Der ePass – eine Sicherheits- und Datenschutzanalyse[1]

Dr. Martin Meints, Marit Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98
24103 Kiel
LD102@datenschutzzentrum.de
LD10@datenschutzzentrum.de

Abstract: Im November 2005 begann in Deutschland die Ausgabe des neuen Reisepasses (ePass), der in der ersten Stufe seiner Einführung ein digitales Gesichtsbild des Passinhabers enthält. Mit der zweiten Stufe ist seit dem 01.11.2007 die Speicherung von Fingerabdrücken auf dem ePass hinzugekommen. Damit steht für die Kontrolle von Reisenden das zweite biometrische Merkmal zur Verfügung. Der vorliegende Beitrag setzt sich mit den Sicherheits- und Datenschutzrisiken beider Stufen des ePasses vergleichend auseinander, die sich für die Nutzer ergeben können. Anhand zweier Szenarien werden die Risiken bewertet. Der Artikel schließt mit konkreten Empfehlungen für Passinhaber und für die Gestalter von Reisepässen und anderen elektronischen Identifikationsdokumenten.

1 Einleitung

Auf Grundlage des Dokuments 9303[2] der International Civil Aviation Organization (ICAO) für maschinenlesbare Reisedokumente (Machine Readable Travel Documents, MRTDs) wurde mit der EU-Verordnung 2252/2004[3] ein neuer Standard für Reisepässe (ePässe) auch für die Bundesrepublik verbindlich. Die Einführung erfolgte in zwei Stufen. In der ersten Stufe wurde ab November 2005 ein kontaktlos auslesbarer Chip (auch als RFID-Chip bezeichnet) eingeführt, auf dem neben den im Pass abgedruckten personenbezogenen Daten der maschinenlesbaren Zone (Datengruppe 1) auch ein digitales Bild des Gesichtes gespeichert ist (Datengruppe 2)[4]. Hinzu kommen einige so genannte Sicherheitsobjekte (insb. Hashwerte der im RFID-Chip gespeicherten Daten und eine Signatur über diese Werte). Optional können auch öffentliche Schlüssel

[1] Die Arbeiten an diesem Artikel wurde mit Mitteln der Europäischen Union im Rahmen des Projektes FIDIS – Future of Identity in the Information Society (http://www.fidis.net/) gefördert. Bedanken möchten wir uns bei den Reviewern für ihre hilfreichen Anmerkungen.
[2] Informationen sind über http://mrtd.icao.int/ verfügbar.
[3] Siehe http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf
[4] Als JPEG-2000 Bild gemäß ISO 19792-5

gespeichert werden, die zur aktiven Authentisierung (Active Authentication) des RFID-Chips eingesetzt werden können (Datengruppe 15).

In der zweiten Stufe werden ab 01.11.2007 zusätzliche Daten im RFID-Chip gespeichert[5]. Diese beinhalten insbesondere die digitalen Bilder der beiden Zeigefinger (Datengruppe 3) und als weiteres Sicherheitsmerkmal einen öffentlichen Schlüssel (Datengruppe 14). Der Zugriffschutz bezogen auf diese zusätzlichen Daten wurde erheblich verbessert, während es beim Zugriffsschutz auf die bisher gespeicherten Daten nur geringfügige Änderungen gibt [BSI07], [KN07]. Ziele der elektronischen Aufrüstung der Pässe waren nach Angaben des Bundesinnenministeriums im Jahr 2005 eine Verbesserung der Fälschungssicherheit, die Nutzung der Biometrie zur Fahndung nach Straftätern und Terroristen[6] und Erleichterungen im Reiseverkehr[7].

Dieser Artikel ist wie folgt aufgebaut: Kapitel 2 erläutert die Risiken aus Datenschutz- und Datensicherheitssicht, die mit der ersten Realisierungsstufe des ePasses einhergehen. Dieses Kapitel enthält auch zwei Angriffsszenarien, die für den ePass durchgespielt und evaluiert werden. Kapitel 3 erläutert die Änderungen bei der Einführung der zweiten Stufe des ePasses und bewertet sie. Kapitel 4 fasst die Ergebnisse zusammen und gibt Handlungsempfehlungen sowohl für die künftige Technikgestaltung als auch für den konkreten Umgang mit dem ePass.

2 Risiken der ersten Stufe des ePasses

2.1 Sicherheitslücken und -risiken

Sicherheitslücken der ersten Stufe des ePasses wurden vielfältig in der Literatur untersucht. Aus Sicht der Autoren sind insbesondere relevant:

1. Unzureichende Wirksamkeit des Zugriffschutzes Basic Access Control (BAC): BAC kann wegen geringer Entropie des Schlüssels (bis zu 56 Bit) gebrochen (u.a. [BG05], [Ro06]) und wegen unzureichenden Schlüsselmanagements umgangen werden. Die benötigten Daten zur Berechnung des BAC-Schlüssels sind in der maschinenlesbaren Zone (MRZ) des Passes enthalten. Dies führt dazu, dass der Passinhaber nicht in jeder Situation die Kontrolle über den Schlüssel sowie dessen Speicherung und Nutzung hat, da Pässe in einigen Ländern (z.B. Italien, der Slowakei und Tschechien) teilweise bis zu acht

[5] JPEG-2000 Bild gemäß ISO 19792-4
[6] Siehe http://www.bmi.bund.de/nn_163950/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2005/10/ePass.html
[7] Siehe http://www.bmi.bund.de/nn_163950/Internet/Content/Nachrichten/Archiv/Reden/2005/06/ePass.html)

Stunden z.B. in Hotels (und damit nichtstaatlichen Stellen) abgegeben werden müssen (u.a. [MH06], [Ko07]).[8]

2. Die Reichweite des Auslesens kann von den vorgesehenen 10-15 cm auf bis zu 50 cm gesteigert werden (u.a. [Ro06]).

3. Das Abhören von Kommunikation zwischen (berechtigtem) Lesegerät und Ausweis ist aus bis zu 5 m mit Spezialtechnik möglich (u.a. [Ro06]).

4. Die internationalen Regelungen bezogen auf organisatorische Sicherheitsmaßnahmen entsprechen vor allem außerhalb Europas nicht den Vorgaben einschlägiger Normen, z.B. der ISO/IEC 27001. Die Kontrolle über relevante Systemteile und die damit verarbeiteten Daten ist über die 189 Mitgliedsstaaten der ICAO verteilt. Es fehlen überdies eine auf Verträgen basierende, internationale Festlegung eines einheitlichen Sicherheitsniveaus bei der Lese- und Überprüfungsinfrastruktur, gegenseitige Auditierung der Umsetzung und Durchsetzung dieses Sicherheitsniveaus.
   In Europa gibt es einige organisatorische Sicherheitsmaßnahmen, z.B. eine über das Schengen-Informationssystem verfügbare Liste der verlorenen oder gestohlenen Pässe.[9] Darüber hinaus sind technische Sicherheitsmaßnahmen dokumentiert[10] [BSI05], [KN07]. Eine umfassende, alle Lebenszyklen des Passes und der zugehörigen Lesesysteme umfassende europäische Sicherheitskonzeption ist jedoch aus den öffentlich zugänglichen Quellen nicht erkennbar (u.a. [Me07]).

5. Fehlendes Lebenszyklenmanagement und fehlende Wartbarkeit des ePasses: Informationen zum sicheren Umgang der Bürger mit ePässen stehen kaum zur Verfügung, eine zentrale Anlaufstelle für diesbezügliche Fragen existiert nicht. Eine Aufrüstung einmal ausgegebener und in Deutschland 10 Jahre gültiger Pässe mit neuen Sicherheitsfunktionen oder aktualisierten biometrischen Referenzdaten ist nicht möglich. Vorhandene Sicherheitslücken können daher sehr lange ausgenutzt werden. Auch bei einigen Lesegeräten wurden inzwischen Verwundbarkeiten nachgewiesen.[11] Über die Wartbarkeit dieser Geräte ist öffentlich bislang wenig bekannt geworden. Probleme kann auch die Qualität der Biometrie mit sich bringen, da die Passinhaber in den 10 Jahren der Gültigkeit des ePasses ihr Aussehen ändern können (z.B. durch Stehenlassen

---

[8] In einigen europäischen Mitgliedsländern ist die Situation noch kritischer als in der Bundesrepublik. So fehlt z.B. in Belgien von November 2004 bis Juli 2006 BAC völlig (siehe http://diplobel.fgov.be/en/press/homedetails.asp?TEXTID=26303), in den Niederlanden war in den ersten Versionen die Seriennummer mit dem Gültigkeitsdatum verknüpft, so dass die Entropie noch deutlich unter 56 Bit sank [Ro06], und in Schweden sind nach einer den Autoren vorliegenden Auskunft der Polizeidirektion Värmland vom 05.02.2007 alle für die Berechnung des BAC-Schlüssels benötigten Daten über schwedische Bürger öffentlich zugänglich.

[9] Siehe http://europa.eu/scadplus/leg/de/lvb/l14158.htm

[10] Informationen zu technischen Sicherheitsmaßnahmen sind z.B. im Rahmen der Protection Profiles BSI-PP-0016-2005 und BSI-PP-0017-2005, zertifiziert im Jahr 2005 durch das Bundesamt für Sicherheit in der Informationstechnik (BSI; siehe http://www.bsi.de/zertifiz/zert/report.htm), verfügbar.

[11] Siehe http://www.wired.com/politics/security/news/2007/08/epassport und http://www.focus.de/digital/computer/sicherheitsluecken_aid_68760.html

eines Bartes), erkranken oder altern und dadurch die Fehlzurückweisungen zunehmen können.[12]

6. Für den Fall des Versagens der biometrischen Verifikation, z.B. infolge von technisch bedingter Fehlzurückweisung (False Rejection), wurde kein verbindliches Ersatzverfahren festgelegt. Dies gefährdet möglicherweise die Einreise der Betroffenen oder kann andere unangenehme Folgen haben, die für diese unverständlich und nicht vorhersehbar sind.

7. Die Passvergabe ist kein verlässlicher Prozess: In 14 europäischen Ländern, darunter auch die Bundesrepublik Deutschland, konnten in einem Test staatliche Pässe mit Bildern offiziell erworben werden, die nicht vom berechtigten Inhaber des Passes stammten. [13]

8. Der RFID-Chip des ePasses konnte geklont werden, d.h. die Informationen ließen sich auf einen leeren Chip übertragen.[14] Die Funktion der aktiven Authentisierung (Active Authentication), die ein Kopieren verhindern kann, ist für die ICAO-Mitgliedsstaaten lediglich optional. Ein Durchlaufen der Active Authentication ist daher nicht sichergestellt. Darüber hinaus weist die Active Authentication bekannte Schwächen auf [KN07].

