

Die Anforderungen der ICAO an Reisedokumente mit Biometrie

**Ausarbeitung zum Seminar „Biometrische Systeme“ am
Fachbereich Informatik der Technischen Universität
Darmstadt im Wintersemester 2004/2005**

Alexander Klink
klink@mathematik.tu-darmstadt.de

Januar 2005

Inhaltsverzeichnis

1	Einführung	3
2	International Civil Aviation Organization	3
3	Der ePassport	5
3.1	Zielvorgaben	7
3.2	Anwendungen	7
3.2.1	Während des Enrolments	8
3.2.2	An der Grenze	8
3.3	Technische Ausgestaltung	9
3.3.1	Bilddaten	9
3.3.2	Speichermedium	11
3.3.3	Datenorganisation	13
3.4	Logical Data Structure	13
3.5	Kryptographische Absicherung	15
3.5.1	Public Key Infrastruktur	15
3.5.2	Passive Authentication	16
3.5.3	Basic Access Control	16
4	Stand der Dinge	17
5	Mögliche Probleme	17
6	Abschließende Bewertung	19

Abbildungsverzeichnis

1	Personalausweis mit Machine Readable Zone	4
2	Das ePassport-Logo	6
3	Schematische Darstellung von ISO 19794-5	10
4	Auswirkung von Komprimierung auf die Performanz	10
5	Position der RFID im Pass	12
6	Die Logical Data Structure	14

1 Einführung

Diese Ausarbeitung entstand im Rahmen des Seminars „Biometrische Systeme“ am Fachbereich Informatik der TU Darmstadt. Das Seminar wurde von Dr. Christoph Busch und Henning Daum von Institut Graphische Datenverarbeitung der Fraunhofer Gesellschaft geleitet. Diese Ausarbeitung behandelt das Thema „Anforderungen der ICAO an Reisedokumente mit Biometrie“ und ergänzt den Vortrag, der am 25. Januar gehalten wurde. Die Folien zum Vortrag finden sich unter [K105].

2 International Civil Aviation Organization

Bei der Vorbereitung für das Seminar stolperte ich zunächst über eine Abkürzung: ICAO steht für „International Civil Aviation Organization“ (internationale Organization für zivile Luftfahrt) und ist seit 1947 eine Unterorganisation der Vereinten Nationen. Vom Status innerhalb der UN ist sie etwa mit WHO, UNESCO oder ITU zu vergleichen. Ihr gehören 188 Staaten an, die gemeinsam Prinzipien und Techniken der internationalen Luftfahrt entwickeln und sich dabei insbesondere auf gemeinsame Standards einigen.

Ein solcher Standard ist etwa das ICAO Document Nr. 9303, welches sich mit „Machine Readable Travel Documents (MRTD)“, also maschinenlesbaren Reisedokumenten (z.B. Pässe oder Visa) beschäftigt. Dabei ist ein MRTD nicht *nur* maschinenlesbar, sondern enthält auch menschenlesbare Informationen. So ist der heutige deutsche Reisepaß, aber auch der Personalausweis schon ein MRTD im Sinne des ICAO-Standards – er enthält eine zweizeilige maschinenlesbare Zone, die die wichtigsten Daten in OCR-B enthält (s. Abbildung 1).

Zur Zeit werden von ca. 120 Staaten solche MRTDs ausgegeben. Dabei handelt es sich zur Zeit hauptsächlich um maschinenlesbaren Pässe (MRPs – „Machine Readable Passports“), nur etwa ein Viertel gibt auch maschinenlesbare Visa (MRVs) aus (vgl. [ICAO04]). Insgesamt wurden seit der ersten Definition über 700 Millionen MRPs ausgegeben (vgl. [ICAO03]). Dass diese dann nicht nur für den Luftverkehr verwendet werden und somit der ICAO eine große Bedeutung bei der Entwicklung von maschinenlesbaren Reisedokumenten zukommt, versteht sich von selbst.

3 Der ePassport

In vorherigen Versionen dieses Reports empfahl die NTWG noch Gesicht, Fingerabdruck und Iris (eines bzw. Kombinationen) als biometrische Merkmale zur Aufnahme in Reisedokumenten. In der Entwicklung stellte sich jedoch heraus, dass das Gesicht das Merkmal ist, das am besten für die Ausgabe von Reisedokumenten geeignet ist. Diese Erkenntnis wurde erstmalig in der sog. Berlin-Resolution als Standard festgeschrieben. Die New Technologies Working Group beschloß daher am 28. Juni 2002 in Berlin, das Gesicht als *das* global interoperable biometrische Merkmal für die maschinenunterstützte Identitätsbestätigung auszuwählen und stellte den Staaten frei, zusätzlich Fingerabdruck und Iris zu verwenden. Diese Entscheidung wurde in der New Orleans Resolution im März 2003 noch etwas genauer beschrieben: Die Gesichtsbilder sollen digital auf einem kontaktlosen IC gespeichert werden (im Gegensatz zur Verwendung des schon bisher vorhandenen Bilds auf der Datenseite des Passes) und auch die anderen biometrischen Merkmale sollen als Bilder digital gespeichert werden. Die Verwendung von Irisbildern als biometrisches Merkmal war zur Zeit der Verabschiedung der New Orleans Resolution noch umstritten, da es ungelöste Probleme mit dem Recht am Verfahren gab, die nach Ansicht der ICAO mittlerweile aber aus dem Weg geräumt sind.

