, Teil 4] angesprochen werden (vgl. [11, 12]).
- *Evaluation gemäß Common Criteria EAL 4+* – sowohl der nPA als auch die alternativen Chipkarten sind gemäß der Vertrauenswürdigkeitsstufe EAL 4+ der Common Criteria evaluiert (vgl. [13, 14] und SigV, Anlage 1, I. 1.1 b).
- *Starke Authentisierung des Karteninhabers* – mit den betrachteten Chipkarten ist eine starke Authentisierung des Karteninhabers mit Besitz und Wissen (PIN) möglich (vgl. [11, 15]).
- *Gemeinsame Identitätsattribute* – die folgenden Attribute sind (wenn auch in unterschiedlichen Codierungen) sowohl auf dem nPA als auch auf der eGK gespeichert (vgl. [15, Abschnitt 6.3.7], [16, Abschnitt 3.4] und [11, Table E.1]):
  - Titel,
  - Vorname,
  - Nachname[2],
  - Adresse,
  - Geburtsdatum,

[2] Bei der elektronischen Gesundheitskarte sind neben dem Element `Nachname` auch die eigenständigen Elemente `Vorsatzwort` und `Namenszusatz` vorgesehen.

– Geschlecht.

Darüber hinaus enthält [58, Table 7] eine Liste der gebräuchlichsten X.501-Attribute, die im Subject-Element eines X.509-Zertifikates enthalten sein können. Da X.509-basierte Zertifikate bei Signaturkarten in der Regel frei auslesbar sind, können diese auf der Karte vorhandenen Attribute auch leicht für den Chipkarten-basierten Identitätsnachweis genutzt werden. Da ein Zertifizierungsdiensteanbieter gemäß § 11 SigG haften würde, wenn er seine in SigG und SigV definierten Pflichten verletzen und einem Dritten, der auf die Angaben im qualifizierten Zertifikat vertraut, deshalb ein Schaden entstehen würde, darf man davon ausgehen, dass die in einem qualifizierten Zertifikat auf einer Signaturkarte enthaltenen Attribute sehr sorgfältig überprüft wurden und deshalb ein sehr hohes Maß an Vertrauenswürdigkeit besitzen.

2.2.2 Unterschiede

Auf der anderen Seite existieren hinsichtlich des Chipkarten-basierten Identitätsnachweises die folgenden Unterschiede zwischen dem nPA und alternativen Chipkarten:

- *Transport-Schnittstelle* – Während die eGK und heute übliche Signaturkarten eine kontaktbehaftete Schnittstelle gemäß [10, Part 3] besitzen, bietet der nPA eine kontaktlose Schnittstelle gemäß [17]. Aus diesem Grund wird die beim elektronischen Identitätsnachweis genutzte eID-PIN nicht im Klartext zum nPA übertragen, sondern für den Aufbau eines kryptographisch geschützten Kanals mit dem Password Authenticated Connection Establishment (PACE) Protokoll (siehe [11, Abschnitt 4.2]) verwendet.
- *Authentisierung des Terminals für Datenzugriff* – Für den Zugriff auf die oben genannten Identitätsattribute muss beim nPA eine Authentisierung des zugreifenden Diensteanbieters mit dem Terminal Authentication Protokoll gemäß [11, Abschnitt 4.4] erfolgen. Die grundsätzliche Notwendigkeit für den Zugriff auf die einzelnen Datengruppen muss gemäß § 21 Abs. 2 Nr. 3 PAuswG bei der Beantragung eines Berechtigungszertifikates nachgewiesen werden und diese Zugriffsrechte werden dann im so genannten Certificate Holder Authorization Template (CHAT) (vgl. § 2 Abs. 4 PAuswG, [11, Annex C] und [10, Part 8]) des Berechtigungszertifikates festgelegt. Die Zugriffsberechtigung wird vom Ausweis selbst geprüft und das Berechtigungszertifikat muss täglich erneuert werden (vgl. [18, Tabelle 21]). Da dem Ausweisinhaber im Zuge dieses Authentisierungsvorganges Informationen über die Identität des Diensteanbieters und den Zweck der Datenübermittlung angezeigt werden und er im Einzelfall die Übermittlung bestimmter Daten ausschließen (vgl. § 18 Abs. 5 PAuswG) kann, bevor er durch Eingabe der eID-PIN in die Datenverarbeitung einwilligt, kann ein Benutzer-zentrierter und sehr datenschutzfreundlicher Identitätsnachweis realisiert werden. Auf der anderen Seite ist der Zugriff auf die

oben genannten Identitätsattribute bei der eGK – zumindest gemäß der derzeit verfügbaren Spezifikationen [12, 15, 16] – nicht beschränkt. In ähnlicher Weise geht man davon aus, dass X.509-basierte Zertifikate nicht vertraulich behandelt werden müssen.

3. Bedrohungen und Sicherheitsmaßnahmen

Betrachtet man die verschiedenen Systemkomponenten des abstrakten Referenzmodells, so sind die in Abbildung 2 angedeuteten und in den folgenden Abschnitten näher diskutierten Bedrohungen zu berücksichtigen.