2.2 Datenschutzrisiken

Auch Datenschutzaspekte des ePasses der ersten Stufe, die gegenüber den traditionellen papiergebundenen Pässen vor allem durch den Einsatz von Biometrie entstehen, wurden bereits an anderer Stelle untersucht (u.a. [Me07]). Der ePass weicht in zahlreichen Punkten von den Empfehlungen zur datenschutzgerechten Implementierung biometrischer Systeme der Art. 29-Datenschutzgruppe, niedergelegt im „Working Paper 80“[15], ab:

1. Es werden biometrische „Rohdaten“ anstelle von Templates benutzt. Biometrische Rohdaten lassen sich als kontextübergreifende Identifikatoren verwenden, woraus sich über eine mögliche Verkettung das Risiko von Verstößen gegen das Datenschutzprinzip der Zweckbindung und damit eine missbräuchliche Nutzung dieser Daten ergibt. Darüber hinaus können aus biometrischen Rohdaten ergänzende, für die Authentisierung nicht benötigte und in einigen Fällen gesundheitsbezogene Informationen gewonnen werden

[12] Siehe die Stellungnahme von C. Busch zum „Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften“ vor dem Innenausschuss des Deutschen Bundestages am 23.04.07, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung07/Stellungnahmen_SV/Stellungnahme01.pdf

[13] Siehe BBC-Reportage: „My faked passport and me“, http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm

[14] Siehe z.B. K. Zetter, Hackers Clone E-Passports, Wired News, August 3, 2006; siehe http://www.wired.com/news/technology/1,71521-0.html

[15] Siehe http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_de.pdf

(u.a. [Co03], [VGr07]).[16] Dies widerspricht dem Grundsatz der Datenminimierung. Durch fehlende Widerrufbarkeit von Referenzdaten ergeben sich daneben auch potenzielle Sicherheitsrisiken, z.B. das Risiko des Identitätsdiebstahls.

2. Auch die vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen stellen die Zweckbindung und den Verzicht auf dauerhafte Speicherung biometrischer (und anderer personenbezogener) Daten im Ausland nicht sicher.

3. Die gemeinsame Speicherung von biometrischen und anderen personenbezogenen Daten auf dem RFID-Chip erleichtert Verkettung und damit wiederum die Verletzung der Zweckbindung.

2.3 Angriffszenarien

Neben Angriffen durch Personen, die im Rahmen nationalgesetzlicher Aufgaben einen berechtigten Zugriff auf Pässe, Systeme oder Systemkomponenten und damit alle oder Teile der Daten des ePasses haben (Innentäterszenarien), wurden zwei Angriffszenarien durch externe Angreifer in der Literatur diskutiert (u.a. [Ko07], [LK+07]).

Das erste Szenario ermöglicht das Verfolgen einzelner Passträger (oder kleiner Gruppen). Es wurde auch dargestellt, dass dieses Szenario für das personenbezogene Auslösen bestimmter Ereignisse genutzt werden kann.[17] Dieses Szenario setzt voraus, dass die Daten der MRZ des ePasses dem Angreifer bekannt sind. Da das Durchlaufen der BAC-Authentisierung ca. 1 Sekunde benötigt, ist dieses Szenario praktisch auf Einzelpersonen oder kleine Gruppe mit bis zu 10 Personen beschränkt, wenn ein längerer mit Lesegeräten ausgestatteter schmaler Korridor eingesetzt werden kann. Eine Verfolgung bei unbekannter MRZ ist praktisch unmöglich [KN07].

Das zweite Szenario basiert auf dem Abhören der Kommunikation zwischen einem autorisierten Lesegerät und einem ePass und ermöglicht so einen Missbrauch der ausgelesenen Daten, z.B. zum Zweck des Identitätsdiebstahls. Da in diesem Fall die Zeit für das Durchlaufen der BAC-Authentisierung entfällt, ist ein Brute-Force-Angriff auf die BAC-Schlüssel durchaus mit modernen Cluster- oder GRID-Systemen in überschaubarer Zeit machbar.

Die folgende Abbildung zeigt schematisch die beiden Szenarien:

---

[16] Eine Übersicht über überschießende, teilweise auch gesundheitsbezogene Informationen, die aus biometrischen Rohdaten und möglicherweise auch Templates gewonnen werden können, gibt für gängige biometrische Verfahren unter kritischer Berücksichtigung nichtwissenschaftlicher Methoden wie Iridologie das FIDIS-Deliverable „Biometrics in Identity Management“ [KM08].

[17] Siehe Präsentation von A. Pfitzmann vor dem Innenausschuss des Deutschen Bundestag am 23.04.2007, siehe http://dud.inf.tu-dresden.de/literatur/Berlin2007_04_23PaesseBiometrieRFIDv4.pdf und spätere Zeitungsmeldungen, z.B. http://www.sueddeutsche.de/,tt3m3/computer/artikel/323/82241/

