Vom elektronischen Reisepass zum Personalausweis: RFID und personenbezogene Daten – Lessons Learned !?

Harald Baier, CASED/Hochschule Darmstadt,
baier@cased.de

Tobias Straub, Duale Hochschule Baden-Württemberg Mannheim,
straub@dhbw-mannheim.de

Abstract: Seit 2005 werden in Deutschland Reisepässe mit einem integrierten, kontaktlosen Chip, der biometrische Daten des Inhabers speichert, ausgegeben. Diese Einführung wurde durch eine kontroverse Diskussion um den Datenschutz der auf dem Chip gespeicherten personenbezogenen Daten begleitet. Der für 2010 geplante elektronische Personalausweis verwendet teilweise dieselbe Technologie wie der Reisepass, bietet dem Inhaber aber zusätzlich durch Authentisierungs- und Signaturfunktionen weitere Einsatzmöglichkeiten in nicht-hoheitlichen, Internet-basierten Anwendungen.

Dieser Beitrag zeichnet die technische Fortentwicklung als Reaktion auf veröffentlichte Schwächen nach und bewertet die Wirksamkeit der getroffenen Maßnahmen im Hinblick auf den Schutz der persönlichen Daten des Inhabers. Es wird diskutiert, inwieweit der Entstehungsprozess von elektronischem Reisepass und elektronischem Personalausweis Modell-Charakter haben kann für die Einführung vergleichbarer Systeme mit kontaktloser Übertragungstechnologie.

1 Einleitung

Drahtlose Kommunikation stellt für deren Befürworter eine Erleichterung dar, ermöglicht sie doch komfortabel den Datenaustausch ohne Kabelsalat oder physischen Kontakt. Für deren Kritiker hingegen ist drahtlose Datenübertragung eher ein Sicherheitsrisiko. Das ist spätestens seit dem Masseneinsatz von WLAN in Institutionen und Haushalten in der öffentlichen Diskussion.

Als die ersten Konzepte für den elektronischen Reisepass (ePass) durch die Internationale Zivilluftfahrtorganisation ICAO einen kontaktlosen Chip (RF-Chip) für die Speicherung und den Datenaustausch mit den Kartenlesern vorsahen, entbrannten ähnliche Diskussionen. Gerade Datenschützer sahen große Risiken, dass unautorisiert Daten des ePasses aus- oder mitgelesen werden. Bis heute stehen sich Befürworter und Kritiker des kontaktlosen ePasses ohne Konsens gegenüber.

Konnte sich das Bundesministerium des Innern (BMI) bei dem ePass noch darauf berufen, dass drahtlose Chips durch internationale Gremien vorgeschrieben wurden, so ist die aktuelle Situation bei der Einführung des elektronischen Bundespersonalausweises (ePerso) eine andere: Grundsätzlich hätte sich das BMI nun auch für kontaktbehaftete Chips entscheiden können, wird aber nach aktueller Planung ab November 2010 kontaktlose Chips

als Trägermedium verwenden.

Hinsichtlich der Diskussion um Gefahren und Risiken bei der Realisierung des ePasses gibt es eine lange Historie. In diesem Beitrag soll nachgezeichnet werden, welches die wesentlichen Kritikpunkte im Hinblick auf den Schutz personenbezogener Daten auf dem ePass sind und ob diese für den ePerso ebenfalls zutreffen oder sie vom BMI ausgeräumt wurden.

Ausgangspunkt unserer Betrachtungen ist dabei die Tatsache, dass ePass und ePerso jeweils über die Luftschnittstelle angesprochen werden. Unser zentrales Ergebnis ist, dass durch ausgefeilte Zugriffsprotokolle die Daten auf ePass und ePerso adäquat geschützt sind, dass aber nach wie vor die Frage offen bleibt, warum das BMI beim ePerso an der drahtlosen Technik festhielt und warum man sich bei der ICAO für diese sicherheitskritische Technik entschied. Die Betrachtungen haben dabei ausdrücklich nicht zum Ziel, eine Bewertung vorzunehmen, welchen Sicherheitsgewinn der ePass oder der ePerso im Hinblick auf die Fälschung oder den Missbrauch im Vergleich zu den klassischen Papier-Ausweisdokumenten erzielt.

Der vorliegende Beitrag ist wie folgt aufgebaut: Zunächst zeichnen wir in Abschnitt 2 nach, unter welchen Randbedingungen die zwei Generationen der ePässe eingeführt wurden und stellen den Planungsstand des ePerso dar. Danach beschreiben wir in Abschnitt 3 die generellen Vor- und Nachteile von RF-Technik im Kontext elektronischer Ausweisdokumente. Anschließend diskutieren wir in Abschnitt 4 die relevantesten Angriffsszenarien auf personenbezogene Daten, insbesondere im Hinblick auf präventiven Schutz der Daten beim ePass bzw. eine Verbesserung der Maßnahmen bei der Einführung des ePerso; dabei liegt ein Augenmerk auf dem unautorisierten Auslesen von Daten. Wir schließen diesen Beitrag in Abschnitt 5 mit einer Bewertung und einem Ausblick.

2 Hintergrund der Einführung elektronischer Ausweisdokumente

Als Reaktion auf die Terroranschläge vom 11. September 2001 und die damit einhergehende Verschärfung von Sicherheitsmaßnahmen beschäftigte sich auch eine Initiative der internationalen Zivilluftfahrtorganisation (ICAO) mit der Weiterentwicklung der Pässe und Visa ([ICA06a], [ICA06b]). In Gremien der UN wurden weltweit verbindliche Standards für maschinenlesbare Reisedokumente (Machine Readable Travel Documents, MRTDs) formuliert, die insbesondere die Ausstattung hoheitlicher Dokumente zum Grenzübertritt mit einem kontaktlosen Chip vorgeben.

Dieser Chip dient einerseits der digitalen Speicherung der persönlichen Angaben wie Name und Geburtsdatum, wie sie bisher ohnehin im aufgedruckten maschinenlesbaren Bereich (Machine Readable Zone, MRZ) vorhanden waren. Andererseits enthält er aber nun zusätzlich biometrische Merkmale des Inhabers in digitalisierter Form, nämlich das Gesichtsbild und zwei Fingerabdrücke (in der Regel die beiden Zeigefinger).

