Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Dokumentation der gleichnamigen Tagung am 30. November und 1. Dezember 2012

Auszug

Oepen, Dominik (2013): Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland. In: Arbeitsgruppe Informatik in Bildung und Gesellschaft (Hg.): Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen. Tagung, 30.11./1.12.2012, Berlin: Humboldt-Universität, S. 37-60.

Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland

Transkript

Dominik Oepen

Einleitung

Von offizieller Stelle wird häufig betont, dass die Ausweisdokumente, die wir hier in Deutschland haben, einen hohen Standard an Datensicherheit, aber auch Garantien, was die Privatsphäre der Ausweisinhaber und die Transparenz angeht, haben (Bender et al. 2008, Rossnagel et al. 2008, Quiring-Kock 2009). Ich möchte heute darauf eingehen, welche technischen Mechanismen verwendet werden, um diese angeblichen Eigenschaften zu realisieren, was diese Techniken tatsächlich erreichen können und wo die Grenzen davon liegen.

Dazu gebe ich zunächst eine kurze Einführung in elektronische Ausweisdokumente. Das ist ein sehr breites Thema, darum werde ich das vergleichsweise kurz abhandeln müssen. Der Fokus liegt dann auf den Ausweisdokumenten, die hier in Deutschland tatsächlich eingeführt wurden. Das sind drei Stück: der elektronische Reisepass (ePass), der neue Personalausweis (nPA) und der elektronische Aufenthaltstitel (eAT). Der Fokus soll auf der Technik liegen, die zum einen Zugriffsschutz implementiert, zum anderen Mechanismen, die eine möglichst datensparsame Nutzung gewährleisten sollen.

Wenn man über elektronische Ausweisdokumente spricht, dann gibt es sehr viele Gremien und Institutionen, die an der Standardisierung beteiligt sind, aber man kann sicherlich sagen, dass auf internationaler Ebene eine der wichtigsten Institutionen die ICAO ist. ICAO steht für International Civil Aviation Organisation. Das ist eine Institution, die es bereits seit den fünfziger Jahren gibt und die bereits seit den achtziger Jahren Standards für maschinenlesbare Reisedokumente entwirft. Das zentrale Dokument ist dabei das ICAO-Dokument 9303 (ICAO 2008, ICAO 2008a), welches die sogenannten *Machine Readable Travel Documents* spezifiziert und welches mittlerweile von einer Vielzahl von Ländern adaptiert wird. Ich hatte jetzt die Zahl über 100 Länder gefunden, wir haben vorhin schon gehört, es sind jetzt 191 Länder. Vielleicht sind es dann mittlerweile auch mehr als 300 Millionen Passdokumente, die bisher weltweit ausgegeben wurden. Man kann auf jeden Fall sehen, dass der Standard weit verbreitet ist.

Maschinenlesbar bedeutete damals nicht unbedingt auf elektronischem Weg maschinenlesbar, sondern in den achtziger Jahren bedeutete dies zunächst einmal optisch lesbar. Vielleicht kennen Sie alle die maschinenlesbare Zone (*Machine Readable Zone*, MRZ) aus Ihrem Reisepass: Das sind drei Zeilen unten in Ihrem Reisepass, die in einem standardisierten Format, in einer maschinenlesbaren Schrift Informationen über den Passinhaber enthalten.

Nach den Terroranschlägen am 11. September hat sich relativ schnell etabliert, dass das optische Auslesen nicht mehr reicht, sondern es wurde im Mai 2003 der Beschluss

gefasst, die Dokumente nicht mehr nur auf optischem Wege verarbeitbar zu machen, sondern jetzt eben auch auf elektronischem Wege. Zu diesem Zweck sollten RFID-(Radio-Frequency-Identification-)Chips in den Pässen verbaut werden und auf diesen Chips sollten – neben den aufgedruckten Daten – auch biometrische Daten der Passinhaber gespeichert werden. Dabei waren zunächst ein digitales Gesichtsbild vorgesehen, optional aber auch Fingerabdrücke, Irisscans und es sind auch noch weitere biometrische Merkmale spezifiziert.

RFID ist ein schwieriger Begriff, weil das eine ganze Palette an Technologien umfasst, die teilweise recht unterschiedliche Eigenschaften haben. Im Rahmen elektronischer Ausweisdokumente sprechen wir eigentlich immer von dem ISO-Standard 14443 (ISO 14443-4 2000), das ist eine Nahfunktechnologie, die bei spezifikationskonformem Betrieb Reichweiten von ungefähr fünf bis zehn Zentimetern erreicht. Es wurden natürlich schon viele Untersuchungen angestellt, ob man diese Reichweite nicht eventuell vergrößern kann, um beispielsweise unberechtigten Zugriff auf einen Ausweis oder Reisepass zu erhalten. Nach meinem Kenntnisstand ist da der Stand der Forschung so, dass in Modellierung und Simulation Reichweiten von 40 bis 50 Zentimetern vorausgesagt werden (Kfir/Wool 2005), die erreicht werden können und in der Praxis ist der Rekord bei etwa 25 Zentimetern (Finke/Kelte 2004, Kirschenbaum/Wool 2008). Das war jetzt 2006, eventuell gibt es da schon neuere Erkenntnis-

se, dass man noch näher an die 40 Zentimeter rankommt, aber ich glaube, über einen halben Meter ist bisher noch niemand hinausgekommen.

