DuD
Datenschutz und Datensicherheit

Implementierung großer biometrischer Systeme[1]

Kriterien und deren Anwendung am Beispiel des ePasses

Martin Meints

Welche Kriterien müssen biometrische System mit zahlreichen Nutzern erfüllen? Im vorliegenden Beitrag werden wesentliche Kriterien aus internationalen Standards und „Good-Practice" Vorgehensmodellen hergeleitet. Diese Kriterien werden auf den ePass angewandt und Vorschläge für die Weiterentwicklung von Technik- und Sicherheitskonzept vorgestellt.

Dr. Martin Meints

Dr. Meints ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz und arbeitet dort vor allem im EU-Projekt FIDIS.

E-Mail: LD102@datenschutzzentrum.de

1 Einleitung

Biometrische Systeme stützen sich weitgehend auf elektronische Komponenten und Software, so dass sie als IT-Systeme klassifiziert werden können. In diesem Beitrag werden aus internationalen Standards zur IT-Sicherheit wie ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 17799 ('Code of Practice' der British Standards) und ISO/IEC 15408 (Common Criteria) wesentliche IT-Sicherheits- und Qualitätskriterien für biometrische Systeme entwickelt. Dabei wird insbesondere dargestellt, worin die Herausforderungen bei großen Systemen mit vielen erfassten Nutzern liegen.

Neben den ausführlich dargestellten IT-Sicherheitskriterien sind jedoch weitere, vor allem rechtliche, Aspekte zu berücksichtigen. Auf die aus Sicht des Autors wesentlichsten Kriterien wird im folgenden Kapitel hingewiesen.

Die dargestellten Kriterien werden dann auf eines der größten existierenden biometrischen Systeme angewandt: den ePass und die zugehörige, weltweite Authentisierungsinfrastruktur. Aus den erzielten Ergebnissen werden mögliche Handlungsoptionen zur Verbesserung des derzeitigen Technik- und IT-Sicherheitskonzeptes bezogen auf die Biometrie hergeleitet.

2 Kriterien der IT-Sicherheit

2.1 Aufbau eines ISMS

Bei Verfahren kann zur Erreichung kontrollierter Sicherheit ein Information Security Management Systems (ISMS) betrieben werden, in das alle beteiligten Betreiber und Nutzer des Systems eingebunden sind. Zu den Strukturen eines ISMS gehören:

- Aufbau einer geeigneten organisatorischen Struktur
- Aufbau eines IT-Sicherheitsprozesses u.a. mit IT-Sicherheitsvorfallmanagement und Notfallvorsorge
- Abstimmung der Schnittstellen zu anderen (Teil-)Betreibern des Systems über geeignete SSLAs und Auditschemata

Im Zuge des Aufbaus des ISMS sind Regelungen und Sicherheitsinformationen bzw. Schulungen für die Administratoren, die Bediener, aber auch die Teilnehmer (Nutzer und zu authentisierende Personen) am biometrischen System erforderlich.

Grundlage für die Wirksamkeit eines ISMS ist ein geeignetes Kontrollmodell (s. Gateway in diesem Heft):

- Kontrolle durch den Besitzer und gleichzeitig einzigen Nutzer des Systems
- Zentrale Kontrolle bei Einsatz eines Systems in einer Organisation
- Verteilte Kontrolle mit auf Vertrauen basierender, standardisierter Sicherheit bei mehreren Betreibern
- Verteilte Kontrolle mit mehrseitiger Sicherheit

Für große biometrische Systeme mit zahlreichen Nutzern ist vor allem das dritte Modell verteilter Kontrolle mit auf Vertrauen basierender, standardisierter Sicherheit relevant.[2]

2.1 Technik-, Sicherheits- und Betriebskonzept

Notwendig sind ein aufeinander abgestimmtes Technik- und IT-Sicherheitskonzept (u.a. nach §9 BDSG). Grundlage dafür sollte eine umfassende Anforderungsanalyse sein. Weitere wesentliche Teilkonzepte sowie

[1] Wesentliche Teile dieser Arbeit sind mit Mitteln der Europäischen Union im Rahmen des „Projektes Future of Identity in the Information Society" (FIDIS, www.fidis.net) gefördert worden.