Erklärte Ziele dieser Erweiterung mit zusätzlichen Sicherheitsmerkmalen waren es, die Fälschungs- und Manipulationssicherheit von Reisedokumenten zu erhöhen und den Missbrauch rechtmäßiger Dokumente im Falle einer Weitergabe bzw. eines Verlusts oder Dieb-

stahls zu erschweren ([ICA06a], [KN07]). Auch wird die Einführung des elektronischen Personalausweises mit denselben Zielen begründet [Bun08].

In diesem Beitrag betrachten wir folgende Systeme:[1]

- Den in Deutschland 2005 eingeführten *elektronischen Reisepass der ersten Generation* (in diesem Beitrag mit ePass 1.0 bezeichnet).
- Den aktuell in Deutschland ausgegebenen *elektronischen Reisepass der zweiten Generation*, auf dem technischen Stand von 2007 (ePass 2.0), der gegenüber dem ePass 1.0 in Details verändert wurde.
- Den durch die bisher veröffentlichten Spezifikationen beschriebenen *elektronischen Bundespersonalausweis* (ePerso[2]), dessen Einführung für 2010 geplant ist und der momentan in Pilotversuchen getestet wird.

Die Akzeptanz einer Technologie durch den Benutzer, die ihn in seinen Persönlichkeitsrechten betrifft, wird nicht allein durch technische, sondern auch sehr stark durch gesellschaftliche Faktoren bestimmt. Aus diesem Grund zeichnen wir im Folgenden die Schritte der Einführung (ePass, Abschnitt 2.1) bzw. Planung (ePerso, Abschnitt 2.2) und die begleitende öffentliche Diskussion nach. Technische Details werden in den jeweiligen Abschnitten besprochen.

2.1 Einführung des elektronischen Reisepasses

Der elektronische Reisepass der ersten Generation wurde in Deutschland am 01. November 2005 eingeführt. Zentrales Ziel, das die Bundesregierung mit dem Umstieg auf den ePass 1.0 erreichen wollte, war die Verringerung des Missbrauchs gegenüber dem klassischen Papierpass. Dazu integriert der ePass 1.0 einen Chip, der die auf dem ePass gedruckten Daten elektronisch speichert (einschließlich Gesichtsbild des Inhabers als biometrisches Merkmal). Die elektronischen Daten können über eine drahtlose Schnittstelle ausgelesen werden: Der ePass 1.0 verwendet also einen RF-Chip (Radio Frequency Chip).

Das Missbrauchsszenario, das dem ePass 1.0 zu Grunde liegt, ist das Fälschen eines Passes, etwa durch Manipulation eines echten Dokuments einer anderen Person oder – im schwerwiegenderen Fall – durch das Erstellen eines neuen Dokuments im Rahmen einer Totalfälschung. Dem wird begegnet, indem die aufgedruckten Daten zusätzlich elektronisch gespeichert und mit einer digitalen Signatur versehen werden (so genannte *passive Authentisierung*).

[1] Interessant, aber in diesem Beitrag aus Platzgründen nicht möglich, wäre es, weitere Systeme in die vergleichende Untersuchung mit einzubeziehen: Etwa die Reisepässe anderer Staaten oder etwa auch einen "abstrakten ICAO-Reisepass", der nur über die von der ICAO als verpflichtend vorgeschriebenen Merkmale verfügt. Letzterer würde im Hinblick auf das Datenschutz-Niveau eine untere Schranke darstellen. Beispielsweise wurde in den zunächst ausgegebenen US-amerikanischen Reisepässen nicht das in Abschnitt 4 beschriebene Verfahren Basic Access Control implementiert.

[2] Der besseren Unterscheidbarkeit wegen verwenden wir hier nicht die ebenfalls gebräuchliche Abkürzung ePA.

Im Vorfeld und während der Einführung maschinenlesbarer Reisedokumente gab es in 2005 und 2006 kontroverse, teilweise geradezu polemische Diskussionen. Diese wurden vor allem von Sicherheitsexperten und deren Gremien (z.B. dem Chaos Computer Club e.V., CCC) geführt, die einen Mehrwert an Sicherheit durch den Reisepass bezweifelten, teilweise sogar die Gefahr für Leib und Leben seines Inhabers heraufbeschworen.[3]

Die Debatten um den ePass verschwanden Ende 2006 und flammten Mitte 2007 wieder auf. Denn am 01. November 2007 stand die Einführung der zweiten Generation des ePasses an, die nunmehr auch die Speicherung des rechten und linken Zeigefingers auf dem RF-Chip vorsahen (ePass 2.0). Das hierbei auszuschließende Missbrauchszenario ist, dass ähnlich aussehende Personen den gleichen ePass zur Identitätsfeststellung verwenden könnten. Eine Unterscheidung kann anhand des Fingerabdrucks geschehen, da dieser bei zwei verschiedenen Personen (selbst von Zwillingen) mit sehr hoher Wahrscheinlichkeit differiert. Übersehen wurde dabei allerdings die Möglichkeit, durch übergestülpte Fingerabdruck-Attrappen[4] oder Angriffe auf den organisatorischen Ablauf in den Meldebehörden diesen Mechanismus auszuhebeln.

2.2 Planung des elektronischen Personalausweises

Parallel zur Einführung des ePasses wurde bereits die technische Spezifikation und Erprobung des elektronischen Personalausweises (ePerso) und eine entsprechende Gesetzesinitiative auf den Weg gebracht. Für die Nutzung als hoheitliches Ausweisdokument verwendet der ePerso, wie im Folgenden beschrieben wird, sehr ähnliche Funktionen wie der ePass. Neu sind allerdings die für den Bürger optionalen Erweiterungen eines multifunktionalen Tokens für die Authentisierung im Internet (so genannte *eID-Funktion*) sowie die nachladbare qualifizierte elektronische Signatur (QES).

Der ePerso kann bei Reisen in bestimmte Länder (z.B. innerhalb der EU) den ePass 2.0 ersetzen. Daher war zu erwarten, dass die hoheitliche Ausweisfunktion im ePerso identisch zu derjenigen im ePass 2.0 ist. Allerdings wurde im Rahmen der Erarbeitung des Grobkonzeptes für den ePerso die Verwendung der Fingerabdrücke als biometrisches Merkmal nicht mehr als verpflichtend vorgesehen, sondern nur noch optional. Das Bundesministerium des Innern weist in der Begründung zum Gesetzentwurf [Bun08] aber ausdrücklich darauf hin, dass beantragenden Bürgern die Einbeziehung der Fingerabdrücke in den ePerso empfohlen werden soll, um Missbrauch bei Verlust zu verhindern. Dennoch ist diese Inkonsistenz eine Bestätigung all derjenigen, die die Sinnhaftigkeit der Verwendung von Fingerabdrücken im ePass 2.0 anzweifeln.