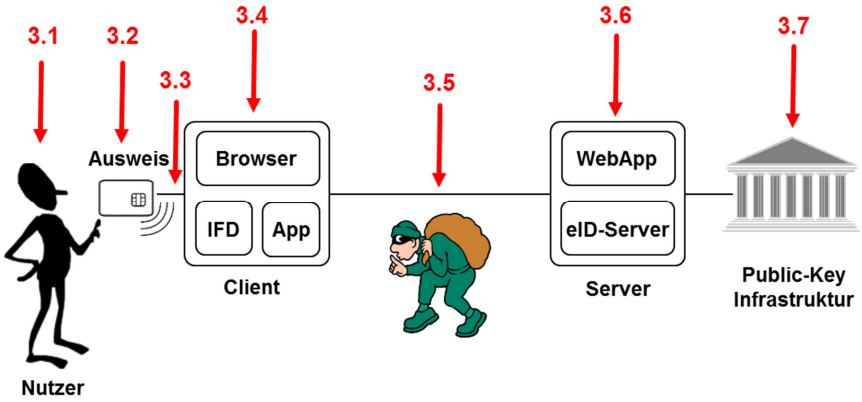

Abb. 2. Bedrohungen beim Chipkarten-basierten Identitätsnachweis

3.1 Nutzer

Will ein Nutzer seine Identität mittels Chipkarte nachweisen, so spielt neben dem Besitz der Karte das Wissen über die dazugehörige PIN eine entscheidende Rolle. Die Kombination dieser beiden Faktoren ermöglicht es dem Benutzer, eine starke, auf mehreren Faktoren basierende, Authentisierung [19, Abschnitt 6.1.4] durchzuführen und sich somit gegenüber einer dritten Partei eindeutig auszuweisen.

Für einen Angreifer stellt die PIN daher ein besonders lohnenswertes Angriffsziel dar. Verwendet der Benutzer nur einen Basis-Kartenleser [20, Abschnitt 3.1], so muss die PIN über den Computer eingegeben werden. Dies kann entweder über die normale Tastatur geschehen oder mittels einer Bildschirmtastatur. In beiden Fällen ist es dem Angreifer möglich, die PIN mit Hilfe einer geeigneten Schadsoftware, z.B. einem Trojaner (siehe z.B. [21]), der Tastatureingaben aufzeichnet und Bildschirmfotos anfertigt, mitzuschneiden.

Um sich vor dem Diebstahl der PIN durch Schadsoftware zu schützen, sollten daher möglichst Kartenterminals eingesetzt werden, die über ein eigenständiges Tastaturfeld verfügen.

Eine weitere Möglichkeit für Angreifer an die PIN eines Benutzers zu gelangen, stellt das sog. Phishing [21, 22] dar. Hierbei werden dem Benutzer falsche Sachverhalte vorgetäuscht, die ihn ermutigen sollen seine PIN preiszugeben. In [23] beschreibt Jan Schejbal ein entsprechendes Szenario für den nPA. Ausgangspunkt ist eine Altersverifikation mit Hilfe der eID-Funktion des nPA. Der Benutzer muss durch einen Mausklick die Altersverifikation starten. Hierbei wird allerdings nicht die installierte eID-Applikation, wie z.B. die AusweisApp [6], gestartet, sondern mittels JavaScript ein Fenster dargestellt, das identisch zu dem der graphischen Darstellung der AusweisApp ist. Dem Benutzer wird dabei suggeriert, dass die AusweisApp gestartet ist und diese die Eingabe seiner PIN erwartet. Gibt der Benutzer nun seine PIN ein, so gelangt der Angreifer in den Besitz dieser und kann u.U. die Identität des Benutzers missbrauchen. Die Seite, die diesen Phishing-Angriff demonstriert, ist unter der Adresse *https://fsk18.piratenpartei.de* zu finden. Während in der wissenschaftlichen Literatur einige spezifische Maßnahmen zur Bekämpfung des Phishing vorgeschlagen wurden [24, 25, 26], scheint die wichtigste Maßnahme die Schaffung eines entsprechenden Sicherheitsbewusstseins [27] der Nutzer zu sein.

3.2 Ausweis

Chipkarten werden grundsätzlich als probates Mittel für die sichere Speicherung und den sicheren Transport von Schlüsselmaterial betrachtet. Trotz des hohen Maßes an Sicherheit, das eine Chipkarte bietet, kann mit entsprechend hohem Aufwand das auf der Chipkarte hinterlegte Schlüsselmaterial extrahiert werden.
Die Sicherheit einer Chipkarte basiert laut [28] auf vier Segmenten:

- Dem Kartenkörper,
- der Chiphardware,
- dem Betriebssystem und
- der Chipkartenapplikation.

Im Folgenden werden nur die Segmente Chiphardware, Betriebssystem und Anwendung betrachtet. Hierbei werden die unterschiedlichen Arten von Angriffen erläutert, gegen welche Segmente sie gerichtet sind und welche Schutzmaßnahmen gegen sie ergriffen werden können.

Neben den Angriffen über die soziale Ebene, die auf den Nutzer abzielen (siehe Abschnitt 3.1), werden in [28] Angriffe auf der physikalischen Ebene und Angriffe auf die logische Ebene unterschieden, die jedoch miteinander kombiniert werden können.

