A Security Review of the Biometric Passport

I. Background

International developments

- After 9/11 international move towards stronger identification of citizens & travellers
- US: Visa waiver program after 25 Oct 06 only for countries with biometric passport
- Standards developed by ICAO: *International Civil Airline Organisation*
- EU regulations & timeframe
**Role of the Netherlands**

- Large trial “2B or not 2B” (6 cities, 15,000 participants, Sept’04-Feb’05), see later
- Philips main supplier of “smartMX” chips
- SDU Identification (inter)nationally active as document supplier (and also within ICAO and ISO).
- Issuance started 28 Aug’06, at first with facial scan only, without fingerprints (both passports and national identity cards)

**Own involvement**

- Membership of “expert council” set up by ministry of internal affairs
- Production of own terminal-side software
- Commercial consultancy/testing for ministry
- Role in discussion in media

**Disclaimer:** no biometry expert

---

**Passport fraud**

- Forgery of modern passports (NL, Ger, ...) very difficult
- Production of passports is now centralised
- Criminal organisations collect lots of passports, and look for reasonable matches
- Passports also borrowed for illegal border crossing
- **Look alike fraud** is source of concern
- Hence original aim: biometric **Verification**

**Reasonable security goals**

Passport chip with contactless access requires:

- **Passport reader authenticates** itself first and behaves “properly”
  - Clarity about storage & use of biometric data
- **No identifying information is released** without the consent of the passport’s holder
  - This should include identification numbers of chips and country identification: risk of bomb targeted at individuals/nationals.
- Receiver must be able to **check authenticity and integrity** of contained data
II. Standards & requirements

ICAO on MRTD
- MRTD: Machine Readable Travel Document
- Open standards, for states and suppliers
- PKI task force with members from US, UK, Can, Ger, NL.
- Only facial image mandatory; fingerprints, iris scan, etc. optional
- Only integrity check mandatory; several other protection mechanisms optional
- See http://www.icao.int/mrtd

EU on MRTD
- Facial scan included before 28 Aug ’06
- Fingerprints later, ≤ 3 year after agreement on protection mechanism
- Basic Access Control mandatory:
  - Access key for RFID chip extracted from Machine Readable Zone (MRZ)
- Intended as consent to read

NL on MRTD
- Introduction in 2 stages, started 28 Aug ’06
- Also authenticity check required
- Original aim (2002): verification only, with decentralised storage of biometric data
- New aims (Jan. 2005, “letter on terror”):
  - identification, called “on line verification”
  - central database of biometric data
  - meant as contribution to effectivity of identification laws
- Parliamentary approval still pending.
Outcome biometry trial in NL

- Report **2B or not 2B** appeared in Oct '06, online available, also in English: [www.europeanbiometrics.info/images/resources/88_630_file.pdf](http://www.europeanbiometrics.info/images/resources/88_630_file.pdf)
- Focus on enrollment, not so much verification (only false negatives relevant)
- Real difficulties for ages <12 and >60
- Overall success rate both fingerprints: \( \approx 90\% \) (faces not really tested; only 5 day interval)
- Useful experiment, with lots of practical experience (eg. exchange of fingers)

Protection mechanisms

<table>
<thead>
<tr>
<th>Protection level</th>
<th>To protect</th>
<th>Mechanism</th>
<th>EU</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic access ctrl</td>
<td>access &amp; confidentiality</td>
<td>encryption via key from MRZ</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Passive authent.</td>
<td>integrity of content</td>
<td>signature by SDU (by NL)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Active authent.</td>
<td>authenticity of document</td>
<td>signing of challenge</td>
<td>−</td>
<td>+</td>
</tr>
<tr>
<td>Extended access ctrl</td>
<td>confidentiality of fingerprints</td>
<td>BSI proposal</td>
<td>+</td>
<td>n.a.</td>
</tr>
</tbody>
</table>

Metallic “Faraday cage” additional option.

International PKI

- **Country Signing CA** (NL) signs certificate of **Document Signer** (SDU)
- SDU signs “security object” in chip, for integrity (passive authentication)
- Passport chip contains:
  - SDU certificate
  - own public key (hash in security object)
- Self-signed country certificates distributed at first via diplomatic post, later electronically.

III. High level protocols
Basic Access Control I

- “Consent” & confidentiality mechanism
- MRZ info yields 3DES “document basic access keys” $K_{ENC}$, $K_{MAC}$, fixed for lifetime
- Relevant MRZ input: passport nr. + birth date + expiry date
- Entropy somewhere between 50 and 60 bits
- Brute force attack:
  - for skimming (neighbour in train) card too slow
  - possible on eavesdropped data (passport numbering system relevant)

Basic Access Control II

\[
Psp \quad \begin{array}{c} N_P \\ (8 \text{ byte}) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} \quad \begin{array}{c} \text{Rdr} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array}
\]

\[
Psp \quad A := N_P || N_R || K_R \\
K_{ENC}(A) \cdot K_{MAC}(K_{ENC}(A)) \\
\begin{array}{c} \text{Rdr} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array}
\]

\[
Psp \quad B := N_P || N_R || K_P \\
K_{ENC}(B) \cdot K_{MAC}(K_{ENC}(B)) \\
\begin{array}{c} \text{Rdr} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array}
\]

Session keys are then derived from $K_P$ and $K_R$, for rest of communication.