Die elektronische Identitätsfeststellung (eID) soll es zunächst Anbietern von Dienstleistungen im Internet ermöglichen, eine zuverlässige Authentifizierung von Kunden zu ermöglichen – das betrifft sowohl den Erstkontakt bei der Kundenregistrierung als auch bei der dauerhaften Nutzung einer Dienstleistung. Je nach angefragten Daten gibt der

[3] So das Beispiel einer „RFID-fähigen Bombe“, die unbemerkt die Identität oder Nationalität eines Passinhabers in der Nähe ausliest und abhängig davon explodiert (siehe `http://blogs.zdnet.com/Ou/?p=289`).

[4] Siehe etwa die Anleitung vom CCC unter `http://www.ccc.de/biometrie/fingerabdruck_kopieren`.

Kunde nur die Daten frei, die im jeweiligen Kontext benötigt werden, auch ist die Nutzung von Pseudonymen möglich. Zum Beispiel genügt zur Registrierung in einem Online-Kasino, das nur von Erwachsenen genutzt werden darf, die Übermittlung, ob der Kunde volljährig ist oder nicht. Das genaue Alter ist irrelevant und soll nicht vom Anbieter ausgelesen werden können. Der ePerso ist darüber hinaus in der Lage, durch die *Terminal-Authentisierung* (siehe Abschnitt 4.3) auch die Identität des Diensteanbieters zu prüfen. Damit sollen Phishing-Angriffe verhindert oder zumindest erschwert werden.

3 Generelles Für und Wider von RFID-Technologie

Die Integration der von der Öffentlichkeit noch nicht hinreichend verstandenen RF-Technologie in Reisepässen hat, gepaart mit Schreckensszenarien rund um missbrauchte biometrische Daten, zu einer Reihe von, – wie wir noch sehen werden – nicht immer begründeten, Ängsten und Widerständen geführt.

Die von der ICAO standardisierte Ausstattung von MRTDs mit einem zusätzlichen Chip verfolgt zwei Ziele: Zum einen sollte ein weiteres, schwer fälschbares Sicherheitsmerkmal integriert werden. Zum anderen sollte der Chip die automatisierte Kontrolle biometrischer Merkmale unterstützen und damit die Bindung des Dokuments an seinen rechtmäßigen Inhaber verstärken.

Diese Ziele können prinzipiell durch Mikroprozessor-Chips realisiert werden, die über eine kontaktlose oder kontaktbehaftete Schnittstelle von einem Lesegerät angesprochen werden können. Aufgrund der Vorgaben der ICAO wurden die MRTDs (also ePass 1.0, ePass 2.0) mit kontaktlosen Chips konzipiert.

Im Hinblick auf den ePerso hat Deutschland grundsätzlich Wahlfreiheit zwischen kontaktbehafteten oder kontaktlosen Chips, die Bundesrepublik favorisierte für den ePerso die RF-Technologie. Das zugehörige Grobkonzept des Bundesministerium des Innern ([BMI08]) beschreibt selbst einige Realisierungen elektronischer Identitätsdokumente in der EU oder darüber hinaus. Die meisten der darin aufgeführten Länder mit solchen Ausweisdokumenten haben sich für kontaktbehaftete Chips entschieden (Belgien, Estland, Italien, Spanien, Hongkong). Das Grobkonzept nennt dann zunächst die Kompatibilität mit dem ePass 2.0 als Grund, um auch den ePerso kontaktlos zu realisieren.

Als Vorteil einer kontaktlosen Übertragung per RFID werden der geringere Verschleiß und die einfachere Handhabbarkeit im Vergleich zu den Steckvorgängen einer kontaktbehafteten Chipkarte sowie die Unempfindlichkeit aufgrund der vollständigen Umhüllung mit Plastik oder anderem Material angeführt ([BMI08], [ICA06a]). In Bezug auf die elektronischen Reisepässe hat die Bundesregierung keine Wahl: Durch die Festlegung der ICAO muss jeder deutsche ePass gemäß dem relevanten Standard ISO 14443 [ISO08] kontaktlos realisiert werden.

Oftmals argumentieren Verfechter der kontaklosen Chips mit der einfacheren Handhabung von RF-Chips im Vergleich zu kontaktbehafteten Chips. Allerdings ist bei der hoheitlichen Funktion stets ein direktes Auflegen des RF-Chip auf das Lesegerät erforderlich. Damit sind aus Sicht der Autoren die Vorteile der Berührungslosigkeit hinfällig. Auch ein häufig

vorgebrachtes Argument der durch Kontaktlosigkeit möglichen längeren Laufzeit ist aus unserer Sicht nicht valide, da es keine wirklichen Erfahrungswerte dafür gibt. Außerdem hieße dies im Umkehrschluss, dass Länder mit kontaktbehafteten Ausweisdokumenten mit gleicher Gültigkeitsdauer wie deutsche Pässe oder Personalausweise sich für eine fehleranfälligere Technik entschieden hätten.

Bei einem RF-Chip nimmt man dagegen die Nachteile in Kauf, dass der Aufbau jeder drahtlosen Verbindung unbemerkt von einem Dritten initiiert, gestört sowie von ihm die zwischen berechtigten Entitäten übertragenen Daten (auch wenn sie verschlüsselt sind) aufgezeichnet werden können (so genanntes *Sniffing*).

Dies setzt jeweils eine räumliche Nähe von Angreifer und Chip voraus. Die in ePass 1.0, ePass 2.0 und ePerso verwendeten Chips arbeiten gemäß dem o.g. Standard ISO 14443 mit einer spezifizierten Lesereichweite von 5 bis 10 cm. Allerdings ist zu beachten, dass unter Laborbedingungen Signale auch in 2 bis 3 m Entfernung mitgelesen werden können. Eine Reichweiten-Studie des Bundesamtes für Sicherheit in der Informationstechnik (MARS, [BSI08b]) konnte in einer Entfernung von $2{,}30$ m noch alle, in $2{,}45$ m Entfernung allerdings nur noch die Hälfte aller übermittelten Kartennummern richtig lesen. Die (optimistische) theoretische Berechnung des BSI ergibt eine Maximalreichweite von 4 m.

