How To Secure Electronic Passports

Marc Witteman & Harko Robroch
Riscure
02/07/07 - Session Code: IAM-201
Other personal info on chip

Other **less common data fields** that may be in your passport

- Custody Information
- Travel Record Detail(s)
- Endorsements/Observations
- Tax/Exit Requirements
- Contact Details of Person(s) to Notify
- Visa
What is the Electronic Passport logo and what does it mean?

The Electronic Passport logo (shown below) is the international symbol for an electronic passport. It signifies that the passport contains an integrated circuit or chip on which data about the passport and passport bearer is stored. The logo will be displayed at border inspection lanes at all airports and transit ports equipped with special data readers for Electronic Passports.
Our involvement in electronic passports

- Published weakness in BAC static key in July 2005
- Performed security testing on electronic passport technology
- Security Test Lab
  - smart cards
  - embedded devices
Overview

• **Passport threats and protection mechanisms**

• Security challenges and solutions
  — Inspection terminal configuration
  — Access control to personal data
  — Contactless chip

• Conclusion
What to protect against?

1. **Passport forgery**
   - Criminal organization makes a false passport
   - High-tech and more difficult

2. **Look-alike fraud**
   - Criminal organization steals many passports
   - Look for the best match
   - Low-tech and relatively easy
1. To address passport forgery
   - Store a certificate with passport holder data
   - Store a private key on a smart card
   - Active Authentication offers this under ICAO

2. To address look-alike fraud
   - Add personal biometric data
   - Biometric software should reduce false accepts
Overview of protection mechanisms in ICAO

• A passport implements **one** valid combination
• A terminal implements **each** of these

Authentication
(Passive, Active, Biometrics)

Who can access my data?

Does this passport belong to this person?

Access Control
(None, Basic or Extended)
Test your own passport at Amsterdam Airport

• Public access to a terminal
• Displays personal info from chip
Overview

• Passport threats and protection mechanisms

• Security challenges and solutions
  — Inspection terminal configuration
  — Access control to personal data
  — Contactless chip

• Conclusion
Risk

• Complex standard with many options; how well will terminals do?
• Most attention is on the passport, not the terminal

Challenges and solutions

• Implementation errors form a risk

• Let’s discuss two specific implementation challenges
  1. Many options to be supported by the terminal
  2. Proper RSA certificate verification not trivial

How would you detect a false acceptance?
1. Many options to be supported by the terminal

- Typical standardization **compromise**
- Protocol **options**
  - Basic Access Control
  - Active Authentication
  - Extended Access Control
  - Document signer key on passport
  - Biometrics
- Cryptographic **options**
  - Passive Authentication: RSA (PSS / PKCS1), DSA, ECDSA
  - Hashing: SHA-1, 224, 256, 384, 512
2. Proper RSA verification not trivial

**An example** in Passive Authentication

- Passport may use PKCS1
- Last year, Daniel Bleichenbacher discovered **vulnerability** in some PKCS1 implementations (with exponent 3)

**Exploit prerequisites**

- Inspection system with this vulnerability
- Country that uses PKCS1 with RSA exponent 3

*Then, you may fool a terminal with a self-made PKCS1 RSA certificate*
Overview

• Passport threats and protection mechanisms

• Security challenges and solutions
  — Inspection terminal configuration
  — **Access control to personal data**
  — Contactless chip

• Conclusion
Access control to personal data

**Risks to protect against**

- Rogue terminal
- Eavesdropping by a 3rd party
- Tracking individuals
- Recognition of citizenship

**Challenges and solutions**

- How strong is BAC?
- Using the UID to track individuals
- Extended Access Control is underway
Weakness in Basic Access Control

**Static** access key is derived from MRZ data:
- Date of birth
- Date of expiry
- Passport number

Reduce entropy to 35 bits

Prediction & dependency

Publication in July 2005

Static access key is derived from MRZ data:
- Date of birth
- Date of expiry
- Passport number

Reduce entropy to 35 bits

Publication in July 2005
Is 35 bit sufficient to protect personal data?