Gründe für die Verwendung des Gesichts als biometrisches Merkmal sind laut ICAO insbesondere folgende (s. [TR04], S. 17):

- Ein Foto des Gesichts enthält keine Information, die ein Mensch nicht sowieso schon routinemäßig der Öffentlichkeit präsentiert
- Das Foto des Gesichts ist bereits international sozial und kulturell akzeptiert
- Es wird im Moment schon zur Passherstellung verwendet und ist daher auch schon in diesem Zusammenhang bekannt
- Der Benutzer muß während des Enrolments nichts anfassen oder mit physikalischen Geräten interagieren
- Es müssen keine neuen und teuren Enrolment-Prozeduren eingeführt werden

3 Der ePassport

- Die Benutzer (insbesondere Kinder) müssen für das Enrolment nicht physisch anwesend sein
- Man kann es immer aufnehmen
- Für Fahndungslisten und ähnliches ist das Gesicht oft das einzig verfügbare biometrische Merkmal

Daher schreibt der jetzige Report das Gesichtsmerkmal als verbindlich vor und gibt den Staaten die Freiheit, zusätzlich noch Fingerabdrücke und/oder Iris-Merkmale hinzuzufügen. In zusätzlichen Reports wird beschrieben, wie die Daten in Form einer „Logical Data Structure“ (LDS) auf dem Reisedokument gespeichert werden und wie die Public Key Infrastruktur (PKI) aussieht, um diese Daten zu schützen und zu authentifizieren. Der Report bezieht sich hauptsächlich auf maschinenlesbare Pässe (MRPs) und benutzt den trendigen Namen „ePassport“ um solch einen Pass mit Biometriemerkmale zu bezeichnen. Um die Verwendung von Biometrie im Pass zu kennzeichnen wurde ein Logo entworfen, das die Verwendung eines kontaktlosen ICs symbolisieren soll und unterhalb des Schriftzugs „PASSPORT“ auf dem Cover des Passes angebracht wird (vgl. Abbildung 2).

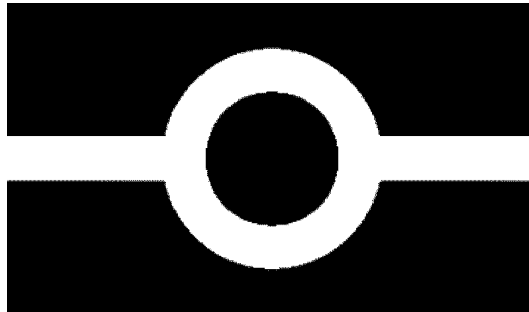


Abbildung 2: Das ePassport-Logo, Quelle: [TR04]

3.1 Zielvorgaben

Folgende Zielvorgaben hat sich die ICAO beim Entwurf des ePassports gegeben (vgl. [TR04], S. 6):

- **globale Interoperabilität** – es besteht ein entscheidender Bedarf, die biometrischen Merkmale so zu spezifizieren, dass sie global interoperabel eingesetzt werden können. Aus dieser Anforderung heraus entstand die spätere Ausgestaltung, die biometrischen Merkmale als Bilder und somit quasi als Rohdaten anstatt als Templates zu speichern.
- **Einheitlichkeit** – durch das Standards setzen werden die möglichen Lösungsvarianten, die von Staaten verwendet werden erheblich verkleinert.
- **Durchführbarkeit** – die Standards müssen durch die Staaten implementierbar sein, ohne dass viele verschiedene Systeme vorgehalten werden müssen um allen möglichen Variationen und Interpretationen des Standards zu begegnen.
- **technische Zuverlässigkeit** – Richtlinien müssen eingeführt werden, um sicherzustellen, dass die Staaten Lösungen verwenden, die eine hohe Zuverlässigkeit in der Identitätsverifikation haben. Weiterhin muss eine ausreichende Qualität der von den Staaten erstellten Daten und deren Integrität gesichert sein, um eine präzise Verifikation sicherzustellen.
- **Haltbarkeit** – es muss sichergestellt sein, dass die verwendeten Systeme die im Moment verwendeten 10 Jahre Haltbarkeit der Reisedokumente erreichen. Da die ICAO sich dessen auch nicht sicher ist, schlägt sie auch vor, die Gültigkeit von Reisedokumenten etwa auf 5 Jahre zu verkürzen.

3.2 Anwendungen

[TR04] beschreibt einige mögliche Anwendungen des ePassports. Grundsätzlich gibt es dort zwei Verwendungsarten: während des Enrolments und im „wirklichen Betrieb“ an der Grenze. Andere Anwendungsszenarien sind zunächst einmal eine Frage des Datenschutzes, so könnte z.B. auch bei der Erstellung eines Bankkontos die Bank die biometrischen Merkmale vergleichen

wollen. Zur Ausgestaltung dieser sonstigen Anwendungen schweigt sich die ICAO aber aus.

3.2.1 Während des Enrolments

Während des Enrolments werden die biometrischen Merkmale aufgenommen, die im ePassport gespeichert werden sollen. Diese lassen sich nun leicht in ein biometrisches Template wandeln und dann mit bereits vorhandenen Datenbanken vergleichen. So könnte etwa bei Antragsstellung eine Fahndungsdatenbank durchsucht werden oder eine evtl. vorhandene Datenbank von Antragsstellern, um die Ausstellung eines weiteren Passes zu verhindern.