Als radikale Maßnahme zum Selbstdatenschutz wurde verschiedentlich die komplette Zerstörung des RFID-Chips durch den Inhaber selbst vorgeschlagen. Da ein Ausweisdokument Eigentum der Bundesrepublik ist, handelt es sich dabei um Sachbeschädigung, die allerdings in der Praxis bei entsprechender Ausführung schwer nachweisbar sein dürfte. Der Inhaber könnte seine Verantwortung mit dem Verweis auf Produktionsfehler des Chips oder der Zerstörung durch Dritte, denen das Dokument ausgehändigt wurde, abstreiten. Trotz eines defekten Chips (und damit Wegfall eines Sicherheitsmerkmals) bleiben Pass und Personalausweis gültige Dokumente [ICA06b]. In öffentlich zugänglichen Quellen ist stets davon die Rede, dass zusätzliche Kontrollen vorgenommen werden können, wobei nicht offen gelegt wird, welche dies im Einzelnen sind.

Dass ein defekter Chip nicht allzu viele Unannehmlichkeiten für den Inhaber des Dokuments mit sich bringen würde, lässt sich vermuten vor dem Hintergrund, dass das Sicherheitsmerkmal Fingerabdruck nicht einheitlich in ePersos gespeichert ist und daher für hoheitliche Zwecke *nicht* vorausgesetzt werden kann (nach den Diskussionen im Gesetzgebungsverfahren wurde entschieden, die Aufnahme von Fingerabdrücken in den ePerso in das Ermessen des Inhabers zu stellen). Dies gilt zunächst für hoheitliche Anwendungen in Deutschland, sollte aber auch bei der Verwendung des ePerso als Passersatz innerhalb der EU gelten (Vertreter des BMI propagieren stets, dass ein ePass 2.0 mit defektem RF-Chip von anderen Staaten problemlos akzeptiert wird).

Aus Sicht der Autoren hätte die Entscheidung für RFID im ePerso kritischer hinterfragt werden sollen. Gerade vor dem Hintergrund, dass die hoheitliche Funktion nur eine von dreien im ePerso ist, sehen wir das Argument der Kompatibilität zum ePass 2.0 als nachrangig an. Viele Diskussionen und ausgefeilte Schutzmaßnahmen wären dem BMI und dem BSI erspart geblieben, wenn man auf kontaktbehaftete Chips gesetzt hätte.

4 Diskussion der Technik unter dem Blickwinkel Datenschutz

In den folgenden Abschnitten werden einige technische Aspekte unter dem Blickwinkel Datenschutz diskutiert. Dabei wurde bewusst eine Auswahl getroffen sowie die Detailtiefe der Darstellung aufgrund der Seitenbegrenzung angepasst. Die von uns dargestellten Aspekte spiegeln die in der Öffentlichkeit am meisten diskutierten Eigenschaften des ePass bzw. des ePerso wider.

Jeder dieser Abschnitte ist nach folgendem Schema strukturiert:

- Liste der für diesen Aspekt relevanten personenbezogenen Daten.
- Angriffsszenarien.
- Implementierte Schutzmaßnahmen zur Abwehr dieser Angriffe.
- Bewertung.
- Verbesserungspotenzial.
- Tabellarische Zusammenfassung.

4.1 Tracking – Erstellung von Bewegungsprofilen über Chip-Eigenschaften

Relevante personenbezogene Daten: Während des Verbindungsaufbaus mit einem drahtlosen Chip findet üblicherweise zunächst ein so genanntes *collision avoidance protocol* (siehe etwa [Fin06]) Anwendung, um einen bestimmten Chip über seinen eindeutigen Identifier in einer potenziell großen Menge anderer Chips gezielt anzusprechen. Da der Chip in einem Ausweisdokument eindeutig dem Inhaber zugeordnet ist, handelt es sich beim Chip-Identifier um ein personenbezogenes Datum. In beschränktem Umfang gilt dies auch für die einem Chip eigene Funkcharakteristik (die sich durch so genanntes *Radio Fingerprinting* ermitteln lässt, [AO05]).

Angriffsszenario: Die feste ID eines Chips im Communication Layer kann zur unbemerkten Wiedererkennung einer (unbekannten, aber eindeutig bestimmbaren) Person bzw. deren Re-Identifikation verwendet werden. Ein typisches Szenario ist z.B. in einem Geschäft gegeben, in dem ein Kunde bei der Bezahlung einmalig eine Kredit- oder Kundenkarte benutzt und damit seinen Namen offen gelegt hat, dem über ein verstecktes Lesegerät an der Kasse die ID des Chips zugeordnet wird. Der Fall der unbemerkten Re-Identifikation nach einem in der Vergangenheit autorisierten regulären Lesezugriff wird in Abschnitt 4.2 besprochen.

Implementierte Schutzmaßnahmen: Gegen diese Möglichkeit schützen Chips, die keine feste ID verwenden, sondern für jeden Kommunikationsvorgang dynamisch eine zufällige ID aus einem hinreichend großen Bereich wählen. Dieser Mechanismus ist für ePass 1.0, ePass 2.0 und ePerso gleichermaßen implementiert.

Bewertung: Zunächst erscheint uns die Schutzmaßnahme unter der Annahme, dass der Pseudozufallszahlengenerator über eine entsprechende Qualität verfügt, geeignet, das dargestellte Angriffsszenario auszuschließen. Unter dieser Voraussetzung ist ein unbemerktes Tracking auf Basis der vom Chip im Verbindungsaufbau übermittelten ID nicht möglich. Von Seiten des BMI/BSI sind allerdings keine Aussagen zur Funktionsweise oder Qualität des Generators bekannt. Wie Avoine und Oechslin [AO05] zeigen, ist bezüglich der dynamischen IDs von RFID-Chips durchaus eine gewisse Skepsis gegenüber den Implementierungen der Hersteller angebracht. Die Gefahr des Radio Fingerprintings schätzen wir aufgrund der derzeit verfügbaren Erkenntnisse und alternativer Methoden wie etwa die Erfassung über ohnehin vorhandene Überwachungskameras als vernachlässigbar ein.

Verbesserungspotenzial: Der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD[5]) oder der Chaos Computer Club haben darüber hinaus vorgeschlagen, einen Faraday-Käfig (d.h. eine metallische Schutzhülle) zu verwenden. Damit kann jeder Bundesbürger einen unbefugten und unbemerkten Verbindungsaufbau mit seinem Ausweisdokument durch eine leicht nachvollziehbare, wenngleich auch etwas umständliche Maßnahme, verhindern.

