About Machine Readable Travel Documents
Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication

Jean Monnerat, Serge Vaudenay, Martin Vuagnoux

EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

http://lasecwww.epfl.ch/
1 ICAO-MRTD

2 Non-Transferable Proofs
ICAO-MRTD

Non-Transferable Proofs
1 ICAO-MRTD
   - ICAO-MRTD Overview
   - Data Structures and PKI
   - MRTD Cryptography
   - Security and Privacy Issues

2 Non-Transferable Proofs
Objectives

to enable inspecting authorities to securely identify visitors with the help of machine-readable digital information

→ biometrics
→ contactless IC chip
→ digital signature + PKI

maintained by UN/ICAO (International Civil Aviation Organization)
MRTD History

- 1968: ICAO starts working on MRTD
- 1980: first standard (OCR-B Machine Readable Zone (MRZ))
- 1997: ICAO-NTWG (New Tech. WG) starts working on biometrics
- 2001 9/11: US want to speed up the process
- 2004: version 1.1 of standard with ICC
- 2006: extended access control under development in the EU
How to Distinguish a Compliant MRTD
MRTD in a Nutshell

- Data authentication by digital signature + PKI aka **passive authentication**
- Access control + key agreement based on MRZ_info aka **basic access control (BAC)**
- Chip authentication by public-key cryptography aka **active authentication (AA)**
1 ICAO-MRTD
   - ICAO-MRTD Overview
   - Data Structures and PKI
   - MRTD Cryptography
   - Security and Privacy Issues

2 Non-Transferable Proofs
MRZ Example

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC
LDS Structure

- DG1 (mandatory): same as MRZ
- DG2 (mandatory): encoded face
- DG3: encoded finger(s)
- DG4: encoded eye(s)
- DG5: displayed portrait
- DG6: (reserved)
- DG7: displayed signature
- DG8: data feature(s)
- DG9: structure feature(s)
- DG10: substance feature(s)
- DG11: add. personal detail(s)
- DG12: add. document detail(s)
- DG13: optional detail(s)
- DG14: (reserved)
- DG15: KP\textsubscript{AA}
- DG16: person(s) to notify
- DG17: autom. border clearance
- DG18: electronic visa
- DG19: travel record(s)
- SO\textsubscript{D} (mandatory)
Structure

- list of hash for data groups DG1–DG15
- formatted signature by DS (include: information about DS)
- (optional) $C_{DS}$
one PKI per country
- one CSCA (Country Signing Certificate Authority)
  - $C_{CSCA}$: self-signed CSCA public key $K_{PuCSCA}$
  - $C_{CSCA}$ distributed to other countries by diplomatic means
- possibly many DS (Document Signer) per country
  - $C_{DS}$: certificate for a DS public key $K_{PuDS}$
- $SO_D$: signature of (part of) LDS in MRTD
ICAO-MRTD

1. ICAO-MRTD Overview
2. Data Structures and PKI
3. MRTD Cryptography
4. Security and Privacy Issues

2. Non-Transferable Proofs
Basic Access Control

**goal**
prevent from unauthorized access by the holder (privacy)

- read MRZ (OCR-B)
- extract MRZ_info
- run an authenticated key exchange based on MRZ_info
- open secure messaging based on the exchanged symmetric key

→ proves that reader knows MRZ_info
MRZ_info

PMFRADUPONT<<<<JEAN<<<<<<<<<<<<<<<<<<<<<<<<<
74HK8215<6CHE7304017M0705121<<<<<<<<<<<<<<03

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC
Secure Messaging

**goal** authentication, integrity, confidentiality of communication

→ secure channel based on 3DES
Passive Authentication

**goal** authenticate LDS

- after getting $SO_D$, check the included certificate $C_{DS}$ and the signature
- when loading a data group from LDS, check its hash with what is in $SO_D$

$\rightarrow$ stamp by DS on LDS
Active Authentication

**goal** authenticate the chip

- proves that ICC knows some secret key $K_Pr_{AA}$ linked to a public key $K_{Pu_{AA}}$ by a challenge-response protocol ($K_{Pu_{AA}}$ in LDS authenticated by passive authentication)

$\rightarrow$ prove that the chip is not a clone
Active Authentication Protocol

IFD

pick RND.IFD
check

← nonce || RND.IFD

Σ ← Sign_{KPr_{AA}}(F)

ICC
Sequence of Steps for Identification

1. Read MRZ (OCR-B)
2. Resolve collisions to ICC
3. Access denied?
   - Yes: BAC + open sec. messaging
   - No: Passive authentication
4. MRZ matches?
   - Yes: Check AA (if supplied)
   - No: Check biometrics
ICAO-MRTD

1. ICAO-MRTD Overview
2. Data Structures and PKI
3. MRTD Cryptography
4. Security and Privacy Issues

Non-Transferable Proofs
Coming From Wireless Technology

(claimed to be possible at a distance of 10m)

- detecting the proximity of an e-passport
  - threat: giving valuable information to passport theafs
  - threat: privacy (in some cases) by tracking people

- data skimming
  - threat: privacy

- unauthorized access
  - threat: privacy
Coming From IC Chip

- too much trust in automated process, lazy identification
  **threat**: identity theft
- malicious cookies put in MRTD
  **threat**: privacy
- dependence on the technology: DoS attack could kill the IC chip
  **threat**: waste of time at border controls
- abuse of automatic recognition
  **threat**: privacy
- leakage of digital evidence
  **threat**: privacy
Digital Evidence: Challenge Semantics Attack

challenge semantics in AA:

- evidence that $D$ existed when MRTD was queried

\[
\text{RND.IFD} = H(D)
\]

\[
\text{evidence} = (D||\text{LDS}||\Sigma)
\]

- evidence that MRTD was accessed at time $t$

\[
\text{RND.IFD} = H(\text{social}(t-1))
\]

\[
\text{evidence} = \text{timestamp}_t(\text{social}(t-1)||\text{LDS}||\Sigma)
\]
Digital Evidence: Transferable LDS Authentication

- signed personal data (name, age, gender, face, etc)
- can no longer hide/deny name, age, gender...
- when DG11 is used: more personal data (place of birth etc)
- personal profiles can be sold if they come with a proof
1 ICAO-MRTD

2 Non-Transferable Proofs
ICAO-MRTD

Non-Transferable Proofs
- Notions of Non-Transferability
- ZK Protocols for MRTD
Mafia Fraud + Fully Non-Transferable Proof

Prover
- knowledge

Verifier
- $K_p$

Mafia
- 😞

proof of knowledge

proof of knowledge or of knowing a secret key attached to $K_p$

→ need PKI for verifiers: maybe an overkill
Zero-Knowledge: Offline Non-Transferability

- Prover
- Verifier
- Prover
- Cheater
- Simulator
- Cheater

- proof of knowledge leaks nothing that can later be used
- data of distribution $D$
- data of distribution $D$
Sigma Protocols

Prover

Verifier

secret: $x$

commitment

challenge

response

check
Example: GPS Identification

**Prover**

parameters: $g, A, B, S$

public key: $I (I = g^s)$

secret key: $s \in [0, S]$

pick $r \in [0, A - 1]$

$x \leftarrow g^r$

pick $c \in [0, B - 1]$

$y \leftarrow r + cs$

$y \leftarrow r + cs$

Verifier

input: $I, g, A, B, S$

check $g^y = xI^c$

and $0 \leq y < A + (B - 1)(S - 1)$
Fiat-Shamir Signature

Basic Fiat-Shamir identification protocol:

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>pick ( r, x = r^2 \mod n )</td>
<td>( v, x ) ( \rightarrow ) ( e ) ( \leftarrow ) ( e = 0 ) or ( 1 )</td>
</tr>
<tr>
<td>( y = rs^e \mod n )</td>
<td>( y ) ( \rightarrow ) check ( y^2 v^e \equiv x )</td>
</tr>
</tbody>
</table>

Conversion into a signature:
- use random coins from \( H(\text{message, previously seen transcript}) \)
- simulate the verifier using these coins
- the signature is the final transcript
Honest vs Malicious Verifier

- for Sigma-protocols: the signature is unforgeable
- malicious verifier that simulates the previous conversion: it produces a signature
- consequences: Sigma-protocols are not ZK
- maybe honest-verifier ZK
- verifiers playing the challenge semantics are not honest
- challenge semantics in GPS identification: $c = H(\text{semantics}, x)$
- UDVSP [Baek et al. Asiacrypt05]: same
ICAO-MRTD

Non-Transferable Proofs
- Notions of Non-Transferability
- ZK Protocols for MRTD
Converting Sigma Protocols into ZK Protocols

**Prover**

- **secret**: \( x \)
- pick \( c_P \)
- check(\( c_V, \gamma, \delta \))

\( (\gamma, \delta) \leftarrow \text{commit}(c_V) \)

**Verifier**

- pick \( c_V \)
- check

(\( c_P \oplus c_V \))
Proof of Signature Knowledge based on GQ

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>formatted digest:</strong> ( X )</td>
<td><strong>formatted digest:</strong> ( X )</td>
</tr>
<tr>
<td><strong>signature:</strong> ( x )</td>
<td><strong>public key:</strong> ( N, e )</td>
</tr>
</tbody>
</table>

- **pick** \( y \in \mathbb{Z}_N^* \)
- **pick** \( c_P \in \{0, 1\}^\ell \)
- \( Y \leftarrow y^e \mod N \)
- **check** \((c_V, \gamma, \delta)\)
- \( z \leftarrow yx^c \mod N \)

\( (c = c_P \oplus c_V) \)

- **pick** \( c_V \in \{0, 1\}^\ell \)
- \( (\gamma, \delta) \leftarrow \text{commit}(c_V) \)
- **check** \( z^e = YX^c \mod N \)
Easy AA from Previous Passive Authentication

proof of holding a signature of SOD

↓

proof of holding a secret signature of SOD
**AA based on GPS**

**Prover**

- **parameters:** \( g, A, B, S \)
- **public key:** \( I (I = g^s) \)
- **secret key:** \( s \in [0, S] \)

- \( \text{pick } r \in [0, A - 1] \)
- \( \text{pick } c_P \in [0, B - 1] \)
- \( x \leftarrow g^r \)
- \( y \leftarrow r + cs \)
- \( \text{check}(c_V, \gamma, \delta) \)

**Verifier**

- **input:** \( I, g, A, B, S \)

- \( \text{pick } c_V \in [0, B - 1] \)
- \( (\gamma, \delta) \leftarrow \text{commit}(c_V) \)
- \( y \)
- \( y \leftarrow r + cs \)
- \( \text{check } g^y = xI^c \)
- \( \text{and } 0 \leq y < A + (B - 1)(S - 1) \)
- \( (c = c_P + c_V \mod B) \)
Conclusion

- privacy threat of MRTD coming from wireless channel
- privacy threat of MRTD coming from leakage of evidence
- weakly non-transferable proofs
- proof of signature knowledge based on GQ
- fix of AA
Q & A