Nachdem der Pass hergestellt wurde, kann mit Hilfe der bei Abholung aufgenommenen Merkmale sichergestellt werden, dass der Pass von seinem legitimen Besitzer abgeholt wird.

Als zusätzliches Feature ließe sich z.B. auch die Identität der Mitarbeiter, die am Enrolment und an der Herstellung des Passes beteiligt sind, verifizieren. So könnte z.B. ein Audit-Log digital signiert werden um die Herstellung eines Passes an bestimmte Personen zu binden und damit Fälschungen zu vermeiden.

3.2.2 An der Grenze

An der Grenze gibt es verschiedene Möglichkeiten, die Identität des Passbesitzers zu verifizieren, die sich im Aufwand unterscheiden.

Als einfachste Methode bietet sich der Test an, ob die Identität mit den biometrischen Daten im Reisedokument übereinstimmt. Die wohl in der späteren Praxis am häufigsten verwendete Anwendung wird der 2-Wege-Test sein, bei dem durch Aufnahme der aktuellen biometrischen Daten diese mit den elektronisch im Reisedokument gespeicherten verglichen werden. Der 3-Wege-Test entspricht dem 2-Wege-Test und vergleicht zusätzlich noch die Daten mit den biometrischen Daten in einer Enrolment-Datenbank. Dieser Test wird zumindest in Deutschland jedoch aufgrund des Fehlens einer solchen Datenbank aus

Datenschutzgründen nicht angewendet werden können. Daher müssen zur Sicherstellung, dass die Daten im Pass noch denen entsprechen, die beim Enrolment aufgenommen wurden, andere Sicherheitsmaßnahmen ergriffen werden, die im Kapitel zur Public Key Infrastruktur beleuchtet werden. Schlußendlich würde in einem 4-Wege-Test der 3-Wege-Test durchgeführt und gleichzeitig noch ein visueller Vergleich zwischen dem im Chip gespeicherten Foto und dem auf der Datenseite des Passes abgedruckten Foto vorgenommen.

3.3 Technische Ausgestaltung

3.3.1 Bilddaten

[TR04] und seine Anhänge beschreiben hauptsächlich die technische Ausgestaltung des ePassports, die hier im folgenden dargestellt werden soll.

Wie bereits erwähnt, sollen die biometrischen Merkmale als Bilder gespeichert werden, die Speicherung von Templates ist optional. Die Speicherung dieser Bilddaten, erfolgt nach den ISO-Standards (bzw. den Entwürfen, die z.Z. gemacht werden) 19794-5 (Facial Image Data), 19794-6 (Iris Image Data) und 19794-4 (Finger Image Data), die auch als Anhang zu [TR04] veröffentlicht wurden. Die entsprechenden Standards speichern neben der reinen Bildinformation auch noch Metadaten zu den Bildern, z.B. für das Gesicht Informationen zu Haarfarbe, der Pose auf dem Bild, etc. (siehe auch Abbildung 3).

Zur Bildgröße für Gesichtsbilder gab es Untersuchungen von Passports Australia (vgl. [TR04], Anhang B und C), die anhand von rund 1000 Fotos Abschätzungen für eine Komprimierungsrate gaben. Bei einer angestrebten Performanzrate von 99% des Wertes bei unkomprimierten Bildern ergab sich eine Größe von ca. 15-20 KiB (vgl. dazu Abbildung 4) als JPEG bzw. JPEG2000. Eine interessante Information aus der Studie ist die Beobachtung, dass eine Komprimierung die FRR (Falsch-Rückweisung-Rate) zwar erhöhte, nicht jedoch die FAR (Falsch-Akzeptanz-Rate). D.h. insbesondere wenn es nur um die Überwindungssicherheit eines Systems geht, scheint eine Komprimierung das System nicht zu beeinflussen.

Das Gesichtsbild soll nach ICAO entweder identisch zum Portraitfoto auf der Datenseite sein, kann evtl. aber auch ein Ausschnitt sein. Dieser Ausschnitt

