



# 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*



## Role of the Netherlands

- Large trial “2B or not 2B” (6 cities, 15.000 participants, Sept’04-Feb’05).
- Philips main supplier of “smartMX” chips
- SDU Identification (inter)nationally active as document supplier (and also within ICAO).



## 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 goal

Chip in passport with wireless 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.8/33



### Biometric Passport

#### 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>

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.9/33



### Biometric Passport

#### EU on MRTD

- Facial scan included before 28 Aug '06
- Fingerprints later,  $\leq 3$  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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.10/33



### Biometric Passport

#### NL on MRTD

- Outcome biometry trial: (as yet unknown)
- Introduction in two stages; start < 28/6/'06.
- 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.11/33



## Protection mechanisms

	to protect	mechanism	EU	US
passive authent.	<i>integrity of content</i>	<i>signature by SDU (by NL)</i>	+	+
active authent.	<i>authenticity of document</i>	<i>signing of challenge</i>	- NL +	+
basic access ctrl	<i>access &amp; confidentiality</i>	<i>encryption via key from MRZ</i>	+	-
extended access ctrl	<i>confidentiality of fingerprints</i>	??	+	n.a.

US: metallic “Faraday cage”; allows eavesdrop

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.12/33



## 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.

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.13/33



## III. High level protocols

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.14/33



## Basic Access Control I

- 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:
  - senseless with document, . . . with MRZ!
  - in principle on eavesdropped data (passport numbering system relevant)
- “Consent” & confidentiality mechanism

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.15/33



## Basic Access Control II

**Psp**  $\xrightarrow[N_P]{(8 \text{ byte})}$  **Rdr**

**Psp**  $\xleftarrow[K_{Enc}\{A\}, K_{MAC}[K_{Enc}\{A\}]}{A := N_P || N_R || K_R}$  **Rdr**

**Psp**  $\xrightarrow[K_{Enc}\{B\}, K_{MAC}[K_{Enc}\{B\}]}{B := N_P || N_R || K_P}$  **Rdr**

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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.16/33



## Active authentication, against cloning

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

**Psp**  $\xleftarrow[N_R]{(8 \text{ byte})}$  **Rdr**

**Psp**  $\xrightarrow{\text{Sig}(N_R || \text{padding})}$  **Rdr**

Possible risk of signing location + timing data in  $N_R$ , for tracking.

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.18/33



## Passive authentication

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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.17/33



## 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.19/33



## IV. Passports for private use?

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.20/33



## Biometric Passport

### Secure logon via your passport

- Give your machine / local network:
  - your passport 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.21/33



## Biometric Passport

### Digital signature via your passport?

**Better not**, because:

- anyone who holds your passport can sign for you. [Sign software might check picture . . .]
- sign-challenges only 64 bit (attack: 32)  
Possible fix: break up sign-message
- 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”

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.22/33



## V. Low level stuff

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.23/33



## 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.24/33



## 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

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.25/33



## 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”

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.26/33



## VI. Demonstration & Implementation

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.27/33



## Demonstration



## Implementation – Details

- Java Terminal – using BouncyCastle crypto library
  - Crypto ( $\approx 2$  KLOC)
  - Parsing ( $\approx 2$  KLOC)
  - GUI ( $\approx 1.5$  KLOC)
- C (for speed tests) – using OpenSSL crypto library
  - Crypto ( $\approx 2$  KLOC)
- JavaCard Applet
  - Applet size ( $\approx 10$  KB byte code)



## Implementation – Experiences

- Many, many standards
  - Good thing
  - ICAO standards are publicly available
  - ISO standards are not publicly available
  - Good crypto library helpful
  - Protocols often underspecified for abnormal situations
- Not difficult, but many details
- Problems with contactless readers



## VII. Conclusions



## Conclusions I

- Biometric passports are on their way
- General approach (ICAO, EU): careful.
- Basic Access Control possibly weak link.
- Protection of fingerprints not settled yet
- Open communication with Ministry & SDU
- Function creep risks:
  - Who will use passport's biometrics? Welfare authorities, banks, casinos etc.?
  - Central storage: risks of compromise, misuse, etc.

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.32/33



## Conclusions II

- Large scale use of biometrics uncertain:
  - Substantial false positives/negatives to be expected
  - No replacement of compromised biometric identifiers possible
- Set-up for improved identity management can lead to large scale identity theft.
- See also overview paper by: Juels (RSA labs), Molnar & Wagner (UC-Berkeley) at:  
<http://eprint.iacr.org/2005/095>

Jacobs / Wichers Schreur (SafeNL 24/6/05) – p.33/33