Das gilt allerdings nur für das aktive Ansprechen eines Chips; wenn man versucht, aktiv eine Verbindung zu einem Ausweis aufzubauen, dann kann man das ungefähr über diese Reichweite schaffen. Das passive Abhören geht technologiebedingt über sehr viel weitere Entfernungen. Also, wenn ich eine bestehende Kommunikation mit einem Dokument und einem Lesegerät belauschen möchte, dann geht das auch über eine Entfernung von mehreren Metern.

Elektronische Ausweisdokumente in Deutschland

Die Einführung elektronischer Reisedokumente in Deutschland erfolgte schrittweise. Bereits vor der Einführung des ersten Dokuments, des elektronischen Reisepasses, wurde die sogenannte eCard-Strategie des Bundes beschlossen (BMWi, Kowalski 2007). In diesem Strategiepapier hat die Bundesregierung festgeschrieben, dass sie die Verbreitung von Chipkarten in allen Bereichen von eBusiness und eGovernment stark fördern möchte und dass sie vor allem elektronische Authentisierungsdienste und elektronische Signaturdienste fördern möchte. In diesem Strategiepapier wurden dann beispielhaft einige Chipkarten, wie etwa die Jobkarte, ELENA, die elektronische Gesundheitskarte, ELSTER und der elektronische Personalausweis, als wegweisende Projekte aufgeführt.

Man kann an dieser Stelle schon sehen, dass nicht unbedingt alle diese Dokumente erfolgreich eingeführt wurden.

Was allerdings erfolgreich eingeführt wurde, ist der elektronische Reisepass. Wie wir das vorhin schon gehört haben,[1] ist das in zwei Phasen erfolgt: Im November 2005 wurde der Reisepass mit Chip eingeführt. Damals waren auf dem Chip noch keine Fingerabdrücke abgespeichert, sondern lediglich das digitale Gesichtsbild und die aufgedruckten Daten. Erst im November 2007 wurde dann die Abspeicherung von zwei Fingerabdrücken verpflichtend. Nachfolgend wurden dann im November 2010 der neue Personalausweis eingeführt und im September 2011 der elektronische Aufenthaltstitel. Und diese drei Dokumenttypen möchte ich jetzt im Detail beleuchten.

Zum elektronischen Reisepass haben wir eigentlich schon alles gehört, daher dazu nur relativ kurz: Er ist ein Ausweisdokument, welches genau eine Applikation bietet, nämlich die ePass-Applikation. Diese Applikation ist dafür gedacht, mich an der Grenze auszuweisen, beziehungsweise ist der Zugriff allgemein für hoheitliche Zwecke vorgesehen, also für Polizeibeamte, für Zoll- und Grenzbeamte, etc. Innerhalb der ePass-Applikation sind drei Datengruppen gespeichert: die maschinenlesbare Zone ist nochmal digital gespeichert, außerdem das biometrische Gesichtsbild und in der Datengruppe Drei die Fingerabdrücke des Ausweisinhabers. Darüber hinaus sind kryptografische Signaturen gespeichert für alle Datengruppen, die dafür dienen sicherzustellen, dass die

1 Im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Daten, die ausgelesen werden, auch tatsächlich authentisch sind. Auf diese Authentizitätssicherung gehe ich später noch im Detail ein.

Der neue Personalausweis bietet dagegen mehr als nur eine Funktion. Genauer gesagt sind es drei Applikationen, die auf dieser Karte laufen: Das sind die ePass- oder Biometrie-Applikation, die im wesentlichen kompatibel ist zu der Applikation, die wir aus dem elektronischen Reisepass kennen, dann die eID-Applikation, die konzipiert wurde, um die Authentisierung des Ausweisinhabers über das Internet zu realisieren – vor allem über das Internet. Es waren auch mal Automaten für Zigarettenkauf oder ähnliches im Gespräch, aber der Hauptanwendungszweck waren auf jeden Fall immer eBusiness- und eGovernment-Anwendungen über das Internet. Und die dritte Applikation ist die eSign-Applikation zur Erstellung von qualifizierten elektronischen Signaturen (BSI 2012b). Man sieht, wie sich die eCard-Strategie widerspiegelt in diesem Dokument: Es sollten elektronische Authentisierung und Signaturfunktionen gefördert werden und deshalb wurden genau diese Funktionen jetzt auch auf dem Ausweisdokument untergebracht. Wichtig ist es jetzt anzumerken, dass es bei der ePass-Applikation dann doch einen kleinen Unterschied zum Reisepass gibt, nämlich, dass die Speicherung der Fingerabdrücke optional ist. Als Ausweisinhaber muss ich mich bei der Beantragung des Ausweises entscheiden, ob ich Fingerabdrücke abgeben möchte oder nicht und kann eben auch gezielt darauf verzichten. Genauso optional sind die eID-Applikation und die eSign-Applikation. Auch hier kann ich bei der Bean-

tragung des neuen Personalausweises sagen, ich möchte die eID-Applikation nicht nutzen; die eSign-Applikation muss eh erst durch das Nachladen eines Zertifikates nutzbar gemacht werden. Ich kann auch zu einem späteren Zeitpunkt die eID-Applikation freischalten lassen, wenn ich mich zuerst dagegen entschieden habe oder sie deaktivieren lassen, wenn ich sie zuerst habe aktivieren lassen. Das sind allerdings kostenpflichtige Vorgänge.