Bei Angriffen über die physikalische Ebene unterscheidet [28] zwischen statischen Angriffen, bei denen die Chipkarte außer Betrieb ist, und dynamischen Angriffen, bei denen die Chipkarte in Benutzung ist. Statische Angriffe über die physikalische Ebene sind für den Angreifer nicht zeitkritisch, während bei dynamischen Angriffen die Zeit eine entscheidende Rolle spielt. Für beide Angriffe werden entsprechende Werkzeuge benötigt (z.B. Messgeräte, Elektronenmikroskope), die den materiellen Aufwand für den Angreifer stark in die Höhe treiben.

Weiterhin können Angriffe als passiv oder als aktiv klassifiziert werden (vgl. [28]). Bei passiven Angriffen wirkt der Angreifer nicht verändernd auf die Funktion der Chipkarte ein. Hierunter fällt beispielsweise die Messung und anschließende Auswertung der Stromaufnahme, die die Chipkarte für die Durchführung von bestimmten Operationen benötigt. Die Leistungsanalyse von Chipkarten wird in [29] beschrieben und wird als Simple Power Analysis (SPA) bzw. in einer erweiterten Form als Differential Power Analysis (DPA) bezeichnet. Damit eine Chipkarte vor einer Leistungsanalyse mittels SPA/DPA geschützt ist, muss sie für jede Operation die gleiche Leistungsaufnahme besitzen. Hierdurch kann nicht mehr ermittelt werden, welche spezifische Operation gerade ausgeführt wird.

Bei aktiven Angriffen wird direkter Einfluss auf die Funktion der Chipkarte genommen, beispielsweise durch das Einstreuen von Hardwarefehlern. In [30] wird ein theoretisches Modell beschrieben, das aufzeigt, wie privates Schlüsselmaterial bei asymmetrischen Kryptoalgorithmen durch Manipulation an der Hardware berechnet werden kann. Dieser Angriff ist auch als Bellcore-Angriff (Bellcore-Attack) bekannt. Für symmetrische Kryptoalgorithmen wurde in [31] eine Erweiterung des Bellcore-Angriffs mit dem Namen Differential Fault Analysis (DFA) vorgestellt. Der Bellcore-Angriff sowie die DFA sind aktive Angriffe, die auf die logische Ebene einer Chipkarte abzielen. Laut [28] sind moderne Chipkarten gegen diese Angriffe immun.

Obwohl Chipkarten häufig mit dem Ziel der „Tamper Resistance“ [32], oder auch Fälschungssicherheit, entwickelt werden und Angriffe auf die Chipkartenhardware in der Regel mit einem sehr hohen technischen und zeitlichen Aufwand verbunden sind, können sie leider nicht komplett ausgeschlossen werden [33]. Beispielsweise stellte Christopher Tarnovsky auf der Black Hat 2010 in Washington D.C. einen Angriff auf einen Mikrocontroller der populären Chipfamilie Infineon SLE 66PE vor [34], der u.a. in Chipkarten und weiteren Sicherheitsmodulen eingesetzt wird. Tarnovsky konnte in seinem Labor den Aufbau des Mikrocontrollers rekonstruieren und das geheime Schlüsselmaterial auslesen. Für den Angriff hat er über sechs Monate benötigt; seine Laborausstattung hat etwa 200.000 US $ gekostet. Auch wenn moderne Chipkarten gemäß dem derzeitigen Stand von Wissenschaft und Technik als äußerst sicher gelten und die implementierten Sicherheitsmaßnahmen nur mit erheblichem zeitlichen und finanziellen Aufwand überwunden werden können, empfiehlt es sich dennoch, Maßnahmen für den unwahrscheinlichen Fall der Entdeckung einer systematischen Schwachstelle in der Hardware zu ergreifen, wie dies beim neuen Personalausweis mit der Ein-

führung der nur für privilegierte Terminals zugreifbaren Datei EF.ChipSecurity (siehe [11, A.1.2.3]) geschehen ist.

3.3 Transportschnittstelle des Ausweises

Bei kontaktlosen Chipkarten gemäß ISO/IEC 14443 [17], wie z.B. beim neuen Personalausweis, erfolgt die Übertragung der Daten zum Kartenterminal auf Transportebene grundsätzlich unverschlüsselt, so dass die ausgetauschten Chipkartenkommandos (Application Protocol Data Units, APDUs) mit entsprechenden Mitteln [35] leicht abgehört und manipuliert werden könnten.

Aus diesem Grund sollten Daten zwischen kontaktlosen Chipkarten und Lesegeräten nur verschlüsselt und authentisiert ausgetauscht werden. Hierzu bietet sich das Password Authenticated Connection Establishment (PACE) Protokoll an, wie es beim nPA zum Einsatz kommt (siehe [11, Abschnitt 4.2]). Hierbei wird ein kryptographisch gesicherter Kanal zwischen dem Chip und dem Kartenterminal aufgebaut, der über ein im Chip bekanntes und im Kartenterminal eingegebenes Passwort (PIN) authentisiert wird. Die auf diese Weise ausgetauschten Schlüssel werden dann für den kryptographischen Schutz der Chipkarten-Kommandos im Rahmen des so genannten „Secure Messaging“ gemäß [10, Part 8] genutzt. Eine formale Sicherheitsanalyse des PACE-Protokolls findet sich in [36].