[2] Siehe Gateway in diesem Heft

eine Good-Practice-Beschreibung des Vorgehens bei IT-Projekten findet sich im V-Modell XT[3], das seit 4.11.2004 für Bundesbehörden verbindlich ist.

Das IT-Sicherheitskonzept muss technische und organisatorische Aspekte über alle Phasen des Lebenszyklus aller Komponenten des biometrischen Systems betrachten. Wichtige Elemente sind eine umfassende Risikoanalyse, die alle relevanten Aspekte aus Sicht aller Beteiligten (Betreiber, Dienstleister, Teilnehmer etc.), geeignete Maßnahmen zur Reduzierung, Vermeidung und Verlagerung von Risiken und eine Abschätzung verbleibender, zu tragender Restrisiken beinhaltet. Beim Einsatz kombinierter Technologien sind Risiken, die sich aus deren Kombination ergeben können, gesondert zu betrachten.[4]

Bei großen Systemen bewährt sich ein Technikkonzept, das bereits auf etablierte Lösungen und Standards für vergleichbare Anwendungsbereiche zurückgreift. In Fällen, wo dies nicht möglich ist, müssen Sicherheitstests besonders sorgfältig unter Labor- und realen Einsatzbedingungen, auch in Massentests, durchgeführt werden. Nach Abschluss der jeweiligen Testphasen müssen Sicherheits- und Technikkonzept unter Berücksichtigung der Testergebnisse überarbeitet werden (Co-Evolution der Konzepte).

Da derartige Systeme oft für einen langen Zeitraum eingesetzt werden sollen, ist die Wartbarkeit von technischen Komponenten ein wichtiger Faktor. Hierzu gehört unter Sicherheits-, aber auch Qualitätsgesichtspunkten ein geeignetes Patch-, Update- und Upgrademanagement.

Schließlich wird für die Operatoren und Administratoren des Systems ein Betriebskonzept benötigt. Es beinhaltet neben technischen Hintergrundinformationen auch operative Handlungsanweisungen für den effektiven Umgang mit dem System.

Gerade bei großen und komplexen Systemen hat sich ein Peer-Review der Konzepte durch unabhängige, externe Experten bewährt. Die fertig gestellten Konzepte sind freizugeben, ihre Implementierung ist zu dokumentieren und abzunehmen.

[3] Siehe http://www.kbst.bund.de/nn_836802/Content/Standards/V__Modell/vmodell__node.html__nnn=true

[4] Skalierungseffekte bei großen biometrischen Systemen wurden bereits im Beitrag „Ein biometrisches Bezahlsystem für Kaufhäuser“ in diesem Heft behandelt.

3 Rechtliche Kriterien

Bei den rechtlichen Kriterien spielt in Europa in jedem Fall das Datenschutzrecht eine bedeutende Rolle. Die entsprechenden Kriterien und Empfehlungen der Art. 29-Arbeitsgruppe sind bereits an anderer Stelle zusammengefasst worden.[5]

Je nach Umfeld und Anwendungszweck des biometrischen Systems sind weitere, oft sehr spezifische Rechtsgrundlagen zu beachten. In dem Fall, dass der Staat das biometrische System betreibt, muss er diese zusammen mit dem Parlament schaffen. Eine Auflistung soll an dieser Stelle nicht erfolgen. In jedem Fall ist die Beachtung der jeweiligen rechtlichen Kriterien in die bereits erwähnte Anforderungsanalyse aufzunehmen.

