E-Passport Testing
Ensuring Global Acceptance

By: Jos Chehin
Date: 17 November 2006
Location: ASML
Global Acceptance of the e-Passport

- Interoperability
- Functionality
- Security

Test Standards

e-Passport Standards
Agenda

❖ The e-Passport

❖ The ICAO/ISO e-Passport Standards

❖ Test coverage of the Application Protocol and Logical Data Structure Test Standard

❖ Findings and Conclusions
The e-Passport

- Contactless chip
  - Processing capability
  - Data storage

- PKI

- Biometrics (Face, fingerprint, eyes)

- Secure electronic identification
The e-Passport Standards

- ISO 14443
- Public Key Cryptography conform to the ICAO PKI standard
- The ISO 7816-4 Standard
- Standard for the e-Passport Logical Data Structure (LDS)

OSI Layer 1-4
OSI Layer 6-7
OSI Layer 6-7
OSI Layer 6-7
Testing the e-Passport Hardware

- Collis SmartWave box
  - Reads/simulates
- Test Suite’s
- Low level interoperability

- Low level interoperability test events (ISO 14443):
  - Cross-over testing
  - ‘interoperability’ rates
    - 93% in Singapore
    - 87% in Berlin
    - Readable ≠ ISO/ICAO conformance
e-Passport Security Mechanisms

Security mechanisms:
- Passive Authentication (Mandatory)
- Active Authentication (Optional)
- Basic Access Control (Optional)
- Extended Access Control (Optional)

“Issuing States MAY choose additional security, using more complex ways of securing the chip and its data.”
e-Passport Smartcard Commands

- e-Passport to reader communication on APDU level

- Passive Authentication
  - SELECT READ BINARY(B0/B1)

- Active Authentication
  - SELECT READ BINARY(B0/B1)
  - INTERNAL AUTHENTICATE

- Basic Access Control
  - SELECT GET CHALLENGE MUTUAL AUTHENTICATE

- Extended Access Control

ISO 7816-4,8 Application OSI Layer 6-7
The e-Passport LDS

ISSUING STATE or ORGANIZATION
RECORDED DATA

- Document Type
- Issuing State or organization
- Name (of Holder)
- Document Number
- Check Digit - Doc Number
- Nationality
- Date of Birth
- Sex
- Date of Expiry or Valid Until Date
- Check Digit - DOE/UD
- Optional Data
- Check Digit - Optional Data Field
- Composite Check Digit

- Encoded Identification Feature(s)
  - Global Exchange Feature
    - Encoded Face
    - Encoded Finger(s)
    - Encoded Eye(s)

- Displayed Identification Feature(s)
  - Displayed Portrait
  - Reserved for Future Use
  - Displayed Signature or Usual Mark

- Encoded Security Feature(s)
  - Data Feature(s)
  - Structure Feature(s)
  - Substance Feature(s)
  - Additional Personal Detail(s)
  - Additional Document Detail(s)
  - Optional Detail(s)
  - Reserved for Future Use
  - Active Authentication Public Key Info
  - Person(s) to Notify

ADDITIONAL PERSONAL DETAIL(S)
- Additional Personal Detail(s)

ADDITIONAL DOCUMENT DETAIL(S)
- Additional Document Detail(s)

OPTIONAL DETAIL(S)
- Optional Detail(s)

PERSON(S) TO NOTIFY
- Person(s) to Notify

ICAO LDS

Personalisation
Testing the e-Passport Application and LDS

- ICAO/ISO Test Standard

- Security
  - Security Mechanisms

- Smartcard commands
  - Positive
  - Negative

- The LDS
  - Encoding of the LDS data objects
Test Coverage of the ICAO PKI Test Standard

<table>
<thead>
<tr>
<th></th>
<th>Mandatory</th>
<th>EU</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Auth.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Auth.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Access Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Access Control</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Table with colors indicating coverage status]
## Test Coverage of the ICAO LDS Test Standard

<table>
<thead>
<tr>
<th></th>
<th>Mandatory</th>
<th>EU</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>EF.COM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG1 Machine Readable Zone (MRZ)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG2 Encoded Face</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG3 Encoded Finger (s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG4 Encoded Eye (s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG5 Displayed Identification features : DG7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG8 Encoded Security Features : DG10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG11 Additional personal details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG12 Additional Document Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG13 Optional Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dg14 Reserved for future use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG15 Active Authentication Pk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG16 Persons to notify</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EF.SOD</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Test Coverage of the ICAO LDS Test Standard

<table>
<thead>
<tr>
<th>Category</th>
<th>EU</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>EF.COM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG1 Machine Readable Zone (MRZ)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG2 Encoded Face</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG3 Encoded Finger (s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG4 Encoded Eye (s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG5 Displayed Identification features</td>
<td></td>
<td></td>
</tr>
<tr>
<td>:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG8 Encoded Security Features</td>
<td></td>
<td></td>
</tr>
<tr>
<td>:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG11 Additional personal details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG12 Additional Document Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG13 Optional Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dg14 Reserved for future use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG15 Active Authentication Pk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DG16 Persons to notify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EF.SOD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- Green: Mandatory
- Red: EU
- Green: US

**Notes:**
- Mandatory EU US Test Coverage of the ICAO LDS Test Standard
Smartcard Command APDU Tests

Number of Positive / Negative tests defined per ISO 7816 command

- SL: 11 positive, 2 negative
- B0: 6 positive, 2 negative
- B1: 1 positive, 2 negative
- B0sfi: 2 positive, 2 negative
- B1sfi: 1 positive, 1 negative
- GC: 0 positive, 0 negative
- MA: 1 positive, 1 negative
- AA: 0 positive, 0 negative

Legend:
- Yellow: Positive Tests Defined
- Green: Negative Tests Defined
ISO 7816 Command Test Coverage Matrix

<table>
<thead>
<tr>
<th>CLA</th>
<th>P1</th>
<th>P2</th>
<th>Lc</th>
<th>Crypt</th>
<th>Data</th>
<th>CC</th>
<th>TLV</th>
<th>Offset</th>
<th>SM</th>
<th>Le</th>
<th>Rtn bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>P</td>
<td>N</td>
<td>P</td>
<td>N</td>
</tr>
</tbody>
</table>

- **B1sfi**
- **B0sfi**
- **B0**
- **B1**
- **SEL**
- **GC**
- **MA**
- **IA**
Findings

- Some optional, but important security features not covered by the ICAO test standard (AA, EA)

- e-Passport chip response on incorrect commands not tested thoroughly (negative tests)

- Gaps in the test specification
Recommendation

- Additional tests need to be developed to fill up gaps in the test specification
-End-