Datengruppe	Inhalt
DG 1	Dokumenttyp
DG 2	Ausgebender Staat
DG 3	Ablaufdatum
DG 4	Vorname(n)
DG 5	Familienname
DG 6	Ordensname/Künstlername
DG 7	Doktorgrad
DG 8	Geburtsdatum
DG 9	Geburtsort
DG 13	Geburtsname
DG 17	Adresse
DG 18	Wohnort ID

Tabelle 1

Datengruppen der eID-Applikation

Schauen wir uns nun die Datengruppen der eID-Applikation an. Die sind hier (Tabelle 1) aufgelistet. Es sollte eigentlich größtenteils verständlich sein, was die einzelnen Datengruppen bedeuten.

Wichtig ist es hierbei festzuhalten, dass ein Dienst, bei dem ich mich als Ausweisinhaber anmelde, nicht per se auf alle diese Daten zugreifen kann. Wir werden nachher sehen, dass der Dienstanbieter zur Nutzung dieser Funktion ein sogenanntes Dienstanbieterzertifikat benötigt und in diesem Zertifikat ist festgeschrieben, welche Daten der Dienstanbieter auslesen darf. Er ist also beschränkt in seinem Zugriff auf die eID-Applikation und kann nicht alle Daten über den Nutzer erfassen, sondern nur diejenigen, für die er vorher bei der Beantragung des Zertifikates glaubhaft machen konnte, dass es für die Erbringung seines Dienstes zwingend notwendig ist, dass er diese Daten erhebt. Dafür gibt es die neu geschaffene Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt und wenn ich die eID-Funktion als Dienstanbieter nutzen möchte, muss ich zunächst einmal glaubhaft machen, dass ich für meinen Geschäftszweck gewisse Daten zwingend erheben muss. Hier sehen wir die Datensparsamkeits- und Transparenzaspekte, die beim neuen Personalausweis eine Rolle spielen. Jetzt kann man natürlich spekulieren, wie gut diese Prüfung erfolgt; es gibt da so einige Dienste in der freien Wildbahn, bei denen man sich so fragt: Wie sind denn die damit durchgekommen? Aber prinzipiell dürfen nur die jeweils notwendigen Daten erhoben werden.

Ein interessantes Detail gibt es dazu noch: Nämlich gelten diese Einschränkungen lediglich für Dienstanbieter aus der Privatwirtschaft. Als Dienstanbieter muss ich also belegen, auf welche Daten ich zugreifen darf. Inspektionssysteme, also solche Terminals, die eigentlich

für den Grenzübergang gedacht sind, können die Berechtigung zum kompletten Zugriff auf die Applikation erhalten. Das heißt, ein Grenzkontrollsystem hat auf einmal nicht mehr nur noch Zugriff auf die Passapplikation, sondern zusätzlich noch auf die in der eID-Applikation abgespeicherten Daten.

Ein weiteres technisches Detail ist, dass in der eID-Applikation – im Gegensatz zur ePass-Applikation – keine Signaturen gespeichert sind. Der Grund dafür ist, dass man verhindern wollte, dass Dienstanbieter Daten, welche aus einem Ausweis ausgelesen wurden, weiterverkaufen können. Sie können ohne diese Signaturen nämlich nicht glaubhaft machen, dass es tatsächlich aus einem Ausweis ausgelesene Daten sind. Hier wurde auf einen Sicherheitsmechanismus, welcher noch bei der ePass-Applikation des Reisepasses eingeführt wurde, verzichtet, um den Datenschutz in gewisser Weise zu stärken.

Neben dem Zugriff auf verschiedene Datengruppen bietet die eID-Applikation noch drei sogenannte spezielle Funktionen, die ebenfalls entworfen wurden, um Dienste mit einem möglichst hohen Maß an Datensparsamkeit implementieren zu können. Hierbei handelt es sich um die *Restricted Identification*, die *Altersverifikation* und die sogenannte *Wohnort-ID*. Die Restricted Identification dient dazu, dass sich ein Ausweisinhaber pseudonym bei einem Dienst anmelden kann, ohne dass mehrere Dienste miteinander kooperieren können, um denselben Ausweisinhaber dienstübergreifend zu tracken. Man kann sich das mit einem Beispiel veranschaulichen: Wenn ich mich mit meinem Personalausweis bei Amazon und bei

der Schufa anmelde, dann erhalte ich verschiedene Pseudonyme bei diesen Diensten und die Dienste können nicht miteinander kooperieren, um herauszufinden, dass ich dieselbe Person bin. Es bleibt hier außen vor, dass es natürlich weiterhin andere Möglichkeiten gibt, den Nutzer zu verfolgen. Das Ziel war es, mit der Onlineauthentisierung keine neuen Mechanismen zum Nutzertracking zu bieten und einmal exemplarisch zu versuchen, das Ganze so datensparsam wie möglich zu realisieren. Es gibt pro Kombination aus Ausweisinhaber und Dienstanbieter genau ein Pseudonym, es ist also eindeutig für die Kombination aus Ausweis und Dienst, aber nicht verkettbar, wir haben also hier die Unlinkability, die wir vorhin[2] vorgestellt bekommen haben.