3 Der ePassport

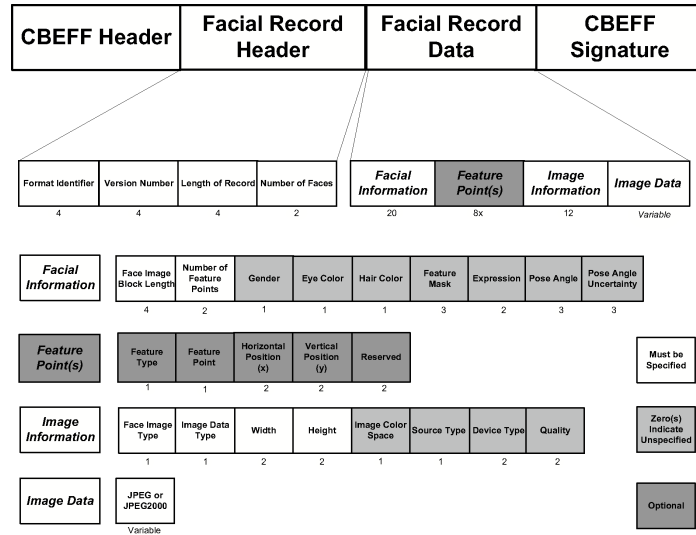


Abbildung 3: Schematische Darstellung von ISO 19794-5, Quelle: [TR04], Anhang D

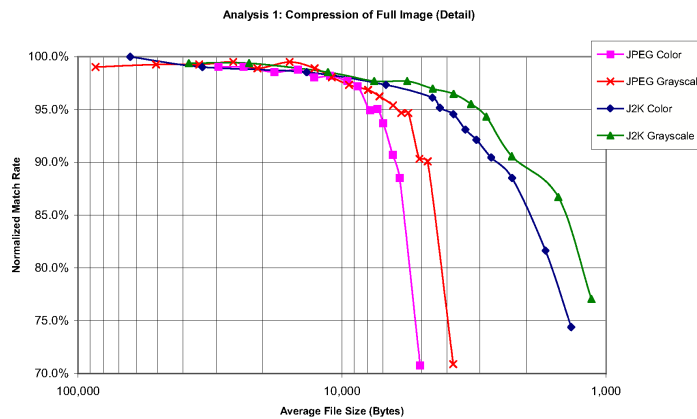


Abbildung 4: Auswirkung von Komprimierung auf die Performanz, Quelle: [TR04], Anhang B

muss das Gesicht von horizontal von Kante zu Kante und vertikal von Kinn zu Frisurende zeigen. In der oben bereits erwähnten Studie zeigte sich, dass solch ein Ausschnitt ca. 0,5% Verlust in der Erkennungsleistung zur Folge hat. Da für einen menschlichen Betrachter der Vergleich zwischen Bild und Person mit einem kompletten Portrait deutlich einfacher ist, schreibt [TRO4] jedoch vor, dass auch das Foto der Datenseite zu speichern ist, falls ein Ausschnitt gewählt wurde.

Ähnliche Untersuchungen ergaben für den Fingerabdruck eine optimale Bildgröße von 10 KiB, für ein Irisbild 30 KiB.

3.3.2 Speichermedium

Der Report schreibt vor, dass die Daten auf kontaktlosen IC-Chips (auch RFID – Radio Frequency IDentification genannt) gespeichert werden sollen. Als Alternativtechnologien kamen noch einige weitere Speichermedien in Frage, die aber aus verschiedenen Gründen nicht gewählt wurden.

So scheiden zweidimensionale Barcodes und Magnetstreifen wegen ihrer Kapazitätsbeschränkungen aus – auf ihnen wäre nur eine Speicherung von (wenigen) Templates möglich. Außerdem sind sie – ebenso wie kontaktbehaftete ICs – nur mit einem direkten Kontakt auslesbar, kontaktlose ICs sind in dieser Hinsicht gerade an Grenzübergängen deutlich praktikabler. Kontaktlose ICs haben außerdem den Vorteil, dass sie in Pässe der üblichen Form und Größe einbaubar sind, für kontaktbehaftete ICs etwa müsste zuerst das Format geändert werden.

Eine Kapazität von mindestens 32 KiB wird vorgeschrieben, da sich so ein vorgeschriebenes Bild, Text (etwa die MRZ und zusätzliche Daten) sowie eine Signatur speichern lassen. Sollen zusätzliche biometrische Merkmale und evtl. davon sogar noch mehrere (z.B. mehrere Fingerbilder verschiedener Finger) gespeichert werden, braucht man natürlich mehr Speicherplatz. Die ICAO empfiehlt hier eine Größe von mindestens 512 KiB, da der Overhead (Betriebssystem, etc.) bei Chips, die größer als 64 KiB sind, bis zur Hälfte der Größe des IC betragen können. Effektiv blieben bei einem 512 KiB-Chip also nur rund 256 KiB für Daten übrig.

3 Der ePassport

Zur Position im Pass selbst gibt es verschiedene Möglichkeiten (vgl. Abbildung 5, die jeweils Vor- und Nachteile haben).

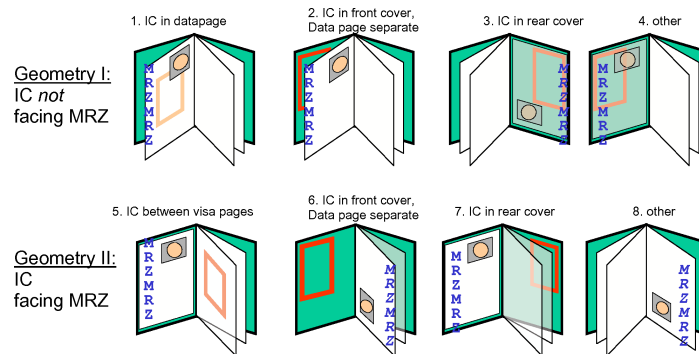


Abbildung 5: Position der RFID im Pass, Quelle: [TR04]

So hat die Position auf der Datenseite zwar den Vorteil, dass alle Daten an der gleichen Position sind und von der Plastiklaminierung profitiert wird, andererseits muss so natürlich nur eine Seite gefälscht werden, um eine Identität auszutauschen. Eine Positionierung in der Mitte des Passes hat den Vorteil, dass der IC optimal geschützt ist, den Nachteil, dass er erst spät in der Herstellung eingebaut werden kann. Ein Positionieren auf den Innenseiten des Covers hat den Vorteil, dass der IC schon von Anfang an dort eingebaut werden kann, jedoch den Nachteil, dass dort die empfindlichste Stelle ist, was Knicke angeht. Außerdem besteht die Möglichkeit, dass die Goldschrift auf dem Cover die Radiowellen blockiert. Auch die Fälschungssicherheit ist hier nicht die beste. Eine letzte Möglichkeit besteht darin, den IC in eine extra Seite innerhalb des Passes einzunähen.