Solution

• Country can use unpredictable passport numbers

• But, protection remains limited due to static key that is visible for any person who had access to the passport

Example: In Aug 2006, Dutch passport moved to unpredictable numbers to reach entropy of 66 bits
UID is another challenge

- UID is a low-level RF identification number (32 bit)
- UID **threatens privacy** in two ways

**Solution:** *Randomize the UID*

**Performance challenge**
- UID very shortly after power up
- On-board random generator

Broadcast 2A73B9F0
Extended Access Control

- To access **most sensitive** data on chip (e.g. biometric data)
- Implements mutual authentication

Who can access my data?

Access Control
(Extended)
Certificate infrastructure

Foreign country

Country CA

Document Verifier

Inspection terminal

Short validity period

Your country

But a chip does not know what time it is

verify

verify

Time

Country CA

Document Verifier

Inspection terminal

Short validity period

But a chip does not know what time it is

verify

verify

Time

Certificate infrastructure
Certificate validation problem

Two solutions can be used for **lost or stolen terminals**

1. The terminal verifies itself
   
   ➔ **Is this a sound security principle?**

2. Compare with previous date
   
   ➔ **What is a risk here?**
Overview

• Passport threats and protection mechanisms
• Security challenges and solutions
  — Inspection terminal configuration
  — Access control to personal data
  — Contactless chip
• Conclusion
Contactless chip

Use of *contactless* technology appropriate?

- Introduces access and eavesdropping issues
- Shielding is applied (e.g. USA)
- Contact-based chip technology eliminates several issues
Overview

- Passport threats and protection mechanisms
- Security challenges and solutions
  - Inspection terminal configuration
  - Access control to personal data
  - Contactless chip
- Conclusion
• Inspection terminal implementation is complex

• **Country can improve privacy protection** by
  — Maximize passport number entropy
  — Randomize UID

• Extended Access Control is promising but also has a **small inherent weakness**

• Moving to a **contact** smart card would **eliminate several issues**

😊
Conclusion (2) – The electronic passport ...

- **Improves** forgery protection **when**
  - Each passport has a chip
  - Inspecting officer knows it should have a chip

- **Does not address** look-alike fraud **until**
  - Reliable biometrics are added to passports

- **Introduces** privacy **concerns**
  - Contactless (RF) is used
  - Easy way to fill a country’s database
  - Adding biometrics also challenges privacy requirements
Thank you. Questions?

Marc Witteman  
*Chief Technology Officer*
witteman@riscure.com

Harko Robroch  
*Managing Director*
robroch@riscure.com

Visit us at the smart card pavilion booth 1742

Riscure B.V.  
Rotterdamseweg 183c  
2629 HD Delft  
The Netherlands

Phone: +31 (0)15 2682664  
Http://www.riscure.com
References

- International Civil Aviation Organisation web site on MRTDs: www.icao.int/mrtd/
- Bleichenbacher attack on RSA implementations: http://www.imc.org/ietf-openpgp/mail-archive/msg14307.html
## Appendix A: protection mechanisms & shortcomings

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Protection</th>
<th>Shortcoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>- -</td>
<td>Personal data readable</td>
</tr>
<tr>
<td>BAC</td>
<td>Privacy info</td>
<td>Can be cracked</td>
</tr>
<tr>
<td>EAC + BAC</td>
<td>Most sensitive info</td>
<td>Certificate validation</td>
</tr>
<tr>
<td>Passive Auth</td>
<td>Content OK</td>
<td>Can make clone of chip</td>
</tr>
<tr>
<td>Active Auth +</td>
<td>Passport OK</td>
<td>Minor: abuse of signing feature</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Passp holder OK</td>
<td>Mass deployment?</td>
</tr>
</tbody>
</table>
Appendix B: Bleichenbacher’s PKCS-1 attack

- Normal RSA payload structure: `padding || Length || Hash`
- Verifier skips padding, decodes length and reads Hash
- Modified RSA payload structure: `padding || Length || Hash || Tail`
- Manufacture signature whose cube value matches modified structure
- Inspection system that does not check absence of Tail and uses Length to read the Hash will not detect the forgery
Appendix C: false passport detection