Aus unserer Sicht hätte man trotz Entscheidung für einen kontaktlosen Chip den Bedenken des unbemerkten Verbindungsaufbaus und der Anforderung der Kontrollierbarkeit durch den Inhaber schon beim Design des Ausweisdokuments Rechnung tragen können: Durch Einbringen metallischer Folie in den Einband des ePasses würde gleichsam datenschutz- und benutzerfreundlich bei minimalen Kosten das Angriffsszenario des unbemerkten elektronischen Auslesens definitiv verhindert.[6] Beim ePerso ist dies zwar aufgrund der Form der Chip-Karte nicht möglich, allerdings könnte man sich hier z.B. einen kleinen Schalter auf der Karte vorstellen, der mit dem Finger geschlossen würde. Dabei müsste es sich nicht unbedingt um einen mechanischen (und damit anfälligen) Schalter handeln, sondern z.B. um zwei Kontakte nahe beieinander, deren Überbrückung den Zugriff gestattet.

Tracking	ePass 1.0	ePass 2.0	ePerso	Verbesserung
Technik	überall dynamische IDs			Faraday-Käfig, Schalter
Datenschutz	hoch	hoch	hoch	maximal

4.2 Skimming – Unbemerkter unautorisierter Zugriff auf Datensegmente

Relevante personenbezogene Daten: Die elektronisch gespeicherten Daten sind in ePass oder ePerso in verschiedenen Datengruppen organisiert. In der Datengruppe 1 des ePasses sind die auf dem ePass aufgedruckten personenbezogenen Stammdaten elektronisch gespeichert: Herausgebender Staat, Passnummer, Ablaufdatum sowie Geschlecht, Name, Geburtstag und -ort des Inhabers. In Datengruppe 2 wird das Gesichtsbild des Besitzers

[5] `www.foebud.org`

[6] Allerdings besteht dabei weiterhin die Gefahr, dass ein Ausweisdokument, welches zwar bewusst aus der Hand gegeben wurde, etwa beim Check-In im Hotel, doch elektronisch gegen den Willen des Inhabers gelesen werden könnte. Wollte man dieses Szenario ausschließen, so müsste eine vom Inhaber zu steuernde und nachvollziehbare Aktivierung/De-Aktivierung des Chips, z.B. durch eine PIN, ermöglicht werden.

elektronisch gespeichert. Beim ePerso sind dies ähnliche Daten.

Angriffsszenario: Ein Angreifer versucht, ohne Wissen und damit ohne Zustimmung des Dokumenteninhabers die elektronisch gespeicherten Daten der Datengruppen 1 und 2 über die drahtlose Schnittstelle gemäß ISO 14443 auszulesen. Das unbemerkte unautorisierte Auslesen wird als *Skimming* bezeichnet.[7].

Implementierte Schutzmaßnahmen: Zur Vermeidung dieses Angriffs sind die Schutzmaßnahmen in ePass und ePerso grundverschieden. ePass 1.0 und ePass 2.0 verwenden als Schutzmaßnahme *Basic Access Control* (BAC, Anhang H in [BSI08a]). Die Idee hinter BAC ist einfach: Nur wenn der Auslesende bereits teilweise weiß, was auf dem ePass aufgedruckt ist, darf er auf die Daten der Datengruppen 1 und 2 zugreifen. Realisiert wird BAC daher dadurch, dass aus Teilen der Datengruppe 1 ein symmetrischer kryptographischer Zugriffschlüssel abgeleitet wird[8]. Nur wenn das Lesegerät den RF-Chip auf diese Weise überzeugt, dass es den Zugriffschlüssel kennt, darf es die Daten aus den Datengruppen 1 und 2 auslesen.

Im ePerso wurde hingegen das auf Diffie-Hellman basierende PACE-Protokoll (Password Authenticated Connection Establishment, [BSI08a], [BKMN08]) implementiert. Zugriff auf den ePerso wird nur einem Lesegerät gewährt, das eine aufgedruckte 6-stellige numerische *Karten-PIN*[9] kennt.

Bewertung: Zunächst muss bei diesem Angriffsszenario berücksichtigt werden, dass sich der Angreifer (oder ein von ihm kontrollierter Leser) in räumlicher Nähe zu dem auszulesenden Dokument befinden muss. Zwar trifft die in Abschnitt 3 zitierte MARS-Studie des BSI nur Aussagen über passives Mitlesen (Sniffing), in [BKMN08] ist für aktives Auslesen von einer Reichweite von 25 cm Entfernung die Rede. Darüberhinaus wird jeder Zugriffsversuch mit einer Dauer von 1 Sekunde veranschlagt.

Zwar gehen die Einschätzungen über die Entropie von BAC-Zugriffschlüsseln weit auseinander (siehe Abschnitt 4.4), dennoch erscheint BAC mit einer effektiven Schlüssellänge von 40 Bit vor dem Hintergrund der doch eher geringen Sensibilität der Daten sowie des hohen Zeitaufwands in der Größenordnung einiger Jahre[10] ausreichend.

Interessanterweise ist das neue Verfahren PACE im Hinblick auf den Schutz gegen Skimming schwächer als BAC: Da die Kenntnis der aufgedruckten Karten-PIN hinreichend für den Verbindungsaufbau ist, reduziert sich der mittlere Aufwand für das Raten auf $500.000 \approx 2^{19}$ Versuche. Dies reduziert, wenn man wiederum 1 Sekunde für jeden Versuch annimmt, den Zeitaufwand auf sechs Tage.

Unter diesen Randbedingungen ist ein unbemerktes Auslesen ohne Kenntnis der aufgedruckten Daten damit weiterhin als eher unrealistisch einzuschätzen. Verglichen damit dürfte der Aufwand für einen einfachen Taschendiebstahl deutlich geringer sein.

---

[7] Von „Skimming“ spricht man auch im Zusammenhang mit einer Variante von Bankkarten-Betrug, bei der Magnetstreifen heimlich kopiert werden. Diese Bedeutung ist hier jedoch nicht gemeint.

[8] Konkret sind dies die numerischen Felder der Maschinenlesbaren Zone (MRZ), die mit Prüfziffern abgesichert sind: Passnummer, Geburtsdatum, Ablaufdatum [KN07].

[9] Nicht zu verwechseln mit der geheimen PIN derselben Länge, die die eID-Funktion aktiviert.

[10] Im Mittel sind 2^{39} Versuche erforderlich, von denen jeder 1 Sekunde dauert, woraus sich $2^{39}\ \mathrm{Sekunden} = 17420\ \mathrm{Jahre}$ ergeben.

