



A Review of the Biometric Passport



I. Background



Contents

- I. Background
- II. Standards & requirements
- III. High level protocols
- IV. Passports for private use?
- V. Identity management issues
- VI. Conclusions

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

Jacobs (Tilt 15/2/06) – p.4/34



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
- Commercial consultancy for ministry
- Role in discussion in media

Disclaimer: no biometry expert

Jacobs (Tilt 15/2/06) – p.5/34



Passport fraud

- Forgery of modern (NL) passports 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**

Jacobs (Tilt 15/2/06) – p.6/34



Reasonable security goals

Chip in passport with contactless access requires:

- Passport **reader authenticates** itself first
- **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

Jacobs (Tilt 15/2/06) – p.7/34



II. Standards & requirements

Jacobs (Tilt 15/2/06) – p.8/34



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 (Tilt 15/2/06) – p.9/34



Biometric Passport

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

Jacobs (Tilt 15/2/06) – p.10/34



Biometric Passport

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

Jacobs (Tilt 15/2/06) – p.11/34



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
- Focus on enrollment, not so much verification (only false negatives relevant)
- Real difficulties for ages <12 and >60
- Overall succesrate both fingerprints: ~ 90% (faces not really tested; only 5 day interval)
- Useful experiment, with lots of practical experience (eg. exchange of fingers)



Protection mechanisms

	to protect	mechanism	EU	US
basic access ctrl	<i>access & confidentiality</i>	<i>encryption via key from MRZ</i>	+	+(new)
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 +	+
extended access ctrl	<i>confidentiality of fingerprints</i>	<i>BSI proposal</i>	+	n.a.

Metallic “Faraday cage” possibly added (in US)



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



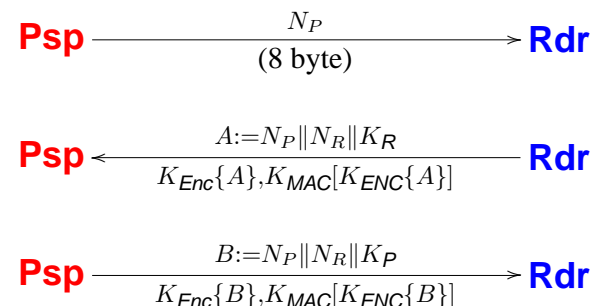
Basic Access Control I

- “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 (neighbor in train) card too slow
 - possible on eavesdropped data (passport numbering system relevant)

Jacobs (Tilt 15/2/06) – p.16/34



Basic Access Control II



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

Jacobs (Tilt 15/2/06) – p.17/34



Basic Access Control III

- July'05: Marc Witteman (Riscure) finds:
 - NL passportnrs. 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)
- Ministry: issuance order deeply entrenched in procedures and checks
- ICAO is studying strengthening of Basic Access Control

Jacobs (Tilt 15/2/06) – p.18/34



Passive authentication

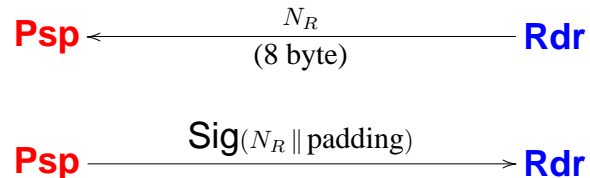
- Read “Security Object” from chip with:
 - SDU certificate
 - public key for active authentication
 - hashes of *all* passport data
 - SDU signature
- Authenticity check consists of:
 - SDU-certificate, using NL public key
 - signature by SDU, using SDU-certificate
 - hashes, after reading data
- Cloning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

Jacobs (Tilt 15/2/06) – p.19/34



Active authentication, against cloning

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



Risk of signing location + timing data in N_R , for tracking. Bas. Acc. Ctrl. offers some protection.

Jacobs (Tilt 15/2/06) – p.20/34



IV. Passports for private use?

Jacobs (Tilt 15/2/06) – p.22/34



Extended access control

- 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

Jacobs (Tilt 15/2/06) – p.21/34



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

Jacobs (Tilt 15/2/06) – p.23/34



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”

Jacobs (Tilt 15/2/06) – p.24/34



V. Identity management issues

Jacobs (Tilt 15/2/06) – p.25/34



Trend towards a situation in which:

- everything about everyone is recorded
- individual freedom (hopefully) remains, . . .
- . . . but in a much stricter framework: trespassing of rules will be noticed
- you may be held accountable for all your deeds—already in this life ;–)
- dependency increases on powers that set and check the rules (shift of balance)
- life is safer, but also more boring.

Jacobs (Tilt 15/2/06) – p.26/34



Any room left for privacy?

- If so, then it must be realised via technical means: PET = Privacy Enhancing Technologies
- Making everyone always identifiable introduces unacceptable risks: RFID-bombs
- Privacy is essential for **personal security**—in contrast to the one-sided view as impediment to **public security**.
- Don't treat citizens as ear-marked cattle, but give them control over authentication

Jacobs (Tilt 15/2/06) – p.27/34



Identification as negotiation

- In the future we all carry smart id-tokes (GSM, id-card, implanted chip)
- Basic rule: environment should authenticate itself first
- Token may then decide to display part of its identity—according to personal policy
- Environment can demand proofs (eg. via biometry) before giving rights/services
- Forced identification possible, at authenticated lawful e-checkpoints.

Jacobs (Tilt 15/2/06) – p.28/34



VI. Conclusions

Jacobs (Tilt 15/2/06) – p.29/34



Conclusions I

- Biometric passports are on their way, but holders have no control
- Open communication with Ministry & SDU
- Security goals reached?
 - Integrity & authenticity well-protected
 - Confidentiality weak
 - Reader authentication only in EU (but unauthenticated access still possible)
- Protection of fingerprints not fully settled yet
- Further tests of cards foreseen

Jacobs (Tilt 15/2/06) – p.30/34



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

Jacobs (Tilt 15/2/06) – p.31/34



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

Jacobs (Tilt 15/2/06) – p.32/34



Conclusions IV

- Passport fraude 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

Jacobs (Tilt 15/2/06) – p.33/34



Further reading / info

- Juels (RSA labs), Molnar & Wagner (UC-Berkeley) at:
<http://eprint.iacr.org/2005/095>
- Kc (U-Colombia) & Karger (IBM) at:
<http://eprint.iacr.org/2005/404>
- Identity management via:
<http://www.prime-project.eu.org>
- Slides etc. via:
<http://www.cs.ru.nl/B.Jacobs>

Jacobs (Tilt 15/2/06) – p.34/34