DuD
Datenschutz und Datensicherheit

Identitätsdokumente

eIDs und maschinenlesbare Ausweise

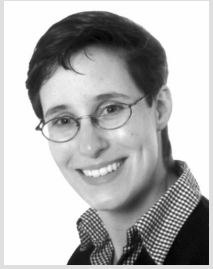
Martin Meints, Marit Hansen

Welche Arten von offiziellen Identitätsdokumenten gibt es? Wofür werden sie eingesetzt? Welche Technologien finden Verwendung? Dieser Artikel gibt eine Übersicht über europäische Identitätsdokumente, bewertet den neuen europäischen Reisepass unter Datenschutz- und Sicherheitsgesichtspunkten und fasst aktuelle Trends zusammen.

Dr. Martin Meints

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein im Projekt FIDIS.

E-Mail: LD102@datenschutzzentrum.de



Marit Hansen

Leiterin des Referats „Privacy-Enhancing Technologies“ des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein; Arbeitsschwerpunkt: Identitätsmanagement.

E-Mail: LD10@datenschutzzentrum.de

Einleitung

Im Rahmen des Projektes „Future of Identity in the Information Society“ (FIDIS) wurde eine Studie zu Identitätsdokumenten in Europa erarbeitet [MeHa06]. Der vorliegende Artikel fasst die wesentlichen Ergebnisse dieser Studie zusammen und gibt einen Ausblick auf weitere geplante Aktivitäten des FIDIS-Projektes bezogen auf Identitätsdokumente.

Auf dem CEN/ISSS-Workshop 2004 [CEN04, S. 68] wurde „electronic Identity” (kurz eID) definiert als technische Lösung mit dem Ziel,

- „die Identität einer natürlichen oder juristischen Person beim Zugang zu elektronischen Services zu garantieren und
- um das Vertrauen der in einer elektronischen Transaktion beteiligten Parteien herzustellen“[1].

Im erweiterten Sinne verstehen wir unter eIDs auch maschinenlesbare Reisedokumente, da diese zumindest elektronisch unterstützt eine Authentifizierung rechtmäßiger Besitzer erlauben.

1 Klassifizierung

Identitätsdokumente lassen sich nach einer ganzen Reihe von Kriterien klassifizieren. Typische Kriterien sind:

- Art des Dokumentes: *prozedural*, d.h. nicht an ein bestimmtes technisches Speichermedium gebunden oder spezifische Chipkartenlösung (*kartengebunden*);
- Eingesetzte Technologie wie elektronische Signaturen, Chipkartentechnologie, Radio Frequency Identification (RFID), Biometrie und Hintergrundsysteme (PKI, Referenzdatenbanken und Systeme zur Authentisierung);
- Verwendungszwecke; dies sind vor allem: maschinenlesbare Reisedokumente (Ausweise oder Reisepässe), elektronisches Signieren, Authentifizierung von Versicherten und Speicherung / Transport von personenbezogenen Daten in den Bereichen Gesundheit und Sozialversicherung.

Existierende oder geplante Lösungen für Identitätsdokumente in Europa lassen sich unter Berücksichtigung der oben genannten Kriterien in die folgenden Gruppen einteilen, die in den folgenden Abschnitten genauer beschrieben werden:

- Traditionelle Ausweisdokumente;
- Maschinenlesbare Reisedokumente nach aktuellem ICAO-Standard;
- Elektronische Signaturlösungen und Bürgerkarten;
- Speziallösungen für staatliche Zwecke.

1.1 Traditionelle Ausweisdokumente

Traditionelle Ausweisdokumente werden nach wie vor in zahlreichen Europäischen Ländern ausgegeben, in den meisten Ländern bis auf wenige Ausnahmen (z.B. Griechenland) gibt es aber Konzepte oder bereits laufende Projekte, diese vollständig abzulösen oder um eIDs, meist digitale Signaturkarten, zu ergänzen. Diese Dokumente werden daher im Folgenden nicht ausführlich behandelt.