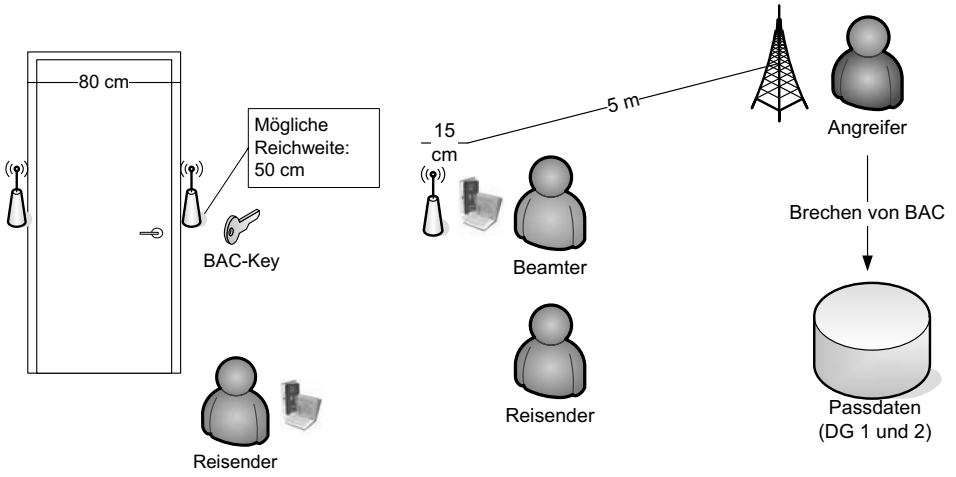

Abbildung 1: Szenario 1 (Verfolgung) und Szenario 2 (Abhören)

2.4 Bewertung der vorgestellten Szenarien

Zur Bewertung dieser beiden Szenarien eignen sich die Kriterien, die Bruce Schneier mit seiner Attack-Tree-Methode 1999[18] veröffentlicht hat. Er schlägt vor, für die Bewertung von Angriffen die prinzipielle Durchführbarkeit sowie den Aufwand, die Kosten und die persönlichen Risiken für den Angreifer zu bewerten. Ebenso soll der für den Angreifer entstehende Nutzen beleuchtet werden.

Beide Szenarien aus dem vorigen Abschnitt sind zunächst einmal unter technischen Gesichtspunkten als grundsätzlich durchführbar einzuschätzen.

Das Szenario 1 hat potenzielle Anwendungen bei Staaten, die Reisende überwachen möchten und im Besitz der Daten der MRZ sind (z.B. durch das Vorlegen des ePasses an der Grenze, im Hotel o.ä.). Auch die Nutzung durch privatwirtschaftliche und kriminelle Organisationen für Überwachungszwecke ist denkbar. Hierbei bemisst sich der Nutzen jedoch auch daran, ob nicht kostengünstigere und mit tragbaren Risiken verbundene Alternativverfahren zur Verfügung stehen, was häufig der Fall sein wird.

Im Fall der Nutzung durch kriminelle Organisationen kann daneben das Auslösen personenspezifischer Ereignisse interessant sein, auch im Sinne der Anwendung von Mafia-Methoden. Terroranschläge, die auf hohe Zahlen von Betroffen und nicht auf bestimmte Individuen ausgerichtet sind, lassen sich jedoch ebenfalls – teilweise einfacher – auf andere Weise herbeiführen.

[18] Siehe http://www.schneier.com/paper-attacktrees-ddj-ft.html#rf7

Die Umsetzung dieses Szenarios ist mit technischen und organisatorischen Aufwendungen verbunden. Es verlangt eine Kontrolle der Räumlichkeiten, in denen die Überwachungseinrichtungen installiert werden. Darüber hinaus muss erreicht werden, dass sich die zu überwachenden Personen ausreichend lange im Erfassungsbereich der Lesegeräte aufhalten (für 10 Personen erfordert dies also ca. 10 Sekunden). Diese müssen zudem so eingestellt sein, dass sie mit der abgestrahlten Energie zu Aktivierung und Versorgung des RFID-Chips im Pass nicht durch gefühlte Wärme die Aufmerksamkeit des Betroffenen erregen. Auch müssen die Lesegeräte für eine unauffällige Realisierung die je nach einsetzender Organisation und Einsatzland gültigen gesetzlichen Bestimmungen erfüllen (z.B. Strahlenschutz, um nicht den Betroffenen zu schädigen).

In Mitgliedsländern der Europäischen Union ist die Nutzung dieses Szenarios privatwirtschaftlichen Organisationen gesetzlich zumindest gemäß Datenschutzgesetzen verboten. Die Umsetzung dieses Szenarios ist daher mit dem Risiko rechtlicher Konsequenzen sowie erheblicher Ruf- und Imageschäden verbunden, was zumindest am Markt etablierten Unternehmen schrecken dürfte. Diese Risiken bestehen aber nicht notwendigerweise in ähnlicher Weise außerhalb von Europa.

Unter Berücksichtigung dieser Fakten scheint vor allem das Auslösen von personenspezifischen Ereignissen mit kriminellem Hintergrund interessant zu sein. Auch das Tracken (d.h. Verfolgen) von Reisenden im außereuropäischen Ausland durch staatliche und privatwirtschaftliche Organisationen kommt in Betracht, wenn der zu betreibende Aufwand einem ökonomisch zu rechtfertigen Nutzen gegenüber steht. Dies wird eher vereinzelt der Fall sein, zumal zunächst der Aufbau einer Infrastruktur von Lesegeräten zum Tracken nötig wäre. Allerdings könnte man sich auf Verkehrsknotenpunkte, Hotels und wichtige Gebäude konzentrieren.

Das Szenario 2 hat seine Anwendung überwiegend bei privatwirtschaftlichen Organisationen, da staatliche Organisationen über bestehende oder zu erstellende Gesetze und Verordnungen an diese Daten üblicherweise leichter (und dann legal) herankommen können. Der Nutzen dieses Szenarios liegt wohl eher bei der Beschaffung biometrischer Rohdaten (Gesichtsbilder, die für ein automatisiertes Matching gegen digitale Daten optimiert sind) als bei den Daten der MRZ, die einfacher und möglicherweise unauffälliger auch aus dem Pass auf anderen Wegen (z.B. Innentäter, Filmaufnahmen etc.) beschafft werden können. Biometrische Rohdaten sind auch deshalb potenziell interessant, weil sie wie bereits dargestellt zusätzliche, in einigen Fällen auch gesundheitsbezogene, Informationen beinhalten (u.a. [Co03], [VGr06]).

Auch eine kriminelle Motivation ist denkbar, etwa zur Nutzung der biometrischen Daten für Identitätsdiebstahl. Dies setzt jedoch relativ schwach abgesicherte biometrische Systeme voraus, die Gesichtserkennung einsetzen. Derartige Systeme sind zurzeit nicht weit verbreitet; dieser Nutzen also als eher beschränkt einzustufen.

Die Umsetzung dieses Szenarios ist ebenfalls mit technischen und organisatorischen Aufwendungen verbunden. Entweder muss der Angreifer große und möglicherweise auffällige Antennen einsetzen, oder es ist ebenfalls eine Kontrolle der Räumlichkeiten,

in denen die Überwachungseinrichtungen verdeckt installiert werden, erforderlich. Darüber hinaus müssen Bit-Fehler in der Datenübertragung vermieden werden [KN07], wozu möglicherweise Repeater eingesetzt werden könnten. Derartige Maßnahmen erhöhen jedoch die Kosten für den Angreifer. Kosten verursacht auch die benötigte Rechenkapazität zum Brechen der BAC-Schlüssel.

Die Risiken für die privatwirtschaftlichen Organisationen entsprechen im Wesentlichen denjenigen, die bereits beim Szenario 1 aufgeführt wurden. Vor diesem Hintergrund kommt eine Nutzung des Szenarios 2 vor allem außerhalb Europas durch privatwirtschaftliche Organisationen in Betracht, wenn der zu betreibende Aufwand einem ökonomisch zu rechtfertigen Nutzen gegenüber steht. Dies wird eher vereinzelt der Fall sein.

Mit Sicherheit ist das eingangs erwähnte Szenario des Datendiebstahls durch Innentäter bei beiden Stufen des ePasses als relevant einzustufen. An der Ausstellung und Nutzung nehmen die 189 ICAO-Mitgliedsländer teil. In diesen Ländern sind wiederum zahlreiche Behörden, teilweise auch private Organisationen und Personen (z.B. Hotels) in die Ausstellung und Nutzung eingebunden. Alleine in der Bundesrepublik gibt es 5.200 Meldebehörden,[19] die an der Ausstellung beteiligt sind. Hinzu kommen die Polizeidienststellen des Bundes und der Länder. Die Zahl der mit der Ausstellung und Nutzung beauftragten Mitarbeiter dürfte 250.000 deutlich überschreiten.

Eine Bewertung der Risiken für den Angreifer ist jedoch deshalb nicht möglich, weil die vorbeugend getroffenen Sicherheitsmaßnahmen weitgehend nicht öffentlich bekannt sind.

3 Die zweite Stufe des ePasses

3.1 Änderungen mit der Einführung der zweiten Stufe

Unter Sicherheitsgesichtspunkten bringt bei Nutzung aller zusätzlichen Funktionen die zweite Stufe des ePasses innerhalb Europas einige Verbesserungen. So wurden der Zugriffsschutz durch Erhöhung der Entropie bei BAC über geänderte Seriennummern und durch Einführung von Extended Access Control (EAC) sowie die Verschlüsselung bei Übermittlung zusätzlicher Daten (insb. der Fingerabdrücke) erheblich verbessert.[20]

Beim Versagen eines biometrischen Merkmals steht mit den Fingerabdrücken beider Zeigefinger ein weiteres biometrisches Ersatzverfahren zur Verfügung. Da die Passvergabe mit der Erhebung von Fingerabdrücken in der Meldebehörde verbunden ist, wird die Verlässlichkeit des Ausgabeprozesses erhöht und der beschriebene diesbezügliche Angriff (Punkt 7 in Abschnitt 2.1) erschwert. Ferner wird das Kopieren

[19] Siehe z.B. http://www.sueddeutsche.de/deutschland/artikel/611/112499/print.html
[20] Siehe z.B. http://www.bmi.bund.de/cln_028/nn_1082274/Internet/Content/Themen/PaesseUndAusweise/Einzelseiten/Wichtige__Aenderungen__1__November.html

des Passes durch zusätzliche nicht auslesbare Sicherheitsmerkmale wie öffentlicher Schlüssel erschwert.

3.2 Bewertung dieser Änderungen

Diese zusätzlichen Funktionen, insbesondere der verbesserte Zugriffsschutz Extended Access Control (EAC), sind noch kein ICAO-Standard und werden daher außerhalb Europas nicht unterstützt; die zugehörigen Sicherheitsverbesserungen stehen daher dort nicht zur Verfügung. Zudem bestehen alle in Abschnitt 2.4 beschriebenen Risiken fort, da der RFID-Chip im neue ePass bezogen auf wesentliche Funktionen wie BAC, Datengruppen und -formate abwärtskompatibel zum bisherigen sein muss, um international ausgelesen werden zu können.