Allerdings können beide Verfahren nicht dagegen schützen, dass ein Angreifer, der den BAC-Schlüssel bzw. die Karten-PIN bereits kennt (sei es von einem durch den Inhaber ihm oder einem Dritten gegenüber autorisierten Zugriff), den Inhaber umbemerkt reidentifizieren und damit Bewegungsprofile bilden kann.

Verbesserungspotenzial: Bei Ausweisdokumenten ohne RFID-Funktionalität war es für den Inhaber klar erkenn- und steuerbar, welche Personen Zugriff darauf erhalten. Durch die Möglichkeit des drahtlosen Auslesens wird dieses Konzept zunächst aufgeweicht, da eine Aktion des Inhabers nicht mehr erforderlich ist. Mit BAC wurde versucht, den Prozess der bewussten und willentlichen Übergabe des Dokuments nachzubilden, um ein unbemerktes Auslesen zu verhindern.

Wir halten fest, dass dieses Prinzip beim erstmaligen Gebrauch funktioniert, jedoch untauglich ist, eine Re-Identifikation (ggf. unter Kollaboration mehrerer Parteien) zu verhindern. In dieser Hinsicht ist PACE auch keine Verbesserung. Das beabsichtigte Prinzip hätte anstelle einer digitalen Hilfskonstruktion besser mit dem bereits in Abschnitt 4.1 erwähnten, intuitiven Aktivieren der RFID-Funktionalität realisiert werden sollen.

Skimming	ePass 1.0 ePass 2.0	ePerso	Verbesserung
Technik	BAC	PACE	Faraday-Käfig, Schalter
Datenschutz	hoch	mittel	maximal
gg. Re-Ident.	kein		maximal

4.3 Sniffing – Mitlesen einer autorisierten Kommunikation

Oft wird dieses Angriffsszenario auch als *passives Mitlesen* bezeichnet, weil der Angreifer nicht aktiv in die autorisierte Kommunikation eingreift.

Relevante personenbezogene Daten: Wir nehmen an, dass die von einem Sniffing-Angriff betroffenen Daten die gleichen sind wie in Abschnitt 4.2, also die Datengruppen 1 und 2. Hintergrund dieser Annahme ist, dass die übrigen Daten, insbesondere die biometrischen Daten (Fingerabdrücke) durch andere technische Maßnahmen geschützt sind.

Angriffsszenario: Ein Angreifer versucht, ohne Wissen und damit ohne Zustimmung des Dokumenteninhabers die zwischen RF-Chip und autorisiertem Lesegerät drahtlos übertragenen Daten abzufangen, zu speichern, zu entschlüsseln und schließlich zu lesen. Ein derartiger Ciphertext-Only-Angriff ist prinzipiell immer möglich, sofern sich der Angreifer in Empfangsreichweite des Signals befindet.

Implementierte Schutzmaßnahmen: Zur Vermeidung dieses Angriffs kommen die in Abschnitt 4.2 beschriebenen Verfahren BAC und PACE zum Einsatz.

Bewertung: PACE erscheint uns angesichts der verwendeten kryptografischen Sicherheitsparamter auf absehbare Zeit angemessen sicher, einen Sniffing-Angriff wirksam zu unterbinden. PACE verwendet eine anonyme Diffie-Hellman-Schlüsselvereinbarung, in der die Karten-PIN nur als Indiz dient, dass das Dokument vorliegt, jedoch nicht für die

Ableitung eines Verschlüsselungsschlüssels dient.[11] Ein passiver Angreifer hat jedoch – dies ist die grundlegende Eigenschaft von Diffie-Hellman – keine Möglichkeit, den Klartext zu ermitteln, selbst bei Kenntnis der lediglich zur schwachen Authentifikation dienenden Karten-PIN.

BAC bietet keinen vergleichbaren Schutz. Im Unterschied zu einem aktiven Auslesen kann der Angreifer hier bequem offline einen Brute-Force-Angriff auf alle möglichen Zugriffschlüssel starten. Unterstellt man die mit üblicher Hardware realistische Zahl von 1 Mio. Versuche pro Sekunde, so benötigt ein Brute-Force-Angriff auf BAC bei einer Entropie von 40 Bit im Durchschnitt nur noch $2^{39} \cdot 10^{-6}$ Sekunden $= 6.4$ Tage. Auch bei relativer Öffentlichkeit der geschützten Daten zeigt dies, dass BAC gegen Sniffing-Angriffe keinen ausreichenden Schutz bietet. Zwar bleibt die Schwierigkeit, die autorisierte Kommunikation fehlerlos zu beobachten, was den Aktionsradius des Angreifers auf mehrere Dezimeter um Lesegerät/RF-Chip begrenzt, dennoch erscheint uns Sniffing als ein nicht angemessen ausgeschlossener Angriff.

Verbesserungspotenzial: Es steht zu vermuten, dass BMI und BSI das kritisierte BAC als Reaktion gegen PACE austauschen wollen.[12]

Unklar ist aufgrund der derzeit verfügbaren Spezifikationen, ob der ePerso auch noch BAC implementiert und unter welchen Bedingungen ein Protokoll-Downgrade von PACE auf BAC erfolgen kann. Da der ePerso etwa bei Reisen in der EU den ePass 2.0 ersetzen kann und PACE lediglich in deutschen Personalausweisen implementiert werden soll, ist es aus Gründen der Abwärtskompatibilität zu befürchten, dass der ePerso auch BAC unterstützt. Stattdessen sollte ausschließlich PACE oder ein vergleichbar sicheres Verfahren zum Einsatz kommen.

In der folgenden Tabelle wird auch das Sniffing von biometrischen Daten mit betrachtet. Im ePass 1.0 ist dabei lediglich das digitale Foto des Inhabers gespeichert, welches allerdings nur per BAC geschützt ist[13]. ePass 2.0 und ePerso verwenden das Verfahren *Extended Access Control* (EAC, auch als *Terminal Authentication* bezeichnet), bei dem das Lesegerät zertifikatsbasiert vom Chip im Ausweisdokument authentifiziert und autorisiert wird.