Technische Merkmale dieser Dokumente sind:

- Speicherung von Ausweisdaten wie Name, Geburtsname, Geburtstag, Straße und Wohnort, Nationalität etc.;
- Aufdruck eines Passfotos;
- Polycarbonatlaminierung;
- Maschinenlesbare Zone, die mittels OCR (Optical Character Recognition) unter

[1] Im englischsprachigen Original lautet der Text: „*Electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction.*“

Einsatz von Scannern gelesen werden kann.

Diese Dokumente werden typischerweise für die Authentifizierung von Bürgern gegenüber Behörden und in der Privatwirtschaft sowie beim Grenzübertritt eingesetzt.

1.2 Maschinenlesbare Reisedokumente

Die heutigen maschinenlesbaren Reisedokumente entsprechen den aktuellen technischen Standards der „International Civil Aviation Organisation“ (ICAO), die im Document 9303[2] zusammengefasst sind. Diese wurden mit der Verordnung 2252/2004[3] in europäisches Recht übertragen. Diese Identitätsdokumente (ePassports) lösen seit November 2005 die traditionellen Reisepässe in Europa ab.

Gegenüber dem traditionellen Ausweisen weisen diese Dokumente die folgenden technischen Merkmale auf:

- Digitale Speicherung von Ausweisdaten;
- Berührungslose Auslesbarkeit durch Einsatz von RFID unter Nutzung des Standards ISO/IEC 14443;
- Speicherung von zwei biometrischen Merkmalen (spätestens ab Mitte 2006 digitales Gesichtsfoto und ab Anfang 2008 zusätzlich Fingerabdruckdaten) unter Nutzung der Standards ISO/IEC 19794-2 bis 19794-6.

Diese Dokumente werden im Folgenden noch detaillierter beschrieben und unter Datenschutz- sowie IT-Sicherheitsgesichtspunkten analysiert.

1.3 Elektronische Signaturlösungen

Lösungen für eine elektronische Signatur zeigen ein breites Spektrum unterschiedlicher Ausprägungen. Zu ihnen zählt mit der FINEID (seit 1999 ausgegeben) die älteste europäische eID. Sie können prozedural (z.B. die österreichische Bürgerkarte, die auf verschiedenen Chipkarten, SIMs oder USB-Sticks installiert werden kann[4]) oder kartengebunden (z.B. in Belgien etc.) sein. In den meisten Fällen werden kontaktgebundene Chipkarten eingesetzt; berührungslos auslesbare Karten finden derzeit noch keine Verwendung.

Daneben können diese Dokumente auch weitere Zwecke erfüllen. In Belgien etwa ist die Bürgerkarte auch der nationale Personalausweis, in Österreich kann die Bürgerkarte dazu verwendet werden, den Bürger gegenüber Behörden und Unternehmen im eGovernment oder elektronischen Geschäftsverkehr zu authentifizieren. Die hierzu eingesetzten sektorspezifischen PINs haben internationale Anerkennung von Datenschützern erlangt, da sie die Verkettung unterschiedlicher Transaktionen zumindest erschweren.[5] Sowohl in Österreich als auch in Finnland[6] ist eine Integration der Funktion der Gesundheitskarte möglich.

Unterschiede gibt es im Geschäftsmodell, das hinter der elektronischen Signaturfunktion steht. Während die meisten europäischen Länder auf ein kommerzielles Betreibermodell für die elektronischen Signaturen und PKI im Wettbewerb mehrerer Anbieter setzen (z.B. Finnland, Österreich, Deutschland etc.), haben andere ein zentrales, staatliches Betreibermodell gewählt (z.B. Belgien).

1.4 Speziallösungen

In mehreren Ländern, in denen ein staatlich reglementiertes System von Kranken- oder Sozialversicherungen besteht, werden bzw. wurden verschiedene „Kartenlösungen“ entwickelt (z.B. Deutschland) oder bereits eingeführt (z.B. eCard als Gesundheitskarte in Österreich). Auch hier können die Lösungen prozedural, wie die in Deutschland geplante JobCard, oder kartengebunden wie die eCard in Österreich sein.

Gemeinsamer Zweck dieser Lösungen ist die zuverlässige Authentifizierung von berechtigten Versicherten gegenüber den Leistungserbringern und Versicherungsinstitutionen.