4 Anwendung auf den ePass

Der Europäische ePass basiert auf den technischen Standards und Vorgaben, die seit 2004 von der International Civil Aviation Organisation (ICAO)[6] für internationale maschinenlesbare Reisedokumente erstellt und verabschiedet worden sind. Sie sind in einer neuen Version des Dokuments 9303[7] zusammengefasst und später auch von der International Standardization Organisation (ISO)[8] als ISO/IEC 7501 normiert worden. Diese Standards sind für die 189 Mitgliedsstaaten der ICAO verbindlich.
Mit der Verordnung 2004/2252/EU[9] wurden jedoch die technischen Anforderungen gegenüber dem Dokument 9303 um gegenüber Basic Access Control (BAC) verbesserten Zugriffsschutz (u.a. Extended Access Control, EAC) erweitert. Für Europa werden Gesichtserkennung und Fingerabdrücke als biometrische Merkmale festgelegt.

Mit der Einführung elektronischer Komponenten wie dem RFID-Chip und darauf gespeicherten biometrischen Merkmalen wird der ePass zum Bestandteil zahlreicher, verteilter Authentisierungssysteme und der ePassinhaber deren Nutzer. Damit sind die vorgestellten Kriterien grundsätzlich auf den ePass anwendbar.

Das Technikkonzept des Passes ist weitgehend bekannt. Für den Einsatz von Biometrie stehen die folgenden Datenformate zur Verfügung (HeWa05):
Gesichtserkennung: ISO/IEC 19794-5
Fingerabdrücke: ISO/IEC 19794-4
Diese Formate sind digitale Bilddateien, die in festgelegter Auflösung, Farbpalette und Kompression in einem festgelegten Format (JPEG 2000) gespeichert werden. Für die Gesichtsbilder gibt es darüber hinaus detaillierte Vorgaben für die Kopfhaltung, den Bildausschnitt, mögliche Bekleidung etc.

Bei den Fingerabdrücken soll – offenbar aus Interoperabilitätsgründen[10] – auf die von der ICAO ebenfalls vorgeschlagenen Minutienformate verzichtet werden.[11] Somit werden durchgängig biometrische Rohdaten eingesetzt bzw. sollen eingesetzt werden. Da diese zur Authentisierung nicht benötigte, jedoch in vielen Fällen gesundheitsbezogene Informationen enthalten (u.a. VGr06, Col03), sind sie besonders schützenswert. Das IT-Sicherheitskonzept sollte dem durch besonders wirksame Maßnahmen gemäß der Anlage zu §9 Satz 1 BDSG Rechnung tragen.

Die biometrischen Daten werden auf einem RFID-Chip gespeichert, der mit einem Zugriffschutz (Basic Access Control, BAC) versehen ist. Als Weiterentwicklung mit deutlich verbessertem Konzept ist Extended Access Control (EAC) vorgesehen) vorgesehen.[12]

4.1 Qualitätsaspekte

Die Implementierung der Biometrie für den ePass ist unzureichend getestet worden. In der Bundesrepublik ist nur ein Test mit ca. 2.000 Teilnehmern öffentlich bekannt gewordenen, und zwar im Rahmen der BSI-Studie BioPII am Frankfurter Flughafen.[13] Die gewählte Methodik der Studie wurde insbesondere im Hinblick auf die Zahl und Auswahl der Teilnehmer bereits deutlich

[5] Siehe Beitrag „Biometric applications and the data protection legislation“ in diesem Heft.

[6] http://www.icao.int

[7] Hintergründe und Bestellmöglichkeiten für das Dokument 9303 finden sich unter http://mrtd.icao.int

[8] http://www.iso.org

[9] Siehe http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf

[10] Siehe Beitrag „Ähnlichkeitseigenschaften von Minutiendatensätzen zur Beurteilung von Interoperabilität“ in diesem Heft.

[11] Siehe http://www.interoptest-berlin.de/pdf/Carter_Munde_-_Brussels_Interoperability_Group.pdf

[12] Siehe auch Beitrag „Kontaktlose Chips im deutschen Reisepass – ein Überblick über Sicherheits-merkmale, Risiken und Gegenmaßnahmen“ in diesem Heft.

[13] Der Abschlussbericht ist über http://www.bsi.de/literat/studien/biop/biop_2.htm verfügbar.

kritisiert (KrKu05). Im Übrigen standen beim ePass eher Interoperabilitäts- gegenüber Sicherheitstests im Vordergrund.[14] Mit den intensiven Massentests (bis zu je 10.000 und 100.000 Teilnehmer in acht Testregionen), die bei der Gesundheitskarte bereits durchgeführt werden bzw. noch vorgesehen sind, kann sich der Test der Biometrie für den ePass europaweit auch unter Berücksichtigung anderer Studien (hier ist insbesondere BZK05 zu nennen) nicht messen. Insbesondere sind keine Labortests zur Überprüfung des Sicherheitskonzeptes, so genannte Hackertests, bekannt geworden.

Die Studie BioPII lässt erkennen, dass die Kompression der biometrischen Rohdaten die Qualität der Erkennung gegenüber unkomprimierten Rohdaten in fast allen Fällen verschlechtert. Bei einer Fehlakzeptanzrate (FAR) von 0,01% wurde eine Fehlzurückweisungsrate (FRR) von bis zu 3% beobachtet. Bei der niederländischen Studie (BZK05) traten beim Fingerabdruck Enrolmentfehler (Failure to Enrol, FTE) auf. Organisatorische Maßnahmen hat es nach Abschluss der Studien nicht gegeben, obwohl dies bezogen auf die ERR gefordert worden und auch sinnvoll ist (BZK05).

Bei der Einführung des ePasses 2005 gab es in zahlreichen europäischen Ländern, darunter auch in Deutschland, Probleme mit der Einhaltung der ISO-Norm bei den digitalen Passbildern. So sind Passbilder elektronisch erfasst worden, die teilweise nicht den Normen entsprachen. Die Meldebehörden haben sich in einigen Fällen rechtlich gegenüber den Antragstellern mit der so genannten Lichtbilderklärung abgesichert.[15] Die Probleme mit der Qualität der digitalen Passbilder sind offenbar nach wie vor nicht komplett ausgeräumt.[16] Welche Auswirkungen dies auf die Fehlerquote bei der biometrische Identifizierung hat, ist bislang offenbar noch nicht systematisch untersucht worden.

Das Technikkonzept des ePasses ist auf eine lange Lebensdauer ausgelegt. ePässe sind in der Bundesrepublik 10 Jahre gültig. Leider sind weder Hard- noch Softwarekomponenten des ePasses wartbar, Updates können nicht eingespielt werden. Für den regelmäßigen Austausch, etwa jedes halbe Jahr, ist die gewählte ePasstechnik deutlich zu teuer. Technik- oder Sicherheitslücken können so nicht rasch beseitigt werden und gefährden die Sicherheit des Bürgers für die Gültigkeitsdauer des Dokumentes.

4.2 Datenschutzaspekte

Den Empfehlungen der Art. 29-Arbeitsgruppe zur Implementierung von Biometrie wurde weitgehend nicht gefolgt:

- Es werden keine Templates gespeichert, sondern biometrische Rohdaten. Die Art der Herstellung und Qualität des digitalen Passbildes für den ePass unterscheidet sich grundsätzlich von bisherigen Passbildern oder privaten Schnappschüssen – diese Bilder sind auf maschinelle Auswertbarkeit hin optimiert. Bei digitalen Gesichtsbildern wurden bereits erfolgreich Versuche unternommen, ergänzenden Informationen automatisiert auszuwerten (VGr06).
- Biometrische Daten werden zusammen mit anderen persönlichen Informationen gespeichert.
- Passinhaber habe keine freie Wahl, auf Biometrie verzichten zu können; sie können lediglich auf den Pass und damit die Möglichkeit, international zu reisen, verzichten.
- Die biometrischen Merkmale können bei der bestehenden Implementierung der ePässe nicht widerrufen werden. Bei Verlust oder Diebstahl des ePasses bleiben sie gültig, ein neuer ePass nutzt die gleichen, möglicherweise unveränderten Rohdaten (z.B. bei Verwendung des gleichen Fotos als Vorlage) wie der ursprüngliche Pass.
- Die EU-Kommission hat beschlossen, (noch) kein zentrales Register in Ergänzung zur dezentralen Speicherung auf dem ePass für biometrische Daten aufzubauen. In anderen Ländern wird dies jedoch praktiziert, auch für Reisende aus europäischen Ländern. Ein Beispiel hierfür sind die USA.[17] Der Verzicht auf eine zentrale Speicherung ist also aus Sicht des Bürgers nicht effektiv durchgesetzt.
- Die Richtlinie 2004/2252/EU legt fest, dass die erhobenen biometrischen Daten nur für den Zweck der Identifizierung bei internationalen Reisen verwendet werden dürfen. Doch auch in diesem Falle ist die Zweckbindung nicht effektiv durchgesetzt – außereuropäische Länder sind im Bezug auf die Nutzung biometrischer Daten aus europäischen ePässen völkerrechtlich nicht zur Einhaltung der im Ausgabeland geregelten Zweckbindung verpflichtet. Technisch kann eine Zweckbindung mit heutigen Mitteln nicht zuverlässig durchgesetzt werden (s. verschiedene gescheiterte Ansätze zum Digital Rights Management, DRM).
- Für den Fall des technisch bedingten Versagens der Biometrie (FRR, FTE) wurden keine alternativen Vorgehensweisen oder Identifizierungsverfahren festgelegt. Reisende werden den möglicherweise nicht nachvollziehbaren Entscheidungen und Verfahrensweisen der Grenzbeamten des jeweiligen Einreiselandes ausgeliefert sein. Bei bis zu 3% FRR kann dies in einer Boeing 747 mit ca. 700 Passagieren 21 Reisende betreffen. Eine Information der ePassinhaber, wie in diesem Falle vorzugehen ist, hat es seitens des Bundesinnenministeriums und der Meldebehörden bislang nicht gegeben.

4.3 Sicherheitsaspekte

Bei der Umsetzung des Sicherheitskonzeptes ist wie bereits erwähnt die Kontrolle über das System und das Verhalten der Nutzer ein wesentlicher Aspekt. Schaut man sich die Kontrolle bezogen auf das ePass-gestützte Identifizierungssystem, den ePass und die darauf gespeicherten Daten an, so ist sie breit gestreut. Zusätzlich zu den 189 ICAO-Mitgliedsstaaten, also deren Grenzbeamten und den Passbehörden mit ihren Mitarbeitern, liegt die Kontrolle auch bei den Passinhabern und möglicherweise Dritten aus der Privatwirtschaft. In zahlreichen Ländern (z.B. Italien, Slowakei, Tschechien etc.) muss der Pass bei der Übernachtung in dem Hotel abgegeben werden und kann dort bis zu acht Stunden einbehalten werden. Da wesentliche Informationen für die Berechnung des Schlüssels von BAC der Maschinenlesbaren Zone

[14] Siehe http://www.heise.de/ct/hintergrund/meldung/73803.
Im Jahr 2006 zogen andere Länder wie Australien, die USA und Singapore mit eigenen Tests unter realen Einsatzbedingungen nach. Die Ergebnisse, die mit ebenfalls ca. 2000 Teilnehmern erzielt wurden, sind als „erfolgreich“ bezeichnet worden (s. http://www.biometricinsight.com/files/BiometricInsight_June06.pdf). Sie sind aber u.a. wegen der Unterschiede bei der biometrischen Merkmalsausprägung der Teilnehmer nicht unbedingt auf Europa übertragbar.

[15] Siehe http://www.heise.de/newsticker/meldung/65858

[16] Siehe http://www.heise.de/newsticker/newsticker/meldung/83033

[17] Siehe z.B. http://de.wikipedia.org/wiki/Biometrie

(MRZ)[18] entnommen werden, ist ein effektives Schlüsselmanagement für BAC nicht mehr gegeben (MeHa06).[19]

Darüber hinaus ist technisch nicht sichergestellt, dass beim berechtigten oder unberechtigten Auslesen des ePasses personenbezogene Daten und biometrische Rohdaten nicht für andere Zwecke verwendet werden. Weder das ePass-ausstellende Land, noch der ePassinhaber haben eine Kontrolle über die jeweiligen Lese- und Verifikationssysteme in anderen Ländern.