Sniffing	ePass 1.0	ePass 2.0	ePerso	Verbesserung
Technik	BAC	BAC/EAC	PACE/BAC	nur PACE
Datenschutz	niedrig		hoch	hoch
sofern abw.komp.	n/a		niedrig	n/a
biometr. Daten	niedrig[14](BAC)	hoch (EAC)		n/a

[11] In einem Challenge-Response-Protokoll übermittelt der ePerso eine per PIN verschlüsselte Zufallszahl an das Lesegerät. Diese Zufallszahl legt Domainparameter auf einer elliptischen Kurve fest, die für Diffie-Hellman genutzt wird. Nur bei Kenntnis der richtigen Zufallszahl verwendet der Leser die richtigen Domainparameter und kann daher den ePerso davon überzeugen, die entschlüsselte Zufallszahl und damit die PIN zu kennen.

[12] Der Übergang von BAC zu PACE wird vom BSI in [BKMN08] prozedural aufgrund der Anforderungen der eID-Funktion, bei der es ebenfalls Verwendung findet, begründet: Ein Auslesen optischer Merkmale für Authentisierungen über das Internet ist nicht sinnvoll. Daher wollte man eine 2-Faktor-Authentisierung mittels Besitz (der Karte) und Wissen (der geheimen, nicht der Karten-PIN).

[13] siehe `http://www.ccc.de/epass/stellungnahme-bmi`

[14] gespeichert ist nur das Gesichtsbild

4.4 Mechanismus der Ermittlung des Zugriffsschlüssels

Da, wie bereits erwähnt, an mehreren Stellen die Verfahren BAC bzw. PACE zum Einsatz kommen, soll deren kryptografische und konzeptionelle Stärke in diesem Abschnitt nochmals gesondert betrachtet werden. Als Szenarien sind passive oder aktive Angriffe auf die Luftschnittstelle zu betrachten.

Gemeinsam haben beide Verfahren, dass sie das optische Lesen des Dokuments im Protokoll voraussetzen und dadurch einen „out-of-band"-Kanal schaffen wollen. Während bei BAC das Lesen bei Grenzkontrollen i.d.R. durch eine OCR-Software und nur im Fehlerfall manuell geschieht, ist die letztere Variante als Regelfall für PACE beim ePerso vorgesehen.

Relevante personenbezogene Daten: Zunächst der BAC-Schlüssel, dann die damit verschlüsselten Daten der Gruppen 1 und 2 im Falle von ePass 1.0 und ePass 2.0. Beim ePerso ist die Karten-PIN eine Zufallszahl, die im Gegensatz zum BAC-Schlüssel keine personenbezogenen Daten (wie Seriennummer, Geburtsdatum) enthält.

Angriffsszenario: Wir gehen dabei von einem gezielten Angriff mittels Brute-Force aus, bei dem der Angreifer die Zielperson visuell beobachtet oder bereits gewisse ihrer Eigenschaften anderweitig in Erfahrung gebracht hat.

Implementierte Schutzmaßnahmen: Das bereits beschriebene BAC mit einer optimistisch angenommenen Schlüssellänge auf Niveau von DES (Data Encryption Standard).

Bewertung: In [KN07] wird der volle Suchraum bei BAC mit 56-Bit angegeben (also 2^{56} mögliche Zugriffschlüssel). Diese Kalkulation ist aber deutlich zu optimistisch. Einfache Überlegungen zeigen, dass der Suchraum höchstens in der Größenordnung 2^{40} liegt, was in [KN07] als 'reduzierter Suchraum' bezeichnet wird.

Wir schätzen im Folgenden die Anzahl der BAC-Zugriffschlüssel im ePass 1.0 ab. Berechnungen des BSI findet man z.B. in [BSI], [KK05], [KN07], eine detaillierte Betrachtung der Entropie von Zugriffschlüsseln in [JMW05].

1. Passnummer: Diese besteht aus 9 Dezimalstellen. Allerdings ist die Passnummer keine Zufallszahl, denn von den 9 Stellen sind die ersten 4 Stellen die Behördenkennzahl, die bei einem gezielten Angriff als bekannt vorausgesetzt werden kann. Bleiben höchstens 5 Dezimalstellen, die durch die Bundesdruckerei vergeben werden. Wir gehen also von maximal 10^5 Möglichkeiten aus.
2. Geburtsdatum: Während das BSI mit 100 Jahren rechnet, grenzen wir das Alter auf ein Intervall von höchstens 10 Jahren (Geburtstag $\pm$ 5 Jahre) ein.
3. Ablaufdatum: Hier setzt das BSI 10 Jahre an. Da es den ePass aber erst seit ca. 3,5 Jahren gibt, gibt es nur für diesen Zeitraum mögliche Ablaufdaten.

Unsere Abschätzung für die Anzahl der Schlüssel ist höchstens

$$10^5 \cdot 365{,}25 \cdot 10 \cdot 3{,}5 \cdot 365{,}25 \leq 4{,}67 \cdot 10^{11} \approx 2^{39} \tag{1}$$

Solche passiven Lese-Angriffe auf BAC bei Pässen anderer Länder wurden erfolgreich

demonstriert (z.B. in den Niederlanden[15]). Daher sind Zugriffschlüssel der Länge 40 Bit zu wenig, um einem Brute-Force-Angriff standzuhalten. Werden aufsteigende Seriennummern verwendet, und ist dem Angreifer eine aktuelle Seriennummer bekannt, grenzt dies den o.g. Bereich der 10^5 Möglichkeiten signifikant ein. Erst im ePass 2.0 werden die Seriennummern teilweise pseudozufällig vergeben. BAC ist aufgrund der kurzen effektiven Schlüssellänge nicht geeignet, Vorbehalte gegen RFID zu zerstreuen, wenngleich der Plaintext nicht allzu wertvolle Informationen enthält.

BAC und PACE haben gleichermaßen den Nachteil, dass der Vorteil der einfacheren Handhabung einer berührungslosen gegenüber einer kontaktbehafteten Technologie reduziert wird. Im Hinblick auf die Praktikabilität ist der Zugewinn relativ gering. Andererseits wird er durch sehr aufwändiges Protokolldesign erkauft, das das Riskio unentdeckter Implementierungsfehler birgt.

Verbesserungspotenzial: Das vorgenannte Problem hätte man sich durch den Einsatz von kontaktbehafteter Technologie ersparen können, die im Bereich der Smartcards seit langem etabliert und auch von zahlreichen Ländern für Personalausweise eingesetzt wird.

Anstelle von PACE könnte man auch ein Verfahren mit beidseitiger starker Authentifikation basierend auf Berechtigungszertifikaten für Lesegeräte nutzen. Schlüssellängen können dabei – im Rahmen des durch den Chip unterstützten Bereichs – beliebig gewählt werden. Berechtigungszertifikate sind bereits für den hoheitlichen Bereich im Einsatz [SHR06] sowie für die eID-Funktion geplant. Ein Nebeneffekt davon ist, dass man nicht-hoheitliche Anwendungen auf das rein optische Lesen des Dokuments beschränkt und jegliches elektronisches Lesen ausschließt.