Technisch werden hierbei neben spezifischen, kontextbezogenen Kennungen (z.B. Versicherungsnummern) auch weitere personenbezogene Daten, Fotos oder sogar Schlüssel und Zertifikate zur Erstellung digitaler Signaturen auf den Karten gespeichert.

Die untersuchten Speziallösungen weisen ein sehr breites Spektrum von Anwendungsfeldern und sehr spezifischen, meist nationaltypischen Problemen in der Projektplanung, -konzeption und -umsetzung auf. Sie werden in diesem Beitrag nicht weiter analysiert.

2 Analysen und Trends

Intensiv werden in der FIDIS-Studie zu eIDs die aktuellen Konzepte für maschinenlesbare Reisedokumente und elektronische Signaturlösungen analysiert. Dabei zeigen sich insbesondere in der Konzeption maschinenlesbarer Ausweisdokumente zahlreiche Schwächen.

2.1 Maschinenlesbare Ausweisdokumente

2.1.1 Rechtliche Aspekte

Die EU-Rahmengesetzgebung für Datenschutz und den Schutz der Privatsphäre, insbesondere die Europäische Menschenrechtscharta und die Datenschutz-Richtlinie 95/46/EG, sind anwendbar. Allerdings stellt sich in diesem Zusammenhang die Frage, ob die hier gewählte Art der Maschinenlesbarkeit verhältnismäßig im Sinne der Rechtssprechung des Europäischen Gerichtshofes für Menschenrechte ist.

Ferner wird die gewählte Rechtsgrundlage (Regulierung) in Frage gestellt. Das Konzept maschinenlesbarer Ausweise sieht einen Zugriff auf die Daten durch Institutionen der so genannten „Dritten Säule“ (Institutionen der nationalstaatlichen Sicherheit wie Polizei und Militär) vor. Hierfür können Artikel 62 und 66 des EU-Vertrages als EU-weite Regelungsgrundlage nicht herangezogen werden[7]. Artikel 18 Abs. 3 des EU-Vertrages schließt eine EU-weite Regelung für Reisepässe, Personalausweise, Aufenthaltsgenehmigungen und andere derartige Dokumente sogar ausdrücklich aus.

[2] Eine Übersicht über das Document 9303 mit den zugehörigen Standards findet sich unter http://www.icao.int/mrtd/publications/doc.cfm.

[3] Download: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_385200412229en00010006.pdf.

[4] Siehe http://www.buergerkarte.at/de/was_ist_die_buergerkarte/auspraegungen_der_buergerkarte.html.

[5] Siehe z.B. http://www.ptapde.gr/news/PR_e-PRODAT_20051215.pdf.

[6] Siehe http://www.fineid.fi/vrk/fineid/home.nsf/pages/2F1722857B8D77C5C2257054002C5C6B.

[7] Vergleiche hierzu auch die aktuelle Rechtsprechung des EuGH zur Passagierdatenübermittlung an die USA, siehe http://www.datenschutz.de/news/detail/?nid=1849.

Ein weiterer Kritikpunkt ist, dass hier technische Standards eines nicht demokratisch legitimierten Gremiums (z.B. Arbeitsgruppe TAG 15 der ICAO im Bezug auf den Biometrieeinsatz) ohne parlamentarischen Prozess in EU-weit geltendes Recht umgesetzt wurden.

2.1.2 Datenschutz und Datensicherheit

Der vorgesehene Einsatz biometrischer Authentifizierung wirft zahlreiche Probleme auf. Kritikpunkte sind vor allem:

- Qualitätsaspekte biometrischer Verfahren (v.a. Fehlerkennung, Fehlzurückweisung und Scheitern des Enrolments);
- Fehlende international standardisierte Verfahren in Fällen, bei denen Biometrie technisch versagt (Fehlzurückweisung) oder nicht anwendbar ist (Enrolment nicht möglich). Aktuelle Studien an den Flughäfen Schiphol in Amsterdam im Auftrag des niederländischen Innenministeriums [BZK05] und am Flughafen Frankfurt im Auftrag des Bundesamtes für Sicherheit in der Informationstechnologie [BSI05] belegen, dass diese technisch nicht gelösten Probleme nach wie vor der organisatorischen Lösung bedürfen;
- Die Freigabe des Einsatze biometrischer Rohdaten (digitaler Fotos) von Gesicht (ISO/IEC 19794-5) und Fingerabdrücken (ISO/IEC 19794-4) ermöglicht die Auswertung überschießender, in zahlreichen Fällen gesundheitsbezogener Daten [GaMeWa05];
- Fehlende Widerrufbarkeit (Austauschbarkeit) biometrischer Identifizierungsmerkmale; weder Gesicht noch Fingerkuppen können im Falle der Kompromittierung ausgetauscht werden;
- Ungelöste Sicherheitsprobleme heutiger biometrischer Verfahren, vor allem durch so genanntes „Spoofen“ von biometrischen Sensoren auch ohne aktive Beteiligung der „Inhaber“ der biometrischen Merkmale (siehe hierzu auch die Forschungsergebnisse des Niederländischen Forensischen Instituts [GeSo06]).

RFID wird erst seit kurzer Zeit für Identitätsdokumente eingesetzt und ist von der technischen Grundkonzeption auf unbeschränkten Zugang zu bzw. Zugriff auf die im Chip gespeicherten Daten ausgelegt. Für den Einsatz in maschinenlesbaren Ausweisdokumenten wurde mit Basic Access Control (BAC) ein kryptographischer Zugriffsschutz eingeführt. Dieser erweist sich jedoch unter zwei Gesichtspunkten als kryptographisch schwach:

- Die effektive Schlüssellänge der hier eingesetzten symmetrischen Verschlüsselung beträgt nur 35, in einigen Fällen sogar nur 28 Bit [BeGi05]; zum Vergleich: das BSI empfiehlt im Rahmen des E-Government-Handbuches den Einsatz des Algorithmus AES mit 128 Bit Schlüssellänge.[8]
- Der Schlüssel kann der maschinenlesbaren Zone des Ausweises selbst entnommen werden; der Ausweisinhaber kann somit nicht kontrollieren, wer über den Schlüssel zu seinem Ausweis verfügt.

Eine Ausnutzung der aufgezeigten Schwächen ist über Mithören und Offline-Entschlüsselung[9] der Kommunikation zwischen RFID-Chip auf dem Ausweis und Reader[10] sowie über Bibliotheksangriffe (unter Nutzung von Schlüsselbibliotheken) auf den Ausweis möglich. Neben dem unbefugten Auslesen der biometrischen Daten ermöglicht dies auch eine Identifizierung des Ausweisinhabers sowie ein Verfolgen des Standortes, wenn der Einsatz eines geeigneten Netzes stationärer (oder mobiler) Lesegeräte möglich ist.

Dieses Bedrohungsszenario wird üblicherweise als wenig relevant eingestuft mit dem Hinweis auf die begrenzte Reichweite von 10 bis 15 cm, die mit zugelassenen Lesegeräten erreichbar sind. Doch bereits 2004 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) nachgewiesen, dass bei ISO 14443-kompatiblen Systemen leicht 10 m Leseabstand mit technisch angepassten Lesegeräten erreicht werden können [BSI04]. Damit ist ein vom Ausweisinhaber unbemerktes Verfolgen und Auslesen des Chips im Ausweis über beträchtliche Distanzen durchaus möglich und realistisch.

Hinzu kommt, dass die Durchsetzung einer weltweiten Zulassung und Zertifizierung von Lesegeräten nur schwer erreichbar sein wird. Insgesamt sind alle Lesegeräte aus Sicht der Ausweisinhaber als nicht unbedingt vertrauenswürdig einzustufen, da sie sich gegenüber dem Ausweis oder dessen Inhaber nicht authentifizieren. Im Gegensatz dazu authentifiziert sich aber der Chip auf dem Ausweis sehr wohl gegenüber dem Lesegerät (passive Authentisierung und elektronische Signatur der ausstellenden Behörde).

