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 starts 28 Aug ’06, at first with facial scan only, without fingerprints

Own involvement

- Membership of “expert council” set up by ministry of internal affairs (Jacobs)
- Participation in enrollment procedure, resulting in test passport (Oostdijk)
- Production of own terminal-side software (Wichers Schreur) & test development
- Role in discussion in media

Disclaimer: no biometry experts

Passport fraud

- Forgery of modern (NL) passports very difficult
- Production of passports has been centralised
- Criminal organisations collect large numbers of passports, and look for reasonable matches
- **Look alike fraud** is source of concern
- Hence original aim: biometric **Verification**

Reasonable security goals

Chip in passport with contactless access requires:

- **No identifying information is released** without the consent of the passport’s holder. This should include identification numbers of chips and country identification (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 (foreseen soon)
- **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, starting 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
Outcome biometry trial in NL

- Report appeared in Oct ’06, also in English (available online)
- Focus on enrollment, not so much verification (only false negatives relevant)
- Real difficulties for ages <12 and >60
- Overall success rate both fingerprints: ~ 90% (faces not really tested; only 5 day interval)
- Useful experiment, with lots of practical experience (e.g. exchange of fingers)

Protection mechanisms

<table>
<thead>
<tr>
<th>Protection</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” possibly added (in US)

International PKI

- **Country Signing CA** (NL) signs certificate of **Document Signer** (SDU)
- SDU signs “security object”, for 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” $K^\text{ENC}$, $K^\text{MAC}$, fixed for lifetime
- Relevant MRZ input: passport nr. + birth date + expiry date
- Entropy somewhere between 50 and 60 bits
- Brute force attack:
  - for skimming (neighbor in train) card too slow
  - possible on eavesdropped data

Basic Access Control II

$$\begin{align*}
Psp & \quad N_P \\
    & \quad (8 \text{ byte}) \\
    & \quad \text{Rdr} \\
\end{align*}$$

$$\begin{align*}
Psp & \quad A := N_P \parallel N_R \parallel K_R \\
    & \quad K^\text{Enc}(A) \parallel K^\text{MAC}[K^\text{Enc}(A)] \\
    & \quad \text{Rdr} \\
\end{align*}$$

$$\begin{align*}
Psp & \quad B := N_P \parallel N_R \parallel K_P \\
    & \quad K^\text{Enc}(B) \parallel K^\text{MAC}[K^\text{Enc}(B)] \\
    & \quad \text{Rdr} \\
\end{align*}$$

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

Basic Access Control III
- July’06: Marc Witteman (Riscure) finds:
  - NL passport nr. used in ascending order
  - About 5000 per day
  - Check digit formula discovered
  - Substantial reduction of entropy (to $\sim 35$ bits)
  - Ministry: issuance order deeply entrenched in procedures and checks
  - ICAO is studying strengthening of Basic Access Control

Passive authentication
- Read “Security Object” from chip with:
  - SDU certificate
  - public key for active authentication
  - hashes of all passport data
  - SDU signature
- Authenticity check consists of:
  - SDU-certificate, using NL public key
  - signature by SDU, using SDU-certificate
  - hashes, after reading data
- Cloning still possible.
Active authentication, against cloning

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

\[
Psp \xrightarrow{\text{SR}} \text{Rdr} \quad (8 \text{ byte})
\]

\[
Psp \xrightarrow{\text{Sig}(\text{SR} \parallel \text{padding})} \text{Rdr}
\]


Extended authentication

- For fingerprint protection; optional for ICAO
- Required by EU, but no EU-standard yet
- German (BSI) proposal under consideration:
  - 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 \( K_{MAC}, K_{ENC} \) (from MRZ)
  - your passport public key
- Authenticate yourself via challenge-response: “what you have”
- Possibly add picture check: “what you are”.
- Will be implemented by RU

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

**Better not**, because:

a. anyone who holds your passport can sign for you. [Sign software might check picture . . .]

b. sign-challenges only 64 bit (hash-attack: 32)
   Possible fix: break up sign-message

c. Proof of identity requires release of your MRZ (and hence access to your chip), since:
   - MRZ contains your name + birth date
   - hash of MRZ signed by authorities, as part of “security object”

---

**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 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.
- With fixed identifier “tree walking protocol”
  - in current SDU test passport (4 byte id)
  - allows tracing and targeting
- SDU: “deployed card will use random identifier”

Reader implementation I

- Sample passport provided to RU, with ad hoc protection of fingerprints (via symmetric key)
- Own Java Terminal written – using BouncyCastle crypto library
  - Crypto (≈ 2 KLOC)
  - Parsing (≈ 2 KLOC)
  - GUI (≈ 1.5 KLOC)
- Intention to release it as open source

Reader implementation II

- Many, many standards. ICAO public, but ISO not.
- Protocols often underspecified for abnormal situations
- Implementation not difficult, but many details
- Interoperability problems with contactless readers – may happen also in practice

VI. Conclusions
Conclusions I

- Biometric passports are on their way
- General approach (ICAO, EU): careful.
- Basic Access Control weak link.
- Protection of fingerprints not fully settled yet
- Open communication with Ministry & SDU
- Further tests of cards foreseen (also rôle of LaQuSo)

Conclusions II

- Biometry much overrated:
  - Silly approach: “same password, used everywhere” (no template protection)
  - Large scale use of biometrics uncertain
  - Substantial false positives/negatives to be expected
- Identification goals are undermined:
  - by widespread use in other applications
  - if many citizens (obnoxiously) put their fingerprints on the web

Conclusions III

- Function creep risks:
  - Who will use passport’s biometrics? Welfare authorities, banks, casinos etc.?
  - Central storage: risks of compromise, misuse, etc.
- Set-up for improved identity management can lead to large scale identity theft.
- Real challenges (also for privacy!) are in the integration in backoffice databases
- Slow increase of use to be expected

Conclusions IV

- Passport fraud will become more difficult
- But the few (if any) who manage to break the system get unprecedented power (issue their own passports . . .)
- Will it stop terrorists? No, since they go for easy, soft targets
- Will it work? Probably, after a while
- Will it help? A bit, mostly to deter/catch stupid criminals
Further reading / info

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

*Thanks for your attention!*