Darüber hinaus weist EAC bedingt durch das Technikkonzept Verwundbarkeiten auf, die in einer Risikoanalyse betrachtet wurden [BSI07]. Die Verwundbarkeiten sind wie folgt begründet:

- Der RFID-Chip im ePass hat keine Batterie und infolge dessen keinen Zeitchip. Der Chip kann daher nur Zeitstempel speichern, die er bei jedem Auslesen übermittelt bekommt. Ein selten benutzter ePass kann die Aktualität von Zertifikaten, die ihm ein Lesegerät präsentiert, nur bedingt überprüfen.

- Lesegeräte müssen auch ohne Online-Zugang zur dahinterliegenden Public Key Infrastructure (PKI) funktionieren. Daraus ergibt sich die Notwendigkeit, dass ein Lesegerät alle für die Authentisierung gegenüber dem Chip im ePass benötigten Zertifikate speichern muss.

Ein Diebstahl eines autorisierten Lesegeräts versetzt einen Angreifer damit in die Lage, zumindest vorübergehend ePässe unautorisiert auszulesen. Dieses beschriebene Risiko wird dadurch verringert, dass die Zertifikate in den Lesegeräten nur eine sehr kurze Gültigkeit haben. Auch an dieser Stelle wird nochmals deutlich, wie wichtig Maßnahmen gegen Innentäter für die Sicherheit des ePasses und die dort gespeicherten Daten sind.

Da den Autoren derzeit keine offiziellen Quellen zur Verbesserung der Entropie der BAC-Schlüssel zur Verfügung stehen, kann diese nicht abschließend bewertet werden.[21] In jedem Fall wird die Umsetzung des Szenarios 2 jedoch erschwert. Die bereits erwähnten Mängel im Schlüsselmanagement bestehen aber unverändert fort – das Szenario 1 ist weiterhin als umsetzbar zu bewerten.

---

[21] Nicht-offizielle Quellen (z.B. http://de.wikipedia.org/wiki/Reisepass) lassen darauf schließen, dass das neue Schema für Seriennummern nur ausgewählte Buchstaben ergänzt, während sich bei der Behördenkennzahl zwar das Vergabeschema, nicht jedoch die Entropie erhöht. Sollten diese Aussagen stimmen, erreicht die Entropie des Seed für die Berechnung des BAC-Schlüssels nach wie vor nicht die vom Bundesamt für Sicherheit in der Informationstechnik in den IT-Grundschutz-Katalogen 2006 (M2.164, siehe http://www.bsi.de/gshb/deutsch/m/m02164.htm) empfohlenen 100 Bit für symmetrische Schlüssel.

Erhebliche Probleme bestehen offenbar nach wie vor mit der Sicherheitskonzeption über alle Lebenszyklen des ePasses. Dies hat eine Überprüfung der Datensicherheits- und Datenschutzkonzeption in Meldebehörden durch Landesdatenschutzbeauftragte u.a. in Mecklenburg-Vorpommern, Thüringen und Sachsen Ende 2007 ergeben.[22]

Die Datenschutzrisiken haben sich erheblich vermehrt, da weitere biometrische Rohdaten auf dem RFID-Chip gespeichert werden. Während Angriffe durch Externe erschwert sind, stehen Innentätern mehr und sensiblere Daten zur Verfügung, da Fingerabdrucksysteme im Consumerbereich (z.B. integriert in Notebooks) wie im kommerziellen Bereich (z.B. Pay-by-Touch-Systeme[23]) zunehmend verbreitet werden. Ein ebenfalls kritischer Nebeneffekt könnte sich aus der Gewöhnung der Bürger an das Einlesen von Fingerabdrücken an Lesegeräten ergeben: Viele werden nicht unterscheiden, ob sie ihren Fingerabdruck in einer deutschen Meldebehörde, im Supermarkt zum Bezahlen oder im Fitnessstudio zur Einlasskontrolle abgeben, und in all diesen Fällen können die Betroffenen üblicherweise den Grad der Sicherheit von Lesegeräten und den restlichen biometrischen Verfahrens nicht einschätzen.

Insgesamt stehen einigen Verbesserungen der Sicherheit (und damit in Teilbereichen gesunkenen Sicherheitsrisiken) erheblich gestiegenen Datenschutzrisiken gegenüber.

4 Zusammenfassung und Empfehlungen

Zusammenfassend ergibt sich, dass vor allem Risiken für den Datenschutz und die Datensicherheit durch Innentäter bestehen, gleichzeitig aber über die umgesetzten Sicherheitsmaßnahmen wenig bekannt geworden ist. Auch die analysierten Szenarien des Verfolgens und Anhörens können in Einzelfällen bei geeigneter Motivationslage und verfügbaren Ressourcen Relevanz haben. Offenbar existiert keine ganzheitliche Sicherheitskonzeption, die alle beteiligten Stellen (auch international), alle technischen Komponenten sowie alle Lebenszyklen abdeckt. Dies ist aber nach aktuellen Normen für die Informationssicherheit, wie z.B. ISO 27001 oder IT-Grundschutz, eine Grundvoraussetzung für das Erreichen eines angemessenen und verlässlichen Sicherheitsniveaus.

In diesem Umfeld muss man darauf hinweisen, dass angesichts unterschiedlicher, möglicherweise widersprüchlicher Sicherheitsziele (z.B. Sicherheit reisender Bürger, innere Sicherheit von Staaten, effiziente Terrorabwehr etc.) und der Souveränität von Staaten derartige Anforderungen im internationalen Kontext bezogen auf den ePass nicht einfach umsetzbar sind. Besinnt man sich jedoch auf den ursprünglichen Zweck von Pässen, nämlich den eigenen Bürgern sicheres Reisen im Ausland zu ermöglichen und ihnen dort – soweit unter Berücksichtigung der Souveränität des Gastlandes möglich – Schutz zukommen zu lassen, so ergibt sich dafür eine gewisse Priorisierung bei

[22] Siehe z.B. http://www.taz.de/1/politik/deutschland/artikel/1/gravierende-maengel-bei-passstellen/?src=SZ&cHash=a3748b1db4 und http://www.lfd.m-v.de/dschutz/presse/pm-epass.pdf
[23] Siehe z.B. http://www.pcwelt.de/start/sicherheit/archiv/131377/

möglicherweise konkurrierenden Sicherheitszielen. Die folgenden Empfehlungen wurden auf Basis dieser Priorisierung formuliert.

Der ePass ist eingeführt und wird auch weiterhin Verwendung finden. Folgende Verbesserungen sind für die kurzfristige Umsetzung zu empfehlen[24]:

1. Die Risiken, die sich aus dem Angriffszenario 1 ergeben, können durch Einsatz geeigneter Schutzhüllen minimiert werden. Je nach eingesetzten Materialien können sich die Schutzhüllen jedoch hinsichtlich ihrer Abschirmwirkung bei der relevanten Frequenz von 13,56 MHz und ihrer mechanischen Robustheit unterscheiden. In den USA sind abschirmende Materialien standardmäßig in die Buchdeckel des Reisepasses integriert.[25] Bislang bieten nur wenige Meldebehörden den Bürgern Schutzhüllen zum Kauf an.[26] In jedem Falle sinkt beim Einsatz solcher Schutzhüllen die Entfernung, aus der der RFID-Chip im Reisepass ausgelesen werden kann.

2. Die Risiken, die sich aus dem Angriffsszenario 2 ergeben, können durch Schirmung von Lesegeräten (z.B. durch konstruktive Maßnahmen an den Lesegeräten und geeignete Aufstellung in geschirmten Kontrollpunkten) und organisatorische Maßnahmen (wie z.B. Abstand Wartender an Kontrollpunkten) wirksam minimiert werden. Während der Abstand Wartender in zahlreichen Ländern auf Flughäfen üblicherweise realisiert ist, fällt die Umsetzung der übrigen Maßnahmen unterschiedlich aus. ePass-Lesegeräte sind auch in Deutschland bislang nur teilweise geschirmt.[27]

3. Der Passinhaber sollte den ePass nur dann mitführen und benutzen, wenn dies unbedingt erforderlich ist. Ansonsten sollte er sicher verwahrt werden.

4. Passinhaber sollten vor Antritt einer Reise ins Ausland den Zeitstempel beim Auslesen an einem vertrauenswürdigen Lesegerät z.B. in einer Meldebehörde oder am Flughafen aktualisieren.

5. Unter keinen Umständen sollte bei den bestehenden Datenschutz- und Sicherheitsrisiken die heutige ePass-Technologie auf den Personalausweis übertragen werden – dies ist jedoch vom Bundesministerium des Innern (BMI) geplant [En06]. Die bestehenden Risiken durch Innentäter sind bei dem gewählten Kontrollmodell (Zahl der beteiligten Organisationen und Mitarbeiter mit Zugriff auf die sensiblen Daten) kaum lösbar. Innerhalb der 189 ICAO-Mitgliedsstaaten erscheint eine einheitliche Sicherheitskonzeption auf einem

---

[24] Siehe hierzu auch die Budapest-Erklärung (http://www.fidis.net/press-events/press-releases/) und [KM+07]
[25] Siehe z.B. http://www.perfectcash.de/?id=1266&m=88
[26] Z.B. die Hansestadt Lübeck, siehe https://www.datenschutzzentrum.de/presse/20071031-epass-schutzhuelle.htm
[27] Siehe Bilder von Lesegeräten von der Bundesdruckerei (http://www.bitkom.org/files/documents/BDR_Praesentation_Workshop_ePass.pdf) und dem BMI (http://www.bmi.bund.de/nn_122688/Internet/Content/Common/Bilder/Themen/PaesseUndAusweise/epass__leser.html)

angemessenen Niveau, die Berücksichtigung von Datenschutzaspekten, gegenseitige Auditierung und Durchsetzung der Sicherheitsmaßnahmen auf Basis der gegenwärtigen Technik unwahrscheinlich.
Die Gestaltung von elektronischen Personalausweisen ist besonders wegen der geplanten europäischen Standardisierung der „European Citizen Card (ECC)" interessant.[28] Deutschland und Frankreich treiben diese Standardisierung zurzeit voran. Bislang orientieren sich die Konzepte am ICAO-Standard und verlangen beispielsweise nicht EAC für alle sensibleren Daten. Dies betrifft insbesondere die biometrisch optimierten Gesichtsbilder, die bei den Personalausweisen durchaus den Genuss einer erhöhten Absicherung genießen sollten. Im Vergleich zu den 189 ICAO-Staaten wäre eine Einführung eines aus Datenschutz- und Datensicherheitssicht verbesserten elektronischen Personalausweises für die europäischen Mitgliedsstaaten auf jeden Fall einfacher. Es ist nicht unrealistisch, davon auszugehen, dass sich Sicherheitsmaßnahmen, z.B. in Bezug auf Lesegeräte, im europäisch harmonisierten Rahmen durchsetzen ließen. Schließlich wäre ein Erfolg in diesem Anwendungsfeld auch einer Verbesserung des ICAO-Standards dienlich, so dass die nächste ePass-Generation hoffentlich weniger Kinderkrankheiten aufweist.