Als Folge der nicht garantierbaren und damit unklaren Vertrauenswürdigkeit von Lesegeräten und den etablierten Prozessen der Ausweiskontrolle durch staatliche, aber auch private Organisationen (z.B. Hotels in Italien und Tschechien), wobei der Ausweis teilweise für eine längere Zeit außer Hand gegeben werden muss, ist davon auszugehen, dass weder der Ausweisinhaber noch der ausstellende Staat die Kontrolle über die auf dem Ausweis gespeicherten Daten einschließlich biometrischer Merkmale haben kann.[11]

Eine weiteres Sicherheitsproblem wurde im August 2006 bekannt: Mit geringem Aufwand kann man die RFID-Chips auf dem Pass klonen und die geklonten Chips in andere Pässe (zusätzlich) so einbauen, dass bei einer Passkontrolle die Informationen vom geklonten Chip eingelesen werden.[12] Dies würde dann nicht auffallen, wenn ein Abgleich der vom Chip eingelesenen Daten mit den aufgedruckten Ausweisdaten unterbliebe, z.B. bei automatisierten Grenzkontrollen oder weniger Sorgfalt bei der Passkontrolle. Eine unerkennbare Manipulation der Daten auf dem Chip, z.B. von Name oder Geburtsdatum, scheint heutzutage wegen der kryptographischen Hashwerte allerdings (noch) nicht möglich zu sein.

> Insgesamt kommt die FIDIS-Studie zu dem Schluss, dass bezogen auf den Einsatz von Biometrie bereits existierende, unter Datenschutz- und Datensicherheitsgesichtspunkten deutlich bessere Lösungen keine Berücksichtigung fanden und finden. Noch deutlicher fällt die Kritik am Einsatz von RFID aus. Für den

[8] Siehe http://www.bsi.bund.de/fachthem/egov/download/2_Krypto.pdf.

[9] Es ist davon auszugehen, dass sich diese Problem über die 10-jährige Gültigkeit der Ausweise durch die rasante Entwicklung von Rechenleistung bei Computern erheblich verschärfen wird. Die benötigten Zeiten zur Entschlüsselung werden sich in diesem Zeitraum erheblich verkürzen.

[10] Dieser Angriff wurde bereits erfolgreich auf den niederländischen Reisepass durchgeführt und hat 2 Stunden in Anspruch genommen. Siehe hierzu http://www.heise.de/tp/r4/artikel/21/21907/1.html.

[11] Die Umsetzung aktueller Überlegungen in einigen Mitgliedsländern, maschinenlesbare Ausweise auch als Standardauthentisierungssysteme für die Wirtschaft zu öffnen (siehe http://www.heise.de/newsticker/meldung/71912), wird dies Problem erheblich verschärfen.

[12] Der deutsche Sicherheitsexperte Lukas Grunwald zeigte dies am 3. August 2006 auf der Konferenz „Black Hat USA 2006“ in Las Vegas, siehe http://www.wired.com/news/technology/1,71521-2.html.

hier vorgesehenen Einsatzzweck bietet die Technologie nur wenige Datenschutz- und Datensicherheitslösungen und muss daher als noch unausgereift eingestuft werden. Und die wenigen existierenden Lösungen, wie etwa der Einsatz von Faraday'schen Käfigen[13] zur Einschränkung unbefugten und unbemerkten Auslesens, werden bei den derzeitigen maschinenlesbaren Ausweisen nicht oder in der Umsetzung unzureichend (wie bei BAC) eingesetzt.

2.1.3 Trends

Mit der Umsetzung des so genannten „Extended Access Control" (EAC) soll auf europäischer Ebene ab 2007 der Zugriffschutz für die im Chip gespeicherten Informationen erheblich verbessert werden. Da wesentliche Hintergrundinformationen zu diesem Konzept nicht öffentlich zur Verfügung standen, wurde es in der Studie nicht bewertet. Für die übrigen genannten Kritikpunkte wird derzeit jedoch anscheinend nicht an Lösungen gearbeitet.[14]

In einigen EU-Staaten wie z.B. Frankreich (Projekt INES) und Deutschland [En06] wird die Umsetzung dieses technischen Konzeptes auch für die nationalen Ausweise verfolgt.

2.2 Elektronische Signaturlösungen

2.2.1 Analyse

Mit der Richtlinie 1999/93/EG vom 13.12.1999 steht eine europaweit anerkannte und gültige Rechtsgrundlage für den Einsatz elektronischer Signaturen für alle Mitgliedsländer der EU zur Verfügung.