Die Vorgabe bezüglich der Haltbarkeit der Chips beträgt von Seiten der ICAO erst einmal 10 Jahre, da dies die übliche Gültigkeitsdauer ist. Wie schon oben erwähnt scheint dieser Wert jedoch unrealistisch (Chiphersteller geben selbst eine Lebensdauer von 2-3 Jahren an), so dass empfohlen wird, die Gültigkeitsdauer von Pässen evtl. auf fünf Jahre anzupassen.

Bezüglich der Lesegeräte gilt auch eine Sonderregelung: Prinzipiell sollen die Lesegeräte ISO 14443 erfüllen. Bei Tests mit Lesegeräten, die diesem Standard genügen, gab es jedoch einige Probleme, so dass in einem eigenen Anhang

zu [TR04] die speziellen Anforderungen der ICAO beschrieben werden. Diese sind mit den Herstellern in Treffen abgesprochen worden und in der Realität zu großen Teilen mittlerweile realisiert.

Da die Daten der Machine Readable Zone im Chip enthalten sind, bräuchte man eigentlich keine OCR-Leser mehr. Es wird jedoch davon ausgegangen, dass für den Sicherheitsgewinn (und für die Vereinfachung der Basic Access Control, dazu später mehr) weiterhin die MRZ ausgelesen wird und dafür Kombileser hergestellt werden.

3.3.3 Datenorganisation

Die Daten sind auf dem Chip in einer sogenannten „Logical Data Structure“ (LDS), die in [LDS04] beschrieben ist, gespeichert. Zur Struktur dieser LDS folgt noch ein eigenes Kapitel. Die Integrität der Daten wird durch digitale Signaturen in Verbindung mit einer Public Key Infrastruktur gewährleistet, welche ebenfalls später in einem eigenen Kapitel erläutert wird.

3.4 Logical Data Structure

Die Logical Data Structure beschreibt die Daten, die auf dem IC enthalten sind (bzw. sein können) in detaillierter Form (vgl. Abbildung 6).

So können zusätzlich zu den üblichen, in der MRZ enthaltenen, Daten auch Zusatzinformationen über den Besitzer des Passes, Daten über (physikalische) Sicherheitsmerkmale des Passes, etc. vorhanden sein. In späteren Versionen soll es evtl. auch die Möglichkeit geben, Visa und andere Reisedaten innerhalb dieser LDS zu speichern. Die Daten sind in (vorerst) 16 sogenannten „Data Groups“ enthalten, die sich durch entsprechende Dateinamen auf dem IC ansteuern lassen können.

Interessant für die spätere Anwendung ist die Datei EFSOD, die digital signierte Hash-Werte der einzelnen Data Groups enthält.

Zur genaueren Spezifikationen, was wo wie gespeichert wird, sei auf [LDS04] verwiesen.