Basic Access Control III

- July’05: Marc Witteman (Riscure) finds:
  - NL passport nos. used in ascending order
  - About 5000 per day
  - Check digit formula uncovered
- January’06: eavesdropping shown on TV
- Substantial reduction of entropy (to ~ 35 bits)
- ICAO rejects strengthening of Basic Access Control (april’06)
- NL: issuance order becomes random (but eg. not in Germany)

Passive authentication: integrity

- Read “Security Object” from chip with:
  - SDU certificate (& public key for AA)
  - hashes of all passport data
  - SDU signature
- Authenticity check consists of:
  - check SDU-certificate with NL public key
  - check SDU-signature with SDU-certificate
  - check hashes, after reading data
- Cloning still possible: Grunwald at Black Hat (aug’06) for German passport (without AA)
Active authentication: authenticity

Passport has private (RSA) key, with public key in (signed) security document.

\[
P_{\text{sp}} \xrightarrow{N_R} \xrightarrow{(8 \text{ byte})} R_{\text{dr}}
\]

\[
P_{\text{sp}} \xrightarrow{\text{Sig}(N_R \ || \ \text{padding})} R_{\text{dr}}
\]


Extended access control

- For fingerprint protection; optional for ICAO
- Required by EU
- German (BSI) proposal:
  - Readers must authenticate, via certificates
  - New Diffie-Hellman session key for data protection
  - Certificate revocation is problematic
- Each country controls itself who can read fingerprints: limited use foreseen

Secure logon via your passport

- Give your machine / local network:
  - your passport \( K_{\text{MAC}}, K_{\text{ENC}} \) (from MRZ)
  - your passport public key
- Authenticate yourself via challenge-response: “what you have”
- Strengthened “two factor” authentication possible with:
  - combination with traditional password
  - or picture check: “what you are”
- Will be implemented by RU

IV. Passports for private use?
Digital signature via your passport?

*Better not*, because:

- Embedded private key used for challenge-response: incompatible with signing
- Anyone who accesses your passport can sign for you—e.g. at border crossing

V. Card & reader

Card info I

- SmartMX Chip from Philips (P5CT072), with:
  - 72Kbyte EEPROM
  - contactless interface (ISO/IEC 14443 A)
  - 3DES, RNG, RSA, SHA1 (ECC?)
- High certification: level EAL5+ of Common Criteria
- JavaCard OS: IBM JCOP41 version 2.20
  Certification by German BSI ongoing
- Passport Java applet written by SDU: closed source

Card info II

- *Writing* to chip (e.g. for visa, children etc.) not foreseen.
- No certainty about absence of *backdoors*. But secret access should be detectable via extensive monitoring
Contactless issues

- Operation distance < 10 cm; eavesdrop < 10m?
- Multiple cards may be in reach of reader
- **Anti-collision** protocol described in ISO 14443-3.
- NL: deployed card uses random identifier
- With fixed identifier “tree walking protocol”
  - 4 byte identifier
  - allows covert tracing and targeting

VI. Conclusions

Conclusions I

- Security goals reached?
  - Integrity & authenticity well-protected
  - Confidentiality weakest (∼ 70 bit entropy, ideally)
  - No reader authentication (so far); no clarity about backoffice use of biometrics
  - NL implemented all available protection measures
- Choice for wireless connections hard to understand.

Conclusions II

- Biometric passports big social experiment:
  - Unwilling citizens may destroy chips
  - Action group may start campaign to do so
  - Such sabotage may destroy whole project
- Citizens have no control over what happens to their biometric data. Concerns:
  - Big brother / police state getting closer
  - Identity fraud
- On card reader & verification needed for trust
Conclusions III

- Biometry much overrated:
  - Silly: “same password, used everywhere”
  - Large scale use of biometrics uncertain
  - Many false positives/negatives expected
- Identification goals are undermined:
  - by widespread use in other applications
  - if many citizens (obnoxiously) put their fingerprints on the web
  - fingerprints are lost for high-level security by this setup: too many copies around

Conclusions IV

- Will it stop terrorists? No, since they go for easy, soft targets
- Will it reduce look-alike fraud? Probably, after a while
- Will it reduce crime? A bit, mostly by catching/deterring stupid criminals

Further reading / info

- Juels (RSA labs), Molnar & Wagner (UC-Berkeley) at:
- Kc (U-Colombia) & Karger (IBM) at:
- Own passport paper (LNCS 4266) via:
- Slides etc. via: