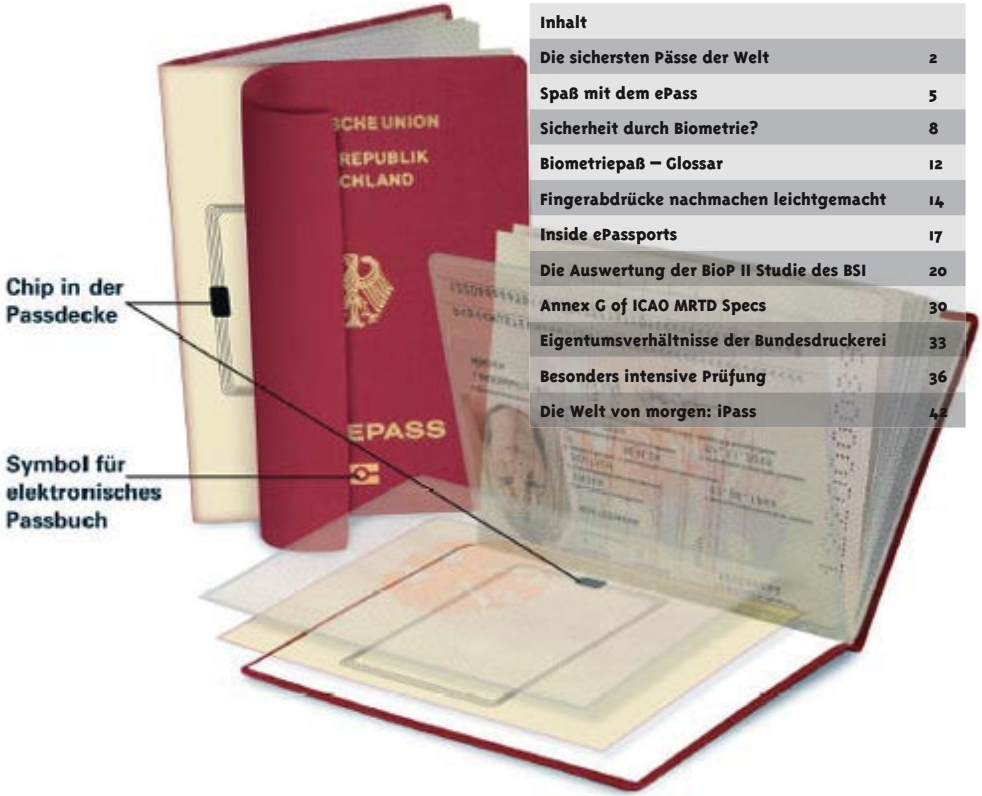
die datenschleuder. #87

ERFASSUNGS UNION

SCHNÜFFELREPUBLIK
DEUTSCHLAND

ÜBERWACHUNGS PASS

ISSN 0930-1054 • 2005 • 2,50 EUR
Postvertriebsstück C11301F



Bildquelle: http://www.bmi.bund.de/Internet/Content/Common/Bilder/Themen/Informationsgesellschaft/DatenundFakten/Biometrie__ePass,property=poster.jpg

Inhalt

Die Datenschleuder Nr. 87

Herausgeber (Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V., Lokstedter Weg 72, 20251 Hamburg, Fon: *+49.40.401801-0*, Fax: *+49.40.401801-41*, <*office@ccc.de*> Fingerprint*: 1211 3D03 873F 9245 8A71 98B9 FE78 B31D E515 E06F*

Redaktion (Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Pf 64 02 36, 10048 Berlin, Fon: +49.30.28097470, <*ds@ccc.de*> Fingerprint: *03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04*

Druck
Pinguindruck Berlin, *http://pinguindruck.de/*

ViSdP und Produktion
Tom Lazar, <*tom@tomster.org*>

Chefredaktion
Dirk Engling <erdgeist> und Tom Lazar <tomster>

Redaktion dieser Ausgabe
Zapf Dingbatz, Martin Haase, Constanze Kurz, Andreas Lehner, Frank Rosengart, starbug, Harald Welte.

Layout
erdgeist, Antenne Springborn, Constanze Kurz, Roland Kubica

die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Dieses Sonderheft der Datenschleuder ist dem neuen deutschen ePass gewidmet. Wir betrachten die technischen und politischen Details in großer Ausführlichkeit, die wir angesichts dieses ersten großen Schrittes hin zur Totalüberwachung der Bevölkerung für geboten halten.

Unter dem Deckmäntelchen der Terrorismusabwehr werden mit dem ePass gänzlich andere Ziele verfolgt. Mit genügender Terrorfurcht wurde die öffentliche Meinung so weichgekocht, daß alles, wo "Sicherheit" draufsteht, kritiklos hingenommen wird. Selbst die DDR-Staatssicherheit hatte sich nicht getraut, eine flächendeckende Erfassung der Fingerabdrücke ihrer Bevölkerung vorzunehmen. Das Innenministerium unseres demokratischen Rechtsstaats hat da weniger Skrupel.

Demokratie ist eine feine Sache - wenn sich denn die Regierenden daran halten. Die Entscheidung zur Totalerfassung wurde nicht demokratisch legitimiert. Über den Umweg ICAO und EU drückte das Innenministerium ein Verfahren durch, das im Deutschen Bundestag bei rationaler Diskussion kaum durchgekommen wäre. Eine sachliche Begründung zur Notwendigkeit fand selbst auf direkte Nachfrage von Abgeordneten nicht statt. Es gibt einfach keine guten Argumente dafür, nur sehr viele dagegen.

Der Überwachungsstaat ist nicht mehr nur ein Schreckgespenst der fernen Zukunft. Er steht direkt vor der Tür. Unsere Politiker haben eine Vision von einer Zukunft, die den dramatischen Ausbau von Repressions- und Überwachungsmöglichkeiten erfordert. Biometrie in allen Ausweisdokumenten ist nur ein Puzzlestein dabei. Der Reisepaß ist nur der erste Schritt, die Personalausweise werden folgen.

Daß es jetzt noch keine zentrale Biometrie-Datenbank gibt, bleibt kein Dauerzustand. Spätestens nach dem nächsten Anschlag in Europa wird die Legitimation da sein. Wer regt sich schon über eine klitzekleine Datenbank auf, wenn es denn der Sicherheit dient... Besonders widerlich an der Angelegenheit ist der Zusammenhang mit der fehlgeschlagenen Privatisierung der Bundesdruckerei und den "Bedürfnissen" der deutschen Biometrie- und Chipkartenindustrie. Um schnöden finanziellen Interessen des Staates und der Industrie nachzukommen, wird sehenden Auges ein sicherheits- und technologiepolitisches Desaster erster Ordnung in Kauf genommen, das obendrein die Grundfesten der Informationellen Selbstbestimmung massiv unterminiert.

Der Hang zu technischen Großabenteuern ist den deutschen Politikern offenbar nicht auszutreiben. Die Redaktion ist, wie immer, sehr interessiert an technologischen Forschungen unserer geneigten Leser, an Dokumenten, die das gemeine Volk eigentlich nicht in die Finger bekommen sollte, und natürlich an Erfahrungen mit dem neuen Reisepaß. Zuwendungen bitte wie immer an *<ds@ccc.de>* oder im braunen Umschlag an die bekannte Postadresse.

Auch auf dem 22. Chaos Communication Congress vom 27. bis zum 30. Dezember 2005 wird das Vorgehen gegen den Biometrie-Wahn eine große Rolle spielen, dann schon mit ersten Erfahrungen und Ergebnissen aus der "Hands On"-Forschung mit den neuen Pässen

<Die Redaktion Datenschleuder>

Die sichersten Pässe der Welt

von starbug <starbug@berlin.ccc.de> und
46halbe <46halbe@weltregierung.de>

Die Bundesdruckerei macht mit Otto Schilys neuestem Sicherheitsplacebo den großen Reibach. Seit einigen Wochen ist es offiziell. Ab dem 1. November 2005 werden in Deutschland trotz massiver Kritik von vielen Seiten neue Reisepässe (sog. ePass) mit biometrischen Merkmalen auf RFID-Chips ausgegeben. Deutschland unterbietet dabei bei weitem den vorgegebenen Zeitrahmen der europäischen Verordnung, die ohne Beteiligung des deutschen Parlamentes zustandekam.

Wirtschaftsförderung ohne Rücksicht auf Verluste

Mehr als ein halbes Jahr früher als notwendig wird der Reisepaß nun eingeführt. Die Gründe für die Hast, die das Bundesinnenministerium (BMI) an den Tag legte, liegen auf der Hand. Wer in Europa zuerst ein funktionierendes biometrisches Gesamtsystem zur Grenzkontrolle hat, kann mit Aufträgen in Milliardenhöhe rechnen. Gerhard Schabhüser vom Bundesamt für Sicherheit in der Informationstechnik (BSI) antwortete entsprechend auf die Frage, warum die Einführung der neuen Pässe derart überstürzt vorgenommen wird: "Das hat industriepolitische Gründe." Martin Schallbruch, IT-Direktor des Bundesinnenministeriums, verweist zwar auf einer Informationsveranstaltung zum ePass gemäß der offiziellen Sprachregelung seines Arbeitgebers darauf, daß dieser primär der Erhöhung der Sicherheit diene. Es sei aber ohne Frage gewinnbringend für die deutsche Wirtschaft, weltweit führend auf dem Gebiet der Biometrie und der Chipkartentechnik zu sein, betont er gleich mehrfach.

Die Förderung der Wirtschaft ist ein verständliches Ziel deutscher Politik. Doch was bedeutet der neue Paß für den deutschen Reisenden? Er muß zunächst die deutlich gestiegenen Kosten von 59 Euro (heute 26 Euro) für den normalen Paß bzw. 91 Euro für den Express-Paß tragen. Weit schwerer wiegt aber, daß er die Kontrolle über seine persönlichen biometrischen Daten abgeben muß. Denn was an internationalen Grenzen aus seinem Paß ausgelesen und gespeichert wird, wer Datensammlungen anlegt und für welchen Zweck, ob Abgleiche mit kriminalistischen oder Terroristen-Fahndungs-Datenbanken vorgenommen werden – all das kann niemand kontrollieren und unterliegt selbstverständlich nicht der datenschutzfreundlichen Gesetzeslage in Deutschland. Die digitalen Daten seines Gesichtsbildes und seiner Fingerabdrücke sind zur globalen Speicherung freigegeben.

Die offiziellen Gründe

Offiziell stehen die Terroristen mal wieder an erster Stelle der Gründe für die Einführung des ePasses. Seit dem 11. September 2001 tritt bereits ein gewisser Gewöhnungseffekt ein, daß mit der Terrorabwehr einfach jede Maßnahme begründet werden kann. So soll die Verbesserung des behördlichen Informationsaustausches die Einreise von Terroristen verhindern, indem biometrische Hilfsmittel bei der Personenfahndung genutzt werden. Dazu soll an den Grenzen zweifelsfrei festgestellt werden können, ob der Besitzer des Reisepasses auch der Inhaber ist. Daß die Täter in der Vergangenheit stets gültigen Pässe besessen haben, wird hier einfach ignoriert. Auch der Umstand, daß jeder Bombenleger sich weiterhin einfach außerhalb Europas einen gültigen Paß oder ein Visum besorgen kann, bleibt unerwähnt. Diese unlogische Argumentation wird vom BMI auf jeder Veranstaltung gebetsmühlenartig wiederholt, was sie natürlich nicht wahrer macht.

Das zusätzliche Sicherheitsmerkmal, also der kontaktlose Funk-Mikrochip, soll außerdem die Fälschung erschweren und die Feststellung der Echtheit des Dokuments gewährleisten. Der Bundesinnenminister Otto Schily behauptet, Fälschungen von Pässen würden mit der Speicherung biometrischer Daten "unmöglich gemacht oder mindestens erschwert". Daß die Bundespolizei (früher BGS), der Paßhersteller Bundesdruckerei wie auch das BSI bereits den bisherigen deutschen Paß als hochsicher einstufen, wird geflissentlich verschwiegen. Nach Angaben von Jörg Radek, Bundesvorstand der Gewerkschaft der Polizei, sind Totalfälschungen hierzulande eine seltene Ausnahme; solche in einer guten Qualität, die nicht schon von Grenzbeamten-Azubis erkannt werden, schlicht nicht vorhanden. Der Gipfel des Widersinns ist aber die Tatsache, daß der ePass vollständig gültig bleibt, wenn der Funk-Chip den Geist aufgibt.

Die computergestützte biometrische Identifikation von Personen soll weiterhin zur Effektivierung der Grenzkontrollen dienen und somit für eine Erleichterung des Reiseverkehrs mit dem entsprechenden Zeitgewinn für die Reisenden und für die Bundespolizei sorgen. [1] Dies kann nach den Ergebnissen einer jüngst veröffentlichten BSI-Studie (sog. BioP-II-Studie) zu den Erkennungsleistungen biometrischer Systeme (siehe auch den entsprechenden Artikel in dieser Ausgabe) zumindest in naher Zukunft als ausgeschlossen gelten. Jörg Radek, ebenso wie die Pressestelle des BMI, betont, daß die Technik stets zusätzlich eingesetzt, eine Kontrolle der Reisenden nach den Schengen-Standards jedoch weiterhin erfolgen wird. Von einer Effektivierung kann also keine Rede sein, die Vielflieger und die Urlauber erwartet vielmehr ein erhöhter Zeitaufwand.

Zudem sind die biometrischen Verfahren noch derart fehlerbehaftet, daß zu erwarten ist, daß viele Paßbesitzer von den Geräten an den Grenzen fälschlich zurückgewiesen werden. Genaueres zu den aufgetretenen Unzulänglichkeiten der vier in der BSI-Studie getesteten biometrischen Systemen kann auf über 170 Seiten nachgelesen werden. Zu anderen schwerwiegenden Problemen wie der Überwindungssicherheit der Verfahren findet der geneigte Leser der Studie jedoch keine Angaben. Eine Lebenderkennung etwa ist in den getesteten Verfahren entweder nicht implementiert oder wurde für die Testdauer deaktiviert, um die Erkennungsleis-

tungen zu verbessern. Ebenso waren die Kosten der Systeme nach wie vor kein Thema. So reihen sich die ungelösten Schwierigkeiten mit der übereilt eingeführten Technik aneinander.

Wichtige Fragen danach, ob die für die Signatur und Authentisierung verwendeten kryptographischen Algorithmen zehn Jahre lang die Integrität der Daten auf dem Chip garantieren können, geraten so in den Hintergrund. Auch die Frage nach der Ausgestaltung der benötigten Public Key Infrastruktur (PKI) für die Zertifizierung der internationalen Lesegeräte ist noch immer ungelöst. Die technische Spezifikation wird erst für den Dezember 2005 erwartet. (Siehe dazu auch den Artikel zum Annex G der ICAO-Spezifikation in dieser Ausgabe.)

Die traurige Wahrheit

Es muß deutlich ausgesprochen werden: Die Biometrie in Pässen löst keine Probleme. Wie aus der BioP-II-Studie hervorgeht, an der weniger als 700 regelmäßig aktive Probanden teilnahmen, ist die Technik bei weitem noch nicht einsatzbereit. So werden auf absehbare Zeit die ePässe nicht zur biometrischen Authentifikation verwendet.

Die ebenfalls vom BSI zuvor durchgeführte Studie BioP I [2], die sich mit der Verwendung der automatischen Gesichtserkennung im Grenzverkehr beschäftigte, ermittelte beispielsweise Falschrückweisungsraten (FRR) von 24 bzw. 52 Prozent (bei Falschakzeptanzraten von 0,002 bzw. 0,005 Prozent). Das bedeutet, daß jede vierte bzw. sogar jede zweite Person bei einer Grenzkontrolle fälschlicherweise zurückgewiesen würde. Bei den Fingerabdrücken sah es nicht besser aus. So konnten bei ca. zwei Prozent der Bevölkerung gar keine Abdrücke abgenommen werden, da sie keine ausreichend ausgeprägten Merkmale besaßen. [3]

Die neue BioP-II-Studie läßt die Gesichts-, Fingerabdruck- und Iriserkennungssysteme wiederum nicht gut aussehen. Besonders bei der Gesichtserkennung wird erneut die starke Abhängigkeit der Erkennungsleistungen von Umwelteinflüssen wie dem Umgebungslicht deutlich. Die Interpretation der Ergebnisse unterlag offensichtlich einer politische Einflußnahme, die eine unabhängige Beurteilung der Erkennungsleistungen verhinderte. Die konkrete Datensammlung der Studie bleibt weiter unveröffentlicht. Die vom BSI ermittelten Werte im niedrigen Prozentbereich erscheinen auf den ersten Blick nicht problematisch, rechnet man diese aber auf die Gesamtbevölkerung Deutschlands oder Europas hoch, erkennt man schnell, daß es sich hier um mehrere Millionen Problemfälle handelt.

Und die Personen werden nicht nur einmal betroffen sein, sondern bei jeder Paßkontrolle erneut die Rückweisung durch die biometrischen Geräte erleben müssen. Die damit jeweils verbundenen Extrakontrollen dürften klar gegen den Gleichheitsgrundsatz, verankert im Grundgesetz, verstoßen.

Folgen für alle Paßbesitzer

Im vielzitierten Volkszählungsurteil des Bundesverfassungsgerichtes von 1984 wurde festgestellt, daß jeder Bürger über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst bestimmen darf. Ob die Abnahme biometrischer Merkmale und deren durch den Paßbesitzer nicht mehr kontrollierbare Speicherung in Datenbanken rund um die Welt diesem Urteil zuwiderläuft, ist unter Juristen fraglich. Wünschenswert wäre ein bürgerfreundliches Urteil des Bundesverfassungsgericht zur Frage der ePässe. Als Einzelperson ist eine Klage gegen die Einführung der ePässe jedoch erst dann möglich, wenn man direkt betroffen ist. Man muß sich erst durch die nationalen Instanzen klagen, bevor ein Urteil des Bundesverfassungsgericht oder des europäischen Gerichtshof erwartet werden kann. Ein beträchtlich langer Zeitraum ginge ins Land, ehe entschieden würde. Die biometrische Technik wird dann längst alltäglich und unter erheblichen Kosten eingeführt worden sein.

[1] *http://www.heise.de/newsticker/meldung/60149*
[2] *http://www.bsi.de/literat/studien/biop/index.htm*
[3] *http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf*

Spaß mit dem ePass

von starbug <starbug@berlin.ccc.de> und
46halbe <46halbe@weltregierung.de>

Ihr habt unsere seit einem Jahr regelmäßig wiederholten Hinweise überhört und keinen "alten" Reisepaß beantragt? Jetzt steht ihr vor der Entscheidung, einen neuen ePass mit digitalem Gesichtsbild und RFID-Chip für mehr als doppelt soviel Geld zu holen oder nicht mehr außerhalb Europas verreisen zu können?

Wenn ihr euch für den ePass entscheidet, gibt es hier ein paar Hinweise zum sicheren Umgang und für Spaß am Gerät. Wie ihr in diesem Heft schon gelesen habt oder noch lesen werdet, gibt es ab dem 1. November diesen Jahres eine neue Generation des deutschen Passes. Er beinhaltet, neben den bisher schon vorhandenen Daten und Sicherheitsmerkmalen, zusätzlich einen RFID-Chip, auf dem der Inhalt der Maschinenlesbaren Zone (MRZ) und ein digitales Foto gespeichert werden.

Das Frontalfoto

Das Foto ist dafür ausgelegt, von einer automatischen Gesichtsbilderkennung verwendet zu werden. Daher wird es nicht, wie bisher üblich, im Halbprofil im Paß erscheinen, sondern in der Frontalansicht. Deshalb nun einige Hinweise, was ihr beachten müßt, wenn ihr zum Photographen geht. Schminken solltet ihr dringend unterlassen, starke Lidstriche oder das Nachziehen der Augenbrauen verwirrt die Software und könnte euch fälschliche Rückweisungen an der Grenze bescheren. Eure Persönlichkeit kommt auch ohne Farbe sicher gut zur Geltung.

Auch Piercings oder Tätowierungen im Gesicht sollten gut überlegt sein, denn 10 Jahre sind eine lange Zeit. Man möchte schließlich auch in vielen Monaten noch erkannt werden. Frisuren mit vielen ins Gesicht hängenden Haaren, besonders in der Stirn, sind out, zumindest wenn ihr gern um den Globus reisen wollt.

Zwar sollten solche Hinweise inzwischen alle Photographen mitbekommen haben, in der Realität wird das aber sicherlich nicht der Fall sein. Der Präsident des Centralverbandes Deutscher Berufsfotografen, Hans Starosta, wirkt jedenfalls bei seinem Vortrag auf einer Informationsveranstaltung der Bundesdruckerei noch reichlich unvorbereitet. Auf Nachfragen reagierte er mit Schulterzucken. Und selbst wenn die Fotographen es wissen, ist nicht davon auszugehen, daß sie sich an jedes Detail halten werden, dafür sind die Vorgaben einfach zu ungenau.

Aber es kostet euch ein Lächeln, ihn mit euren neuen Kenntnissen über Gesichtserkennung etwas aufzuklären. Dieses Lächeln spart ihr euch aber bitte beim Shooting, die Software ist noch nicht so ganz ausgereift.

Übrigens, Geld sparen am Fotoautomaten ist keine gute Idee. Die Fotos aus den Automaten entsprechen allein von der Grundqualität der Kameras kaum den Vorgaben für die automatische Gesichtserkennung. Nach neuesten Rechercheergebnissen wurden zumindest einige der Automaten aber schon mit den aktuellen Mustertafeln ausgestattet. Für Spaß in der Kabine ist also auf jeden Fall gesorgt.

Und auch auf mehr oder weniger Spaß mit den Grenzbeamten kann man sich einstellen, wenn man die sowieso kaum funktionierende Gesichtserkennung zusätzlich mit manipulierten Bildern beglückt. Mit bloßem Auge kaum sichtbare Veränderungen des Augenabstands oder der Nasenposition werden mit großer Sicherheit zum Nichterkennen führen. Das ist natürlich nur was für die Hartgesottenen unter euch, die normalerweise viel Zeit beim Verreisen haben. Zwar ist es nicht erlaubt, Bilder in digitaler Form abzugeben, aber daß man heutzutage Paßbilder auch zuhause ausdrucken kann, scheint nicht bekannt zu sein. Lustig wär auch, wenn ihr mal versucht, mit ausgedrucktem Foto und sogar mit einem Foto auf dem Handy die biometrischen Systeme an der Grenze zu überlisten.

Gesichtserkennungstechnisch kaum auswertbare Bilder erzielt man durch das Tragen einer Brille. In der BioP-II-Studie des BSI beispielsweise trugen über 90 Prozent der fälschlicherweise erkannten Personen eine Brille mit dunklem Rand. Tja, die Algorithmen suchen sich eben sehr markante Punkte des Gesichts. Ein schöner Bart tut es übrigens auch.

Allgemein ist anzunehmen, daß die ungenügende Information der Bevölkerung zu massiven Spannungen auf den Meldeämtern führen wird. Also, bereitet euch auf etwas Streß vor, wenn ihr zum Beantragen geht. Es kann davon ausgegangen werden, daß alte Paßfotos schon ab dem 20. Oktober von den Angestellten zurückgewiesen werden, sollten diese schon von der Neuerung erfahren und eine Schulung erhalten haben. Auch die dringend nötige Fortbildung läuft wahrscheinlich aus Geldgründen bisher nur schleppend. Dafür ließ man eine Software schreiben, welche die Qualität der abgegebenen Paßbilder überprüfen soll. Natürlich dauert es einige Zeit, bis alle Meldeämter damit ausgestattet sein werden. Aus anonymen Quellen ist auch leider schon bekannt, daß diese derzeit noch weit von ihrer optimalen Funktionsfähigkeit entfernt ist. Sie findet teilweise nicht einmal die Augen in den Bildern, was eigentlich nur der erste Schritt zur Erkennung ist. Aber das wird sicher noch besser in Version 1.0.

Der RFID-Chip

Trotz des stolzen Betrages von 59 Euro, den jeder bei der Ausstellung eines ePasses bezahlen muß, bleibt der Paß selbst weiterhin Eigentum der Bundesrepublik Deutschland. Deshalb darf man ihn natürlich nicht absichtlich kaputt machen. Was man also nicht machen darf, werden wir sicherheitshalber mal auflisten:

Wer den Paß nach dem versehentlichen Mitwaschen in die Mikrowelle legen will, dem raten wir zur Vorsicht. Ein ungut aussehendes Brandloch könnte die Folge sein. Aber auch Leuchtstoffröhrentester und elektrische Schweißgeräte arbeiten auf Basis von 13,56 MHz - hier kann man die in den Chip eingetragene Leistung durch den Abstand zum Gerät sehr gut steuern. Daher sollte der Chip kaputt gehen, ohne Spuren zu hinterlassen. Natürlich sollte man sowas vermeiden! Obwohl, der Paß bliebe ja weiterhin gültig. Damit könnte man wahrscheinlich auch mehrere Pässe, die sich um das Gerät herum befinden, gleichzeitig zerstören. Also bitte besondere Vorsicht walten lassen.

Und wenn solch ein Gerät durch Zufall an Grenzübergängen oder in den Meldeämtern

steht (da wo die Antragsteller die Daten auf ihrem Paß überprüfen können), würden die Störungen den Auslesevorgang unmöglich machen. Und das will ja wirklich niemand.

Eine andere unbedingt zu vermeidende Möglichkeit ist das häufige Knicken der Paßdecke (die fälscherlicherweise immer als "Deckel" bezeichnet wird). Die Stelle, an welcher der Chip mit der Antenne verbunden wird, ist sehr empfindlich und geht wahrscheinlich schon nach ein paar Biegungen kaputt. Also lieber gar nicht berühren. Selbst wenn man den Paß nur normal mit sich führt, dürfte die Lebensdauer unter 10 Jahren liegen, daher ist eine vorsichtige Handhabung dringend anzuraten.

Man kann sich nun die Fragen stellen: Was passiert, wenn man einen Paß mit kaputtem Chip umtauschen will? Machen die das? Muß man das dann extra bezahlen? Wie oft kann man das denn machen? Für diese Fragen empfehlen wir die Hotline beim Service-Center des BSI: 01805-274-300 (8-17 Uhr für 12 Cent pro Minute).

Man braucht den Paß aber nicht kaputt zu machen, wenn man befürchtet, jemand will ungefragt an die biometrischen Daten ran. Einfaches Mittel um das Auslesen zu verhindern, ist schlichte Alufolie. Dabei muß man diese meist nicht mal komplett um das Dokument wickeln, eine Lage in das Paßbuch zu legen, sollte genügen. Für Verwirrung beim Lesegerät sorgt auch das Einbringen von zusätzlichen Chips in den Lesebereich. Deshalb sind sie übrigens auch davon abgerückt, die Visa auf einem separaten RFID-Chip auszustellen.

Warum sollte man sich aber mit Alufolie vor dem Auslesen schützen sollten? Der Grund ist, daß unberechtigtes aktives und passives Abhören möglich sein könnte. Aktiv hieße, daß der Angreifer Energie erzeugt, um den Chip zu aktivieren, ihn also selbst anspricht. Bis zu einer Entfernung von 10 Metern ist dies möglich. Also empfiehlt es sich, ab und an die Verhaltensweisen der Personen auf der anderen Straßenseite zu beachten. Passives Abhören bedeutet, daß der Angreifer die offizielle Kommunikation zwischen dem Paß und dem Lesegerät (zum Beispiel an der Grenze) mithört. Dieses ist bis zu 30 Metern und unter Laborbedingungen sogar schon bis zu 50 Metern möglich. Es sollten also auch die Personenkraftwagen, die vor dem Flughafen warten, beobachtet werden.

Natürlich hat das BSI vorgesorgt. Um das Auslesen der biometrischen Daten zu verhindern, gibt es kryptographische Sicherungen. Für die digitalen Gesichtsbilder und alle Daten der maschinenlesbaren Zone (MRZ) genügt die sogenannte Basic Access Control. Diese ist keineswegs sicher und kann gebrochen werden. (Siehe auch den Artikel zum Annex G der ICAO-Spezifikation in dieser Ausgabe.) Sollte ein Angreifer die verschlüsselten Daten erhalten haben, kann er sich zuhause in Ruhe an die Brute-Force-Entschlüsselung machen. Hilfreich wäre, wenn der Angreifer die Daten der MRZ in Kopie besäße. Dazu muß er nur einmal kurz den Paß in die Hand bekommen. Man denke an die Paßkopie bei der Hotelanmeldung im Ausland oder die Anmeldung für eine Karte der Fußball-WM 2006.

Vielleicht sollte man doch überlegen, ob Mikrowelle und Alufolie gegen diese Unterwanderung der Informationellen Selbstbestimmung zu erwägen wären...

Sicherheit durch Biometrie?

von Quintus Dalemicus und 46halbe

Die Verpflichtung jeden Bürgers, seine biometrischen Daten in Ausweispapieren anzugeben, stellt in juristischer Hinsicht einen schweren Eingriff in das Grundrecht auf Informationelle Selbstbestimmung dar. Vor dem 11. September 2001 wäre eine solche Maßnahme in Deutschland wohl undenkbar gewesen. Nun wird sie jedoch von den meisten Menschen ohne Aufruhr hingenommen, die allgemeine Sicherheitshysterie macht es möglich.

Offenkundig nutzte der scheidende Bundesinnenminister Otto Schily die Gelegenheit, im Schatten der Anschläge der letzten vier Jahre vorschnell eine Überwachungstechnologie einzuführen, die noch nicht einmal richtig funktioniert. (Siehe dazu den Artikel zur BioP-II-Studie in dieser Ausgabe.)

Die biometrische Technologie kann in einigen Jahren serienreif sein, doch dann könnte sich die politische Landschaft bereits geändert haben. Vielleicht wird Osama bin Laden dann geschnappt sein. Vielleicht wird die Hysterie um den Terrorismus nicht mehr so frisch in den Köpfen der Menschen sein. Vielleicht würden gar biometrische Ausweise, eingeführt mit dem Argument der "Sicherheit", auf Widerstand stoßen. Auch gegenwärtig scheint die Akzeptanz begrenzt, schließlich mußte Schily sein Lieblingsprojekt über den Umweg des EU-Ministerrats auf den Weg bringen und mit Rechtsverordnungen am Bundestag vorbei umsetzen, da ihm Vertrauen und Unterstützung der rot-grünen Bundestagsfraktionen fehlten. Das ganze Vorgehen ist nur ein weiterer Beleg für die schleichende Entmündigung der nationalen Parlamente durch die undemokratische EU. Die Bedenken und Einwände des EU-Parlamentes waren bereits zuvor per Erpressung aus dem Weg geräumt worden.

Die innewohnenden Probleme der biometrischen Systeme lassen sich in zwei Kategorien unterteilen; erstens die Verifizierung vom realen Menschen mit dem gespeichertem Merkmal, obwohl diese nicht übereinstimmen (Falschakzeptanz), zweitens die Abweisung einer geprüften Person, obwohl das gespeicherte Merkmal zu dieser Person gehört (Falschrückweisung). Beide Kategorien von Fehlern bedingen aneinander und sind unakzeptabel, sobald sie gehäuft vorkommen. Fehler der ersten Kategorie führen den angeblichen Sicherheitsgewinn ad absurdum, die Fehler der zweiten Kategorie stellen die betreffenden Personen unter unbegründeten Verdacht. Für diesen Verdacht ist es unerheblich, ob er nun 25, 10 oder 5 Prozent der Menschen betrifft. Für sie wird eine angekündigte "verschärfte Kontrolle", wie immer die auch aussehen mag, nötig. Das ist für die Betroffenen erstens ungerecht, zweitens zeitaufwendig und drittens recht unangenehm, denn für einmal fälschlich zurückgewiesene Paßbesitzer ist die Wahrscheinlichkeit hoch, daß sie von nun an öfter betroffen sein werden.

Sinnvoll gegen Terrorismus?

Was bringt nun der Einsatz biometrischer Ausweispapiere im Kampf gegen den Terrorismus? Kurz gesagt: nichts. Es handelt sich vielmehr um ein Sicherheitsplacebo, mit dem Aktivität suggeriert wird. Die neuen Dokumente sollen angeblich fälschungssicherer sein als bisherige und die Benutzung echter Papiere durch jemanden anderes als den Eigentümer verhindern. Den ersten Punkt kann man getrost als schlechten Scherz verbuchen. Wie weithin bekannt, zählen die deutschen Ausweispapiere heute bereits zu den fälschungssichersten Dokumenten der Welt. In den letzten Jahren gab es nur wenige Fälschungsversuche, und die waren alle-

samt reichlich erfolglos. Das Bundesinnenministerium behauptet jedoch, es gäbe ein großes Gefälle innerhalb der EU, was die Fälschungssicherheit angeht. Das ist wahr, auch hinlänglich bekannt. Die Frage aber, warum dann nicht einfach alle EU-Staaten den jetzigen deutschen Standard übernehmen, bleibt unbeantwortet. Wäre ja auch ein schönes Geschäft für die protegierte Bundesdruckerei. Auch die Aussage Schilys, daß der "21. Attentäter des 11. September" monatelang mit einem gefälschten französischen Paß durch Europa gereist sei, rechtfertigt wohl kaum die Einführung biometrischer Pässe. Der Kriminelle hatte nämlich schlicht einen Meldebeamten bestochen und sich einen Paß ausstellen lassen. Warum Biometrie dies in Zukunft verhindern soll, kann auch Schily nicht erklären.

Der Test auf Übereinstimmung zwischen Paßinhaber und Paßbenutzer ist etwas interessanter. Hierbei unterstellt man dem Inhaber eines EU-Ausweisdokumentes, daß er seinen Paß an einen Doppelgänger, der beispielsweise gesucht wird oder kein EU-Staatsbürger ist, weitergeben könnte, der damit umherreisen würde. Dies zu unterbinden, könnte illegale Einreisen verhindern. Hätte es jedoch die Anschläge in den USA, in Madrid oder in London verhindert? Sicher nicht, da die Täter nicht polizeilich gesucht wurden, legal einreisten und folglich ihre echten Pässe benutzen konnten, biometrisch oder nicht. Das Argument, die neuen Dokumente seien ein Werkzeug gegen den Terrorismus, ist somit in jeder Hinsicht unhaltbar.

Gute Geldanlage bei knapper Kasse?

Ein weiterer Aspekt sind die enormen finanziellen Kosten der ganzen Maßnahme. Dabei findet eine gigantische Fehlallokation von Ressourcen statt. Denn die Milliarden für die Herstellung der Pässe, die Herstellung und Wartung der Lesegeräte, die Schulung des Grenzpersonals etc. fehlen an anderer Stelle. Die Bereitstellung finanzieller Mittel für die Integration von Menschen mit Migrationshintergrund, die Kontrolle an Grenzen auf Waffen und Sprengstoffe, die Ausrüstung und das Training von Rettungskräften, die Resozialisierung von Straffälligen und vieles mehr wäre gesamtgesellschaftlich eine sinnvollere Investition als die Verschwendung für nicht funktionierende biometrische Pässe oder Ausweise.

Sollte die Technologie eines Tages doch funktionieren, drohen uns noch größere Schwierigkeiten. Biometrie und RFID bieten mannigfaltige Möglichkeiten der Überwachung von Menschen. Beides wird nun Schritt für Schritt eingeführt. Erst das digitale Gesichtsbild, dann die Fingerabdrücke, erst im Reisepaß, dann im Personalausweis - die klassische Salami-Taktik.

Gefahren für Freiheit und Demokratie

Die RFID-Chips sind nicht umsonst auch als "Schnüffelchips" bekannt. Mit der entsprechenden Infrastruktur an Lesegeräten, etwa in jeder Tür, in jeder Straßenlaterne oder unter Gehwegplatten, kann man die Bewegungen eines Menschen, der einen solchen Chip bei sich trägt, mühelos verfolgen und archivieren. Beliebige Orwellsche Szenarien kann man sich vorstellen. Ob die kryptographischen Sicherungen die Gefahr, die in den RFID-Chips steckt, dauerhaft eindämmen kann, darf bezweifelt werden.

Neben der Gefahr durch die Schnüffelchips birgt auch der Einsatz biometrischer Merkmale enorme Risiken. Durch die Interventionen des EU-Parlaments konnte gerade noch verhindert werden, daß alle biometrischen Daten in einer zentralen Datei gespeichert werden. Dies hatten die Innenminister der EU in der ihnen eigenen dreisten Selbstverständlichkeit gefordert. Doch auch ohne eine zentrale Referenzdatei besteht die Möglichkeit, daß staatliche "Bedarfsträger" die biometrischen Daten jedes Menschen einsehen können, wenn diese dezentral in den Meldestellen gespeichert und beispielsweise über eine Suchmaschine abgefragt werden. Das wäre praktisch dasselbe wie eine zentrale Datensammlung, es klingt nur nicht so nach Drittem Reich und Zentralkartei.

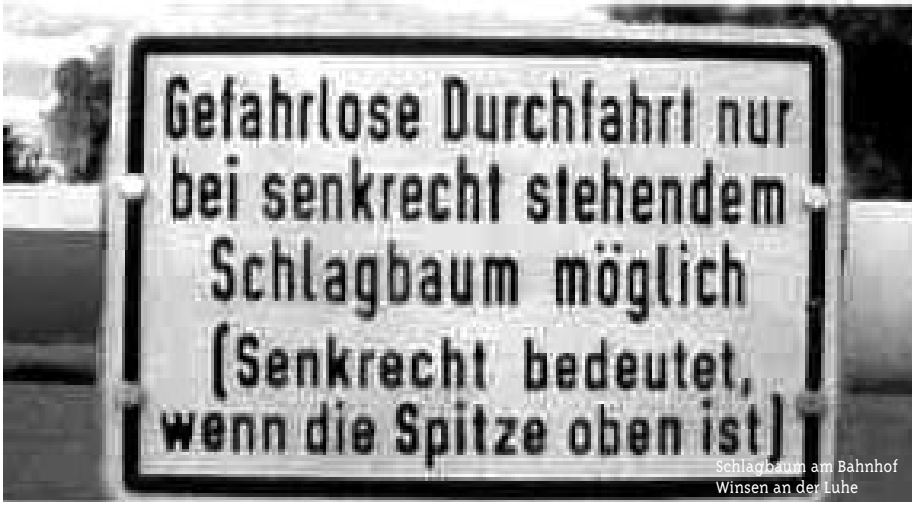
Ein digitalisiertes Gesichtsbild kann mit der Gesichtserkennungssoftware von Überwachungskameras, die sich in Europa wie eine Plage ausbreiten, kombiniert werden. Bisher

werden Menschen vielerorts einfach anonym gefilmt, man könnte mit den Kameras jedoch an das Gesicht der Person auch heranzoomen, es mit biometrischen Daten abgleichen und die Person identifizieren. Hiermit ließen sich die Bewegungen von Menschen überwachen oder die Teilnehmer einer Demonstration identifizieren. Daß der einmal bekanntgewordene Einsatz solcher Techniken Menschen davon abhalten könnte, noch an Demonstrationen teilzunehmen, wäre ein Sündenfall der Demokratie.

Neben dem Bild kommt ab 2007 die Aufnahme des Fingerabdrucks hinzu. Plötzlich müssen gesetzestreue Menschen ihre Fingerabdrücke abgeben wie gewöhnliche Kriminelle. Da jeder Mensch seinen Fingerabdruck an vielen Stellen hinterläßt, öffnet dies der Kreativität von Kriminellen, falsche Fährten am Tatort zu legen, Tür und Tor. So könnten aber auch zufällig die Fingerabdrücke eines Menschen an einem Gegenstand sein, der über irgendwelche Umwege am Schauplatz eines Mordes oder einer Entführung landet. Obgleich diese Person nichts mit der Tat zu tun hat, wird sie plötzlich zum Verdächtigen.

Der ePass wird das Recht auf Informationelle Selbstbestimmung noch weiter aushöhlen. Die Einführung der biometrischen Ausweisdokumente reiht sich ein in eine Folge von Verletzungen dieses Grundrechtes. Die sich immer weiter ausdehnende Videoüberwachung, die automatische Kennzeichenerfassung, der große Lauschangriff, die Jahr für Jahr steigenden Telefonüberwachungsmaßnahmen, die Speicherung von genetischen Informationen in digitaler Form, die Aufhebung des Bankgeheimnisses, die noch immer diskutierte Vorratsdatenspeicherung von Telefon- und Internetdaten; die Liste auf dem Weg zum Überwachungsstaat ließe sich noch fortsetzen. Das alles wird im Namen der "Sicherheit" durchgeführt, und viele Menschen akzeptieren das aufgrund der gestiegenen Angst vor Terrorismus oder Verbrechen. Wohlgemerkt, aus bloßer Angst, denn tatsächlich sinkt die Kriminalität real seit Jahren.

Durch immer mehr Überwachung in Kombination mit den Möglichkeiten durch biometrische Erfassung wird ein Datennetz gesponnen, das die freie Entfaltung der Menschen nachhaltig verändert und zunehmend verhindert. Dies stellt eine Gefahr für die ohnehin durch die Schleichwege über EU-Verordnungen gefährdete Demokratie dar. Wer sich immerzu überwacht weiß, der wird alles tun, um nicht aufzufallen. Die Demokratie lebt jedoch vom Mitmachen und von der Auseinandersetzung.



Schlagbaum am Bahnhof Winsen an der Luhe

Waldarbeiter...

...oder S-Klasse Fahrer?

Biometrische Systeme zur Personenidentifizierung bergen Risiken für ihre Nutzer. Dies mußte kürzlich ein malayischer S-Klasse Besitzer erfahren, als Diebe ihm nicht nur sein Fahrzeug nahmen, sondern ihm mit einer Machete auch den Zeigefinger abhackten, um die mit einem Fingerabdruck-Scanner verbundene Wegfahrsperre zu überwinden.

Dieses und andere Risiken betreffen demnächst auch bei uns Reisepaß- und Personalausweisbesitzer, Edeka-Kunden und alle anderen, die nichts zu verbergen haben.

Über die Risiken und Nebenwirkungen von biometrischen Systemen beschweren Sie sich bei Ihrem Bundesinnenminister.

Biometriepaß – Glossar

Für die Experten im Chaos Computer Club ist der Umgang mit den Fachworten der Biometrie inzwischen Alltag. Um dem Interessierten Neuling auf diesem Gebiet den Einstieg in das Thema zu erleichtern, haben wir die wichtigsten Begriffe kurz zusammengefaßt.

Authentifikation:

Authentifikation ist der Vergleich eines vorher enrolten biometrischen Merkmals gegen ein aktuell vorgezeigtes Merkmal. Dabei unterscheidet man zwischen Verifikation und Identifikation.

BAC (Basic Access Control):

Die BAC ist ein einfaches kryptographisches Verfahren zur verschlüsselten Kommunikation des ePasses mit dem Lesegerät. Der Key wird dabei aus den Daten der MRZ generiert. Da der Schlüsselraum nicht besonders groß und auch relativ leicht zugänglich ist, werden auf diese Weise nur vorgeblich wenig sensitive Informationen, das digitale Gesichtsbild und der Inhalt der MRZ, geschützt.

Biometrie:

Der Begriff Biometrie setzt sich aus den griechischen Worten bio (das Leben) und metron (das Maß) zusammen und bedeutet "die Vermessung des Lebens". Heutzutage bezeichnet der Begriff die Erfassung oder Erkennung von Personen anhand von spezifischen Körpermerkmalen.

EAC (Extended Access Control):

Die EAC ist ein kryptographisches Verfahren zur zusätzlichen Verschlüsselung der Kommunikation für sensitivere Daten des ePasses, wie z.B. die Fingerabdruck- oder Irisbilder. Grundlage ist RSA/DSA mit elliptischen Kurven und Hashes von 224 Bit (in Deutschland). Dabei muß einzelnen Staaten der Zugriff auf die Daten explizit erlaubt werden. Das Keymanagement ist durch eine PKI realisiert.

Enrolment:

Das Enrolment bezeichnet den Vorgang, biometrische Merkmale in das System aufzunehmen. Dabei werden in der Regel mehrere Bilder des Merkmals gemacht. Sie werden in gemittelter Form als Template hinterlegt.

Fehlerraten:

FTA (Failure To Acquire): Die FTA gibt die Wahrscheinlichkeit an, mit der ein Merkmal nicht vom Sensor aufgenommen werden kann.

FTE (Failure To Enrol): Die FTE gibt die Wahrscheinlichkeit an, mit der die Erkennungssoftware aus den Daten des Sensors keine Merkmale extrahieren kann.

FRR (False Rejection Rate): Die Falschrückweisungsrate gibt die Wahrscheinlichkeit an, mit der der rechtmäßige Besitzer der biometrischen Referenzdaten fälschlicherweise zurückgewiesen wird.

FAR (False Acception Rate): Die Falschakzeptanzrate gibt die Wahrscheinlichkeit an, mit der ein fremdes Individuum bei der Präsentation seines biometrischen Merkmals fälschlicherweise als der rechtmäßige Eigentümer der Referenzdaten erkannt wird.

ICAO (International Civil Aviation Organization):

Die internationale Zivilluftfahrtsorganisatio n ist eine Sonderorganisation der Vereinten Nationen, welche mit der Planung des zivilen Luftverkehrs beauftragt ist. Sie wurde 1944 gegründet, hat ihren Sitz in Montreal und verfügt über sieben Regionalbüros. Zu ihren Aufgaben gehört die Regelung der internationalen Verkehrsrechte, die Standardisierung und der Aufbau von Infrastrukturen.

Identifikation:

Die Identifikation ist der 1:n Abgleich gegen mehrere, in einer Datenbank gespeicherten Templates.

LDS (Logical Data Structure):

Standardisiertes Datenformat für weltweite Interoperabilität bei der Speicherung der biometrischen Informationen

MRTD (Machine Readable Travel Documents):

Als maschinenlesbare Reisedokumente nach der ICAO-Spezifikation verstehen sich auch der deutsche Reisepaß sowie der Personalausweis. Beide beinhalten zwei Textzeilen in einer OCR-optimierten Schriftart (OCR-B). In der neuesten Fassung beinhalten die Spezifikationen auch die Aufnahme eines RFID (siehe Artikel).

MRZ (Machine Readable Zone):

Maschinenlesbarer Bereich auf Ausweisdokumenten. In Deutschland beinhaltet er die Ausweisnummer, das Geburts- und das Gültigkeitsdatum sowie Prüfziffern. Diese Daten sind in der Schriftart OCR-B aufgedruckt und können optisch ausgelesen werden. Sie dienen der Verschlüsselung der Kommunikation zwischen Lesegerät und RFID-Chip im ePass.

OCR (Optical Character Recognition):

Texterkennung oder auch Optische Zeichenerkennung ist ein Begriff aus dem IT-Bereich und beschreibt die automatische Texterkennung von einer gedruckten Vorlage.

OCR-B

Eine 1968 von Adrian Frutiger für Monotype entworfene Schriftart, die ebenso wie die ältere OCR-A für das rechnergestütze Auslesen optimiert wurde, aber im Gegensatz zur OCR-A eine bessere Lesbarkeit für Menschen bringt. OCR-B ist zum ISO 1073/II-1976 (E) Standard konform.

PKI (Public Key Infrastructure):

Eine PKI ist eine zertifikatsbasierte Technologie zur Verwaltung und Verteilung von kryptographischen Schlüsseln. Sie dient dem Zugriffsschutz.

RFID (Radio Frequency Identification):

RF-Chips sind winzige Transponder. Sie können per Funk Daten zu einem Lesegerät übermitteln und von diesem zu empfangen. RF-Chips sind in verschiedensten Bauformen und Leistungseigenschaften am Markt erhältlich.

Template:

Als Template wird der Datensatz bezeichnet, der beim Enrolment angelegt wird und das biometrische Merkmal der Person enthält. Templates können entweder in Datenbanken oder auf SmartCards gespeichert werden.

Verifikation:

Die Verifikation beschreibt einen 1:1 Abgleich zwischen dem aktuell gemessenen Merkmal und einem Template. Vor Beginn muß dem System das Merkmal oder eine eindeutige ID übergeben werden, die ein Template repräsentiert.

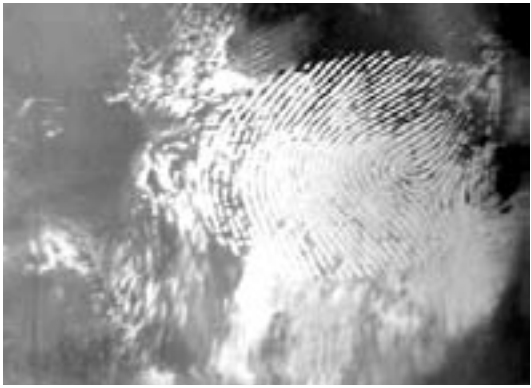
Fingerabdrücke nachmachen leichtgemacht

Eine Anleitung zum Kopieren von Fingerabdrücken mit Haus- und Büromitteln.

Zum Erstellen einer Fingerspitzenattrappe benötigt man natürlich zuerst ein Original. Gute Quellen für Fingerbilder sind Glasoberflächen, Hochglanzpapier und poliertes Metall.

Die Fett- und Schweißrückstände ergeben entlang der Kapillaren das Muster. In Kriminalistenkreisen ist die üblichste Methode zum Sichtbarmachen des Bilds farbiges feines Pulver, welches mit einem weichen Pinsel aufgetragen wird:

Da wir uns jedoch auf Hausmittel beschränken wollen, benutzen wir die niederschlagenden Dämpfe von Sekundenkleber. Dessen Hauptbestandteil, Cyanoacrylat, reagiert hervorragend mit dem Fett im Fingerabdruck. Wer schon einmal Sekundenkleber an den Fingerspitzen hatte, wird das bestätigen können.



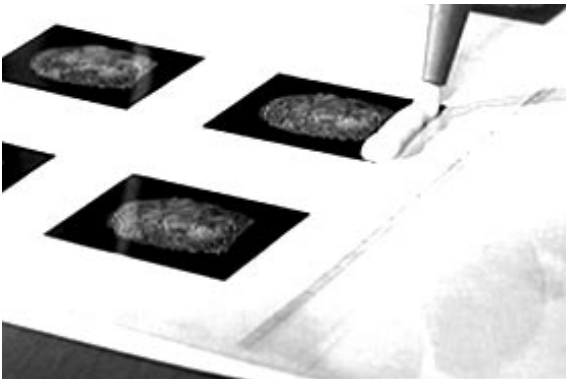
Um den Dampf auf dem Fingerabdruck zu konzentrieren, hält man einfach eine Kappe voll Kleber darüber und wartet, bis er aushärtet.

Für die weitere Bearbeitung am Rechner kann und muß das Bild nun digitalisiert werden. Profi-Equipment ist dazu nicht vonnöten, eine handelsübliche Digitalkamera genügt.

Nun kann am Bildbearbeitungsprogamm die Qualität des Bilds verbessert werden, Kanten deutlicher hervorgehoben und der Kontrast erhöht werden.

Da unsere Fingerattrappe wie ein Stempel funktioniert, muß ein deutliches Relief in die Masse gebracht werden. Der einfachste Weg ist, mit einem Laserdrucker das Negativ des Fingerbilds auf Folie zu drucken.

Der Toner schichtet sich, je nach Helligkeit, in unterschiedlicher Dicke auf der Folie auf. Wir erhalten das gewünschte Relief.



Die Masse, in die wir das Relief prägen, braucht Eigenschaften, die uns unter anderem Holzleim mitbringt: plastisch formbar bis zum Aushärten, danach elastisch auf der Fingerkuppe und natürlich leicht klebend.

Um die optimale Viskosität zu erhalten, kann man gerne noch etwas Glycerin beigeben. Die entstehende Mischung bringt man nun gleichmäßig in dünner Schicht auf die Folie auf.

Nach ein paar Minuten ist der Kleber ausgehärtet und bringt bereits alle Eigenschaften für eine gute Maskierung des eigenen Fingerbilds mit: hohe Elastizität, geringe Dicke (damit die Attrappe nicht auffällt) und natürlich eine Kopie des Fingerbilds, mit dem wir uns verkleiden wollen.

Nun muß die Attrappe nur noch in Fingerabdruckgröße ausgeschnitten und mit ein wenig Kleber (am unbedenklichsten: Maskenkleber, aber nicht in jedem Haushalt zu finden) fixiert werden.

Der Chaos Computer Club wünscht viel Spaß mit ihrer neuen Identität.

Inside ePassports

von Harald Welte <laforge@gnumonks.org>

Electronic passports that are deployed arond the world (including Germany) will be based on RFID technology. To understand its implication, knowledge about those technologies is essential.

Introduction

Technically speaking, ePassports are ICAO compliant MRTD's. ICAO is an international body that already specifies the current OCR readable lines on travel documents. The ICAO MRTD specifications are publicly available from the ICAO homepage.

From a technical point of view, ePassports are ISO 14443-1,2,3,4 compliant contactless smart cards. On top of 14443-4 transport layer protocol, APDU's according to ISO 7816-4 are exchanged. For those readers who are not familiar with smart card technology: ISO 7816-4 *tries to* specify interindustry commands for interchange with ID cards.

The ISO 7816-4 smartcard provides a filesystem based interface to the information stored on the ePassport. The application software issues high-level commands such as "SELECT FILE", "READ BINARY" to the MRTD. The ICAO recommends a minimum memory size of 32kBytes. However, it recommends as much memory as possible, and indicates 512kBytes as a target. As of now, the MRTD chip has to operate in a write once, read many fashion. After the document is issued, it must not be allowed to change any data. Future standards may include the possibility to store electronic visa data.

Organization of Data

Data on the ePassport is organized according to a specification called LDS (logical data structure). LDS specifies a number of DG (Data Groups), as well as the encoding of the data. The most important data groups are:

- DG1 (mandatory) contains the same data as printed on the cover page like name, date of birth, expiration date, document number, nationality, etc.
- DG2 (mandatory) contains the JPEG2000 encoded facial image and corresponding biometric data
- DG3 (optional) contains biometric fingerprint data - not in German passports
- DG4 (optional) contains biometric iris data - not in German passports

ICAO requires data in DG1 and DG2 to be stored unencrypted, since it only resembles the data

Passport-Sample (14443-B) and CM5121 Reader PCB

that is human-readable on the printed pages of the passport. Additional biometric data such as iris and/or fingerprint information may be stored in an encrypted format. As of now, this is up to the issuing country. Any form of encryption is outside the ICAO MRTD specifications and will thus not work interoperable on an international level.

All biometric information stored within LDS is further encoded according to CBEFF (Common Biometric Exchange File Format, NISTIR 6529-A), a common file format that facilitates exchange and interoperablity of biometric data. Each data group is cryptographically signed. The signature is stored in EF.SOD (Security Object Data).

Security Features

Randomization of unique serial number

All ISO14443 compatible RFID chips disclose a unique serial number during the anticollision procedure. This poses the potential threat of pseudonymised tracking. The German BSI therefore requires this randomization of the serial number.

Passive Authentication (mandatory)

Passive authentication performs verification of the EF.SOD signature(s). This assures that the content of the data groups is signed by the issuing country. However, passive authentication does not prevent copying of a MRTD.

Active Authentication (optional)

Active authentication can be employed to verify that the chip has not been substituted. It is based on a challenge response protocol. The MRTD chip contains an active authentication public key pair (KPrAA and KPuAA). A hash representation of KPuAA is stored in EF.SOD and therefore authenticated by the issuing country certifiate. KPrAA is stored in on-chip secure memory.

Basic Access Control (optional, implemented in Geman ePassports)

Basic access control denies access to the MRTD chip until the inspection system proves that it is authorized to access the chip. This proof of authorization is done by deriving a pair of keys (Kmac and Kenc) from the OCR-read machine readable zone (MRZ). BAC can therefore prevent unauthorized "harvesting" of passport data without being noticed by the passport holder. BAC also mandates that any communication following-up to BAC has to be encrypted via ISO 7816-7/8 secure messaging (SM). This

transport level security can be somewhat compared to running TLS on top of a TCP session.

Extended Access Control (optional)
Extended Access Control prevents unauthorized access to additional biometrics. It is similar to Basic Access Control, but requires separate keys and key management. There is no ICAO MRTD standard on how it is implemented or used, and therefore subject to the issuing state.

The Public Key Hierarchy

The PKI hierarchy is obviously nothing that directly affects the passport itself. However, it is integral to the security of the system, so this paper provides a quick overview:

All keys are issued in the familiar form of X.509 certificates. Each issuing state operates its own "Country Singing CA". There is no supernational Root CA. This is neccessary, since every country decides on its own if it recognizes a particular other country. This also means that every reader ("inspection system") has to store the Document Signer Certificate of every recognized issuing country.

The individual ePassports are signed using Document Signer Keys. The Document Signer Keys are in turn signed by the Country Signing CA. Document Signer keys have limited lifetime, and it is recommended that issuing countries delete the private key after the last passport for that key has been issued. Issuing countries have to provide certificate revocation lists (CRLs) at least every 90 days, but not more often than every 48 hours.

The ICAO operates a "public key directory" which will be set up as X.500 directory, updates are performed over LDAP. All communication with the PKD is SSL authenticated. The PKD stores Document Signer Certificates, but not Country signing CA certificates. ICAO verifies signatures of all incoming Certificates and CRL's before making them available. The PKD has public read access on the internet. Country signing CA certificates will be provided bilaterally between countries.

Crypto Algorithms

The ICAO MRTD specification allows RSA, DSA and Elliptic Curve DSA with various minimal key lengths:

Algorithm	*Active Auth*	*Document Signer*	*Country Signing CA*
RSA	*1024*	*2048*	*3072*
DSA	*1024/160*	*2048/224*	*3072/256*
ECDSA	*160*	*224*	*256*

Security threats

Small Keyspace of basic access control
The entropy of the MRZ data used to derive Kenc and Kmac for basic access control is very limited. The nine digit document number is concatenated with the date of birth and the expiration date of the document.

Since ICAO MRTD specifications recommend ePassports not to be valid for more than five years, the expiration date can only be one out of (365*5 = 1325) values.

The date of birth can realistically assume only values between 18 and 90 years old (365*72 = 26280). Also, in case of a specific person, the range of the DOB can often be estimated to a certain range.

Document Numbers are issued sequentially in some countries, and can therefore be reduced to certain ranges. In Germany, the first four digits specify the issuing department, and the following five digits increment sequentially.

Grandmaster Chess Attack

The Active Authentication mechanism is meant to prevemt chip substitution (e.g. carbon copying). However, it cannot prevent a "grandmaster chess attack", where the inspection system talks to a "proxy" chip that would temporarily communicate with the original MRTD.

Die Auswertung der BioP II Studie des BSI

von Zapf Dingbatz und 46halbe

Auf die 170-seitige Studie BioP II, die vom BSI beauftragt wurde, um die Praxistauglichkeit biometrischer Systeme zu testen, lohnt ein etwas längerer Blick. Wir haben ihn gewagt und wollen euch die Ergebnisse nicht vorenthalten.

Vor dem Gesetzemachen sollte die Sachkunde kommen. So wäre es zumindest idealerweise. Biometrie ist ein recht neues und unerforschtes Feld. Also, dachte sich der Gesetzgeber, wäre es eine gute Idee, vor der massenweisen Einführung von biometrischen Merkmalen in Personaldokumenten erstmal zu prüfen, ob das Ganze überhaupt funktioniert. Da das Ergebnis der ersten Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dazu nicht so ganz praxisnah war, wurde nunmehr ein größer angelegter Feldtest angesetzt, die BioP-II-Studie. Durchgeführt von der Secunet Security Networks AG, dem Dienstleister für (fast) alle Fälle des BSI.

Nun interessiert sich aber der dazumalige Innenminister, der allseits beliebte und bekannte Otto Schily, nicht allzusehr für Fakten. Daß die ganze hochgelobte Biometrie nicht funktionieren könnte, war keine in Frage kommende Möglichkeit. Es ging ja schließlich um die Sicherheit des Abendlandes vor den Gefahren des internationalen Terrors und die Förderung der darniederliegenden deutschen Industrie. Also drückten seine Ministerialen unter Schilys Ägide über den Umweg EU und ICAO am Bundestag vorbei durch, daß Fingerabdrücke und Gesichtserkennung in die Reisepässe kommen. Wohlgemerkt, bevor die Ergebnisse der BioP-II-Studie offiziell vorlagen, die doch *"Hilfestellung für die Art und Weise der Einführung der neuen ePässe geben"* sollten. Nicht, daß Schily die Ergebnisse der Studie nicht schon gekannt hat; Mitarbeiter des BSI zeigten bereits ab Frühjahr 2005 Teilergebnisse auf Symposien und Informationsveranstaltungen herum.

Das BSI, eine deutsche Behörde mit allen Vor- und Nachteilen, publizierte mit mehrmonatiger Verspätung dann das Ergebnis mit dem lapidaren Hinweis, daß die politischen Gegebenheiten die Zielsetzung der Studie leider überholt hätten. Nun ist aber das BSI eine nachgeordnete und damit weisungsgebundene Behörde des Innenministeriums. Dies schlug sich dann auch deutlich in der Interpretation der Studienresultate und der Fülle der nicht publizierten Details nieder. Das Amt stellte die Version 1.8 der Studie für einige Stunden online, zog sie dann wieder zurück und publizierte Tage später die Version 2.0.

Durch diesen Zufall ist ein gewisser Einblick in den Prozeß der Bearbeitung möglich. Leider gehen die daraus zu gewinnenden Erkenntnisse nicht über die Bestätigung des Verdachts der dramatischen politischen Einflußnahme hinaus. Eine Version 1.0 oder so mit allen Anhängen wäre sehr interessant (falls die jemand rumliegen hat: email an ds@ccc.de oder im vorgeschriebenen neutralen braunen Umschlag an die bekannte Adresse aus dem Impressum).

Hier nun eine Auswertung der Studie unter Berücksichtigung beider Versionen. Der geneigten Leser kann die Studie als Referenz hinzuziehen, da wir für einige Anmerkungen die Seitenzahlen der Version 2.0 angeben: *http://www.bsi.de/literat/studien/biop/biopabschluss2.pdf*

Aufbau der Studie

Je ein Iris-, ein Gesichts- und zwei Fingerabdruckerkennungssysteme wurden an vier Teststandorten am Flughafen Frankfurt/Main von insgesamt 2081 Mitarbeitern der Fraport AG, der Lufthansa AG und des Bundesgrenzschutzes (heute Bundespolizei) getestet. Der Feldtest gliederte sich in zwei Testzyklen von jeweils acht Wochen.

Es handelte sich um vier bereits am Markt befindliche Produkte. Der sogenannte Testsieger der vorangegangenen BioP-I-Studie der Firma Cognitec Systems GmbH wurde als einziges Gesichtserkennungssystem geprüft. Offenbar hoffte man, sie hätten ihr Produkt mittlerweile verbessert. Außerdem wurden aus acht nicht in der Studie benannten Anbietern nach unklaren Auswahlkriterien zwei Fingerabdrucksysteme der Firmen Dermalog Identification Systems GmbH und Bundesdruckerei GmbH ausgewählt. Der vierte Kandidat war das Iriserkennungssystem von SD Industries GmbH (heute takeID GmbH). Man kann nur spekulieren, was die Tester bewegte, gerade diese Anbieter auszuwählen. In der Studie findet sich nur der Hinweis auf eine *"Marktsichtung"* ohne Angabe der Kriterien.

Hygiene muss groß geschrieben werden

Die Probanden erhielten eine SmartCard (RF-Token) mit einer UserID. Diese sollte den Chip im Paß simulieren. Die verwendeten Chips waren jedoch aufgrund der *"Verfügbarkeit und Kostensituation"* leider nicht ICAO-konform. Schade, war die ICAO-Konformität doch gerade eine wesentliche Zielsetzung der Studie. Die eigentlich vorgesehenen Untersuchungen zur RF-Technik und deren Sicherheitsmechanismen mußten daher nun in eine separate Projektreihe "ILSE" ausgelagert werden.

Ganz zeitgemäß wurde aber die Teilnehmermotivation angegangen. *"Im Rahmen des Enrolments konnten die Testpersonen an einer Verlosung teilnehmen, bei der es Uhren mit projektspezifischem Design zu gewinnen gab. Um einem Sinken der Betätigungszahlen entgegenzuwirken, wurde während des Feldtests eine Incentivierung für Teilnehmer ausgelobt, die eine Mindestanzahl von Betätigungen erreichen."* Wie genau die *"Incentivierung"* aussah, bleibt leider unklar. Stilecht wären Kaffeetassen, Kalender, Kugelschreiber und Klopapier mit "projektspezifischem Design" gewesen. Trotz dieser umfangreichen Motivationsmaßnahmen sprangen etwa 400 Teilnehmer nach dem Enrolment ab, 1600 Probanden sind also die eigentliche Gesamt-Testpopulation.

Enrolment

Die Failure to Enrol (FTE) Rate zeigt an, wieviel Prozent der Teilnehmer nicht erfaßt werden können. Bei der Fingerabdruck- und Iriserkennung sind 0,4 bis 0,99 Prozent der Teilnehmer bereits beim Enrolment gescheitert. Für die Gesichtserkennung konnten zwar alle Probanden enrolt werden, jedoch weist die Studie auf den Umstand hin, daß es in der Praxis Personen geben wird, bei denen aus religiösen oder kulturellen Gründen keine Aufnahmen des Gesichtes möglich sein werden.

Da war ihnen wohl die null Prozent FTE bei der Gesichtserkennung selbst unheimlich. Das unrealistische Enrolment-Setup (speziell von Experten angefertigte Bilder, Nachbearbeitung mit Adobe Photoshop) dürfte aber der eigentliche Grund für die unrealistisch niedrige FTE-Rate sein.

Doch nicht nur das, denn die Messung der FTE in der Studie schließt Fehler, die durch falsche Bedienung der Systeme beim Enrolment entstanden sind, explizit aus. Sie werden gar nicht als Fehlversuch ausgewiesen. In der Praxis ist daher natürlich eine höhere FTE zu erwarten. Hinzu kommt, daß die Ergebnisse der FTE nochmals dadurch geschönt wurden, daß ein Re-Enrolment vorgenommen wurde. Man machte kurzen Prozeß und erfaßte bis zu 5 Prozent der Teilnehmer einfach nochmals. Die Begründung ist so einfach, wie sie vermutlich gelogen ist: *"Systemfehler"*. Behauptet wird, daß während des ersten Enrolments teilweise keine Templates in der Datenbank gespeichert worden wären. Dies erscheint ziemlich zweifelhaft, da jeweils nach einem Enrolment immer eine Testverifikation stattfindet. Diese kann ohne ein Template aber nicht funktioniert haben. Es bleibt also der Verdacht, daß die in der Einführungsphase besonders häufig zurückgewiesenen Personen re-enrolt wurden, um die Ergebnisse der FTE zu verbessern. Günstig ist dabei auch der Mitnahmeeffekt - die Falschrückweisungsrate sinkt ebenfalls. Praktisch bedeutete dieses Vorgehen jedoch, daß 5 Prozent der Personen jeweils einen neuen Paß bekommen würden. Der geneigte Leser darf sich die auf die Gesamtbevölkerung hochgerechneten Zahlen selbst überlegen.

Weitere Probleme zeigten sich bei der Aufnahme der biometrischen Merkmale in die Datenbanken. Die Positionierung vor dem Iriserkennungssystem erwies sich für die Probanden als außerordentliche Schwierigkeit. Besonders bei den Brillenträgern (42 Prozent der Population), die ihre Brille zur Präsentation der Iris abnehmen mußten, zeigte das System von SD Industries während des Enrolments sowie im gesamten Feldtest seine Schwächen. Die Benutzerführung war einfach untauglich (die Sehhilfenträger konnten schlicht die Positionierungsmarkierungen ohne Brille nicht sehen).

In der Studie klingt das dann so: Bei SD Industries *"traten Positionierungsschwierigkeiten gehäuft auf, da Teilnehmer gleichzeitig den richtigen Abstand zum Gerät und den Fokuspunkt (Positionierung des Auges in der Mitte des Spiegels der Sensoreinheit) finden mußten. Teilnehmer mußten sich oft ein Auge zuhalten, um zu fokussieren. Die Kopplung mit einer trägen akustischen Rückmeldung bzgl. des Abstands führte zu 'Schaukel'-Bewegungen. Außerdem wurde von einer Reihe von Teilnehmern die Sensoreinheit nicht auf die der Körpergröße angemessene Position eingestellt. Viele größere Teilnehmer bückten sich, anstatt die Einstellung zu verändern."* Wenn man das mal vor seinem inneren Auge ablaufen läßt, so scheint es an der Grenze in Zukunft auch lustige Momente zu geben.

Personen, die kleiner als 1,55 m waren, konnten gar nicht oder nur unter großen Mühen am Test teilnehmen. Warum auch, der Bürger kann schließlich seine Körpergröße oder Sehstärke den Geräten anpassen, und nicht umgekehrt.

Überwindungssicherheit

Der geneigte Hacker fragt sich bei biometrischen Systemen natürlich als erstes: Kommt man da durch? So ging es offenbar auch den Studienbetreuern beim BSI und den Durchführern bei Secunet. In den Kriterien zur Bewertung der getesten Systeme heißt es denn auch: *"Fake-Resistenz: Biometrische Systeme müssen insbesondere bei unüberwachtem Betrieb eine ausreichende Resistenz gegen Kopien des betreffenden Merkmals aufweisen. In Abhängigkeit des verwendeten Verfahrens kann aber auch bei überwachtem Betrieb eine ausreichende Fake-Resistenz erforderlich sein. Deshalb stellt die Fake-Resistenz ein wichtiges Bewertungskriterium dar."* Deswegen fließt dieses Kriterium dann auch mit atemberaubenden 4 Prozent in die Gewichtung der Gesamtbewertung ein. Eine höhere Gewichtung hätte wohl sonst die Auswertung nachhaltig versaut. Die Ergebnisse der Versuche waren offenbar

ähnlich erschreckend wie jene aus den (bereits hinlänglich in der Datenschleuder publizierten) Forschungen des CCC.

"Bei den hier erfolgten Überwindungsversuchen handelt es sich ganz überwiegend um Labortests, die nur vorläufige Aussagen zulassen. Auf eine detaillierte Darstellung wird in diesem Bericht daher verzichtet." So lautet der peinlich dürre Kommentar zum Thema Überwindungssicherheit in der Studie, in verschiedenen Formulierungsvarianten. Daß die Systeme überwindungssicher sind, konnte also wiedereinmal nicht gezeigt werden. Der IT-Direktor des BMI, Martin Schallbruch, merkte auf einer Informationsveranstaltung an, man wolle schließlich den Fälschern keinen Vorschub leisten. Warum deshalb aber nicht mal die Ergebnisse der Überwindungssicherheitstests publiziert werden, bleibt sein Geheimnis. Er wollte es auch auf Nachfrage nicht lüften. Aufmerksames Lesen der Studie fördert jedoch ein paar Hinweise zu Tage.

Die beiden Fingerabdrucksysteme und das Gesichtserkennungssystem wurden in der Abschlußauswertung (Seite 161) in der Rubrik "Fake-Resistenz" jeweils mit der Note 4 bewertet. Die Erläuterung auf Seite 158 gibt die Note 4 wie folgt an: *"Überwindung mit mittlerem Aufwand erfolgreich (mit Zugriff auf das Merkmal eines Berechtigten)"*. Um das etwas besser einordnen zu können, hier der Klartext der nächstbesseren Note 3: *"Überwindung mit mittlerem Aufwand sowie Spezialwissen und/oder speziellen Hilfsmitteln erfolgreich"*.

Zu deutsch: eine Note 4 bedeutet, daß ohne Spezialwissen und spezielle Hilfsmittel eine Überwindung problemlos möglich ist. Das deckt sich mit unseren Erkenntnissen, auch wenn das BSI vermutlich die in der Datenschleuder beschriebene Vorgehensweise zum Nachbau eines Fingerabdrucks als "Spezialwissen" sowie Holzkaltleim, Digitalkamera und Sekundenkleber als "spezielle Hilfsmittel" einstufen würde.

Der Kommentar des Innenministeriums, daß Details zur Überwindungssicherheit nicht publiziert würden, *"um Fälschern keine Anleitung zu geben"*, ist also absolut wörtlich zu nehmen. Die getesteten Fingerabdruck- und Gesichtserkennungssysteme sind allesamt als so unsicher einzustufen, daß sogar nur moderat clevere Übeltäter kein Problem beim Überwinden haben werden. Beide Fingerabdrucksyste-

Kriterium	Gew.	Cognitec		BDr/NEC		Dermalog		SDI	
		Note	Ergeb.	Note	Ergeb.	Note	Ergeb.	Note	Ergeb.
Erkennungsleistung /Kennzahlen									
ICAO	48,0%	4,29	2,059	3,830	1,838	3,330	1,598	4,430	2,126
Template	12,0%	3,76	0,451	3,630	0,436	3,010	0,361	4,510	0,541
Systemergebnisse									
Mittlere Verarbeitungszeit	0,5%	4	0,02	4	0,02	3	0,015	3	0,015
Systemfehler	1,0%	5	0,05	3	0,03	4	0,04	4	0,04
Ausfallverhalten	1,0%	5	0,05	3	0,03	3	0,03	3	0,03
Administrationsaufwand	0,5%	5	0,025	2	0,01	3	0,015	2	0,01
Robustheit/Langlebigkeit Sensoren	2,0%	1	0,02	2	0,04	1	0,02	1	0,02
Benutzerakzeptanz									
Gesamtbeurteilung	3,0%	4	0,12	3	0,09	3	0,09	2	0,06
Sicherheit	3,0%	2	0,06	2	0,06	2	0,06	2	0,06
Schnelligkeit	3,0%	3	0,09	2	0,06	2	0,06	2	0,06
Einfachheit	3,0%	1	0,03	1	0,03	1	0,03	1	0,03
Bequemlichkeit	3,0%	1	0,03	1	0,03	1	0,03	1	0,03
Benutzbarkeit									
Bedienzeit	3,0%	3	0,09	4	0,12	4	0,12	4	0,12
Benutzbarkeitsprobleme	7,0%	2	0,14	1	0,07	2	0,14	4	0,28
Sicherheit									
Systemsicherheit	1,0%	2	0,02	6	0,06	4,7	0,047	5,3	0,053
Fake-Resistenz	4,0%	4	0,16	4	0,16	4	0,16	2	0,08
Sonstiges									
Inbetriebnahme	2,0%	3	0,06	2	0,04	3	0,06	3	0,06
Support/Service	3,0%	3	0,09	2	0,06	2	0,06	2	0,06
Summe	**100,0%**		**3,57**		**3,18**		**2,94**		**3,68**

me wiesen nicht einmal eine Lebenderkennung auf. Beim Gesichtserkennungssystem wurde die Lebenderkennung mit der Begründung abgeschaltet, daß sonst die False Rejection Rate (FRR) so ansteigen würde, daß ein Praxiseinsatz unmöglich wird (S. 63, Fußnote 2).

Ein weiterer interessanter Aspekt ist die Benotung für die Systemsicherheit. Dabei sah es offenbar noch schlimmer aus als bei der Überwindungssicherheit. "*Systemsicherheit: Dieses Kriterium bewertet die bereitgestellten Systeme hinsichtlich physischer Sicherheit, Sicherheit der Verarbeitungseinheit und Sicherheit der Anwendungssoftware. Da es sich bei den in BioP II eingesetzten Systemen um Prototypen handelt, geht dieses Kriterium nur mit geringem Gewicht in die Bewertung ein.*" Das BSI rechnete also von vornherein damit, nur Systeme geliefert zu bekommen, bei denen die Hersteller froh sind, wenn sie gerade mal so funktionieren. Die Noten weisen hier auf ein Totalversagen aller Systeme, mit Ausnahme der Cognitec Gesichtserkennung.

Die ausgeprägte Paranoia der Studiendurchführer, was die Ergebnisse der Übwindungssicherheitstests betrifft, ist bemerkenswert. Die Schwächen der Systeme sind ja hinlänglich bekannt. Jeglicher Hinweis auf die entsprechenden Anlagen wurde durchgehend in Version 2.0 der Studie getilgt. Daß die Endbenotung für Systemsicherheit und Fake-Resistenz noch in der Studie verblieb, ist vermutlich wohl einzig dem Umstand zu verdanken, daß die Autoren sich nicht komplett lächerlich machen wollten.

Erkennungsleistungen

In der offiziellen Auswertungszusammenfassung werden vorwiegend die Zahlen zur Erkennungsleistung verwendet, die sich auf die sogenannten "*Normalnutzer*" beziehen. Aufgrund der Tatsache, daß die Probanden die Systeme mit sehr unterschiedlichen Häufigkeiten benutzten, wurden sie in Benutzerklassen eingeteilt. Normalnutzer sind als solche Testteilnehmer definiert, die wenigstens 30 Bedienvorgänge durchgeführt haben. Das ist natürlich für einen durchschnittlichen Reisepaßbesitzer hochgradig unrealistisch. Normale Reisende passieren selten mehr als 30 mal pro Jahr eine Schengen-Außengrenze. Somit wenden wir unsere Aufmerksamkeit den "*Wenignutzern*" (0 bis 10 Bedienvorgänge) und den "*sporadischen Nutzern*" (10 bis 30 Benutzungen) zu, die eher dem Profil des normalen Reisenden entsprechen dürften.

In dieser Nutzergruppe finden sich False Rejection Rates jenseits von allem, was noch als "akzeptabel" schöngeredet werden könnte. Je nach verwendetem System (Gesicht und Finger) wurden in der Studie unter optimalen Bedingungen zwischen 4 und 10 Prozent der Nutzer fälschlich zurückgewiesen. Die Iriserkennung wurde selbst nach BSI-Maßtäben total deklassiert, mehr als 20 Prozent der Wenignutzer wurden nicht korrekt erkannt. Das wäre wohl selbst für die hinsichtlich Technikverpeilung in industriellem Maßstab sehr toleranten Deutschen im Alltag an den Grenzübergängen undenkbar. Rechnet man beispielsweise mal die ermittelten Zahlen der FRR auf alle potentiellen Paßbesitzer hoch, so würden mit den vorgeblich recht akzeptablen Ergebnissen der Gesichtserkennung über 5 Millionen Menschen fälschlich zurückgewiesen, wenn man sie realistischerweise in die Gruppe der sporadischen Nutzer einordnet.

Die besonders ganz am Anfang des Feldtests auftretenden signifikant schlechten Erkennungsleistungen gingen dabei erst gar nicht in die Ergebnisse ein. Die Datenbasis verkleinert sich aber noch weiter, denn bei der getesteten Gesichtserkennungssoftware von Cognitec war offenbar auch dadurch nichts mehr zu retten. Kurzerhand wurde hier im laufenden Feldtest eine Umkonfiguration vorgenommen. Zwar waren die geforderten Parameter des Herstellers eingehalten worden, es gab aber "*Systemfehler*". Also mußte mitten im Test ein zweiter Testzyklus begonnen werden. Alles noch mal auf Null. Der Schwellwert, ab welcher eine Verifikation als erfolgreich bewertet wird, wurde bei der Gelegenheit gleich noch von 0,7 auf 0,5 gesenkt.

Die Masterreferenz zur Messung der Erkennungsleistungen blieb dennoch entgegen der Zielsetzung der Studie das jeweilige Systemtemplate des Herstellers. Die Gesichtserkennung von Cognitec in Testzyklus 2 ist hier die einzige Ausnahme. Das Systemtemplate schneidet natürlich gegenüber dem ICAO-Bild bei allen anderen Verfahren hinsichtlich der FRR besser ab. Es ist daher nicht schwer zu erraten, warum bei der Ermittlung der Erkennungsleistungen vom eigentlich zu untersuchenden ICAO-Standard abgewichen wurde. Es ist offenbar jedes Mittel recht, die Ergebnisse zu verschönern.

Dennoch ergab die Auswertung der Ergebnisse noch einiges erstaunliches: Bei allen Systemen wurde ein Teil der Wenignutzer einfach immer zurückgewiesen. Bei der Iriserkennung betraf dies sogar über 50 Personen, bei denen die FRR bei 100 Prozent lag. Diese Teilnehmer hatten sicher wenig zu lachen. In der Studie wird daher vermutet, daß besonders bei der Fingerabdruck- und Iriserkennung das Training für die Merkmalspräsentation *"schwieriger und langwieriger"* sein wird als für die Gesichtserkennung. Bis zum Ende des achtwöchigen Testzyklus ist jedoch ein Sinken der FRR in allen Nutzerklassen zu beobachten. Das läßt doch hoffen. Offenbar auch die Macher der Studie, denn sie behaupten bei der Gelegenheit, daß mit einer *"erhöhten Kooperationsbereitschaft"* seitens der Bürger sowie mit Gewöhnungseffekten gerechnet werden kann. Der Reisende will schließlich schnell in sein Flugzeug und kann sich also ruhig etwas anstrengen.

Die ohnehin dürftigen Ergebnisse der Erkennungsleistungen müssen allerdings mit Vorsicht betrachtet werden, da einige Entscheidungen getroffen wurden, welche die ermittelten Werte noch weiter verschönert haben. In der Studie wird hier von einer gewissen *"Bereinigung"* gesprochen. Zunächst gingen keine Messungen in die FRR ein, die durch *"signifikant variierte Testbedingungen"* beeinflußt worden waren. An den Grenzübergängen müßten demnach also recht homogene Bedingungen herrschen - eine reichlich praxisferne Annahme.

Außerdem präsentierten viele Teilnehmer den falschen Finger (5 bis 7 Prozent) oder das falsche Auge (23 Prozent). Sicher ein Verhalten, das auch in der Praxis oft vorkommen wird. Dieses verschlechtert aber natürlich die Erkennungsleistungen weiter. Also wurde die FRR-Ermittlung sowohl bei dem Fingerabdruck- als auch bei den Iriserkennungssystemen kurzerhand auf Basis eines 1:2-Vergleiches vorgenommen. Das heißt, der Vergleich des aktuell präsentierten Merkmals wurde mit dem primären und dem sekundären Referenzmerkmal (beispielsweise das andere Auge) durchgeführt. Dies senkt wie gewünscht die FRR, führt jedoch gleichzeitig zu einer höheren Falschakzeptanzrate (False Acceptance Rate, FAR).

In die Auswertung gingen außerdem die Ergebnisse der Startphase nicht mit ein. Im Testzyklus 1 war die Dauer dieses sogenannten Teach-Ins immerhin sieben Tage. Die *"signifikant schlechteren Ergebnisse"* dieses Zeitraums wurden für das Ergebnis der FRR komplett weggelassen. Auch im zweiten Testzyklus wurden wieder keine Ergebnisse von ganzen 5 Tagen

Teach-In in die FRR aufgenommen, obgleich die Testteilnehmer mit den Systemen ja bereits vertraut waren und ihnen zusätzlich von Betreuern stets *"Hinweise und Hilfestellungen"* angeboten wurden. Der zukünftige Paßbesitzer kann in der Praxis keine derartigen Trainingsphasen erwarten, schon gar nicht, wenn er zu den ersten Testern im Realszenario gehört. Da winkt dann eher die angekündigte *"intensive Prüfung"* an der Grenze.

Weitere ungelöste Probleme, neben den schon erwähnten Brillen, waren Bärte und Kontaktlinsen. Beispielsweise wurden Voll- oder Teilbartträger von der Cognitec-Software signifikant besser erkannt. Da die Pässe ja 10 Jahre gelten werden, ist anzunehmen, daß die Abnahme eines Bartes zu vermehrten Rückweisungen führen wird. Bei den Brillenträgern zeigte die Gesichtserkennung von Cognitec während des gesamten Tests sehr ausgeprägte Unzulänglichkeiten. 97 Prozent der Personen, die unberechtigt verifiziert wurden, trugen eine Brille. Die Weiterentwicklung des Algorithmus brachte leider auch keine Besserung, das Problem blieb in gleichem Maße vorhanden und ist weiterhin ungelöst.

In den Empfehlungen der Studie heißt es schließlich, eine *"gründliche Untersuchung der Funktionstüchtigkeit, der Erkennungsleistung und der Überwindungssicherheit"* der Verfahren sei angeraten. Dem können wir uns nur nachdrücklich anschließen. Die Aussagekraft der Ergebnisse der Studie ist begrenzt und die Testresultate sind so desaströs, daß ohne einen echten und wirklich umfangreichen Feldtest ein Einsatz der Systeme unverantwortlich erscheint.

Als Hot Fix ist in der neuesten Version des ICAO-Standards die Aufnahme von Templates in die Daten auf dem RFID-Chip vorgesehen (vorerst nur für den *"nationalen oder bilateralen Einsatz"*). Damit sollen die dürftigen Erkennungsleistungen bei den ICAO-Bildern umgangen werden. Für die Gesichtserkennung sollen beim Enrolment manuell diverse Klassifikationsdaten (Bart, hohe Stirn, Augenklappe usw.) erfaßt werden, damit die Herausforderung für die Erkennungssysteme nicht gar zu sportlich ist. Damit ist dann aber die Behauptung, daß bis auf den Fingerabdruck nur Daten erfaßt werden, die ohnehin im Reisepaß vorhanden sind, hinfällig. Die systematische Erfassung derartiger Merkmale öffnet ein komplett neues Problemfeld für den Datenschutz, da somit eine einfache Rasterung beispielsweise für Fahndungszwecke möglich wird.

Praxistauglichkeit

Die Studienergebnisse hinsichtlich der Praxistauglichkeit der getesteten Systeme sprechen eine klare Sprache. Eine Fülle von Detailproblemen sorgte für Frust. Zumindest an dieser Stelle ist die Studie vergleichsweise ehrlich und gibt den Herstellern deutliche Mängellisten mit, die schon sehr deutlich machen, welche Probleme

Merkmal	Cognitec	BDr/NEC	Dermalog	SD Industries
Geschlecht				
Alter				
Ethn. Herkunft				
Ausbildung				
Berufl. Tätigkeit				
Kontaktlinsen				
Brille				
Bart				

Keine Abhängigkeit
Abhängigkeit mit deutlichem Trend
Nicht ermittelbar oder uneinheitliches Verhalten
Kein Betrachtungsobjekt

die Systeme im harten Flughafenalltag plagen werden.

Beim Gesichtserkennungssystem von Cognitec *"bedarf die Benutzeroberfläche dringend einer Überarbeitung. Die jetzige Gestaltung genügt den ästhetischen Ansprüchen der Teilnehmer nicht und unterminiert das Vertrauen in die technische Zuverlässigkeit des Systems. Benutzerführung und Rückmeldung sind nahezu nicht vorhanden."* Obendrein waren etliche Kameras der Cognitec-Gesichtserkennung von Anfang bis Ende der Studie unscharf (die verwendeten Philips-Plaste-Webcams haben keine Mechanik zur Fixierung des Objektivs in einer Fokuseinstellung).

Die beiden Fingerabdrucksysteme *"haben mit Bedenken hinsichtlich Hygiene zu kämpfen"*. Aber nicht nur die Reinigung machte Sorgen, es entstanden auch *"Probleme bei der Positionierung durch die Auflage des Fingers auf den Sensoren. Verschiedene Teilnehmer wußten nicht, wie der Finger aufzulegen war (Höhe und Druck), und einige Frauen mit langen Fingernägeln beschwerten sich über die unbündige Auflage des Dermalog-Gerätes."*

Ein prinzipielles Problem, das bei praktisch allen Systemen auftritt, sind die unterschiedlichen Erfordernisse der Benutzerführung für Viel- und Wenignutzer. Entweder das System ist hinreichend händchenhaltend für Wenignutzer und nervt dadurch Vielnutzer mit langwierigen Anweisungen (*"Teilnehmer empfinden die Stimme auf Dauer als lästig"*). Oder es ist so minimalistisch, daß Vielnutzer schnell durchkommen, es stellt aber Wenignutzer vor verwirrende Rätsel. Für Farbenblinde ist die verwendete Rot/Grün-Ampel für die Ergebnisdarstellung nicht zu gebrauchen.

Im Klartext heißt das, daß die Systeme eigentlich nur unter geduldiger Betreuung durch den Grenzbeamten einzusetzen sind. Eine Verwendung für die "do-it-yourself-Grenzpassage" verbietet sich nicht nur wegen des deutlich erhöhten Risikos von Überwindungsversuchen, sondern auch wegen der mangelnden Bedienbarkeit.

Verarbeitungszeit

Im Rahmen der Studie wurde auch die Verarbeitungszeit für die biometrische Identifikation betrachtet. Zu diesen gemessenen Zeiten kommt jeweils noch die für das Auslesen des RFID-Chips notwendige Zeit hinzu. Die sogenannte Bedienzeit umfaßt dann den kompletten Vorgang vom Auflegen des RF-Token bis zum Verlassen des Geräts. Die gestoppten mittleren Werte liegen hier zwischen 11,1 und 13,3 Sekunden. Nochmal zur Erinnerung: Diese Bedienzeit verlängert sich um weitere 4 bis 5 Sekunden, wenn die SmartCard mit Secure Messaging eingesetzt wird, was dem optimistischsten Szenario für das RFID-Auslesen entspricht (in der Studie wurden die RFID-Chips durch SmartCards substituiert).

Begründet werden die recht langen Bedienzeiten wieder mit den Schwierigkeiten der Teilnehmer, sich an den Geräten richtig zu positionieren, sowie mit dem mangelnden ergonomischen Design und der Gestaltung der Benutzeroberflächen. Während die minimalen und mittleren Verarbeitungszeiten für die biometrische Identifikation in der Größenordnung von 5 bis 10 Sekunden bei allen Systemen noch halbwegs praxistauglich erscheinen, gibt es dramatische Worst-Case-Fälle, bei denen z.B. eine Fingerabdruckerkennung knapp zwei Minuten dauert. Welche Situationen oder Merkmale zu derartigen Schwierigkeiten führten, bleibt aufgrund der fehlenden Anhänge zur Studie leider komplett unklar.

Testpopulation

Ein Feldtest biometrischer Verfahren erfordert besondere Sorgfalt in der Auswahl der Probanden. Deren Zusammensetzung entscheidet, ob die Ergebnisse als repräsentativ betrachtet werden können. Es liegt in der Natur des Menschen, daß seine körperlichen Merkmale dahingehend variieren, wie gut diese ausgeprägt und damit erfaßbar sind. Aufgrund der Tatsache, daß die biometrischen Systeme diese Merkmale nur unzureichend erkennen können, gilt für manche Personen dann auch noch, daß sie häufiger von Rückweisungen betroffen sein werden.

Eine Diskriminierung, gegen die man nichts machen kann - außer stets ein bißchen mehr Zeit einplanen. Beispielsweise bei der Fingerabdruckerkennung ergeben sich Schwierigkeiten bei Personengruppe wie Senioren oder Menschen, deren Fingerkuppen durch Arbeit oder Hobby starker Abnutzung ausgesetzt sind.

In dieser Hinsicht ist die Auswahl der Teilnehmer der Studie zwar der Verbesserung der Erkennungsleistungen förderlich, die Testpersonen repräsentieren jedoch in keiner Weise die Gesamtbevölkerung. Das räumen die Macher der Studie auch ein. Zunächst waren 70 Prozent der Probanden männlich. Dagegen ist im Grunde nichts zu sagen, wäre da nicht das nicht unbedeutende Detail, daß Männer bei den gestesteten Systemen in der Studie wie auch in vorangegangenen Tests durchweg bessere Erkennungsleistungen erzielten. Die unterrepräsentierten Frauen bewirken also eine weitere Beschönigung der Ergebnisse.

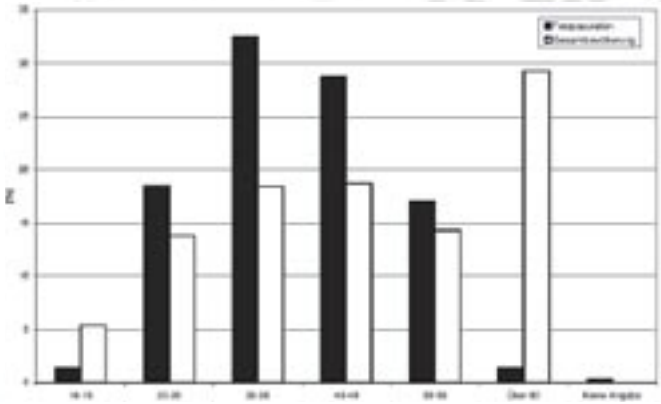
Schlimmer noch die Alterszusammensetzung: Die hinsichtlich der biometrischen Merkmale deutlich schlechter zu erfassenden Menschen ab 60 Jahren tauchen in der Testgruppe kaum auf (lediglich ein Prozent), obwohl sie in der Gesamtbevölkerung einen Anteil von 30 Prozent haben. Betrachtet man nun die einzelnen Nutzerklassen, kann man Zweifel bekommen, ob noch von einem *"Feldtest"* gesprochen werden kann. Besonders die für die Praxis relevanten Wenignutzer waren weniger als 500 Probanden. Das BSI muß also statistisch aussagekräftige Daten wohl mit den unfreiwilligen Betatestern an den Grenzübergängen sammeln.

Was kostet der Überwachungsstaat?

Die Kosten der Biometrie-Einführung werden vom Innenministerium in einer Weise verniedlicht, die stark an vorherige deutsche Technikdesaster erinnert. Auf Anfrage antwortet das BMI, daß die notwendige Hardware im Rahmen von ohnehin anstehenden Ersatzbeschaffungen durchgeführt werde. Das schätzen wir als so nicht haltbar ein.

Wie in der BioP-II-Studie klar dargelegt wird, sind auch nur annähernd praxistaugliche Ergebnisse bei der Gesichtserkennung nur zu erzielen, wenn quasi Laborbedingungen am Grenzübergang geschaffen werden. Um gleichbleibende Lichtverhältnisse und Hintergrundsituationen zu erzeugen, müssen umfangreiche Umbauten durchgeführt werden. Das Gesichtserkennungssystem erfordert einen schnellen Computer, eine Kamera mit brauchbarer Qualität und ein spezielles homogenes Beleuchtungssystem. Schon der Ausfall einer der Ausleuchtungslampen würde den jeweiligen Grenzübergangsschalter außer Gefecht setzen.

Auf der Enrolment-Seite finden sich in der Studie auch diverse Merkwürdigkeiten. Die Fotos für die Gesichtserkennung wurden aufwendig von Experten des Bundeskriminalamtes (BKA) mit einer eigens beschafften digitalen Spiegelreflexkamera im Wert von etwa eintausend Euro erstellt und dann noch mit dem nicht eben preisgünstigen Adobe Photoshop nachbearbeitet. Das ganze klingt so dermaßen unrealistisch im Praxisbezug, daß sich die Frage stellt, warum die Notwendigkeit eines solchen Vorgehens nicht



Das Diagramm zeigt die Altersstruktur der Testteilnehmer an der BioP2-Studie im Vergleich zur Verteilung in der Gesamtbevölkerung Deutschlands.

schon als Disqualifikationskriterium ausreichte. Wenn man das Verfahren auf die Meldestellen extrapoliert, kommen selbst bei Substitution der BKA-Experten durch den Fotografen an der Ecke erhebliche Summen für Software-Lizenzen, Schulungen und Personalaufwand für die zusätzlichen Bearbeitungsschritte zusammen. Wenn jedes Bild nicht nur eingescannt, sondern auch noch nachbearbeitet und (wie in der aktuellen ICAO-Spezifikation vorgesehen) nach verschiedenen Kriterien klassifiziert werden muß, wird es kaum ohne zusätzliches Personal, zusätzliche Computer usw. abgehen.

Die Übermittlung der Daten von den Meldestellen zur Bundesdruckerei soll mit Hilfe der für deutsche Regierungsverschlüsselung standardisierten SINA-Boxen erfolgen (die rein zufällig die Firma Secunet herstellt, die auch die BioP-II-Studie durchgeführt hat). Inwieweit zusätzlich zu den bisher in den Meldestellen vorhandenen SINA-Boxen neue beschafft werden müssen, ist derzeit noch unklar.

Bei Einführung von Fingerabdrücken ist für jede Meldestelle und jeden Grenzübergangsschalter ein schneller Computer mit zusätzlicher Sicherheitshardware (sicheres Speichermodul, SINA-Box für Certificate Updates etc.) für die Extended Access Control, kostenpflichtigem Betriebssystem (freilich alles Windows 2000 Professional) und weiterem Zubehör zu beschaffen. Hinzu kommen natürlich die Kosten für den Fingerabdruck-Scanner. Der Verschleiß der Fingerabdruckscanner ist derzeit unklar. Wie jeder Gegenstand, der nicht aus solidem Metall besteht und einige tausend Mal am Tag von Menschen angefaßt wird, dürfte hier deutlicher Verschleiß anzunehmen sein. In der Studie wird von einem Grauschleier auf den Fingerabdruckbildern der Bundesdruckerei-Geräte nach 4 Monaten berichtet, und das, obwohl die Scanner mehrmals täglich gereinigt wurden. Wir können also davon ausgehen, daß die Scanner an den Flughäfen nur eine recht begrenzte Haltbarkeitsdauer haben werden. Während der Studie wurden im Schnitt etwa 15.000 Sensorbenutzungen pro System durchgeführt, eine Zahl die an einem Flughafen in nur einigen Tagen zustandekommt.

Wenn ca. 6000 Meldestellen im Schnitt mit je vier Gerätesätzen für das Enrolment ausgestattet werden, an den 419 Grenzübergangsstellen im Schnitt je 15 Erfassungssysteme aufgestellt werden (konservative Annahme) und man ca. 5000 Euro pro System ansetzt (ebenfalls äußerst konservativ), ergeben sich alleine für die Hardware Investitionskosten von mindestens 150 Millionen Euro. Hinzu kommen Wartungskosten, Ersatzbeschaffungen, Umbauten für die Gesichtserkennung und die Kompensation der längeren Abfertigungszeiten, zusätzliches Personal, Ausbildungskosten etc. pp. Die Weiterentwicklung und die Anpassung der biometrischen Systeme müssen ebenfalls in eine seriöse Kalkukation eingehen. Hier sollte auch der RF-Chip in Betracht gezogen werden, dessen Lebensdauer für zehn Jahre ohnehin fraglich ist. Die geplante Ausweitung der biometrischen Technik auf den Personalausweis würde zusätzlich auch die Ausstattung mit Geräten für die Polizei berücksichtigen müssen. Alles in allem war die Einführung der Autobahn-Maut dagegen ein Schnäppchen.

Folgerichtig nehmen die Autoren der Studie auch Abstand davon, sich zu den Kosten zu äußern (welcher Beamte widerspricht schon gern Otto Schily). Wie selbstverständlich wird die marode Bundesdruckerei die Herstellung der neuen Pässe übernehmen. Der Rahmenvertrag, den die Bundesregierung alle drei Jahre verlängert, sichert dem vormals dem Bund gehörenden Privatunternehmen den lukrativen Auftrag. Eine EU-weite Ausschreibung des krisensicheren Geschäfts fand nicht statt. Trotz professioneller Produktpräsentation im eigens errichteten Showroom der Bundesdruckerei werden Fragen nach den Kosten für Hard- und Software auch dort nicht beantwortet. Zu den Gesamtkosten der Einführung des ePasses wollte Schily natürlich noch immer keine Angaben machen. Die erhöhte Paßgebühr soll aber wenigstens die jährlichen Betriebskosten für die biometrische Erfassung bei der Neuausstellung decken. Die einmaligen Kosten für die Geräte sollen 2006 im Haushalt der Bundespolizei enthalten sein. Aber auch über deren Höhe schweigt sich Schily aus.

Annex G of ICAO MRTD Specs

Der Annex G der ICAO-Spezifikation für maschinenlesbare Reisedokumente (MRTD) faßt wunderbar kompakt die Schwächen des Systems zusammen. Die an der Erstellung des Standards beteiligten Fachleute wollten wohl ihre Reputation nicht leichtfertig riskieren und haben deshalb die wesentlichen Angriffszenarien relativ ungeschminkt dargestellt. Der Annex liest sich ein bißchen wie "wir wissen, daß es nicht funktionieren wird, aber wir brauchten das Geld".

Technical Report
PKI for Machine Readable Travel Documents offering ICC read-only access
Release : 1.1
Date : October 01, 2004
Annex G – PKI and Security Threats

G.1 Key Management

G.1.1 Country Signing CA and Document Signer Keys

To protect the private keys it is RECOMMENDED to use secure hardware devices for signature generation (Secure Signature Creation Device – SSCD), i.e. the SSCD generates new key pairs, stores and destroys (after expiration) the corresponding private key securely. To protect against attacks on the SSCD including Side-Channel Attacks (e.g. timing, power consumption, EM emission, fault injection) and attacks against the random number generator it is RECOMMENDED to use SSCDs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

When distributing self-signed Country Signing CA Certificates by diplomatic means extreme care must be taken to prevent insertion of a rogue Country Signing CA Certificate. Furthermore, it is RECOMMENDED that States store the received Country Singing CA Certificates in secure hardware devices (Card Acceptor Device – CAD) accessible by the reader devices in a secure manner. To protect against attacks on the CAD, it is RECOMMENDED to use CADs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

G.1.2 Active Authentication Keys

It is RECOMMENDED to generate key pairs for Active Authentication on the chip of the MRTD. As the private key is stored on the chip in secure memory, and the chip hardware has to resist attacks for the whole validity period of the MRTD, it is RECOMMENDED to use chips that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

The available chip technology influences the maximum key length of keys used inside the chip for Active Authentication. Many chips currently do not support key lengths that exceed a security level of 80 bits, which was the reason for choosing this value as recommended minimum. This is a relatively low level of security compared to their validity period of the MRTD. Therefore, it is RECOMMENDED to use longer keys, if supported by the chip.

States that make use of the Active Authentication mechanism to validate a foreign MRTD should also be aware that no revocation mechanism has been specified for compromised Active Authentication keys.

G.1.3 Denial of Service Attacks

Denial of Service Attacks have to be considered when States rely on the Directory for distributi-

on of Document Signer Certificates and CRLs. Those attacks cannot be prevented, it is therefore RECOMMENDED that the Document Signer Certificate required to validate the Document Security Object is also included in the Document Security Object itself. Receiving States SHOULD make use of a provided Document Signer Certificate.

To distribute CRLs bilaterally it is RECOMMENDED to establish multiple channels (e.g. internet, phone, fax, mail, etc.) with other States and to confirm reception of received CRLs.

G.2 Cloning Threats

Compared to paper based MRTDs copying the signed data stored on the RF-Chip is easily possible in general. States concerned about the possibility of having data of their citizens copied to another chip SHOULD implement Active Authentication that prevents this to a certain extent.

G.2.1 Passive Authentication

Passive Authentication does not prevent copying the data stored on the chip. As a consequence, it is possible to substitute the chip of a MRTD against a fake chip storing the data copied from the chip of another MRTD. Receiving States SHOULD verify that the data read from the chip indeed belongs to the presented MRTD. This can be done by comparing DG1 stored on the chip to the MRZ printed on the datapage of the MRTD. If DG1 and the MRZ compare and the document security object is valid and the presented MRTD has not been tampered with (is not counterfeited), then the MRTD and the data stored on the chip can be considered to be belonging together.

G.2.2 Active Authentication

Active Authentication makes chip substitution more difficult, but not impossible: The MRTD presented by the attacker to the inspection system could be equipped with a special chip. This chip works as proxy for a genuine chip located in a remote place: the chip communicates with the attacker, the attacker communicates with another attacker, and the other attacker (temporarily) gains access to the genuine chip. The inspection system is not able to notice that it has authenticated a remote chip instead of the presented chip. This attack is called Grandmaster Chess Attack.

G.3 Privacy Threats
G.3.1 No Access Control

The use of proximity chips already minimizes privacy risks as reader devices have to be very close to the chips, therefore skimming is not considered to be a serious threat. However eavesdropping on an existing communication between a chip and a reader is possible in a larger distance. States wishing to address this threat SHOULD implement Basic Access Control.

G.3.2 Basic Access Control

The Basic Access Keys used to authenticate the reader and to setup session keys to encrypt the communication between chip and reader are generated from the 9 digit Document-Number, the Date- of-Birth, and the Date-of-Expiry. Thus, the entropy of the keys is relatively low. For a 10 year valid MRTD the entropy is 56 bits at maximum. With additional knowledge (e.g. approximate age of the bearer, or relations between Document-Number and Date-of-Expiry) the entropy is lowered even more. Due to the relatively low entropy, in principle an attacker might record an encrypted session, calculate the Basic Access Keys by Brute-Force from the authentication, derive the session keys and decrypt the recorded session. However this still requires a considerable effort compared to obtaining the data from other sources.

G.3.3 Active Authentication (Data Traces)

In the challenge-response protocol used for Active Authentication, the chip signs a bit string that has been chosen more or less randomly by the inspection system. If a receiving State uses the current date, time, and location to generate this bit string in an unpredictable but verifiable

way (e.g. using secure hardware), a third party can be convinced afterwards that the signer was at a certain date and time at a certain location.

G.4 Cryptographic Threats

The recommended minimal key lengths have been chosen so that breaking those keys requires a certain (assumed) effort, independent of the chosen signature algorithm:

Type of Key	Level of Security
Country Signing CA	128 bits
Document Signer	112 bits
Active Authentication	80 bits

G.2.1 Passive Authentication

Passive Authentication does not prevent copying the data stored on the chip. As a consequence, it is possible to substitute the chip of a MRTD against a fake chip storing the data copied from the chip of another MRTD. Receiving States SHOULD verify that the data read from the chip indeed belongs to the presented MRTD. This can be done by comparing DG1 stored on the chip to the MRZ printed on the datapage of the MRTD. If DG1 and the MRZ compare and the document security object is valid and the presented MRTD has not been tampered with (is not counterfeited), then the MRTD and the data stored on the chip can be considered to be belonging together.

G.4.1 Mathematical advances and non-standard computing

According to Moore's Law computation power doubles every 18 month. However, the security of the signature algorithm is not only influenced by computing power, advances in mathematics (cryptanalysis) and the availability of new non-standard computation methods (e.g. quantum computers) also have to be taken into account.

Due to the long validity periods of keys it is very difficult to make predictions about mathematical advances and the availability of non-standard computing devices. Therefore, the recommendations for key lengths are mainly based on the extrapolated computing power. States SHOULD review the key lengths for their own but also for received MRTDs often for reasons mentioned above.

Generating key pairs of a special form may improve the overall performance of the signature algorithm, but may also be exploited for cryptanalysis in the future. Therefore, such special key pairs SHOULD be avoided.

G.4.2 Hash Collisions

While it is computationally infeasible to find another message that produces the same hash value as a given message, it is considerably easier to find two message that produce the same hash value. This is called the Birthday Paradoxon.

In general all messages to be signed are produced by the Document Signer itself. Therefore, finding hash collisions does not help an attacker very much. However, if photographs provided by the applicant in digital form are accepted by the Document Signer without additional randomized modification, the following attack is possible:

• Two persons share their digital photos. Then they repeatedly flip a small number of bits at randomly in each photo until two photos produce the same hash value.

• Both persons apply for a new MRTD using the manipulated photo. Either person can now use the MRTD of the other person provided that it is possible to replace the digital photo in the chip (e.g. by chip substitution).

The hash function SHA-1 only provides 80 bits of security against hash collisions. Thus, it is considerably easier to find a hash collision than to break the Document Signer Key which provides 112 bits of security. Therefore, whenever hash collisions are of concern (e.g. as described above), it is RECOMMENDED not to use SHA-1 as hash function.

Eigentums- und Beteiligungsverhältnisse der Bundesdruckerei

Conrad Brean <ds@ccc.de>

Eine Druckerei für Ausweise sollte eigentlich gewissen Anforderungen an Seriosität genügen, am besten staatseigen sein oder doch wenigstens in soliden Händen. Die Bundesdruckerei ist durch eine desaströse Privatisierung zu einem Objekt windiger Finanzjongleure geworden und dümpelt nun in unklaren Besitzverhältnissen vor sich hin. Hier der Versuch eines Überblicks.

Seit ihrer Gründung 1879 als „Reichsdruckerei" befand sich die Behörde im Staatsbesitz. Nachdem sie 1945 mit „Staatsdruckerei" und durch die Übernahme in die Bundesverwaltung 1951 mit „Bundesdruckerei" zwei Umbenennungen erfuhr, begann für sie nach der Wiedervereinigung Deutschlands der Weg in die Privatwirtschaft.

Auf Beschluß des Bundeskabinetts in der 12. Legislaturperiode erfolgte am 1. Juli 1994 die Umwandlung von einer Behörde in eine privatrechtliche GmbH im Bundesbesitz. Jedoch wurde die Veräußerung der Bundesanteile an der Staatsdruckerei seitens der Regierung Kohl auf 49 Prozent begrenzt. Finanzminister Eichel (SPD) trennte sich später von den restlichen 51 Prozent. Um den Bundesanteil möglichst gewinnbringend zu veräußern, beauftragte das Bundesfinanzministerium im Dezember 1999 das Frankfurter Bankhaus Metzler.

Im November 2000 verkaufte der Bundesfinanzminister die Bundesdruckerei für eine Milliarde Euro an die Beteiligungsgesellschaft "Apax Partners & Co.". Apax Fonds waren bereits damals in der Bundesrepublik unter anderem an der Autobahn Tank & Rast AG beteiligt (deren CEO und COO ab 1991 bei Elf Aquitaine beschäftigt waren), die 1998 privatisiert wurde.

Der Kaufpreis von einer Milliarde Euro galt schon zum Kaufzeitpunkt als deutlich überhöht. Er wurde jedoch nicht vollständig bezahlt: Ein Anteil von 230 Millionen Euro stundete der Bund für zehn Jahre, weitere ca. 450 Millionen Euro gab die Hessische

Landesbank (HeLaBa) als Darlehen. Tilgung und Zinsaufwand für dieses Darlehen betragen jährlich 50 bis 75 Mio. Euro - Summen, die der Konzern für mehrere Jahre nicht aufbringen konnte.

In der Folge wurden die Bundesdruckerei GmbH, die Bundesdruckerei International Services GmbH, die ORGA Kartensysteme GmbH, die Holographic Systems München GmbH, die Maurer Electronics GmbH, die D-Trust GmbH und die INCO SP.Z.o.o. unter dem Dach der authentos GmbH zusammengefaßSteuert, die als Holding fungiert und ihren Sitz in der Berliner Zentrale der Bundesdruckerei in der Oranienstraße 91 hat.

Im Februar 2001 erwarb die authentos-Gruppe das britische Unternehmen Security Printing and Systems Limited und stieg dadurch mit einer Jahresproduktion von 40 Millionen Pässen und Führerscheinen zum weltgrößten Hersteller dieser Dokumente auf.

Im August 2002 wurde die Zahlungsunfähigkeit von authentos abgewendet, nachdem sich Gesellschafter, Kreditgeber und der Bund auf einen Zahlungsverzicht geeinigt hatten.

September 2002 wurde für den symbolischen Kaufpreis von einem Euro die authentos-Gruppe an zwei Zwischenerwerber übertragen: die Berliner JVVG Neununddreißigste Vermögensverwaltungsgesellschaft (94 Prozent) und die Dinos Vermögensverwaltung in Heidelberg (sechs Prozent).

Die Gesellschaft sollte saniert und dann wieder verkauft werden. 300 der 1650 Arbeitsplätze waren akut in Gefahr. Roland Berger erstellte ein Sanierungskonzept. Seit 2002 gab es einige Bewegung in der Führungsebene der Bundesdruckerei.

Die Anwaltssozietät Clifford Chance Pünder ist mittelbarer Mehrheitsgesellschafter der authentos. Sie vertreten vermutlich die Interessen der Neununddreißigsten Vermögensverwaltungsgesellschaft und damit die Verbindlichkeiten gegenüber der Hessischen Landesbank und gelten als Ansprechpartner für mögliche Kaufinteressenten.

Vorsitzender der Geschäftsführung der authentos GmbH und der Bundesdruckerei GmbH war bis 10. Februar 2004 Dr. Ulrich Wöhr. Seither sind der ehemalige Infineon-Manager Ulrich Hamann und Klaus-Dieter Langen Geschäftsführer der authentos GmbH. Diese sind zusammen mit Joachim Eilert ebenfalls Geschäftsführer der Bundesdruckerei GmbH.

Aufsichtsratsvorsitzender der authentos-Gruppe war Prof. Manfred Lahnstein, Mitglied der Trilateralen Kommission und ehemaliges Aufsichtsratsmitglied der Bertelsmann AG. Mittlerweile ist Heinz-Günter Gondert Aufsichtsratsvorsitzender. Er ist Rechtsanwalt und Partner bei der Frankfurter Anwaltssozietät Clifford Chance sowie Steuerberater und Wirtschaftsprüfer bei der Frankfurter PVW GmbH.

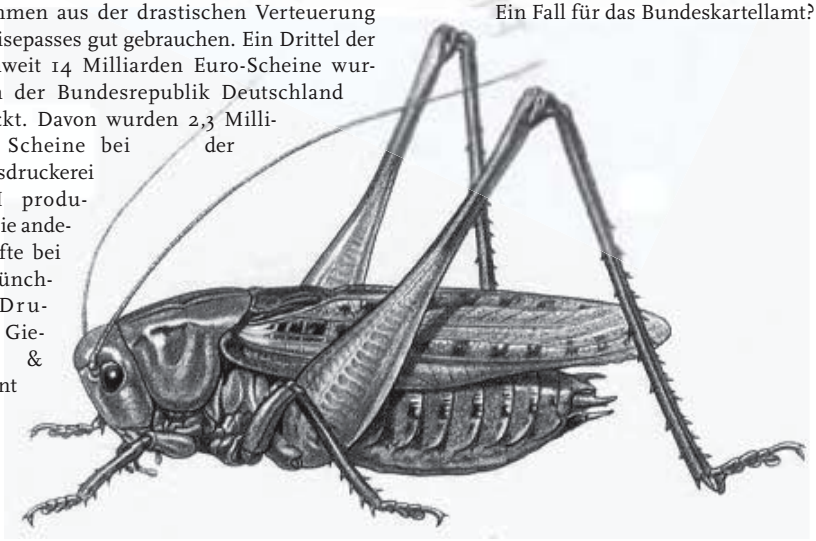
Weitere Aufsichtsratsmitglieder sind, neben den Arbeitnehmervertretern, der Rechtsanwalt Dieter Ostheimer, der Unternehmensberater Dirk Pfeil, der Rechtsanwalt Dr. Wolfgang Scholz (ebenfalls Clifford Chance), Ministerialrat Dr. Wolf-Dieter Schmidberger (Bundesministerium der Finanzen) sowie Dr. Norbert Schraad von der Landesbank Hessen-Thüringen (Stand: Juni 2005).

Die Bundesdruckerei kann die zusätzlichen Einnahmen aus der drastischen Verteuerung des Reisepasses gut gebrauchen. Ein Drittel der europaweit 14 Milliarden Euro-Scheine wurden in der Bundesrepublik Deutschland gedruckt. Davon wurden 2,3 Milliarden Scheine bei der Bundesdruckerei GmbH produziert, die andere Hälfte bei der Münchner Druckerei Giesecke & Devrient GmbH. Dies war im Jahr 2002 abgeschlossen; in der Folge reduzierte sich das Auftragsvolumen der Bundesdruckerei auf die Produktion von weniger als 750 Millionen nachzudruckenden Scheinen. Da sich an der Produktion der Reisepässe kaum etwas ändern wird, können sich Bundesdruckerei und Komponentenhersteller die Mehrkosten aufteilen und dadurch die Konzernbilanzen aufwerten.

Interessant am Verhältnis zur Giesecke & Devrient GmbH ist neben der traditionellen Aufteilung der Druckaufträge auch die personelle Dimension. So wurde Matthias Merx von GDM am 01.10.2004 Leiter der Produktion der Bundesdruckerei, am Ende desselben Monats stieß überraschend Willi Berchtold zur - der bis dahin Vorsitzender der Geschäftsführung von Giesecke & Devrient war - und am 01.01.2005 wurde GDM-Vertriebschef Jörg Baumgartl neuer Leiter Technik, Marketing, Consult und Entwicklung bei der Bundesdruckerei.

Ebenfalls brisant: auch beim sogenannten "Golden Reader Tool", dem Programm zum Auslesen der Tags bei der Grenzkontrolle, wirkten beide Unternehmen mit (neben der Secunet Security Networks AG, dem Bundeskriminalamt und der cv cryptovision GmbH).

Ein Fall für das Bundeskartellamt?



Besonders intensive Prüfung

von Frank Rosengart <frank@rosengart.de> und Constanze Kurz <46halbe@weltregierung.de>

Die Redaktion "Die Datenschleuder." hat anläßlich der bevorstehenden Einführung der Reisepässe Mitarbeiter der "ePass-Hotline" der Bundesregierung um die Beantwortung einiger offener Fragen gebeten. Es antwortete nach nur wenigen Wochen die Pressestelle des BMI. Mehr als ein paar Copy&Paste-Textblöcke konnte sie sich nicht abringen.

1. Frage:

Obwohl es bisher keine verabschiedete ICAO-Spezifikation für den Zugriff auf die erweiterten biometrischen Daten (Finger, Iris) gibt, wird mit der Einführung der ersten Stufe bereits begonnen. Was passiert, wenn es keine zufriedenstellende Lösung gibt? Wird dann die Datenschutz-unfreundliche Variante (Vollzugriff auf alle Felder) gewählt? Oder wird der ePass in der ersten Stufe belassen?

Antwort BMI:

Internationale Standards für die Pässe werden durch die ICAO definiert. Die EU hat sich bei Erlaß der technischen Anhänge zur EG-Verordnung über Normen für Sicherheitsmerkmale und biometrische Daten in den von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten daran orientiert. Die Standards der ICAO wurden insbesondere dort von der EU fortgeschrieben, wo die europäischen Grundsätze des Datenschutzes ein höheres Sicherheitsniveau erforderlich machen, so z.B. im Falle der Bestimmung der kryptographischen Verschlüsselung der Fingerabdrucksdaten (sogenannte "Extended Access Control").

Gemäß der EG-Verordnung sind als erstes biometrisches Merkmal das Gesichtsbild und als zweites Merkmal Fingerabdrücke zu speichern. In den ab November 2005 ausgestellten deutschen Reisepässen wird zunächst nur das Gesichtsbild, das auch als Lichtbild im Paß abgedruckt ist, im RF-Chip gespeichert. Für das Jahr 2007 ist vorgesehen, auch die Fingerabdrücke im RF-Chip abzuspeichern. Die Speicherung der biometrischen Merkmale erfolgt in einem zertifizierten Sicherheitschip mit kryptographischem Koprozessor und kontaktlosem Interface (RF-Chip), der in den Reisepass integriert wird.

Ein unbemerktes Auslesen der biometrischen Daten wird durch einen effektiven Zugriffsschutz ausgeschlossen. Datenschutz und Datensicherheit sind damit gewährleistet. In der ersten Phase, also bei Integration des digitalen Gesichtsbilds in den ePass, wird der Zugang zu den Bild-Daten im Chip nur über das vorherige optische Auslesen der maschinenlesbaren Zone möglich sein.

Für die zweite Phase, d.h. nach Integration der Fingerabdrücke, wird ein zusätzliches kryptographisches Protokoll für den Zugriff auf diese Daten verwendet. Durch die Integration von kryptographischen Sicherheitsmerkmalen, wie z.B. einer digitalen Signatur über die gespeicherten Daten, wird das Sicherheitsniveau der Reisepässe bedeutend erhöht. Gleichzeitig wird über kryptographische Mechanismen das unberechtigte Auslesen bzw. das Abhören der übertragenen Daten der RF-Chips wirkungsvoll verhindert (Basic Access Control und Extended Access Control). Wir arbeiten nicht mit "zufriedenstellenden Lösungen", sondern wir realisieren sichere und technisch perfekte Lösungen.

Kommentar der Redaktion:

Schade nur, daß noch niemand diese Lösungen im Detail kennt. "Technisch perfekte" Sys-

teme hat die Bundesregierung ja schon bei der LKW-Maut und bei der Bundesanstalt für Arbeit realisiert. Was bedeutet also "technisch perfekt"? In jedem Fall bedeutet es leider nicht zwingend "datenschutzfreundlich". Die Frage danach, welche Anforderungen seitens der Bundesregierung an die Technik gestellt werden, bleibt unbeantwortet. Ebenso die Frage, was sie machen wollen, wenn es mit ihrer geplanten PKI nicht klappen sollte. Eine globale PKI gilt bisher schließlich als illusorisch.

2. Frage:

Welchen Ländern außerhalb Europas wird Deutschland die erweiterten biometrischen Daten anvertrauen und was genau sind die Kriterien für einen Lesezugriff auf die Rohdaten?

Antwort:

Die gespeicherten Daten zum Gesichtsbild können weltweit unter den in Antwort 1) genannten Voraussetzungen gelesen werden. Die Daten der Fingerabdrücke sind durch ein zusätzliches kryptographisches Protokoll geschützt. Welche Länder außerhalb der EU auf die Daten der Fingerabdrücke zugreifen, kann deshalb vom ausstellenden Staat geregelt werden.

Kommentar der Redaktion:

Welche Länder außerhalb der EU Zugriff auf die Daten bekommen, war aber grade die Frage. Offensichtlich gibt es hier noch keine Antworten. Alptraum der Datenschützer dürfte ein Zugriff auf die Daten durch Länder wie z.B. die USA sein, wo die gesetzlichen Regelungen oder die übliche Praxis stark von den EU-Standards abweichen. Außerhalb der EU sind die Datenschutzbestimmungen meist weit weniger restriktiv als hierzulande. Biometrischen Datensammlungen ohne jegliche zeitliche Beschränkungen stünde in vielen dieser Länder nichts entgegen.

3. Frage:

Warum sollte der ePass in Deutschland die Hälfte bzw. ein Drittel von dem kosten, was vergleichbare Pässe im Ausland kosten (Deutschland: 59 Euro, Schweiz: 250 SFr)? Wo kann ich nachlesen, wie hoch die jeweiligen Kosten für das Enrolment, den Paß selbst, die Geräte an den Grenzen und für den Betrieb der Infrastruktur (CA etc.) sind? Wie aufwendig ist die Schulung des Personals in den Meldestellen?

Antwort:

Um Ihre Annahmen richtigzustellen, weise ich auf folgendes hin: Bei der Gebührenbemessung wurde darauf geachtet, daß sich Deutschland auch künftig im unteren Bereich vergleichbarer europäischer sowie internationaler Länder befindet. Sämtliche technischen Anforderungen auf europäischer und internationaler Ebene, Datenschutz und -sicherheit, wurden und werden selbstverständlich berücksichtigt.

Die Gebühren setzen sich zusammen aus den Produktionskosten des Passes (Paßbuch, die Herstellung und Integration der Chips sowie das Speichern der biometrischen Merkmale auf dem Chip), den Kosten der zur Erfassung und Qualitätssicherung der biometrischen Merkmale notwendigen Ausstattung in den Paßbehörden (QS-Sicherung der Lichtbilder, Hard- und Software zur Erfassung und QS der Fingerabdruckdaten, ePass-Lesegeräte), den Schulungskosten für die Mitarbeiter in den Paßbehörden sowie der Verwaltungsgebühr.

Die Lesegeräte an den 419 Grenzübergangsstellen werden im Rahmen von Ersatzbeschaffungen erneuert, die unabhängig von der Einführung des ePass sind. Diese Geräte verfügen auch über eine Funktion zum Auslesen von digital gespeicherten Fotographien auf RF-Chips. Bei der Ausstattung mit Lesegeräten entstehen keine zusätzliche Kosten.

Die Änderungen, die sich für die Paßbehörden zum 1. November 2005 ergeben, sind gegenüber dem derzeitigen Verfahren minimal. Daher ist nur ein geringer Schulungsaufwand notwendig.

Für die Einführung der 2. Stufe (Integration der Fingerabdrücke in den Chip) zum 1. März 2007 werden die Mitarbeiter in den Paßbehörden im Zuge des Rollouts der Hard- und Software zur Erfassung und Qualitätsprüfung der Fingerabdruckdaten geschult werden.

Kommentar der Redaktion:

Das würde ja bedeuten, daß entweder die Technologie in Deutschland um ein Vielfaches preiswerter ist als in anderen Staaten oder daß diese Staaten ihre Bürger "abzocken". Beides ist natürlich nicht der Fall. Vielmehr scheut sich das BMI schlicht, die Gesamtkosten zu beziffern.

Daß die Lesegeräte an den Grenzen im Rahmen von "Ersatzbeschaffungen" erneuert werden, würde entweder bedeuten, daß auf eine automatisierte Gesichtsbild- und Fingerabdruckverifikation verzichtet wird. Vielleicht wird aber absichtlich zu den wirklich anfallenden Kosten geschwiegen wird. Die anfallenden Ersatzbeschaffungskosten werden wohl im Etat der Bundespolizei versteckt.

Die bisherigen Lesegeräte für die MRZ in Reisedokumenten kosten je ca. 1500 Euro. Ein automatisches Gesichtsbild- und Fingerabdrucksystem dürfte pro Gerät ein Vielfaches kosten. Der TAB-Bericht spricht übrigens von Gesamtkosten in Höhe von einmalig 670 Millionen Euro und jährlich etwa 610 Millionen Euro an laufenden Kosten.

Daß die Kosten für die Schulung des Personal nur gering seien, widerspricht den Ergebnissen der BioP-II-Studie. Für den der Studie zugrundeliegenden Feldtest waren nämlich umfangreiche Personalschulungen nötig. Außerdem mußten kostspielige Umbauten im Umfeld der Gesichtserkennungssysteme vorgenommen werden, um deren Anforderungen an die Lichtverhältnisse zu erfüllen. Auch solche Kosten gehören zu einer seriösen Kalkulation.

4. Frage:

Auf Ihrer Internetseite steht: "Für Fingerabdrücke als zweites Merkmal sprach die hohe Praxistauglichkeit der hierzu entwickelten Abnahme- und Erkennungssysteme." Welche Tests im realen Betrieb gibt es dazu und wo kann man diese Ergebnisse nachlesen? Wie wird der einfachen Fälschbarkeit von Fingerabdrücken sowohl beim Enrolment als auch bei der Kontrolle begegnet? Mit welchen Maßnahmen müssen Personen rechnen, deren Fingerabdruck nicht als der gespeicherte erkannt wird?

Antwort:

a) Die Ergebnisse der Labor- und Feldtests der Studie BioP II werden vom BSI veröffentlicht (www.bsi.bund.de).

b) und c) Die Aufnahme biometrischer Merkmale in Reisepässen dient dazu, die sichere Identifizierung von Personen durch das Grenzkontrollpersonal zu "unterstützen". Davon unabhängig kontrolliert die Bundespolizei stets nach Schengenstandard.

Kommentar der Redaktion:

Die BioP-II-Studie wurde zwischenzeitlich tatsächlich veröffentlicht - und nach kürzester Zeit wieder von der BSI-Webseite entfernt. Einige Tage später wurde eine leicht veränderte Version veröffentlich. Weiterhin geheimgehalten wird allerdings die Studie zur Überwindungssicherheit der biometrischen Systeme. Auch gibt die Pressestelle zu der Frage nach der einfachen Fälschbarkeit keinen Kommentar ab. Damit ist eine öffentliche Diskussion über den Sicherheitsgewinn unmöglich.

5. Frage:

Worauf beruht die Annahme, daß Systeme zur Gesichtsbild-Verifikation ausgereift und vor allem praxistauglich sind? Die BioFace-Studie des BSI kommt dabei ausdrücklich nicht zu dem Ergebnis, daß die getesten Verfahren praxistauglich sind (vgl. http://www.heise.de/newsticker/meldung/41289)

Antwort:

Die Studie BioP II weist für den Bereich der Gesichtserkennung erheblich bessere Erkennungswerte auf. Diese Ergebnisse konnten mittlerweile durch neue Algorithmen nochmals verbessert werden. Die Nutzungsqualität des Gesamtsystems wurde damit deutlich erhöht.

Kommentar der Redaktion:

Tatsächlich hat sich die Erkennungsleistung im Laufe der Zeit verbessert, wenn auch nicht "erheblich". Von einem "technisch perfekten System" sind aber alle Verfahren laut der Studie meilenweit entfernt. Eine der Hauptforderungen der BioP-II-Studie ist es, daß die Benutzbarkeit der Systeme deutlich verbessert werden sollte. Praxistauglich sind die Verfahren also noch immer nicht.

6. Frage:

Wird der Paß kostenlos umgetauscht, wenn der RFID-Chip zum Beispiel durch mechanische Belastung unbrauchbar geworden ist?

Antwort:

Ein Paß mit unbrauchbarem/defektem RF-Chip ist weiter ein gültiges Reisedokument.

Kommentar der Redaktion:

Da sind wir ja beruhigt. Daß der Chip nämlich zehn Jahre hält, ist nicht allzu wahrscheinlich.

7. Frage:

Welchen Nutzen hat der elektronische Paß, wenn jeder potentielle Terrorist seinen Chip im Paß unbrauchbar macht?

Antwort:

Die Aufnahme biometrischer Merkmale in Reisepässen dient dazu, die sichere Identifizierung von Personen durch das Grenzkontrollpersonal zu "unterstützen". Davon unabhängig kontrolliert die Bundespolizei stets nach Schengenstandard. Wenn der Chip "unbrauchbar" ist, wird mit den klassischen Verfahren die Identität geprüft, wobei dies sicher Anlaß zu besonders intensiver Prüfung wäre.

Kommentar der Redaktion:

Eben darum sollte es die Möglichkeit geben, defekte Pässe umtauschen zu können. Wer möchte schon ständig einer "besonders intensiven Prüfung" bei der Grenzkontrolle ausgesetzt sein, nur weil der Chip versagt? Und möglicherweise wird das gar nicht so selten der Fall sein. Wie wird wohl eine "besonders intensive Prüfung" aussehen, die über den Vergleich von Foto, Augenfarbe und Körpergröße hinausgeht?

Die Frage nach dem Mehr an Sicherheit durch den Chip bleibt natürlich unbeantwortet. Spannend wird, wieviel zusätzliche Arbeit sich das Grenzkontrollpersonal aufhalsen lassen wird, ehe es protestiert gegen die praxisuntaugliche Technik oder aber schlicht durchwinkt. Jörg Radek von der Gewerkschaft der Polizei äußerte bereits seinen Ummut über den zeitlichen Mehraufwand an den Grenzen.

8. Frage:

Können Sie eine gesundheitliche Gefährdung von Grenzbeamten vollständig ausschließen, wenn diese tagtäglich der Funkstrahlung, die ja auch gepulst moduliert ist, ausgesetzt sind? Durch welche Studie wird das belegt, welche Geräte sind auf ihre Abstrahlung hin getestet worden?

Antwort:

Die gesetzlich vorgegebenen Richtwerte für den Strahlenschutz werden von allen im Einsatz befindlichen RFID-Systemen eingehalten.

Kommentar der Redaktion:

Eine konkrete Studie oder Meßwerte gibt es also nicht. Davon abgesehen sind noch keinerlei RFID-Systeme "im Einsatz befindlich", höchstens im Labor- oder Testbetrieb. Die Beschaffung der Geräte beginnt gerade erst.

9. Frage:

Außer Herrn Schily ist eigentlich allen Behörden die Tatsache bekannt, daß wirkliche Paßfälschungen nicht praxisrelevant sind - vielmehr sind Schwachstellen beim Personal in den Meldestellen das Problem. Warum hat Deutschland auf EU-Ebene die elektronischen Pässe durchgepeitscht, obwohl die Technik alles andere als ausgereift ist, die Kosten unklar sind und zum derzeitigen Stand kein Sicherheitsgewinn bringen?

Antwort:

Paßfälschungen sind entgegen Ihrer Annahme durchaus praxisrelevant. Zwar verfügt Deutschland schon heute über einen der fälschungssichersten Dokumententypen der Welt, doch bereits innerhalb der Europäischen Union existiert ein starkes Gefälle der Sicherheitsstandards. Mit der Einführung biometriegestützter Pässe wird eine hohe Fälschungssicherheit in allen EU-Staaten erzielt.

Die technische Lösung ist ausreichend getestet. Die Kosten sind bekannt. Der Sicherheitsgewinn besteht neben der erhöhten Fälschungssicherheit der Reisedokumente in einer erhöhten Sicherheit vor dem Mißbrauch der neuen Pässe durch andere Personen als den eigentlichen Paßinhaber: Der Chip erlaubt eine elektronische Überprüfung, ob der Nutzer des Dokuments tatsächlich der Paßinhaber ist.

Kommentar der Redaktion:

Jörg Radek, der seit vielen Jahren bei der Bundespolizei (früher Bundesgrenzschutz) arbeitet, beziffert Paßfälschungen auf wenige hundert im Jahr. Deren Qualität sei überwiegend unterdurchschnittlich, gute Totalfälschungen höchst selten. Es wäre für Kriminelle auch kaum sinnvoll, sich die Mühe zu machen, mittels Bestechung kann man da einiges Geld sparen. Diese Zahlen erklären jedenfalls nicht, warum die deutschen Paßbesitzer mit ihren bereits hochsicheren Dokumenten ihre digitalen Gesichtsbilder und ihre Fingerabdrücke abgeben sollen.

Die "ausreichend getestete technische Lösung" ist beispielsweise für die Extended Access Control bis heute nicht endgültig spezifiziert. Die EU-Verordnung für die neuen Pässe beschreibt hingegen vor allem herstellungstechnische Sicherheitsmerkmale. Offensichtlich auch aus wirtschaftlichen Interessen wurde die Entwicklung elektronischer Dokumente vorangetrieben (Empfehlung der European Commission, "Biometrics at the Frontiers: Assessing the Impact on Society" ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf), in Deutschland profitiert die authentos Gruppe und ihre Tochter, die Bundesdruckerei GmbH, von den biometrischen Pässen, da keine neuerliche Ausschreibung für die Herstellung gemacht wurde. Wie selbstverständlich erhielt die Bundesdruckerei den lukrativen Auftrag. Begründet wird dies mit einem dreijährigen Rahmenvertrag. (Siehe dazu auch den Hintergrundbericht "Eigentumsverhältnisse Bundesdruckerei" in dieser Ausgabe.)

Daß die Kosten nicht, wie angegeben, "bekannt" sind, zeigt der Entschluß des Bundesrates, sich von der Bundesregierung eine detaillierte Kalkulation der Kosten der "Zweiten Verordnung zur Änderung paßrechtlicher Vorschriften" vorlegen zu lassen. (Bundesrat Drucksache 510/1/05, beschlossen in der 813. Plenarsitzung) Von Beginn an verweigert das BMI eine detaillierte Kostenaufstellung und führt die Parlamentarier wie auch die Steuerzahler konsequent an der Nase herum.

Noch ein Wort zu dem Chip: dieser erlaubt übrigens keine elektronische Überprüfung, ob der Nutzer des Dokuments tatsächlich der Paßinhaber ist. Dies kann einzig allein der Grenzbeamte machen (wie ja mehrfach hier erwähnt).

10. Frage:

Könnte es sein, daß durch die vermeintlich "100% sicheren Pässe" die Grenzbeamten ihr persönliches Gespür zurückfahren und nur noch der Technik vertrauen? Wird dadurch die Gefahr nicht viel größer? Die Argumentation, daß die Technik "nur unterstützend" sein soll, ist dabei nicht hilfreich, da der Gewöhnungseffekt ja trotzdem eintritt.

Antwort:

Die Aufnahme biometrischer Merkmale in Reisepässen dient dazu, die sichere Identifizierung von Personen durch das Grenzkontrollpersonal zu "unterstützen". Davon unabhängig kontrolliert die Bundespolizei stets nach Schengenstandard.

Kommentar der Redaktion:

Ja, das hatten wir jetzt schon dreimal... Es ist klar, daß ein rot blinkender Bildschirm die Aufmerksamkeit der Grenzbeamten erregen wird. Aber wird ein freundliches grünes Signal nicht auch nach einer gewissen Gewöhnungszeit zur Folge haben, daß sie **nicht** mehr so genau hinsehen?

11. Frage:

Funktioniert das Auslesen per Funk auch noch zuverlässig, wenn ich - wie zukünftig geplant - RFID-gestützte Sichtvermerke (Visa) in meinem Reisepaß habe?

Antwort:

Über die Einführung biometriegestützter Visa ist auf europäischer Ebene noch keine Entscheidung getroffen worden. Die EU wird ein zentrales Visum-Informationssystem einrichten, in dem die Lichtbilder und Fingerabdrücke aller Visa-Antragsteller gespeichert werden.

Kommentar der Redaktion:

Daß ich als deutscher Bürger ein EU-Visum in meinem Reisepaß habe, ist wohl eher unwahrscheinlich. Völlig unklar ist, ob der RF-Chip im Paß mit einem RF-Visa außereuropäischer Länder harmoniert. Aber sollten sich die Chips ins Gehege kommen, bleibt der Paß sicher weiter gültig. Man muß ja auch wirklich nicht dauernd verreisen...

Die Welt von morgen: iPass

Maha <maha@elitas.com>

Wir drucken hier das Interview ab, das unsere Korrespondentin Cornelia C. Cortschloss mit der Bundesministerin für Inneres, Justiz und Heimatschutz Gertrud Backstein über die am 1. Juni 2017 bevorstehende Einführung des neuen Bio-iPasses führte.

CCC: Frau Backstein, in wenigen Tagen, nämlich am 1. Juni 2017, soll der neue iPass der zweiten Generation, der Bio-iPass, obligatorisch eingeführt werden. Welche Neuerungen bringt er mit sich?

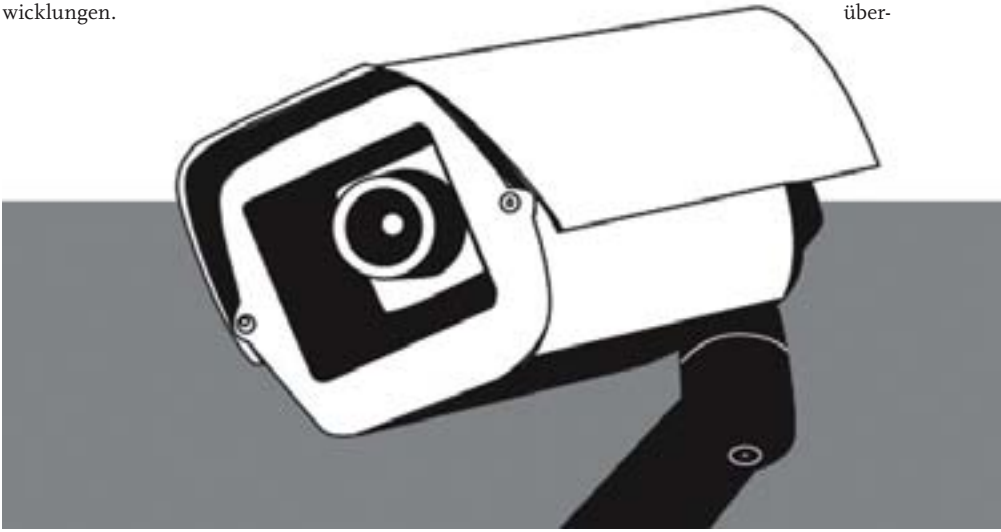
GB: Nach der breiten Akzeptanz, auf die die erste Generation des implantated Passports, kurz iPass getroffen ist, lassen wir das erfolgreiche Konzept eines in den Körper seines Trägers implantierten Reisepasses fast völlig unverändert. Dennoch gibt es eine sehr wichtige Verbesserung: Der Chip bezieht auch Informationen aus den Körperzellen seines Trägers, sodaß im Todesfall ein sogenanntes Death Bit gesetzt wird und das Überwachungsgerät feststellen kann, daß der Träger verstorben ist. Leider ist es noch nicht möglich, den Chip auch zur Krankendiagnostik oder für Alkoholkontrollen zu verwenden. Dies ist das Ziel zukünftiger Entwicklungen.

CCC: Welchen Vorteil hat dann diese Technik, wenn nur der Tod des Trägers festgestellt werden kann?

GB: Wir konnten in der Vergangenheit Fälle beobachten, in denen abgetrennte Körperteile mit dem Chip zur Identifikation verwendet wurden. Dies wird mit dem neuen Bio-iPass nicht mehr möglich sein.

CCC: Aber die Presse berichtete doch unlängst, daß ein Träger des neuen iPasses beim Grenzübertritt festgenommen wurde, weil der iPass anzeigte, daß er schon tot sei.

GB: Wie Sie wissen, erlag die fragliche Person den Verletzungen, die sie sich bei ihrer Festnahme zugezogen hatte. Deshalb konnte nicht ermittelt wer- den, ob über-



haupt ein Fehler vorlag. Ich gehe jedoch nach wie vor davon aus, daß der iPass nach seiner Implantation nicht mehr verändert werden kann.

CCC: In der Vergangenheit wurde kritisiert, daß die Daten auf dem Chip unzureichend verschlüsselt sind. Wird sich mit dem neuen iPass-Chip auf diesem Gebiet etwas ändern?

GB: Nein, der bisherige Verschlüsselungsstandard bleibt bestehen. Inzwischen wird der iPass für viele Sekundäranwendungen zur Identifikation verwendet; er ist Kreditkarte, Autoschlüssel, Payback- und Gesundheitskarte zugleich. Das macht ja gerade seine große Akzeptanz aus! Wir wollten – schon aus Kostengründen – darauf nicht verzichten, so viele Partner wie möglich in das Unternehmen iPass einzubinden. Die Bevölkerung will eine allgemeine Nutzbarkeit des iPasses. Das hier die Bedenken der Datenschützer einmal zurücktreten müssen, ist bedauerlich, aber unvermeidlich.

CCC: Datenschutzverbände wie der Chaos Computer Club oder auch die Datenschutzbeauftragte haben doch...

GB: Ach, kommen Sie mir doch nicht mit diesen ewig gestrigen Bedenkenträgern. Angesichts der Bedrohung durch den Terror sind solche Bedenken lebensgefährlich und stehen dem Aufbau eines modernen, bürokratiefreien Staats entgegen.

CCC: Die Akzeptanz des iPasses ist gesunken, seit er obligatorisch in die Nasenscheidewand implantiert wird. Wollen Sie an der umstrittenen Lösung festhalten?

GB: Die Implantation in die Nasenscheidewand ist ohne äußere Narben möglich, was einem verbreiteten Wunsch entgegenkommt. Wir sehen es als notwendig an, daß der Chip in einem unverdeckten Bereich des Gesichts implantiert ist, da somit keine Möglichkeit besteht, ihn mit Isolationsmaterial zu verdecken und darüber einen anderen Chip anzubringen. Außerdem ist die Nasenscheidewand groß genug, um auch noch zum Beispiel einen Chip mit einem iVisum anzubringen.

CCC: Ist es nicht möglich, das iVisum auf dem iPass zu integrieren?

GB: Leider nicht, da andere Staaten wie zum Beispiel die USA auf eine völlig andere Technologie setzen. Als sich Bayern nach der Aufnahme der Türkei in die EU aus dieser zurückzog und ein US-Bundesstaat wurde, war es nötig, eine schnelle Lösung für die Visumsfrage zu finden, um Grenzformalitäten zu vermeiden, denn eine neue deutsch-deutsche Grenze sollte unbedingt vermieden werden. Daher wurde das US-amerikanische iVisum auch in Europa in großer Zahl implantiert.

CCC: Als sich die Niederlande den USA als Bundesstaat anschlossen, wurde kein spezielles iVisum eingeführt.

GB: Bayern ist ja nicht Holland! Wir wollten nicht ganz Deutschland auf US-Standards umstellen, zumal dieser Standard keinerlei Verschlüsselung vorsieht. Den gläsernen Bürger wollte hierzulande niemand.

CCC: Aber mit dem iVisum für Bayern ist doch dieser Standard neben dem deutschen auch sehr verbreitet.

GB: Niemand ist verpflichtet, sich ein iVisum implantieren zu lassen...

CCC: ...einen iPass aber doch!

GB: Sicher! Der iPass ist ja schon in der ersten Generation seit über einem Jahr obligatorisch, und das ist auch gut so! Allein der Rückgang der Kriminalität ist enorm! Die Vereinfachung von Kontrollen ist für die Bürgerinnen und Bürger sehr bequem. Nicht mal bei Verkehrskontrollen muß mehr angehalten werden!

CCC: Aber auch die Zahl der Kontrollen hat sich vervielfacht, ja potenziert! Wird Deutschland zum Überwachungsstaat?

GB: Nun lassen Sie die Kirche mal im Dorf, Frau Curtsschluss! Unser iPass ist ein Exportschlager. Inzwischen wird er weltweit eingesetzt und ist zum Synonym von Reisefreiheit, ja von Freiheit schlechthin geworden. Kontrollen waren gestern! Heute erledigen das unsere Autobahn-Mautbrücken gleich mit. Und wenn Sie am Strand Ihren Drink bezahlen wollen, müssen Sie nicht mehr Ihre Kreditkarte aus dem Bikini ziehen. Ihr Wunsch wird Ihnen buchstäblich von den Augen – oder besser – von der Nase abgelesen. Das ist doch eine Freiheit, die sich jeder nehmen will!

CCC: Der iPass wird aber auch in vielen umstrittenen Bereichen eingesetzt; ich denke da an DRM, Anwesenheitskontrollen am Arbeitsplatz oder in Schulen und Universitäten.

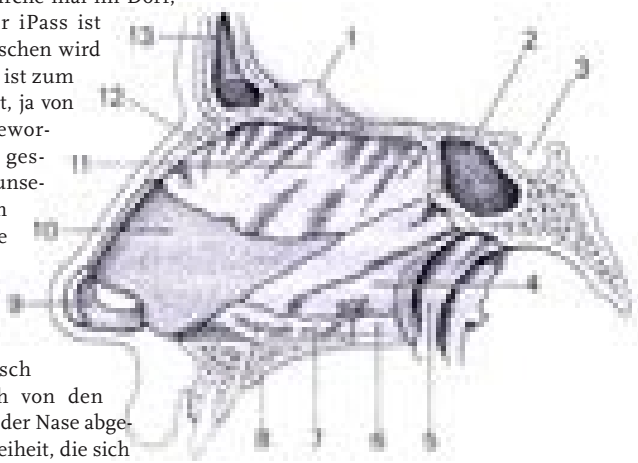
GB: Wissen Sie, DRM war in dem Augenblick akzeptiert, wo es bequem mit dem iPass umgesetzt werden konnte. Raubkopierer gibt es seither nicht mehr; außerdem ist die Arbeitslosigkeit zurückgegangen, seit Schwarzarbeit praktisch unmöglich geworden ist, weil jeder Arbeiter sofort identifiziert werden kann. Ich werte das als Erfolg unserer Politik!

CCC: Aber die Gegner des iPasses beklagen den totalen Verlust der Privatsphäre!

GB: Auch seine Gegner nutzen seine Vorteile! Ich denke, daß von einem Verlust der Privatsphäre gar keine Rede sein kann: Viele Computerprogramme erlauben nur noch Benutzern mit registriertem iPass Zugang zu persönlichen Daten. Der Schutz persönlicher Daten ist doch ein unbestreitbarer Vorteil.

CCC: Es sei denn, jemand kann die Identität eines iPasses stehlen.

GB: Das ist schon technisch unmöglich. Gefälschte iPässe sind und bleiben Science Fiction!



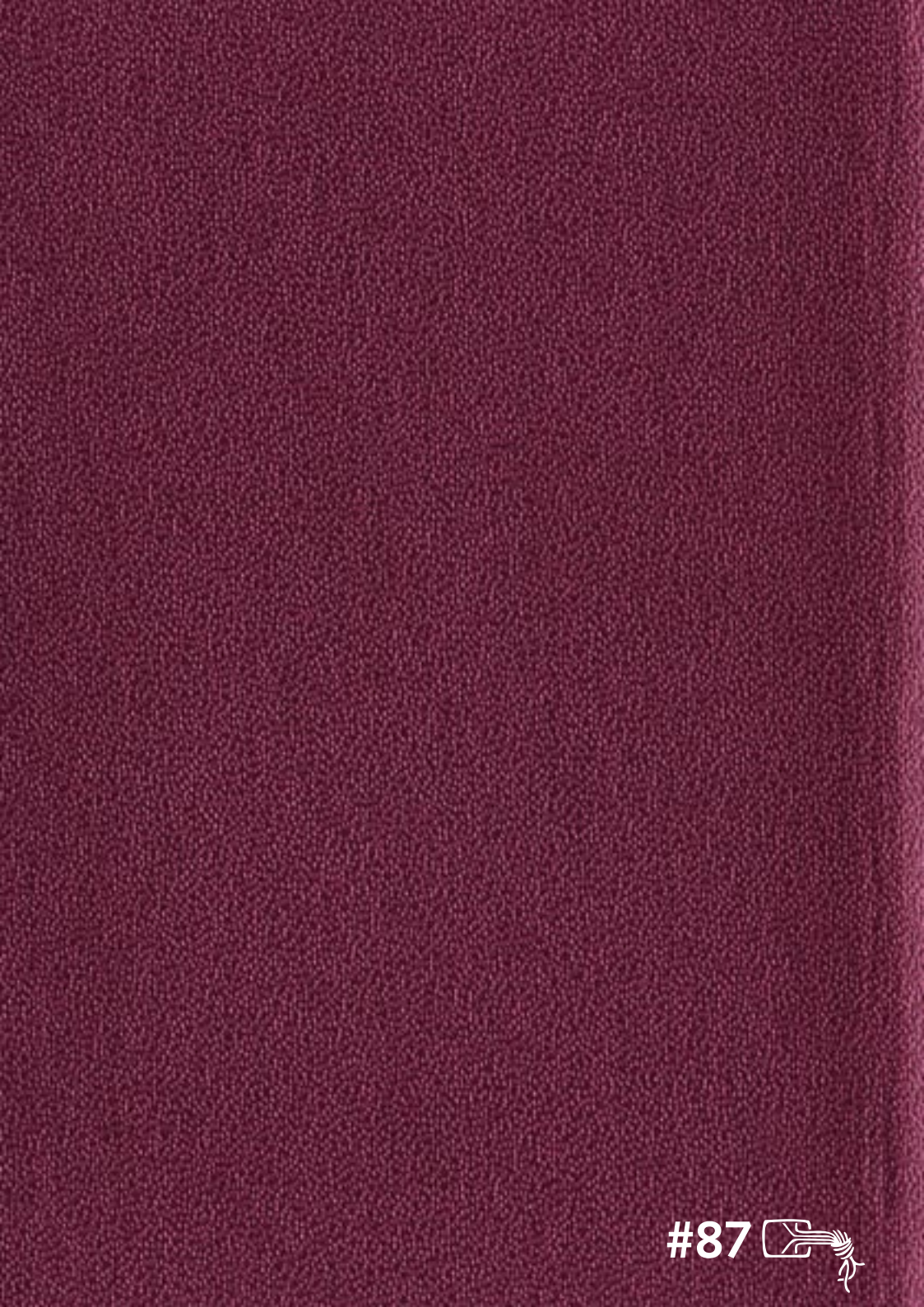
Bundesministerium
für Wahrheit

Überwacht leben mit dem ePass

- Erfassung der Fingerabdrücke aller deutschen Paßinhaber
- Elektronische Speicherung von personenbezogenen biometrischen Daten
- Funkchip zur besseren Überwachung
- Demnächst: Biometrische Personalausweise

Weitere Informationen finden Sie unter:

www.ccc.de/epass/


#87