Schlüssel	ePass 1.0	ePass 2.0	ePerso	Verbesserung
Technik	MRZ-Daten	plus pseudo-zuf. Seriennr.	zufällige Karten-PIN	Public Key-Authentisierung
krypt. Schutz	≤ 40 Bit		≤ 20 Bit	wählbar
elektr. Lesen	auch nicht-hoheitliche Anwendungen			nur hoheitliche A.

5 Bewertung und Ausblick

Wir haben in diesem Beitrag beleuchtet, wie die auf dem RF-Chip von ePass und ePerso gespeicherten Daten durch präventive Zugriffsprotokolle geschützt werden sollen. Wir kommen insgesamt zu dem Schluss, dass unter der Annahme, dass RF-Chips zu verwenden sind, die auf dem ePass und ePerso gespeicherten Daten durch geeignete Schutzmechanismen im Wesentlichen adäquat geschützt sind.

Allerdings bleibt die Antwort auf die zentrale Frage, warum die ICAO RF-Chips vorschreibt, unbeantwortet (wir sind darauf im Detail in Abschnitt 3 eingegangen). Noch unklarer ist, warum sich die Bundesregierung beim ePerso ebenfalls für kontaktlose Technik entschied. Andernfalls wäre jeder Bundesbürger nämlich Herr seiner Daten, da man durch

[15] siehe `http://www.heise.de/newsticker/meldung/69127`

Einstecken der Karte in ein Lesegerät eine offensichtliche Willensbekundung abgibt. Aus Datenschutzsicht ist das eine der Kerneigenschaften, warum die RF-Technik für Ausweise nachteilig ist.

Aber auch aus Sicherheitssicht bleibt unklar, warum kontaktlose Chips verwendet werden, da viele Angriffsszenarien ohne RF-Technik ausgeschlossen wären. Ohne RF-Technik hätten keine Zugriffsprotokolle wie Basic Access Control oder PACE konzipiert werden müssen.

Nimmt man aber als Voraussetzung an, dass RF-Technik eingesetzt werden muss, dann sind ePass (mit den genannten Einschränkungen beim ePass 1.0) und ePerso ein Erfolgsmodell, wie durch gründliche konzeptionelle Arbeit im Vorfeld der Einführung eines technischen Systems sensible Daten angemessen geschützt werden können. Obwohl die auf dem ePass sowie dem ePerso gespeicherten Daten im Vergleich zu den Informationen anderer großer IT-Projekte (z.B. elektronische Gesundheitskarte) relativ unkritisch sind, sind sie aus Sicht der Autoren angemessen geschützt.

Aus unserer Sicht sind in Zukunft noch folgende interessante Aspekte im Zusammenhang mit den Funktionen des ePass 2.0 oder des ePerso zu diskutieren:

1. Welche Rate an defekten RF-Chips in den Ausweisdokumenten wird es geben? Welchen Anteil daran führen die Behörden auf bewusste Manipulationen zurück?
2. Welche Akzeptanz finden die optionalen Fingerabdrücke im ePerso?
3. Wird es auch für die eID oder gar die qualifizierte Signatur des ePerso Identitätsdiebstahl geben? Solange Client-seitig Kartenleser ohne Display und/oder Tastatur verwendet werden können, ist auf Grund von einschlägiger Malware Manipulationen und gravierenden Datenschutzverletzungen Tür und Tor geöffnet. Wird keine dedizierte Hardware für Anzeige und Eingabe von ePerso-Anwendungen eingesetzt, bleiben z.B. Phishing-Angriffe realistisch.
4. Die Multifunktionalität des ePerso erhöht die Komplexität des gesamten Systems. Typischerweise wachsen mit der Komplexität auch die Sicherheitsrisiken. Es bleibt abzuwarten, inwiefern sich dies beim ePerso bewahrheitet.
5. Welche Rolle für die Erreichung des gewünschten höheren Sicherheitsniveaus spielen die Prozesse und IT-Systeme in den Meldebehörden?

Literatur

[AO05] G. Avoine und P. Oechslin. RFID Traceability: A Multilayer Problem. *Proceedings of the 9th conference on Financial Cryptography*, Seiten 125–140, 2005.

[BKMN08] J. Bender, D. Kügler, M. Margraf und I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. *Datenschutz und Datensicherheit (DuD) 3/2008*, Seiten 173–177, 2008.

[BMI08] BMI. Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept, Version 2.0. *BMI-IT 4-644 004*, 2008.

[BSI] BSI. Digitale Sicherheitsmerkmale im elektronischen Reisepass.

[BSI08a] BSI. *Advanced Security Mechanisms for Machine Readable Travel Documents*. TR-03110. 2008.

[BSI08b] BSI. Messung der Abstrahleigenschaften von RFID-Systemen (MARS) – Projektdokument 1: Passives Mitlesen. 2008.

[Bun08] Bundesregierung. Entwurf eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften. *Drucksache 16/10489*, 2008.

[Fin06] K. Finkenzeller. *RFID-Handbuch*. Carl Hanser Verlag München, 2006.

[ICA06a] ICAO. Passports with Machine Readable Data Stored in Optical Character Recognition Format. *Document 9303, Part 1, Volume 1*, 2006.

[ICA06b] ICAO. Specifications for Electronically Enabled Passports with Biometric Identification Capabilities. *Document 9303, Part 1, Volume 2*, 2006.

[ISO08] ISO/IEC. Standard 14443:2008 – Identification cards: Contactless integrated circuit cards. 2008.

[JMW05] A. Juels, D. Molnar und D. Wagner. Security and Privacy Issues in E-Passports. 2005.

[KK05] D. Kügler und H. Kelter. Risiko Reisepass – Schutz der biometrischen Daten im RF-Chip. *c't-Magazin 05/05*, Seiten S. 84–89, 2005.

[KN07] D. Kügler und I. Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. *Datenschutz und Datensicherheit (DuD) 31 (2007) 3*, Seiten 176–180, 2007.

[SHR06] Tobias Straub, Manuel Hartl und Markus Ruppert. Digitale Reisepässe in Deutschland - Prozesse und Sicherheitsinfrastruktur. In *Sicherheit*, Seiten 233–243, 2006.