3 Der ePassport

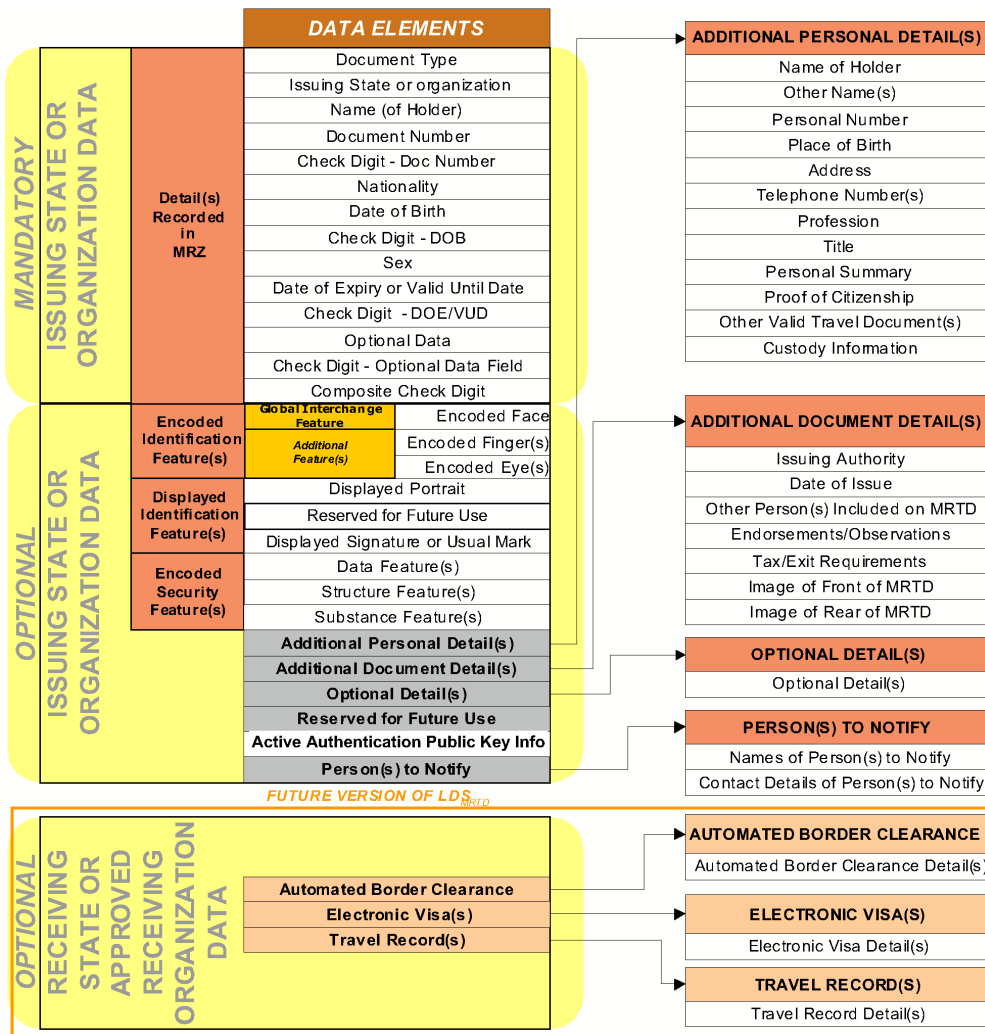


Abbildung 6: Die Logical Data Structure, Quelle: [LDS04]

3.5 Kryptographische Absicherung

Zur Absicherung der Integrität der im Chip gespeicherten Daten schreibt die ICAO in [PKI04] ein digitales Signaturverfahren vor. Weiterhin werden Verfahren zur Verschlüsselung der Kommunikation zwischen Lesegerät und Chip spezifiziert, sowie Verfahren zur Verschlüsselung der Daten auf dem Chip, diese sind jedoch optional.

3.5.1 Public Key Infrastruktur

Für die digitale Signatur wird eine Public Key Infrastruktur verwendet. Das Wurzelzertifikat ist das sogenannte Country Signing Certificate Authority Certificate (C_{SCA}). Dieses Zertifikat wird von einer von den Staaten einzurichtenden Country Signing CA in einer Hochsicherheitsanwendung erstellt. Die Zertifikate der einzelnen Staaten sollen untereinander auf diplomatischem Wege ausgetauscht werden.

Die Country Signing CA signiert ihrerseits mit Hilfe ihres Zertifikats sogenannte Document Signer Zertifikate (C_{DS}). Mit Hilfe der Document Signer Schlüssel werden dann die Daten im ePassport signiert. Genauer gesagt signiert die Document Signer CA mittels RSA, DSA oder ECDSA Hash-Werte (die mittels SHA-1, SHA-224, SHA-256, SHA-384 oder SHA-512 erstellt wurden) der einzelnen Data Groups im LDS.

Zur Verbreitung der Zertifikate wird die ICAO ein LDAP-Verzeichnis betreiben, in dem alle gültigen Document Signer Zertifikate veröffentlicht werden. Dieses Verzeichnis (das sogenannte ICAO Public Key Directory) soll öffentlich, d.h. für alle lesbar, betrieben werden.

Sollte ein Zertifikat einmal (vorzeitig) ungültig werden, muss eine Certificate Revocation List (CRL) innerhalb von 48h auf diplomatischem Wege kommuniziert werden. Die CRLs werden zwar auch im Public Key Directory gespeichert, die Hauptübertragungswege sollen jedoch diplomatische Kanäle sein. Was nun im Falle eines Passes passiert, der mit einem zurückgezogenen Document Signer Zertifikat zertifiziert ist, bleibt den Staaten überlassen, die den Pass verifizieren. Im Allgemeinen ist ein Pass aber noch nicht dadurch ungültig, dass sein Document Signer Zertifikat zurückgezogen wurde, diese Pässe sollten aber einer erhöhten Beobachtung und (physikalischen) Verifikation unterliegen.

3.5.2 Passive Authentication

Mit Hilfe der Passive Authentication kann nun verifiziert werden, ob Daten auf dem IC verändert wurden. Dazu laufen folgende Schritte ab:

1. Das Document Security Object (SO_D) wird gelesen
2. Der Document Signer (DS) wird aus dem Document Security Object gelesen
3. Mit Hilfe des Public Keys des Document Signers wird verifiziert, dass die Signatur des Document Security Objects korrekt ist
4. Mit Hilfe des Public Keys der entsprechenden Country Signing CA wird verifiziert, dass die Signatur des Document Signer Certificates korrekt ist, somit ist der Document Signer eine gültige Signaturinstanz
5. Die relevanten Data Groups werden aus dem LDS gelesen
6. Die Hash-Werte der DGs werden berechnet
7. Die Hash-Werte werden mit denen im Document Security Object verglichen. Sind sie korrekt, kann davon ausgegangen werden, dass die Daten in den Data Groups nicht verändert wurden.

3.5.3 Basic Access Control

Da die Kommunikation zwischen RFID und Lesegerät bis auf einige Meter abhörbar ist (wie z.B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im experimentellen Versuch gezeigt, siehe [FiKe04]), gibt die ICAO als optionale Technik zum Schutz davor die Basic Access Control vor. Da das genaue Verfahren Teil eines anderen Vortrags ist, soll hier nur kurz auf das Prinzip eingegangen werden. Zur sicheren Kommunikation bilden sich bei diesem Verfahren das Lesegerät und der RFID einen gemeinsamen symmetrischen Kommunikationsschlüssel. Die gemeinsamen Daten dazu bestimmen sich aus Daten, die in der Machine Readable Zone angegeben sind. So kann (modulo kryptographischer Angriffe) sichergestellt werden, dass nur jemand, der den

Inhalt der MRZ kennt (d.h. im Zweifelsfall per OCR-Leser gelesen hat), mit dem RFID kommunizieren und damit die dort enthaltenen Daten lesen kann. Da zur Schlüsselbildung allerdings nur die Dokumentennummer, das Geburtsdatum sowie das Ablaufdatum verwendet werden, ist fraglich, ob die Sicherheit bzgl. etwa eines Brute-Force-Angriffes gewährleistet ist.

4 Stand der Dinge

Am 10. Dezember 2004 beschloß der Rat der Europäischen Union – gegen die Empfehlung des Parlaments – für die Mitgliedsstaaten zusätzlich zum Gesichtsbild das biometrische Merkmal Fingerabdruck zu verwenden (vgl. [EU04]). Die Einführung kann jedoch gestuft erfolgen (zunächst Gesichtsbild, dann Fingerabdruck).

Für Deutschland ist geplant, dass ab Herbst 2005 erste Pässe mit Gesichtsbild als biometrisches Merkmal produziert werden, 2007 soll der Fingerabdruck hinzukommen (vgl. [Drs154616]). Zusätzlich soll ab 2007 ein neuer Personalausweis eingeführt werden, der eine sog. „Bürgerkartenfunktion“ für digitale Signaturen im eCommerce beinhalten soll. Interessante Details in der Bundestagsdrucksache 15/4616 sind, dass die Fälschungsrate von deutschen Reisedokumenten sehr niedrig ist (35 Pässe im Jahr 2002) und die Bundesregierung gegen eine Einführung von Irisbildern als biometrisches Merkmal ist, da sie die Patentfrage für ungelöst hält.

5 Mögliche Probleme

Eine Einführung von Biometrie in Reisedokumenten hat natürlich nicht nur Vorteile sondern auch Nachteile. In [TR04] spricht die ICAO einige Probleme und offene Fragen an, die noch zu klären sind.

Zum einen ist Biometrie selbst noch in der aktiven Entwicklung und teilweise sind die Fehlerraten noch nicht auf dem Niveau, das wünschenswert wäre. So zeigt beispielsweise die Studie des Bundesamts für Sicherheit in der Informationstechnik zur Leistungsfähigkeit von Gesichtserkennungssystemen ([BSI04]),

das noch einiger Entwicklungsbedarf herrscht. So hatten drei der sechs getesteten Algorithmen bei einem Sicherheitsniveau „stark“ (FAR = 1%) eine FRR zwischen 2 und 8 Prozent, die anderen drei sogar eine FRR zwischen 8 und 16%. Bei einem Sicherheitsniveau „sehr stark“ (FAR = 0,1%) verschiebt sich das Bild noch ein wenig in Richtung größerer FRRs. Tests vom amerikanischen National Institute of Standards and Technology (NIST) und dem Department of Defence (DoD) ergaben ähnliche Ergebnisse, sowohl für Gesichts- als auch für Fingerbilder (vgl. [TAB03], S. 68f). Ob damit ein reibungsloser Betrieb im Grenzverkehr ermöglicht werden kann, darf bezweifelt werden.

Auch gibt es sowohl im Bereich Biometrie als auch im Bereich der RFIDs keine Langzeitstudien, die etwa die Auswirkung der Alterung sowie die Haltbarkeit von Chips im Bereich von zehn Jahren belegen könnten. Gerade bei der Identifikation sind noch keine Tests mit größeren Datenmengen durchgeführt worden.

Ein großes Problem beim Einsatz von Biometrie ist natürlich der Datenschutz. So unterstützt etwa der Bundesdatenschutzbeauftragte das europäische Parlament in seinen Forderungen nach einem Register der Stellen, die Zugriff auf die im Pass gespeicherten Daten haben und spricht sich gegen eine zentrale Biometriedatenbank aus (vgl. [Scha04]). In einem offenen Brief ([PiStEDR04]) an die Abgeordneten des europäischen Parlaments sprechen sich die Bürgerrechtsorganisationen Privacy International, Statewatch und European Digital Rights gegen eine Aufnahme von Fingerabdrücken in den Pass auf. Der Chaos Computer Club spricht sich sogar komplett gegen biometrische Merkmale in Pässen aus und bezeichnet das System als „fragwürdige Sicherheitssimulation“ (vgl. [CCC04]). Allgemein wird kritisiert, dass eine öffentliche Debatte und Aufklärung der Bevölkerung nicht stattgefunden hat. Unklar ist weiterhin noch, ob die Einführung evtl. das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 verletzt und inwieweit die informationelle Selbstbestimmung gewährleistet ist. Ein weiterer Kritikpunkt ist die Verwendung von biometrischen Rohdaten, die tw. eine Erkennung von Krankheiten ermöglicht. Selbst wenn die Verwendung innerhalb der EU etwa starken Datenschutzrichtlinien genügen würde, ist unklar, inwieweit die Daten von anderen Staaten gespeichert und weiterverwendet würden.

Weitere Problempunkte sind Nichterkennung bzw. Nichtvorhandensein von biometrischen Merkmalen. Bei Gesichtserkennung ist die Fehlerquote beim Enrol-

ment verschwindend gering, jedoch haben etwa 2% der Bevölkerung keine ausreichend ausgeprägten Fingerbildmerkmale (vgl. [TAB03], S. 63). Diese und diejenigen, die Probleme bei der Erkennung hätten, wären in Grenzsituationen häufig einer Diskriminierung durch eine Sonderbehandlung ausgesetzt.