Die Altersverifikation dient dazu, Dienste anzubieten, die nur für eine bestimmte Altersgruppe zugänglich sein sollen – also beispielsweise Dienste, die erst ab 16 oder 18 zugänglich sein sollen –, ohne das tatsächliche Alter des Ausweisinhabers zu erheben. Der Dienst übermittelt dazu ein Referenzdatum an den Ausweis und der Ausweis antwortet: „Ja, der Ausweisinhaber ist vor diesem Referenzdatum geboren“ oder „Nein, das ist nicht der Fall“. Hier geht es also wieder darum, möglichst wenig Daten zu erheben. Die Informatikerfrage ist üblicherweise: „Was ist, wenn man mehrere Anfragen stellt? Kann man dann nicht möglicherweise doch relativ schnell das tatsächliche Alter herausfinden?“ Da ist die Antwort, dass pro Durchlauf des Protokolls genau eine Anfrage gestellt werden kann.

2 Ebenfalls im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Ähnlich ist es mit der Wohnort-ID. Hier sollte ermöglicht werden, Dienste für einen bestimmten Bezirk bzw. für ein bestimmtes geographisches Gebiet zugänglich zu machen, ohne den tatsächlichen Wohnort des Ausweisinhabers erfassen zu müssen. Wieder ist es so, dass ein Referenzdatum an den Ausweis übermittelt werden kann – beispielsweise: „Wohnt der Ausweisinhaber in Brandenburg?" – und dann kommt die Antwort Ja oder Nein zurück. Grundlage dafür ist der sogenannte amtliche Gemeindeschlüssel, welcher verschiedene Auflösungsstufen, wie etwa Gemeinde, Region, Bundesland, vorsieht.

Das neueste elektronische Ausweisdokument in Deutschland ist der elektronische Aufenthaltstitel. In Deutschland benötigen Ausländer aus dem Nicht-EU-Ausland, die ihren ständigen Wohnsitz in Deutschland haben, einen Aufenthaltstitel. Früher waren das einfach Aufkleber in den nationalen Reisepässen der Migranten. Das wurde 2011 ersetzt durch den elektronischen Aufenthaltstitel, ebenfalls eine Chipkarte, die von der Technik sehr stark angelehnt ist an den neuen Personalausweis. Von der Funktionalität sind der nPA und der elektronische Aufenthaltstitel beinahe identisch, es sind auch wieder ePass-Applikation, eID-Applikation und eSign-Applikation vorhanden. Die Dokumente unterscheiden sich dann aber im Detail doch. Ein wichtiger Unterschied ist sicherlich, dass für den elektronischen Aufenthaltstitel die Speicherung der Fingerabdrücke verpflichtend ist, nicht wie beim neuen Personalausweis optional. Besonders interessant ist das in dem Kontext, dass er auch von Kindern ab sechs Jahren benötigt wird, also auch Kinder,

die als Ausländer ihren Wohnsitz in Deutschland haben, müssen ihre Fingerabdrücke abgeben. Wir haben ja vorhin[3] schon gehört, dass das nicht immer so sinnvoll ist, da sich bei Kindern doch noch einiges verändert im Laufe der Zeit, aber so ist der Stand. Kleine Unterschiede sind dann noch, dass die eID über zusätzliche Datengruppen verfügt und, ich glaube, auch einige der Datengruppen aus der eID-Applikation des Personalausweises nicht vorhanden sind. Die Staatszugehörigkeit und verschiedene Nebenbestimmungen zum Aufenthalt sind innerhalb dieser Applikation gespeichert.

Transparenz und Privatsphäre

Soviel zur Funktionalität der Ausweisdokumente in Deutschland, jetzt möchte ich versuchen, den Zugriffsschutz zu erklären. Der elektronische Reisepass implementiert die sogenannte *Extended Access Control* (EAC) nach Version 1, welche in dem eingangs erwähnten ICAO-Dokument 9303 spezifiziert ist. Der Zugriffsschutz lässt sich in zwei Phasen aufgliedern, die sogenannte *Basic Access Control* (BAC) und die *Active Authentication*, welche wiederum aus zwei Protokollen, der *Chip Authentication* (CA) und der *Terminal Authentication* (TA), besteht. Im Rahmen der Basic Access Control wird ein verschlüsselter Kanal aufgebaut zwischen Terminal und Ausweisdokument. Die Grundlage dafür ist wieder die maschinenlesbare Zone: der Ausweis wird optisch eingelesen, auf der Basis der maschinenlesbaren Zone werden zwei symmetrische Schlüssel abgeleitet. Mit diesen

3 Im Vortrag von Prof. Dr. Miloš Vec (zusammengefasst Seite 63).

beiden Schlüsseln kann ich auf die Datengruppen Eins und Zwei zugreifen, also auf das Gesichtsbild und auf die maschinenlesbare Zone. Die Durchführung der Basic Access Control wird häufig mit dem Vorzeigen des Ausweisdokuments verglichen. Das bedeutet, ich muss die maschinenlesbare Zone kennen, um auf die elektronischen Funktionen des Reisepasses zugreifen zu können. Ich muss also schon einmal die codierten Daten optisch eingelesen haben, um sie anschließend noch einmal elektronisch lesen zu können. Zusätzlich erhalte ich Zugriff auf das digitale Gesichtsbild.