Insgesamt muss man zu dem Schluss kommen, dass hier mehrseitige Sicherheitsanforderungen bestehen, die jedoch nicht erfüllt werden. Staatliche Sicherheitsinteressen können u.U. erheblich von den Sicherheitsinteressen der ePassinhaber abweichen. Ein Ausgleich der Sicherheitsinteressen findet nicht ausreichend statt, die Staaten oder Dritte setzen in jedem Falle ohne Aushandlung ihre Sicherheitsinteressen durch.

Ein integriertes IT-Sicherheitskonzept für den ePass ist bisher nicht bekannt geworden. Dies mag aus Gründen der Geheimhaltung nachvollziehbar sein. Es gibt jedoch zahlreiche Indizien dafür, dass das vorhandene Sicherheitskonzept zumindest lückenhaft ist:

- Es wurden bereits gravierende kryptografische Schwächen bei BAC festgestellt (BeGi05). EAC kann dies aus Gründen der Abwärtskompatibilität zu BAC und mangels internationaler Standardisierung nur teilweise verbessern (MeHa06). Der RFID-Chip konnte bereits aus 50 cm Entfernung erfolgreich ausgelesen werden, eine weitere Steigerung der Ausleseentfernung scheint technisch möglich.[20] Ein Faraday'scher Käfig wird bei Europäischen ePässen standardmäßig nicht eingesetzt (MeHa06). Insgesamt bietet BAC keinen wirksamen Mechanismus der Zugriffskontrolle, mindestens nicht für die Gesichtsbilder und weitere Basisdaten, die auf dem RFID-Chip des ePasses gespeichert sind.
- Der RFID-Chip im Pass konnte bereits kopiert (geclont) werden.
- Organisatorische Komponenten des Sicherheitskonzeptes sind bislang nur lückenhaft bekannt geworden, öffentliche Informationen decken vor allem technische Aspekte der IT-Sicherheit ab (MeHa06). Weder gibt es Sicherheitshinweise für die ePass-Inhaber bei der Aushändigung, noch verfügen Meldebehörden über weiterführende Informationen.
- Das Konzept scheint nicht alle Phasen des Lebenszyklus eines ePasses zu umfassen. So sind Sicherheitslücken bei der Ausstellung bekannt geworden. Es ist einer Reporterin der BBC gelungen, auf dem Schwarzmarkt ePässe aus 14 europäischen Ländern mit ihrem digitalen Passbild zu kaufen. Diese sind offenbar von den nationalen Passbehörden, auch in Deutschland, als reguläre Pässe für andere, ähnlich sehende Personen, allerdings mit falschem Passbild, ausgestellt worden.[21]

Seitens der Sicherheitsbehörden in der Bundesrepublik wurde auf diese Sicherheitslücken in der Vergangenheit meist abwiegelnd reagiert (z.B. Pro06).

5 Mögliche Folgen für die Zukunft

Es ist davon auszugehen, dass all diese Regelungs- und Sicherheitslücken bezogen auf biometrische Merkmale kurzfristig nur geringe Auswirkungen haben. Dies gilt zumindest, solange biometrie-gestützte Authentisierung beim Grenzübertritt noch nicht genutzt wird.

Bezogen auf die biometrischen Rohdaten bleibt das Missbrauchspotential über die ergänzenden Informationen. Missbräuche wird der ePassinhaber jedoch nicht oder nur zeitverzögert bemerken, da er den Datenfluss nicht beobachten und kontrollieren kann. Und der Missbrauch treibende „Nutzer“ der biometrischen Daten wird Interesse daran haben, diesen möglichst lange geheim zu halten.