Ein weiteres Problem, das von der ICAO angesprochen wird, ist der Grenzverkehr auf dem Landweg. Ist es an Flughäfen ein leichtes, alle Grenzgänger einzeln zu kontrollieren, so wirft etwa der Autoverkehr einige Probleme auf. Die Frage, wie Autos mit mehreren Insassen bzw. Pendler kontrolliert werden, ist noch offen. Eine Ungleichbehandlung würde hier jedoch ein neues „schwächstes Glied“ eröffnen, andererseits ist unklar, wie eine Aufnahme biometrischer Merkmale in dieser Situation durchgeführt werden kann.

Ein letzter Kritikpunkt sind die immensen Kosten, die solch ein technologisches Projekt aufwirft. So schätzt das Büro für Technikfolgenabschätzung beim Deutschen Bundestag die Kosten je nach Grad der Veränderung des Ausweises auf Werte zwischen 320 und 610 Millionen Euro jährlich. Da die Kosten für die Herstellung des Passes auf die Passinhaber umgelegt werden, ergibt sich so auch eine erhebliche Verteuerung der Kosten für einen Pass. Auch wenn die in der Presse häufig zitierten 130 Euro vom Bundesinnenministerium vehement zurückgewiesen werden, wird bei solch einem massiven Einsatz von Technik der bisherige Preis von 13 bzw. 26 Euro nicht zu halten sein.

6 Abschließende Bewertung

Alles in allem legt die ICAO mit ihrem Technical Report ein aus technischer Sicht relativ ausgereiftes Modell für die Einführung von Biometrie in Reisedokumenten vor. Ob solch eine Einführung aber den gewünschten Sicherheitsgewinn bringt und daher aus Kosten/Nutzen-Überlegungen und aus datenschutzrechtlicher Sicht sinnvoll ist, bleibt – zumindest für mich – noch fraglich.

Literatur

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (2004): *Studie: Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen*

men zum geplanten Einsatz in Lichtbilddokumenten – BioP I. Öffentlicher Abschlussbericht, Version 1.1, <http://www.bsi.bund.de/literat/studien/biop/biopabschluss.pdf>, Zugriff am 30.01.2005

- [CCC04] Chaos Computer Club e.V. (2004): *CCC: Biometrische Merkmale in Ausweisen erhöhen Sicherheit nicht*, Pressemitteilung vom 21. Oktober 2004, <http://www.ccc.de/press/releases/2004/CCC20041020-PE-BIOM.html>, Zugriff am 30.01.2005
- [Drs154616] Deutscher Bundestag (2005): *Drucksache 15/4616. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Ulrike Flach, Rainer Funke, weiterer Abgeordneter und der Fraktion der FDP Drucksache 15/4457 – Biometrische Daten in Ausweispapieren*, <http://dip.bundestag.de/btd/15/046/1504616.pdf>, Zugriff am 30.01.2005
- [EU04] Council of the European Union (2004): *Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States*, <http://register.consilium.eu.int/pdf/en/04/st15/st15152.en04.pdf>, Zugriff am 30.01.2005
- [FiKe04] Finke, Thomas; Kelter, Harald (2004): *Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems*, http://www.bsi.bund.de/fachthem/rfid/Abh_RFID.pdf, Zugriff am 30.01.2005
- [ICAO03] International Civil Aviation (2003): *Biometric identification to provide enhanced security and speedier border clearance for travelling public*, Pressemitteilung vom 28. Mai 2003, <http://www.icao.int/mrtd/download/documents/Annex%20J%20-%20ICAO%20May%202003%20Press%20Release.pdf>, Zugriff am 30.01.2005
- [ICAO04] International Civil Aviation Organization (2004): *Issuance of Machine Readable Travel Documents, Updated 4 October 2004*, <http://www.icao.int/mrtd/overview/documents/MRTD%20List%204%20October%202004.pdf>, Zugriff am 30.01.2005
- [KI05] Klink, Alexander (2005): *Die Anforderungen der ICAO an Biometrie in Reisedokumenten*. Folien zum Seminarvortrag, http://www.alech.de/biometrie_reisedokumente_icao.pdf, Zugriff am 30.01.2005

- [LDS04] International Civil Aviation Organization (2004): *Development of a Logical Data Structure – LDS for optional capacity expansion technologies*, Technical Report, Version 1.7, <http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf>, Zugriff am 30.01.2005
- [PiStEDR04] Privacy International, Statewatch, European Digital Rights (2004): *An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents*, http://www.privacyinternational.org/issues/terrorism/ep_letter_biometrics.html, Zugriff am 30.01.2005
- [PKI04] International Civil Aviation Organization (2004): *PKI for Machine Readable Travel Documents offering ICC Read-Only Access*, Technical Report, Version 1.1, http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf, Zugriff am 30.01.2005
- [Scha04] Schaar, Peter (2004): *Biometrische Merkmale in Pässen nur unter Vorbehalt*, Pressemitteilung vom 02. Dezember 2004, <http://www.bfd.bund.de/Presse/pm20041202.html>, Zugriff am 30.01.2005
- [TAB03] Petermann, Thomas; Scherz, Constanze; Sauter, Arnold – Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (2003): *Biometrie und Ausweisdokumente Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung – Zweiter Sachstandsbericht*, <http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf>, Zugriff am 30.01.2005
- [TR04] International Civil Aviation Organization, Technical Advisory Group on Machine Readable Travel Documents / New Technologies Working Group (2004): *Biometrics Deployment Of Machine Readable Travel Documents. Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents*, Technical Report, Version 2.0, <http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf>, Zugriff am 30.01.2005