Bei der BAC handelt es sich um einen rein symmetrischen Vorgang, die weiteren Protokollschritte sind asymmetrisch. Mit der Chip Authentication wird die Authentizität des Reisepasses nachgewiesen. Der Reisepass weist also nach, dass es sich um einen echten Pass handelt, indem er ein asymmetrisches Schlüsselpaar, welches nicht-auslesbar im Chip des Reisepasses gespeichert ist, verwendet. In die andere Richtung weist das Terminal nach, dass es tatsächlich berechtigt ist, auf den Reisepass zuzugreifen. Dafür benötigt es ein sogenanntes Terminalzertifikat, welches unter bestimmten Bedingungen ausgestellt wird, und natürlich den zugehörigen Schlüssel. Wir haben hier also eine beidseitige Authentifizierung zwischen Terminal und Reisepass, jeweils auf der Grundlage asymmetrischer Kryptografie, und erst danach ist der Zugriff auf die Fingerabdrücke möglich. Die Active Authentication ist also nochmal ein zusätzlicher Schutz der Fingerabdrücke, die im elektronischen Reisepass gespeichert sind.

Für den neuen Personalausweis hat das Bundesamt für Sicherheit in der Informationstechnik Änderungen an dem Zugriffsschutz vorgenommen und dafür die Technische Richtlinie 3110 erstellt. In dieser technischen Richtlinie ist die Extended-Access-Control-Version 2 spezifiziert (BSI 2012a). Hier gibt es die Basic Access Control nicht mehr. Sie wurde durch ein neues Protokoll ersetzt, das sogenannte *Password Authenticated Connection Establishment* (PACE). Dieses Protokoll dient wieder zur Absicherung der Funkschnittstelle: Es soll vermeiden, dass Leute, die sich in Funkreichweite befinden, die Kommunikation zwischen Ausweis und Terminal abhören. Deswegen wird ein verschlüsselter Kanal zwischen der Stelle der PIN-Eingabe und dem Personalausweis aufgebaut.

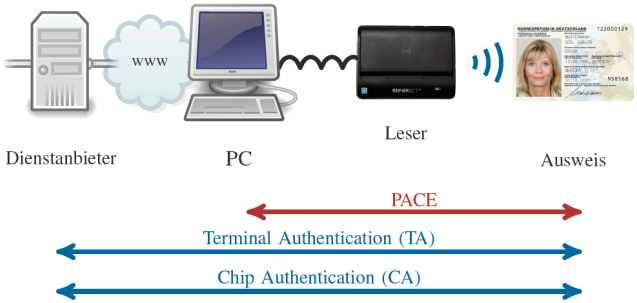

Abbildung 1 – EAC am Beispiel der eID-Funktion mit einem Basisleser

Wenn ich ein Lesegerät mit eigener Tastatur verwende, dann wird der PACE-Kanal zwischen dem Lesegerät und dem Personalausweis aufgebaut und wenn ich ein Lese-

gerät ohne eigene Tastatur verwende, dann wird der Kanal zwischen dem Computer und dem Ausweis aufgebaut.

Was man hier noch sieht, ist, dass die Reihenfolge von Terminal Authentication und Chip Authentication im Vergleich zur beim Reisepass verwendeten EAC-Version 1 umgedreht wurde. Jetzt muss zunächst der Dienstanbieter, bzw. das Inspektionssystem, nachweisen, dass es zum Zugriff auf den Personalausweis berechtigt ist, bevor der Ausweis seine Authentizität nachweist. Wenn man die beiden Versionen der EAC miteinander vergleicht, dann kann man vermuten, dass das BSI versucht hat, die Kritik, die an der ersten Version der EAC geäußert wurde, beim nPA zu entkräften. Man sieht, dass genau an den Stellen, die zuvor häufig kritisiert wurden, Änderungen vorgenommen wurden. Die BAC stand zuvor recht stark im Fokus von Sicherheitsuntersuchungen (Liu et al. 2007, Hoepman et al. 2006, Carluccio et al. 2007). Es wurde argumentiert, dass die abgeleiteten Schlüssel nicht ideal sind und nicht über ausreichend Entropie verfügen, dass es keinen Sicherheitsbeweis für das Protokoll gibt, dass teilweise die maschinenlesbaren Zonen zur Ableitung der symmetrischen Schlüssel in einigen Ländern vorhersagbar sind und man daher die benötigten Schlüssel erraten kann. All diese Kritik sollte nun entkräftet werden, indem ein neues Protokoll mit einem zugehörigen Sicherheitsbeweis innerhalb eines bestimmten kryptografischen Modelles entwickelt wurde.