Bei kontaktbehafteten Chipkarten erfolgt die Übertragung der PIN im Regelfall ohne kryptographischen Schutz, da hier – zumindest bei Chipkartenterminals mit PIN-Pad – von einer physikalisch geschützten und abgeschirmten Übertragung ausgegangen wird.

3.4 Client

Als zentrale Software-Komponente auf dem Rechner des Nutzers nimmt die eID-Applikation (App), die mit dem Browser und dem Kartenterminal (IFD) interagiert, eine besonders exponierte Position ein. Als installierte Anwendung auf dem Rechner ist sie stetig potenziellen Bedrohungen durch Schadsoftware ausgesetzt. In allen bisher veröffentlichten Angriffen auf die AusweisApp [6], der offiziellen eID-Applikation für den nPA, ist ein manipuliertes Betriebssystem der Clientplattform des Nutzers erforderlich. Theoretisch besteht auch immer die Möglichkeit mit manipulierten Eingabedaten die eID-Applikation oder den Ausweis in einen Zustand zu versetzen, der einem Angreifer weitere Angriffsmöglichkeiten eröffnet. Aufgrund der Sicherheitsmechanismen im Chipkartenbetriebssystem, der eingesetzten Zertifikatsinfrastruktur (siehe Abschnitt 3.7), der sicherheitstechnischen Prüfungen und den als sicher bewiesenen Protokollen [36, 37] sind hierfür aber keine Angriffe bekannt.

Neben der AusweisApp existieren noch weitere eID-Applikationen, die aufgrund ihrer zugrundeliegenden Technologie andere Probleme mit sich bringen können. Die wohl am häufigsten eingesetzte Alternative zu lokal installierten Anwendungen stellen Java Applets [7, 38] dar, die im Browser ausgeführt werden. Der große Schwachpunkt bei Applets ist der Mechanismus über den diese an den Client ausgeliefert werden. Es besteht somit bei jedem Start der Anwendung die potenzielle Gefahr, dass der Diensteanbieter, von dem in der Regel das Applet ausgeliefert wird, mittels Cross-Site-Scripting, Man-in-the-Middle o.ä. eine manipulierte Version des Applets oder zusätzlich Schadsoftware ausliefert.

Am Beispiel der AusweisApp, die vermutlich die in Deutschland am weitesten verbreitete und am besten analysierte eID-Applikation ist, zeigt sich deutlich, dass ohne eine kompromittierte Clientplattform bisher kein effektiver Angriff existiert. Schon vor ihrer Veröffentlichung wies der Chaos Computer Club (CCC) auf die Angreifbarkeit der eID-Applikation [39] hin, wenn sie auf einem – z.B. durch einen Trojaner – kompromittierten System läuft und ein Basis-Kartenleser [20, Abschnitt 3.1] im Einsatz ist. Hierbei wird während der Authentisierung des Benutzers gegenüber der Karte die am Rechner eingegebene PIN aufgezeichnet und an einen entfernten Angreifer übertragen. Dabei ist es unerheblich, ob die Tastatur des Rechners oder eine Bildschirmtastatur verwendet wird. Bei Standard- und Komfort-Kartenlesern [20, Abschnitte 3.2-3.3] hingegen scheitert dieser Angriff, da die PIN bei diesen auf dem Eingabefeld des Kartenlesers eingegeben werden muss.

Mit diesem Angriff erlangt der Angreifer Wissen über das Geheimnis (PIN). Um die Identitäts- und Signaturfunktion (eID- und eSign-Funktion) des Ausweises zu nutzen wird allerdings nicht nur das Wissen, sondern auch der Besitz der Karte vorausgesetzt. Rund zwei Monate nach der offiziellen Einführung des neuen Personalausweises und damit auch der AusweisApp wurde diese Kopplung mittels Relay-Angriffen [40] ausgehebelt. Für diesen Angriff werden alle Chipkarten-Kommandos vom Angreifer gesendet und beim Opfer über einen Empfangsdienst an die Karte übergeben. Obgleich die zwei dort vorgestellten Angriffe gegen die eID- und eSign-Funktion sehr ausgefeilt sind, wird wieder ein kompromittiertes System mit einem Basis-Kartenleser bzw. einem nicht zertifizierten höherwertigen Leser vorausgesetzt, da der Angreifer nur bei solchen Kartenterminals die PIN übergeben kann.

Aber selbst beim Einsatz eines Komfort-Kartenlesers [20, Abschnitt 3.3] erfolgt die Anzeige des Zertifikates und die mögliche Beschränkung des Datenzugriffes – analog zur Anzeige der zu signierenden Daten bei der Erzeugung von Signaturen – auf dem Rechnersystem. Somit wäre eine kompromittierte Systemplattform für den elektronischen Identitätsnachweis mit dem neuen Personalausweis auch bei Einsatz solcher Kartenterminals problematisch. Mögliche Angriffspunkte wären hierbei beispielsweise die Manipulation des Bildschirms oder des DNS-Dienstes (Domain Name System). Sofern das Rechnersystem frei von Schadsoftware ist, kann umgekehrt ein vergleichbar sicherer Identitätsnachweis mit alternativen Chipkarten (eGK, Signaturkarten, etc.) realisiert werden.