Für die nachfolgende Stufe des ePasses sollten vermehrt Datenschutzexperten hinzugezogen werden. Dabei sollten die Entwicklung und der Einsatz eines anderen Technikkonzeptes geprüft werden, das die Anforderungen an eine biometrisch gestützte Authentisierung erfüllt, nicht jedoch die Risiken der heutigen Technik beinhaltet. Hierbei kann z.B. an gekapselte Biometrie gedacht werden, bei der sich Sensor, Referenzdaten und Matching-Algorithmus auf einem Gerät unter Kontrolle des Passinhabers befinden. Ein Auslesen biometrischer Referenzdaten aus diesen Systemen ist nicht vorgesehen. Das Konzept der gekapselten Biometrie wurde bereits realisiert.[29]

Auch sollte geprüft werden, ob nicht auf RFID-Technik zur Vermeidung der Risiken des Trackens und Abhörens grundsätzlich verzichtet werden kann. Weitere Verbesserungen lassen sich durch Einführung eines Managements der Lebenszyklen der eingesetzten Technik erreichen. Dies kann dann auch dazu führen, dass die Dauer der Gültigkeit zukünftiger ePässe gegenüber den heute in der Bundesrepublik üblichen 10 Jahren erheblich reduziert wird. In diesem Falle würde ein wesentlicher Grund für den Einsatz der kontaktlosen Übertragungstechnik – der mechanische Verschleiß kontaktgebundener Medien – weniger bedeutend oder entfiele sogar.

[28] Es handelt sich hierbei um CEN TC 224 WG 15 prTS 15480, siehe G. Meister: Standardised authentication protocols based on smart cards – Application context German e-ID card, The European Identity Conference, eema, 13 June 2007, Paris, France,
http://www.enisa.europa.eu/doc/pdf/Workshop/June2007/Presentations/AUTH_Gisela_Meister.pdf
[29] Siehe z.B. http://www.axsionics.ch/tce/frame/main/410.htm

Literaturverzeichnis

[BG05] Beel, J.; Gipp, B.: ePass – der neue biometrische Reisepass. Shaker Verlag, Aachen 2005. Kap. 6 „Fazit“ ist verfügbar unter: http://www.beel.org/epass/epasskapitel6-fazit.pdf

[BSI05] Bundesamt für Sicherheit in der Informationstechnik (BSI): Digitale Sicherheitsmerkmale im elektronischen Reisepass. Bonn 2005. Download http://www.bsi.de/fachthem/epass/Sicherheitsmerkmale.pdf

[BSI07] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC). Version 1.10, Bonn, September 2007. Download: http://www.bsi.de/fachthem/epass/EACTR03110_v110.pdf

[Co03] Cole, S. A.: Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate. University of California, Irvine, 2003. Download: http://www.ksg.harvard.edu/dnabook/

[En06] Engel, C.: Auf dem Weg zum elektronischen Personalausweis. Datenschutz und Datensicherheit 4/2006, S. 207-210, Vieweg Verlag, Wiesbaden 2006.

[KM08] Kindt, E.; Müller, L. (Hrsg.): FIDIS Deliverable D3.10: Biometrics in Identity Management. Frankfurt a.M., im Erscheinen, 2008; S. 83-87.

[KN07] Kügler, D.; Naumann, I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. Datenschutz und Datensicherheit, 3/2006, Wiesbaden 2007; S. 176-180. Download http://www.bsi.de/fachthem/epass/dud_03_2007_kuegler_naumann.pdf

[KM+07] Kosta, E.; Meints, M.; Hansen, M.; Gasson, M.: An analysis of security and privacy issues relating to RFID enabled ePassports. In (Venter, H.; Eloff, M.; Labuschagne, L.; Eloff, J.; von Solms, R., Hrsg.): New Approaches for Security, Privacy and Trust in Complex Environments, Proc. of the IFIP SEC2007, New York 2007.

[LK+07] Liu, Y.; Kasper, T.; Lembke-Rust, K.; Paar, C.: E-Passport: Cracking Basic Access Control Keys with COPACOBANA. Bochum 2007. Download: http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/epasscrack_sharcs_2007.pdf

[Me07] Meints, M.: Implementierung großer biometrischer Systeme. Datenschutz und Datensicherheit 3/2007, Wiesbaden 2007; S. 189-193. Download: http://www.fidis.net/fileadmin/fidis/publications/2007/DuD3_2007_189.pdf

[MH06] Meints, M.; Hansen, M. (Hrsg.): FIDIS Deliverable D3.6 – Study on ID Documents. Frankfurt a.M. 2006; S. 10. Download: http://www.fidis.net/resources/deliverables/hightechid/#c1783

[Ro06] Robroch, H.: ePassport Privacy Attack. 2006. Download: http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf.

[VGr06] von Graevenitz, G.: Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren. LIT Verlage, Berlin 2006.