Außerdem wurde, wie bereits erwähnt, die Reihenfolge von CA und TA vertauscht. Zuvor wurde kritisiert, dass ein Chip, welcher sich vor dem Terminal authentisiert, diese Authentisierung evtl. gegenüber einem Terminal, welches gar nicht zum Zugriff berechtigt ist, ausführt. Das würde eventuell das Tracken des Ausweises erlauben. Jetzt ist es so, dass sich zuerst das Terminal gegenüber dem Ausweis ausweisen muss und dafür ein Zertifikat, welches es zum Zugriff auf den Ausweis berechtigt, vorweisen muss. Erst danach weist sich der Ausweis gegenüber dem Terminal aus. Dahinter steht die kryptografische Best Practice, dass sich zuerst die stärkere von zwei Parteien authentisieren sollte.

Ein weiterer wichtiger Unterschied zum elektronischen Reisepass ist, dass beim nPA kein Zugriff auf die im Ausweis gespeicherten Nutzdaten möglich ist, ohne die komplette EAC durchzuführen.[4] Erst nach der Durchführung von PACE, TA und CA können Daten vom Personalausweis ausgelesen werden. Beim Reisepass hingegen reicht schon die BAC, um auf das Gesichtsbild und die aufgedruckten Daten zuzugreifen.

Interessanterweise ist der elektronische Aufenthaltstitel zur EAC-Version 1 abwärtskompatibel, obwohl er nach dem nPA eingeführt wurde. Der elektronische Aufenthaltstitel unterstützt also für die ePass-Applikation sowohl das neue PACE-Protokoll als auch das alte BAC-Protokoll. Weiterhin ist es hier auch wieder möglich, bereits nach BAC die aufgedruckten Daten auszule-

4 Es ist allerdings möglich, auf dem Funkweg zu erkennen, dass es sich um einen neuen Personalausweis handelt.

sen. Das bedeutet, es wurde zunächst für den neuen Personalausweis ein stärkeres Verfahren entwickelt, dann aber für den Aufenthaltstitel – aufgrund von Abwärtskompatibilität und aufgrund von internationalen Bestimmungen – doch wieder das schwächere, ältere Verfahren beibehalten. Man kann also sagen, dass die Inhaber von neuen Personalausweisen besser geschützt sind als die Inhaber von elektronischen Aufenthaltstiteln.

Für die eID-Funktion sind noch weitere Funktionen verbaut, die ein möglichst hohes Maß an Transparenz gewährleisten sollen. Es ist vorgeschrieben, dass im Rahmen der Terminal-Authentisierung dem Ausweisinhaber zunächst einmal Informationen zum Dienstanbieter angezeigt werden müssen und er auch noch einmal eine Kontrolle über die Daten, die ausgelesen werden sollen, hat.

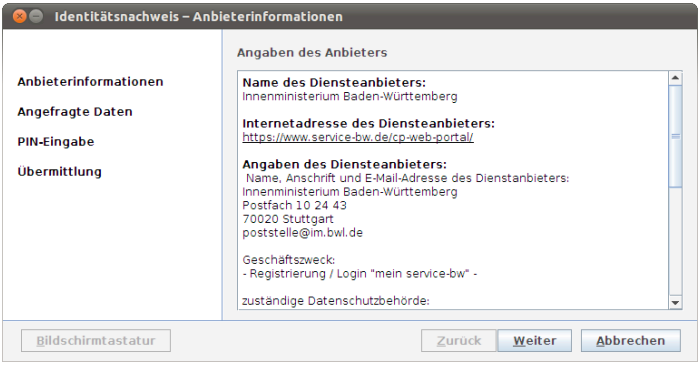

Abbildung 2 – Anzeige der Informationen zum Dienstanbieter

Besonders interessant ist, dass im nächsten Schritt angezeigt wird, auf welche Daten der Dienstanbieter zugreifen darf und dass der Ausweisinhaber die Möglichkeit hat, diese Zugriffsberechtigungen noch einmal einzuschränken. Wenn ein Anbieter jetzt also auf meinen Namen und Nachnamen zugreifen darf, ich aber meinen Nachnamen nicht freigeben möchte, dann kann ich gezielt diese Berechtigung abwählen.

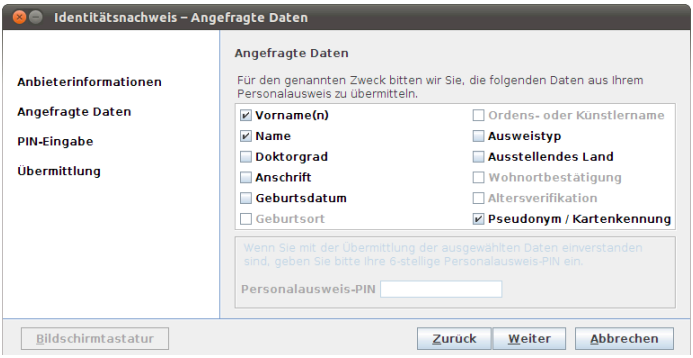

Abbildung 3 – Möglichkeit zur Abwahl von Zugriffsrechten durch den Benutzer

Natürlich kann der Dienstanbieter den Dienst anschließend verweigern. Insofern ist das nicht immer eine wirksame Maßnahme, aber die Mechanismen, die wir vorhin vorgestellt bekommen haben,[5] vor allem die Nutzerkontrolle über die erhobenen Daten, sind hier umgesetzt. Auch das gilt allerdings nur für die eID-Funktion. Bei der Authentisierung gegenüber hoheitlichen Stellen gibt es keine Möglichkeit, die auszulesenden Daten einzuschränken.