Neben solch konzeptionellen Problemen, die durch potenziell unsichere Peripheriegeräte entstehen, besteht natürlich auch immer die Möglichkeit über Fehler in der eID-Applikation den Rechner und damit die Sicherheit der Applikation selbst zu kompromittieren. Ein Angriff auf die Updatefunktion der AusweisApp [41] wurde bereits vorgestellt. Dabei war es durch die mangelhafte Validierung des X.509-basierten Server-Zertifikates möglich, manipulierte Archivdateien als Updates einzuspielen und somit nicht nur die AusweisApp, sondern den gesamten Rechner zu kompromittieren.

3.5 Kommunikationsprotokolle zwischen Client und Server

Ein weiterer Angriffspunkt sind die Transport- und Authentisierungsprotokolle, die zwischen dem Ausweis bzw. der eID-Applikation und dem eID-Server ablaufen. Während beim nPA das Extended Access Control (EAC) Protokoll [11] genutzt wird, dessen Sicherheit in [37] formal bewiesen wurde, ist für den Zugriff auf die auf der eGK oder einer Signaturkarte abgelegten Identitätsattribute (vgl. Abschnitt 2.2) keine Authentisierung notwendig. Dementsprechend müssen die aus der Karte ausgelesenen Daten bei der Übertragung zum eID-Server zwingend durch zusätzliche Maßnahmen geschützt werden. Deshalb kommt dem Einsatz von sicheren Transportprotokollen, wie z.B. TLS [42, 43], und der Bereitstellung einer sicheren Plattform für die eID-Applikation (vgl. Abschnitt 3.4) beim Chipkarten-basierten Identitätsnachweis mit alternativen Chipkarten eine essentielle Bedeutung zu.

Außerdem müssen bei Einsatz alternativer Chipkarten in jedem Fall, und beim nPA zumindest sofern Protokolle für das föderierte Identitätsmanagement (z.B. SAML [44]) genutzt werden, entsprechende Vorkehrungen gegen Man-in-the-Middle (MITM) Angriffe (vgl. [45, Figure 5]) getroffen werden. Da auf der eGK oder auf Signaturkarten private Schlüssel und X.509-basierte Zertifikate vorhanden sind, die für eine starke Client-Authentisierung im TLS-Protokoll und dem darauf basierenden SAML-Holder-of-Key-Binding [46, 47] genutzt werden können, bietet sich dies zur Abwehr von MITM-Angriffen an. Beim nPA – und Karten mit ähnlichen kartenprüfbaren Zertifikaten – hingegen kann das in [48, Teil 7, Abschnitt 3.3.10] beschriebene Verfahren für die Abwehr von MITM-Angriffen und für die Kanalbindung genutzt werden. Darüber hinaus sind in [49] weitere Varianten für die TLS-Kanalbindung beschrieben.

3.6 Server

Das Server-System umfasst eine Web-Applikation (WebApp), die den Dienst bereitstellt und den Identitätsnachweis veranlasst, und einem für den entsprechenden

Ausweis geeigneten Authentisierungsdienst (eID-Server), der die erforderliche Funktionalität für den Chipkarten-basierten Identitätsnachweis bereitstellt. Für den Zugriff auf die im neuen Personalausweis gespeicherten Daten sind Berechtigungszertifikate und zugehörige private Schlüssel nötig, die durch adäquate Sicherheitsmaßnahmen geschützt werden müssen (§ 21 Abs. 2 Nr. 4 PAuswG). Bei den vom Diensteanbieter zu erfüllenden Anforderungen ist der Stand der Technik maßgebend und die Vergabestelle für Berechtigungszertifikate[3] legt in Richtlinien die weiteren technischen und organisatorischen Anforderungen fest, die ein Diensteanbieter zu erfüllen hat, um für die Nutzung von Berechtigungszertifikaten zugelassen zu werden (§ 29 Abs. 2 PAuswV).

Insbesondere muss der Diensteanbieter bei der Beantragung eines Berechtigungszertifikates eine Erklärung abgeben, dass ein Datenschutz- und Datensicherheitskonzept für die nPA-relevanten Systemkomponenten existiert (vgl. [50, Abschnitt V]). Die näheren Anforderungen an den Datenschutz und die Datensicherheit bei der Nutzung von Berechtigungszertifikaten sind in [51, Abschnitt 2.7] und [52, Anhang C] geregelt. Insbesondere wird dort (vgl. Maßnahme 30 in Anhang C, Abschnitt 4.3.4 von [52]) die Erstellung eines Sicherheitskonzeptes gemäß den BSI-Grundschutz-Standards [53, 54, 55] gefordert und eine Grundschutz-Zertifizierung [56] nach ISO 27001 [57] empfohlen.