Seit dem Einsatz der ersten Signatursysteme sind keine gravierenden Angriffe auf die Algorithmen bekannt geworden – insoweit kann die Technologie als recht ausgereift angesehen werden. Unabhängig davon bedürfen das zugrunde liegende Vertrauensmodell (in Personen, Darstellungs- und Signierkomponenten sowie Zertifizierungsstellen) sowie die eingesetzte Kryptographie unter Sicherheitsgesichtspunkten beständig der Beobachtung und ggfs. Anpassung (z.B. im Bereich der Schlüssellängen).

Derzeit werden elektronische Signaturen europaweit unter Datenschutzgesichtspunkten nicht optimiert eingesetzt. So ist z.B. über Zertifikatsinformationen eine Verkettbarkeit von Transaktionen gegeben, was dem Gebot der Datensparsamkeit zuwider läuft und das Prinzip der Zweckbindung nicht technisch umsetzt. Nur in wenigen Ländern sind Alternativen wie digitale Credentials (z.B. bei der österreichischen Bürgerkarte) oder in beschränktem Umfange der Einsatz pseudonymer Signaturen (z.B. in Deutschland) möglich.

Die Nutzung von elektronischen Signaturen ist offensichtlich in allen europäischen Ländern weit hinter den Erwartungen zurückgeblieben. In zahlreichen Ländern (z.B. Belgien und Österreich) ist derzeit der Mangel an Anwendungen ein hemmender Faktor, bei einem kommerziellen PKI-Betreibermodell (z.B. in Deutschland, Finnland und Österreich) kommen noch die Kosten für die Ausstellung und den Betrieb der Signaturlösung bei den Nutzern hinzu. Dieser Faktor entfällt bei Ländern mit einem staatlichen Betreibermodell (wie etwa Belgien), so dass in diesen Ländern mittelfristig bereits mit einer deutlich größeren Nutzung elektronischer Signaturen gerechnet wird.

2.2.2 Trends

Neben der Schaffung neuer Anwendungsfälle für elektronische Signaturen steht deren Interoperabilität über europäische Landesgrenzen hinweg im Zentrum aktueller Entwicklungen. Hierzu werden derzeit zwei alternative Konzeptansätze verfolgt:

- Gateway-Lösungen (z.B. das Konzept im Projekt GUIDE)[15],
- Brücken-Certificate-Authorities (European Bridge-CA, EB-CA[16]), die hierarchisch verschiedene Certificate Authorities international miteinander verbinden.

Im Rahmen des Projektes „Provide eGovernment Good Practice Portability" (PPP)[17] wird derzeit an einem neuen Ansatz zur Vermeidung von Verkettbarkeit bei der elektronischen Authentifizierung gearbeitet. Dabei sollen durch vertrauenswürdige Parteien auf Basis von X.509-Zertifikaten serverseitig erzeugte sektorspezifische Identifier (Credentials) zur Authentifizierung der Nutzer gegenüber Diensteanbietern eingesetzt werden (so genannte Server Derived IDs). Die geplante Lösung ist damit zur bestehenden Public Key-Infrastruktur (PKI) kompatibel.

3 Gestaltungsprinzipien für eIDs

Die FIDIS-Studie berichtet nicht nur über existierende oder geplante eID-Konzepte, sondern greift auch Ideen zur Gestaltung von eIDs auf, die aus Datenschutz- und/oder Datensicherheitssicht viel versprechend sind. Dazu gehört die Arbeit des „Identity Projects" der London School of Economics and Political Science (LSE)[18]: Im Report „The Identity Project – an assessment of the UK Identity Cards Bill and its implications"[19] analysiert das Projekt zunächst die Pläne der britischen Regierung, Identitätsausweise einzuführen, und zeigt Gestaltungsoptionen auf. Daraus hat Niels Bjergstrom, Herausgeber der „Information Security Bulletin", Kriterien für eID-Systeme abgeleitet [Bje05], die sich an einer „Root Identity" pro Person fest machen: In der digitalen Welt benötige man ein nicht bestreitbares, elektronisch lesbares Dokument, das als „digitales Geburtszertifikat" dienen kann, die Wurzelidentität (Root Identity). Folgende Eigenschaften müssten daran geknüpft sein:

- Es müsste eine unabstreitbare Verbindung zum Nutzer bestehen.
- Die Wurzelidentität müsste eine Teilnahme an Autorisierungsprozeduren erlauben, ohne dass personenbezogene Daten versehentlich herausgegeben werden.
- Sie sollte eine Authentifizierung ermöglichen, ohne dass die Identität beeinträchtigt wird, d.h. anonym oder unter Pseudonym, was für die meiste Zeit die Standardeinstellung und damit auch An-

[13] Für die zukünftigen USA-Pässe sollen Metallfasern in dem vorderen Passumschlag vor dem unberechtigten Auslesen schützen. Allerdings wurde gezeigt, dass dieser Schutz unzureichend ist, da sich ein Pass auch in der Tasche öffnen kann: Bereits ein um gut einen Zentimeter geöffneter Pass ließ sich in einer Demonstration auf der Konferenz „Black Hat USA 2006" im August 2006 mehr als einen halben Meter weit auslesen (siehe http://www.wired.com/news/technology/1,71521-2.html).

[14] Die technische Spezifikation zu Extended Access Control kann mittlerweile unter ePass@bsi.bund.de beim BSI angefordert werden (siehe auch http://www.bsi.bund.de/fachthem/epass/eac.htm).

[15] Siehe http://istrg.som.surrey.ac.uk/projects/guide/.

[16] Siehe auch http://www.bridge-ca.org/eb-ca2/index.php?option=com_content&task=view&id=19&Itemid=74.

[17] Siehe http://www.eu-forum.org/article.php3?id_article=258.

[18] Siehe http://is2.lse.ac.uk/IDcard/.

[19] Download: http://is2.lse.ac.uk/IDcard/identityreport.pdf.

forderungen an jedes eID-System in einer freien Gesellschaft ist.
- Die Wurzelidentität sollte eindeutig und ausschließlich den rechtmäßigen Inhaber repräsentieren (mit Hilfe von Public-Key-Verschlüsselung)
- Sofern Identifizierung notwendig ist, sollte die Wurzelidentität eine Teilnahme am Identifikationsprozess ermöglichen.
- Die Wurzelidentität dürfte nicht auf unersetzbaren persönlichen Eigenschaften basieren, da man eine Kompromittierung nicht ausschließen kann.
- Das Token mit der eID-Information (z.B. eine Chipkarte) müsste ersetzbar sein ohne unerwünschte Folgen, d.h. Diebstahl oder Verlust eines Tokens darf nicht eine Übernahme der eigenen Identität ermöglichen.
- Alle Funktionen, einschließlich jeder Offenbarung von Informationen auf dem Token, müssten der vollen Kontrolle des Inhabers unterstehen.

Bjergstrom schlägt vor, die Beziehung zwischen eID und dem Nutzer auf Basis von dessen DNA durchzuführen, ohne dass personenbezogene Daten offenbart werden müssen. In jedem Fall sieht er eine Notwendigkeit für ein eID-System, das so dezentral wie möglich arbeitet, indem die Informationen innerhalb der individuellen eID-Tokens herangezogen werden.

Auch wenn Bjergstrom in seinem mittlerweile viel zitierten Editorial die Anforderungen und mögliche Lösungen nur kurz umreißt und zugibt, dass noch nicht alle Fragen bis zu Ende gedacht sind, besteht hier doch ein Anknüpfungspunkt. Bjergstrom selbst rechnet mit einem Entwicklungsaufwand von einem Jahr für ein Team, dem die besten Experten angehören. Sein Editorial beendet er mit „I think I know the people who can design and produce most of the deliverables but who asks the old editor?"

Es bleibt abzuwarten, inwieweit die eID-Studie von FIDIS sowie Projekte wie Modinis-IDM[20] zu Identitätsmanagement im E-Government oder auf das Thema spezialisierte Blogs wie Stefan Brands' Identity Corner[21] einen Einfluss auf eine eID-Entwicklung nehmen kann, die Datenschutz- und Datensicherheitsanforderungen optimal umsetzt.

[20] Siehe https://www.cosic.esat.kuleuven.be/modinis-idm/.

[21] Siehe http://www.idcorner.org/.