5 Im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Für die Chip-Authentisierung wird, wie bereits erwähnt, ein asymmetrisches Schlüsselpaar verwendet. Dieser asymmetrische Schlüssel könnte zur Identifizierung des Ausweisinhabers verwendet werden, man könnte also das Authentisierungsprotokoll zur eindeutigen Identifizierung des Ausweisinhabers nutzen. Das war allerdings explizit nicht gewollt. Beispielsweise soll bei der Altersverifikation der Dienstanbieter den Nutzer nicht identifizieren können, auch nicht pseudonym. Aus diesem Grund wurde die Chip-Authentisierung nicht mit einem individuellen Schlüsselpaar pro Ausweis realisiert, sondern innerhalb einer Charge von Ausweisdokumenten wird für alle Dokumente derselbe CA-Schlüssel verwendet. Eine Charge ist dabei in etwa die Anzahl an Ausweisen, die in einem Zeitraum von drei Monaten produziert wird. Das sollen in etwa eine Million Ausweise sein. Das bedeutet, dass immer etwa eine Million Ausweise denselben CA-Schlüssel beinhalten. Man hat also ein Anonymitätsset von einer Million Menschen, die denselben Schlüssel verwenden. Auch hier handelt es sich um einen Datensparsamkeitsmechanismus, der umgesetzt wurde, der dann aber auch – ich glaube, es war auf dem 26C3 hier in Berlin (Plötz 2009) – als potentieller Angriffspunkt identifiziert wurde. Die Konsequenz ist, dass ein Angreifer, der einen einzigen Schlüssel bricht, beliebige Ausweise emulieren kann. Es ist auch nicht möglich, anhand des CA-Schlüssels einzelne Ausweisdokumente zu sperren. Wir sehen also einen Trade-Off zwischen Fälschungssicherheit und Datensparsamkeit.

Nachdem dieser potenzielle Angriff vorgestellt wurde, hat das BSI reagiert und eine Datei auf dem Chip spezifiziert, das sogenannte EF.ChipSecurity, die einen zusätzlichen, chip-individuellen Schlüssel beinhaltet. Die ursprüngliche Idee der Gruppenschlüssel wurde also durch die Einführung eines zusätzlichen Schlüssels ausgehebelt. Auf diesen zusätzlichen Schlüssel haben nur sogenannte privilegierte Terminals Zugriff. Angeblich gibt es derzeit noch gar keine derartigen Terminals. Es ist aber davon auszugehen, dass sobald es Zweifel daran gibt, ob ein Schlüssel gebrochen wurde oder nicht, alle Terminals zu privilegierten Terminals gemacht werden.

In den letzten Monaten wurde verstärkt Open-Source-Software zur Verwendung des neuen Personalausweises veröffentlicht. Unter anderem wurde von der Humboldt-Universität in Kooperation mit der Bundesdruckei ein Programm zur Nutzung des nPA veröffentlicht. Auch Firmen aus der Privatwirtschaft – beispielsweise Bremen Online Services – haben solche Programme veröffentlicht. Das wird auch meistens explizit mit dem Anspruch gemacht, das Vertrauen in die Programme und das System an sich zu stärken, damit eine unabhängige Kontrolle erfolgen kann. Zuvor wurde häufig spekuliert, ob mit der AusweisApp auch gleich der Bundestrojaner ausgeliefert wird, bei einer Open-Source-Lösung kann man prinzipiell erst einmal nachgucken, ob das der Fall ist oder nicht. Aber auch da muss man einschränken, dass das kein Allheilmittel ist, dass der Transparenz durch Open Source natürlich Grenzen gesetzt sind. Ich möchte hier verweisen auf den berühmten Aufsatz von Ken Thompson,

„Reflections on trusting trust“ (Thompson 1984): Nur weil ich den Quellcode zu etwas habe, bedeutet das noch nicht, dass es tatsächlich absolut transparent ist.

Weiterhin existiert Open-Source-Software natürlich nur für die eID-Applikation, nicht für die ePass-Applikation und die Chipkarte selbst. Das Lesegerät und der eID-Server sind auch alle nicht Open Source. Ein kleiner Teil der Software ist also etwas besser kontrollierbar als vorher, aber dabei handelt es sich eben nur um einen Teil des Ökosystems. Am Schluss der Extended Access Control entsteht ein Ende-zu-Ende-verschlüsselter Kanal zwischen Dienstanbieter und Ausweis. Das bedeutet, an der Stelle hat der Ausweisinhaber keinerlei Kontrolle mehr darüber, was tatsächlich aus dem Ausweis ausgelesen wird, und muss auf die technische Spezifikation vertrauen, darauf, dass die Daten, die freigegeben wurden, tatsächlich die sind, die ausgelesen werden. In den Personalausweis selber kann man nicht reinschauen.