Auch wenn ein solches Sicherheitskonzept nur beim nPA-basierten Identitätsnachweis gefordert ist, sind entsprechende Betrachtungen auch bei der Nutzung der eGK sicherlich mehr als empfehlenswert.

3.7 Public-Key Infrastruktur

Die dezentralen Komponenten für den Chipkarten-basierten Identitätsnachweis nutzen an verschiedenen Stellen zentrale Public-Key-basierte Vertrauensinfrastrukturen. Die wesentlichen Aspekte der Public-Key Infrastrukturen im Umfeld des nPA sind in [11, 18, 59, 60] geregelt. Eine entsprechende Zertifizierungsrichtlinie für die X.509-Zertifikate auf der eGK findet sich in [61]. Hierbei wird sinnvoller Weise (vgl. [59, 61]) jeweils die Existenz eines entsprechenden Sicherheitskonzeptes (beispielsweise gemäß der BSI-Grundschutz-Standards [53, 54, 55]) gefordert. Auf der anderen Seite entbindet eine Akkreditierung als Zertifizierungsdiensteanbieter (ZDA) gemäß Signaturgesetz hier jeweils von der Pflicht, die Sicherheit der Systeme und Prozesse durch die Vorlage eines spezifischen Sicherheitskonzeptes nachzuweisen. Hierbei ist bedenklich, dass das SigG-spezifische Sicherheitskonzept eines akkreditierten ZDA nicht notwendigerweise alle für den Chipkarten-basierten Identitätsnachweis relevanten Systeme und Prozesse umfassen muss. Deshalb bleibt es zu hoffen, dass die ZDAs hier aus eigenem Interesse alle notwendigen Sicherheitsmaßnahmen ergreifen, so dass sich die DigiNotar-

[3] Siehe http://www.bva.bund.de/vfb.

Katastrophe [62] nicht im Umfeld des Chipkarten-basierten Identitätsnachweises wiederholt.

4. Zusammenfassung

In diesem Beitrag wurde zunächst gezeigt, dass sich ein an § 18 PAuswG angelehntes Verfahren für den „Chipkarten-basierten Identitätsnachweis“ nicht nur mit dem neuen Personalausweis, sondern auch mit alternativen Chipkarten, wie z.B. der elektronischen Gesundheitskarte oder typischen Signaturkarten realisieren lässt. Wie in Abschnitt 2.2.2 gezeigt, besteht der wesentliche Unterschied darin, dass sich das Terminal beim nPA vor dem Datenzugriff authentisieren muss, wohingegen die gespeicherten Identitätsattribute bei der eGK und typischen Signaturkarten frei auslesbar sind. Sofern den verschiedenen in diesem Beitrag beschriebenen Bedrohungen mit entsprechenden Sicherheitsmaßnahmen entgegengewirkt wird – und insbesondere am Client eine geeignete Applikation auf einer vertrauenswürdigen Systemplattform eingesetzt wird – kann ein vergleichbares Niveau in Bezug auf Sicherheit und Datenschutz erreicht werden. Da umgekehrt auf den Einsatz von kostenintensiven Berechtigungszertifikaten und eID-Services[4] verzichtet werden kann, ergeben sich hierdurch wirtschaftliche Vorteile für die Diensteanbieter, die in Verbindung mit geeigneten Intermediärsinfrastrukturen, wie sie im SkIDentity-Projekt [63] vorgeschlagen wurden, möglicherweise zu einer schnelleren Verbreitung des Chipkarten-basierten Identitätsnachweises führen könnten.

Literatur

[1] A. Roßnagel, G. Hornung: Ein Ausweis für das Internet. Der neue Personalausweis erhält einen „elektronischen Identitätsnachweis“, DÖV 2009, SS 301-306
[2] A. Roßnagel, G. Hornung, C. Schnabel: Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht, DuD 2008, SS 168-172
[3] G. Hornung, J. Möller: Passgesetz und Personalausweisgesetz, Kommentar, 2011
[4] D. Hühnlein: Identitätsmanagement - Eine visualisierte Begriffsbestimmung, DuD 3 / 2008, SS. 163-165
[5] D. Eske, D. Hühnlein, S. Paulus, J. Schmölz, T. Wich, T. Wieland: OpeneGK – Benutzerfreundliche und sichere Authentisierung für Mehrwertdienste im Gesundheitswesen, in Tagungsband „perspeGKtive 2010“, GI LNI 174, 2010, Seiten 83-103, http://www.ecsec.de/pub/openeGK.pdf
[6] BSI: Offizielles Portal für die AusweisApp, https://www.ausweisapp.bund.de
[7] D. Hühnlein, M. Horsch, J. Schmölz, T. Wich & al.: On the design and implementation of the Open eCard App, in Sicherheit 2012, GI LNI, 2012

[4] Siehe http://www.ccepa.de/eid-service-anbieter.

[8] B. Kowalski: Die eCard-Strategie der Bundesregierung im Überblick, in BIOSIG 2007: Biometrics and Electronic Signatures, GI LNI 108, Seiten 87–96, 2007
[9] Bundesregierung: eCard-Strategie der Bundesregierung, Pressemitteilung vom 09.03.2005, http://www.bmwi.de/BMWi/Redaktion/PDF/E/ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf , 2005
[10] ISO/IEC 7816: Identification cards – Integrated circuit cards – Part 1-15, International Standards, 1999-2011
[11] BSI: Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control (EAC), BSI TR-03110, Version 2.05, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html
[12] gematik: Die Spezifikation der elektronischen Gesundheitskarte - Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.2 vom 16.09.2008, http://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_egk/gematik_eGK_Spezifikation_Teil1_V2_2_0.pdf, 2008.
[13] BSI: Common Criteria Protection Profile - electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-CC-PP-0020-V3-2010-MA-01, Version 2.9, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/PP0020_V3_ma1b_pdf.pdf;jsessionid=82E4FCD5DE6A2B7761A1A156A8CF3EF6.2_cid248?__blob=publicationFile
[14] BSI: Common Criteria Protection Profile - Electronic Identity Card (ID_Card PP), BSI-CC-PP-0061, Version 1.03, 2009, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ReportePP/pp0061b_pdf.pdf?__blob=publicationFile
[15] gematik: Die Spezifikation der elektronischen Gesundheitskarte - Teil 2: Grundlegende Applikationen, Version 2.2.0 vom 25.03.2008, http://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_egk/gematik_eGK_Spezifikation_Teil2_V2_2_0.pdf, 2008
[16] gematik: Speicherstrukturen der eGK für Gesundheitsanwendungen, Version: 1.6.0 vom 18.03.2008, http://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_egk/gematik_eGK_Speicherstrukturen_V1_6_0.pdf
[17] ISO/IEC: Identification cards - Contactless integrated circuit cards - Proximity cards, ISO/IEC 14443 - Part 1-4, International Standard, 2008-2011
[18] BSI: Certificate Policy für die eID-Anwendung des ePA - Elektronischer Identitätsnachweis mit dem elektronischen Personalausweis, Version 1.28, 10.10.2011 https://www.bsi.bund.de/cae/servlet/contentblob/992808/publicationFile/65003/Certificate_Policy.pdf
[19] NIST: Electronic Authentication Guideline, NIST Special Publication 800-63-1. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[20] BSI: Anforderungen an Chipkartenleser mit nPA Unterstützung, BSI-TR-03119, Version 1.2, 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03119/BSI-TR-03119_V1_pdf.pdf?__blob=publicationFile
[21] C. Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle, 7., überarbeitete und erweiterte Aufl. Oldenbourg, München, 2012
[22] R. Dhamija, J. D. Tygar, M. Hearst: Why phishing works, in Proceedings of the Conference on Human Factors in Computing Systems (CHI), 2006
[23] J. Schejbal: ePerso: PIN-Diebstahl ohne Malware, persönlicher Blog von Jan Schejbal, https://janschejbal.wordpress.com/2011/01/17/eperso-pin-diebstahl-ohne-malware/
[24] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, E. Nunge: Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. in

Proceedings of the 3rd symposium on Usable privacy and security (SOUPS '07), 2007, SS. 88-99

[25] Y. Zhang, S. Egelman, L. Cranor, J. Hong: Phinding phish: Evaluating anti-phishing tools, in Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS), 2007

[26] W. Liu, X. Deng, G. Huang, A.Y. Fu: An antiphishing strategy based on visual similarity assessment, IEEE Internet Computing, Vol. 10, Issue 2, 2006, SS. 58-65

[27] D. Fox: Security Awareness - Oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit, DuD 27, 2003, SS. 676-680

[28] W. Rankl, W. Effing: Handbuch der Chipkarten: Aufbau – Funktionsweise - Einsatz von Smart Cards, 4., überarbeitete und aktualisierte Aufl. Hanser, München, 2002

[29] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. In: Wiener M (ed) Advances in Cryptology – CRYPTO' 99, Springer, Berlin/Heidelberg, 1999

[30] D. Boneh, R. A. DeMillo, R.J. Lipton: On the Importance of Checking Computations, Math and Cryptography Research Group, Bellcore, 1996

[31] E. Biham, A. Shamir: A new cryptanalytic attack on DES, 1996

[32] O. Kömmerling, M. Kuhn: Design principles for tamper-resistant smartcard processors, in Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology (WOST'99), 1999, SS. 9-20

[33] R. Anderson, M. Kuhn: Tamper Resistance - a Cautionary Note, in the Proceedings of the Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, SS. 1-11

[34] W. Jackson: Engineer shows how to crack a 'secure' TPM chip, Government Computer News, http://gcn.com/Articles/2010/02/02/Black-Hat-chip-crack-020210.aspx

[35] G. P. Hancke: Practical eavesdropping and skimming attacks on high-frequency RFID tokens, Journal of Computer Security - 2010 Workshop on RFID Security (RFIDSec'10), Volume 19 Issue 2, April 2011, SS. 259-288

[36] J. Bender, M. Fischlin, D. Kügler: Security Analysis of the PACE Key-Agreement Protocol, in Proceedings of Information Security, LNCS 5735, 2009, SS. 33-48

[37] O. Dagdelen, M. Fischlin: Security Analysis of the Extended Access Control Protocol for Machine Read-able Travel Documents, ISC 2010, SS. 54-68

[38] bos GmbH & Co. KG: Governikus Autent, http://www.bos-bremen.de/de/governikus_autent/1854605/

[39] G. Eist : Praktische Demonstration erheblicher Sicherheitsprobleme bei Schweizer SuisseID und deutschem elektronischen Personalausweis, CCC Blog, 2010, http://www.ccc.de/de/updates/2010/sicherheitsprobleme-bei-suisseid-und-epa

[40] F. Morgner, D. Oepen: „Die gesamte Technik ist sicher" – Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis, 27th Chaos Communication Congress, 2010, http://events.ccc.de/congress/2010/Fahrplan/events/4297.en.html

[41] J. Schejbal: AusweisApp gehackt (Malware über Autoupdate), Persönlicher Blog von Jan Schejbal, 2010, https://janschejbal.wordpress.com/2010/11/09/ausweisapp-gehackt-malware-uber-autoupdate/

[42] T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol, Version 1.2, IETF RFC 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt

[43] S. Gajek, M. Manulis, O. Pereira, A.-R. Sadeghi, J. Schwenk: Universally Composable Security Analysis of TLS, in Proceedings of Provable Security, LNCS 5324, 2008, SS. 313-327

[44] S. Cantor, J. Kemp, R. Philpott, E. Maler: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15.03.2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005

[45] J. Eichholz, D. Hühnlein, J. Schwenk: SAMLizing the European Citizen Card, in A. Brömme & al. (Ed.), BIOSIG 2009: Biometrics and Electronic Signatures, GI-Edition Lecture Notes in Informatics (LNI) 155, 2009, pp. 105-117, http://www.ecsec.de/pub/SAMLizing-ECC.pdf

[46] N. Klingenstein: SAML V2.0 Holder-of-Key Web Browser SSO Profile, OASIS Committee Draft 02, 05.07.2009, http://www.oasis-open.org/committees/download.php/33239/sstc-saml-holder-of-key-browser-sso-cd-02.pdf, 2009
[47] S. Gajek, L. Liao, J. Schwenk: Stronger TLS Bindings for SAML Assertions and SAML Artifacts, Proceedings of the 2008 ACM workshop on Secure Web Services, 2008
[48] BSI: eCard-API-Framework, BSI TR-03112, Version 1.1.1 vom 23.05.2011, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html
[49] J. Altman, N. Williams, L. Zhu: Channel Bindings for TLS, IETF RFC 5929, http://www.ietf.org/rfc/rfc5929.txt
[50] Vergabestelle für Berechtigungszertifikate: Leitlinie für die Vergabe von Berechtigungen für Diensteanbieter nach § 21 Abs. 2 Personalausweisgesetz, Version 1.0, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Leitlinie_VfB_Vergabe_Berechtigungszertifikate.pdf?__blob=publicationFile
[51] Vergabestelle für Berechtigungszertifikate: Technische und organisatorische Anforderungen zur Nutzung von Berechtigungszertifikaten, Version 1.0, http://www.personalausweisportal.de/SharedDocs/Downloads/DE/richtlinie_vfb_berechtigungen.pdf?__blob=publicationFile
[52] BSI: eID-Server, BSI TR 03130, Version 1.4.1 vom 08.10.2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_V1_4_pdf.pdf?__blob=publicationFile
[53] BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002.pdf
[54] BSI: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30757/standard_1003.pdf
[55] BSI: BSI-Standard 100-4: Notfallmanagement, https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30756/standard_1004.pdf
[56] BSI: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits, Version 2.1, 2008, https://www.bsi.bund.de/cae/servlet/contentblob/478206/publicationFile/31003/Pruefschema_V_2_1_pdf.pdf
[57] ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements, 2005
[58] T7 & TeleTrusT e.V.: Common PKI Specification for interoperable Applications – Part 1: Certificate and CRL-Profiles, Version 2.0, 20.01.2009, http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
[59] BSI: EAC-PKI'n für den elektronischen Personalausweis - Rahmenkonzept für den Aufbau und den Betrieb von Document Verifiern, BSI TR 03128, Version 1.1, 08. Oktober 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03128/BSI_TR-03128.pdf?__blob=publicationFile
[60] BSI: PKIs for Machine Readable Travel Documents - Protocols for the Management of Certificates and CRLs, BSI TR 03129, Version 1.10, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03129/BSI_TG_03129.pdf?__blob=publicationFile
[61] gematik: Certificate Policy - Gemeinsame Zertifizierungs-Richtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten, Version 1.2.0, 29.11.2007, http://www.gematik.de/cms/media/dokumente/release_0_5_3/release_0_5_3_pki_zertifikate/gematik_PKI_X_509-Certificate_Policy_ENCAUTOSIG_V1_2_0.pdf
[62] Heise: DigiNotar-Themenseite, http://www.heise.de/firma/DigiNotar

[63] D. Hühnlein, G. Hornung, H. Roßnagel, J. Schmölz, T. Wich, J. Zibuschka: SkIDentity – Vertrauenswürdige Identitäten für die Cloud, D-A-CH Security 2011, SS. 296-304