Fazit

Während die elektronischen Signaturlösungen als insgesamt vergleichsweise ausgereift eingeschätzt werden, gibt es bei den ICAO-kompatiblen, maschinenlesbaren Ausweisdokumenten noch erhebliche Verbesserungsbedarfe. Insgesamt sind die folgenden Risiken und Probleme zu berücksichtigen:
- Erhebliche Risiken des Identitätsdiebstahls auch unter Verwendung biometrischer Merkmale;
- Entwertung klassischer forensischer Verfahren (v.a. Fingerabdruck);
- Überschießende Informationen in biometrischen Rohdaten;
- Qualitätsprobleme von Biometrie und fehlende, standardisierte Alternativverfahren für die Authentisierung von Ausweisinhabern;
- Verkettbarkeit von Authentifizierungen unter Verwendung des Ausweises;
- Durchsetzung der Zweckbindung für personenbezogene Ausweisdaten im internationalen Kontext.

Eine grundlegende technische und konzeptionelle Überarbeitung des Konzeptes für die derzeit ausgegebenen ICAO-kompatiblen, maschinenlesbaren Ausweise scheint den Autoren der Studie dringend geboten. Wegen der besonderen Bedeutung von eIDs sollten für die Erarbeitung solcher Konzepte disziplinenübergreifend die Experten aus den relevanten Bereichen einbezogen werden und auch kritische Stimmen stärker gehört werden. Für eine größtmögliche Akzeptanz und zur Vermittlung der nötigen Medienkompetenz der Bevölkerung sollte die öffentliche Diskussion nachgeholt werden, die bis jetzt fehlt.

> Den Nutzern der derzeitigen Implementierungen kann man nur raten, den Ausweis nur dann zu verwenden und bei sich zu tragen, wenn es unbedingt erforderlich ist, ihn in einem Faraday'schen Käfig (z.B. Alufolie) zu transportieren und ihn bei Nichtbenutzung besonders sorgfältig einzuschließen. Mit diesen Maßnahmen lassen sich die genannten Risiken und Probleme zwar nicht lösen, aber soweit es in der Macht des Ausweisinhabers steht, reduzieren.

Literatur

BeGi05 Beel, J., Gipp, B., *ePass – der neue biometrische Reispass*, Shaker Verlag, Aachen 2005. Download von Kapitel 6 „Fazit": http://www.beel.org/epass/epass-kapitel6-fazit.pdf

Bje05 Bjergstrom, N., *Editorial of Information Security Bulletin Oct. 2005*; http://www.chi-publishing.com/samples/ISB1008 Editorial.pdf

BSI04 Finke, T., Kelter, H., *Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*, Bonn 2004. Download: http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

BSI05 'Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II', Bundesamt für Sicherheit in der Informationstechnologie (BSI), Bonn 2005. Download: http://www.bsi.de/literat/studien/biop/biop_2.htm

BZK05 '2b or not 2b – Evaluatierapport Biometrieproef 2b or not 2b', Ministrie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Amsterdam 2005. Download: http://www.minbzk.nl/contents/pages/43760/evaluatierapport1.pdf

CEN04 CEN/ISSS, 'Towards an electronic ID for the European Citizen, a strategic vision', *CEN/ISSS Workshop eAuthentication*, Brussels, 03.10.2004, S. 1-71. Download: http://europa.eu.int/idabc/servlets/Doc?id=19132

En06 Engel, C., *Auf dem Weg zum elektronischen Personalausweis*, DuD 4/2006, S. 207-210, Wiesbaden 2006.

GaMeWa05 Gasson, M., Meints, M., Warwick, K. (Hrsg.), *FIDIS Deliverable D3.2 – Study on PKI and Biometrics*, Frankfurt a.M. 2005. Download: http://www.fidis.net/487.0.html

GeSo06 Geradts, Z., Sommer, P. (Hrsg.), *FIDIS Deliverable D6.1 – Forensic Implications of Identity Management Systems*, Frankfurt a.M. 2006. Download: http://www.fidis.net/487.0.html

MeHa06 Meints, M., Hansen, M. (Hrsg.), *FIDIS Deliverable D3.6 – Study on ID Documents*, Frankfurt a.M. 2006. Download: http://www.fidis.net/487.0.html