Das Spoofen biometrischer Sensoren anderer Systeme mit „gestohlenen“ ePassdaten wird dann zu einem potenziellen Problem, wenn diese Systeme dieselben Merkmale in einer Einfaktor-Authentisierung verwenden, die Sensoren technisch gegen Spoofing anfällig und bei der Benutzung nicht überwacht sind. Besondere Bedeutung kommt dabei der Wirksamkeit von EAC zu, denn vielfach sind die genannten Anfälligkeiten gegenüber Spoofing vor allem bei existierenden Implementierungen von Fingerabdrucksystemen erfüllt.

Hinzu kommen noch die Risiken, die sich aus der RFID-Implementierung des ePasses, u.U. auch in Kombination mit der Biometrie ergeben, insbesondere Tracking.

Bedenklich sind vor diesem Hintergrund Pläne der Bundesregierung, das lückenhafte Technik- und Sicherheitskonzept des ePasses auf den Personalausweis zu übertragen (Eng06). Dementiert worden ist jedoch die Meldung, im Rahmen der Novelle des Personalausweisgesetzes sei es geplant, die biometrischen ePass-Daten kostenpflichtig der Wirtschaft für Authentisierungszwecke zur Verfügung zu stellen[22]

6 Empfehlungen

Der ePass ist technisch eingeführt und international normiert – eine kurzfristige Ablösung der derzeitigen Technik ist daher realitätsfern. Kurzfristig sollten daher ergänzende organisatorische und technische IT-Sicherheitsmaßnahmen beim derzeitigen Technikkonzept umgesetzt werden. Diese können bei Behörden sein:

- Information der ePassinhaber über mögliche Risiken und vorbeugendes Verhalten, etwa den ePass gut geschützt nur dann bei sich zu tragen und zu verwenden, wenn dies unbedingt erforderlich ist.
- Empfehlung zum Einsatz eines Faraday'schen Käfigs (Alufolie oder metallbedampfte Plastiktüte), wenn der ePass transportiert oder gelagert werden soll. Dies verstärkt den Zugriffschutz und verringert das Risiko des unbefugten Auslesens und Trackens des ePassinhabers.
- Durch geeignete Schirmung von Lesegeräten an Grenzkontrollpunkten kann das unbefugte Abhören erschwert werden.
- Durch Erfassung und Test aller biometrischen Merkmale direkt bei den Meldeämtern kann die beschriebene Methode der Fälschung wirksam unterbunden werden.

[18] Siehe http://www.bsi.bund.de/fachthem/epass/Sicherheitsmerkmale.pdf

[19] In Belgien ist BAC erst in der zweiten e-Pass-Version, also seit Juli 2006, implementiert. In Schweden werden nach einer Auskunft der Polizei Värmland Passnummer und Ablaufdatum (und damit wesentliche Teile des BAC-Schlüssels) auf Anfrage auch Dritten mitgeteilt. Dies wurde Forschern der Karlstad Universität offiziell in einem Schreiben am 05.02.07 mitgeteilt.

[20] Siehe http://www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf

[21] Siehe http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm

[22] Siehe http://www.heise.de/newsticker/newsticker/meldung/74914

- Für den Umgang mit den bekannten Fehlern biometrischer Verfahren (FRR, FTE) sollten Standardprozeduren entwickelt, weltweit abgestimmt und bekannt gemacht werden. Im Entwurf des deutschen Passgesetzes ist eine Angabe zur Qualität der biometrischen Daten vorgesehen, die hierfür eine operative Grundlage schafft.[23]
- Die bestehenden Probleme bezüglich der Kontrolle über die IT-Systeme und die Missbrauchsrisiken für biometrische Daten lassen sich so jedoch nicht wirksam lösen bzw. beseitigen. Daher ist dringend zu raten, den RFID-Chip mit biometrischen Daten aus dem ePass nicht auf Personalausweise zu übertragen. Mittelfristig (d.h. innerhalb der nächsten drei Jahre) sollte ein neues Technikkonzept für den ePass entwickelt werden, das die beschriebenen Probleme löst.