Fazit

Zusammenfassend kann man sagen, dass verschiedene Mechanismen implementiert wurden, insbesondere beim neuen Personalausweis, im Vergleich zu vorangegangenen Dokumenten, die klar darauf abzielen, mehr Transparenz und Datensparsamkeit zu gewährleisten, allerdings vor allem im Bereich eID. Der Bereich der hoheitlichen Authentisierung entzieht sich dem. Man hat unter anderem die kryptografischen Protokolle verbessert, hat aber gerade bei Dokumenten, die für den internationalen Grenzübergang gedacht sind, doch wieder Abwärtskom-

patibilität gefordert und kommt dadurch nicht so recht weg von den alten Spezifikationen. Es gibt starke Anstrengungen zur internationalen Standardisierung. Das BSI bemüht sich die neue Version der EAC auch auf internationaler Ebene zum Einsatz zu bringen. Es gibt bereits eine Ergänzung zum ICAO-Standard, die das PACE-Protokoll nachrüstet, aber es wird vermutlich viele Jahre dauern, bis das in die Pässe einfließt. An verschiedenen Stellen sehen wir auch eine prinzipielle Schwierigkeit, die Balance zu finden zwischen Fälschungssicherheit auf der einen und Datensparsamkeit auf der anderen Seite: zwei Aspekte, die nicht ganz einfach unter einen Hut zu bekommen sind.

Literatur

Bender, Jens, Dennis Kügler, Marian Margraf und Ingo Naumann, 2008: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. In: Datenschutz und Datensicherheit, 3:173-177.

BMWi: Chipkarten-Strategie der Bundesregierung (eCard-Strategie).
http://www.bmwi.de/BMWi/Redaktion/PDF/E/ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

BSI, 2012a: Advanced Security Mechanisms for Machine Readable Travel Documents. Technical Guideline 03110, Bonn, März. Version 2.10.

BSI, 2012b: Architektur Elektronischer Personalausweis. Technische Richtlinie 03127, Bonn, Oktober. Version 1.15.

Carluccio, Dario, Kerstin Lemke-Rust, Christof Paar und Ahmad-Reza Sadeghi, 2007: E-passport: the global traceability or how to feel like a UPS package. In: Information Security Applications, Seiten 391-404. Springer.

Finke, Thomas und Harald Kelte, 2004: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. Technischer Bericht, Bundesamt für Sicherheit in der Informationstechnik.

Hoepman, Jaap-Henk, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk und Ronny Wichers Schreur, 2006: Crossing borders: Security and privacy issues of the european e-passport. In: Advances in Information and Computer Security, Seiten 152-167. Springer.

ICAO, 2008: Doc 9303 – Machine Readable Travel Documents – MRTDs with Machine Readable Data Stored in Optical Character Recognition Format. International Civil Aviation Organisation, 3. Auflage.

ICAO, 2008a: Doc 9303, Machine Readable Travel Documents, Part 3, Specifications for Electronically Enabled MRtds with Biometric Identification Capability, Band 2. International Civil Aviation Organisation, 3. Auflage.

ISO 14443-4, 2000: Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol. ISO/IEC.

Kfir, Ziv und Avishai Wool, 2005: Picking virtual pockets using relay attacks on contactless smartcard. In: Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, Seiten 47-58. IEEE.

Kirschenbaum, Ilan und Avishai Wool, 2008: How to build a low-cost, extended-range RFID skimmer. Dissertation, Tel Aviv University.

Kowalski, Bernd, 2007: Die eCard-Strategie der Bundesregierung im Überblick. In: D. Hühnlein, A. Brömme, E, C. Busch (Herausgeber), BIOSIG, Seiten 87-96.

Liu, Yifei, Timo Kasper, Kerstin Lemke-Rust und Christof Paar, 2007: E-passport: Cracking basic access control keys. In: On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Seiten 1531-1547. Springer.

Plötz, Henryk, 2009: Technik des neuen ePA. Proceedings of the 26th Chaos Communication Congress.

Quiring-Kock, Gisela, 2009: PKI für Bürger – transparent, sicher, datenschutzgerecht? Datenschutz und Datensicherheit, 7:391-395.

Rossnagel, Alexander, Gerrit Hornung und Christoph Schnabel, 2008: Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht. Datenschutz und Datensicherheit, 3:168-172.

Thompson, Ken, 1984: Reflections on trusting trust. Communications of the ACM, 27(8):761-763.

Redaktion: Andrea Knaut, Christian Ricardo Kühne

Satz: Andrea Knaut

Herausgeberin: Andrea Knaut,
Arbeitsgruppe Informatik in Bildung und Gesellschaft,
Institut für Informatik, Humboldt-Universität zu Berlin.
Mit freundlicher Unterstützung durch die
Alcatel-Lucent-Stiftung.

Alcatel-Lucent Stiftung für Kommunikationsforschung

INFORMATIK IN BILDUNG & GESELLSCHAFT

erschienen: August 2013