Biometrie kann darin eine wichtige Rolle spielen, denn sie eignet sich besonders für die Bindung von Besitz (hier den Pass) an eine Person (hier den berechtigten Inhaber). Die Datenschutz- und Kontrollaspekte können durch Einsatz gekapselter Biometrie unter Verwendung geeigneter Templates konzeptionell gelöst werden. Bei gekapselter Biometrie befinden sich Sensor, Technik zur Verifikation und Referenzdaten auf einem Gerät unter Kontrolle des Nutzers. Dies wurde bereits technisch implementiert.[24]

Bei der Überarbeitung sollte darüber hinaus kritisch geprüft werden, in wieweit die RFID-Technik nicht verzichtbar ist.

7 Fazit

In diesem Beitrag wurde eine Reihe für die Sicherheit biometrischer Systeme aus Betreiber- und Nutzersicht relevanten Kriterien aus ISO-Normen und anderen „Good-Practice"-Vorgehensmodellen abgeleitet. Sie wurden auf den ePass und die zugehörigen biometriegestützten Authentisierungssysteme angewandt.

Die Einführung von Biometrie und RFID-Technik macht den ePass zur Komponente eines IT-Systems. Daraus folgt die Notwendigkeit, die Sicherheit des gesamten Systems unter Berücksichtigung anderer Faktoren zu konzipieren, als dies bei der Verwendung von traditionellen Papierdokumenten nötig war. Zugleich besteht auch die Notwendigkeit, Technik- und IT-Sicherheitskonzept international abzustimmen – allein dies ist eine enorme Herausforderung.

Unter diesen schwierigen Rahmenbedingungen ist mit dem ePass ein erstes, sehr großes und weltweit ausgerolltes biometriegestütztes Authentisierungssystem in sehr kurzer Zeit entstanden. Leider erfüllt es wesentliche der vorgestellten Sicherheitskriterien nicht und weist erhebliche konzeptionelle, organisatorische und technisch bedingte Sicherheitslücken auf.

Unter diesem Gesichtspunkt kann man nur die Empfehlung der Autoren der Budapest-Erklärung[25] bekräftigen, mittelfristig ein neues Technik- und IT-Sicherheitskonzept für den ePass zu entwickeln und international abzustimmen.

[23] Siehe Beitrag „Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht" in diesem Heft.

[24] Siehe auch Beitrag „Secure Identity Management mit Multifunktionstoken" in diesem Heft.

[25] Siehe http://www.fidis.net/press-events/press-releases/

Literatur

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

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.

Col03: Cole, S. A., ‚Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate', in Lazer, D., (Hrsg.), *The Technology of Justice: DNA and the Criminal Justice System*, University of California, Irvine 2003. Download via http://www.ksg.harvard.edu/dnabook/

Eng06: Engel, C., ‚Auf dem Weg zum elektronischen Personalausweis', DuD 4/2006, S. 207-210, Vieweg Verlag, Wiesbaden 2006.

HeWa05: Henniger, O., Waldmann, U., ‚ISO/IEC 19794 – Austauschformate für biometrische Daten', in Struif, B., (Hrsg.), *Tagungsband des 15. SIT-Smartcard-Workshops*, Darmstadt, 2005. Download: http://www.sit.fraunhofer.de/~henniger/HW05.pdf

KrKu05: Krissler, J, Kurz, C., ‚Die Ergebnisse der BioP2-Studie zur Leistungsfähigkeit biometrischer Sys-teme', *FIfF Kommunikation* (4) 2005, FIfF, Bremen 2005.

MeHa06: Meints, M., Hansen, M. (Hrsg.), *FIDIS Deliverable D3.6: Study on ID Documents*, Version 1.1, Frankfurt a. M. 2006. Download: http://www.fidis.net/fidis-del/period-2-20052006/#c1338

Pro06: Proll, U., ‚Startsignal ist erfolgt', *Behördenspiegel* Nr. 10, Sonderdruck, Berlin und Bonn, Oktober 2006.

vGr06: Von Graevenitz, G., Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren, LIT Verlage, Berlin 2006.