Biometric Passport
from a Security Perspective

Gildas Avoine

INSA Rennes/IRISA
Institut Universitaire de France
Summary

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
1944: International Civil Aviation Organization (ICAO).

1968: ICAO starts working on MRTD.
  - “A Machine Readable Travel Document (MRTD) is an international travel document (eg. a passport or visa) containing eye-and machine-readable data.” (ICAO).

  - Includes an OCR Machine Readable Zone.
History


- **1998**: First (not ICAO-compliant) electronic passports in Malaysia.

- **1998**: ICAO initiated some work on biometric identification systems and associated means.

- **2004**: ICAO released a new version of DOC 9303, endorsed by ISO/IEC 7501, that defines passports with biometrics and contactless Integrated Circuit (IC), so-called ePassport.
- IC is contactless.
- IC does not contain any battery.
- IC has a microprocessor.
- Communication range is about 10 cm.
- Memory (EEPROM) is about 32KB.
- IC is compliant ISO 14443, ISO 7816.
MEMORY CONTENT

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
Machine Readable Zone

■ Line 1
  ○ Document type
  ○ Issuing country
  ○ Holder name

■ Line 2
  ○ Document number (+ checksum)
  ○ Nationality
  ○ Date of birth (+ checksum)
  ○ Gender
  ○ Date of expiry (+ checksum)
  ○ Options
  ○ Composite check digit
Memory Content

- Data groups (DG).
  - Access requires an authentication: BAC or EAC.

- List of data groups (COM).

- Cryptographic material: certificate, signature and hashes (SOD).
**Passport Content**

**Logical Data Structure (LDS)**

![Logical Data Structure Diagram]

- **ISSUING STATE or ORGANIZATION RECORDED DATA**
  - DG1: Document Type
  - DG2: Issuing State or Organization
  - DG3: Name of Holder
  - DG4: Document Number
  - DG5: Check Digit - Doc Number
  - DG6: Nationality
  - DG7: Date of Birth
  - DG8: Sex
  - DG9: Date of Expiry or Valid Until Date
  - DG10: Check Digit - DOB
  - DG11: Optional Data
  - DG12: Check Digit - Optional Data Field
  - DG13: Composite Check Digit

- **ADDITIONAL PERSONAL DETAIL(S)**
  - DG14: Additional Personal Detail(s)

- **ADDITIONAL DOCUMENT DETAIL(S)**
  - DG15: Additional Document Detail(s)

- **OPTIONAL DETAIL(S)**
  - DG16: Optional Detail(s)

- **PERSON(S) TO NOTIFY**
  - DG17: Person(s) to Notify
CRYPTOGRAPHIC MECHANISMS DEFINED BY ICAO

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
ICAO Security Mechanisms
Overview

**Passive Authentication [Signature]**
-RSA, DSA, ECDSA
- SHA-1, 224, 256, 384, 512

**Active Authentication [Challenge Response]**
-ISO 9796-2

**Basic Access Control [Reader Authentication]**
-TDES/CBC
-Retail-MAC/DES
-SHA-1 (key der.)

**Secure Messaging [Encryption]**
-TDES/CBC
-Retail-MAC/DES

-Modifying data of a given passport
-Forging a fake passport

-Cloning a given passport

-Skimming a passport

-Eavesdropping the communication
Passive Authentication
General Sketch

EF.COM

DG 1
DG 2
DG 3
... 
DG n

hash hash hash ...

EF.SOD

signature
DS certificate
Passive authentication is a mandatory security mechanism.

EF.SOD (RFC 3369) contains the hash value of each present DG, and a signature calculated by the issuing State over these values.

The signature can be checked using the Document Signer (DS) X.509 certificate, available from EF.SOD or ICAO Public Key Directory (PKD).

The DS certificate can be checked using the Country Signing CA (CSCA) X.509 certificate.

- Originally, the ICAO PKD did not publish the CSCA certificates.
- CSCA certificates and revocation lists should be exchanged according to bilateral agreements.
## Certificates in the ICAO Directory

<table>
<thead>
<tr>
<th>Signature</th>
<th>Number of certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>8</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>3120</td>
</tr>
<tr>
<td>RSA-3072</td>
<td>2</td>
</tr>
<tr>
<td>ECDSA-224</td>
<td>31</td>
</tr>
<tr>
<td>ECDSA-256</td>
<td>40</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>3201</strong></td>
</tr>
</tbody>
</table>

### Signature Schemes Used by DS Certificates

<table>
<thead>
<tr>
<th>Signature</th>
<th>Number of certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-2048</td>
<td>4</td>
</tr>
<tr>
<td>RSA-3072</td>
<td>30</td>
</tr>
<tr>
<td>RSA-4096</td>
<td>90</td>
</tr>
<tr>
<td>ECDSA-256</td>
<td>14</td>
</tr>
<tr>
<td>ECDSA-384</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>144</strong></td>
</tr>
</tbody>
</table>

### Signature Schemes Used by CSCA Certificates
Certificates in the ICAO Directory

RSA Exponents in DS Certificates

<table>
<thead>
<tr>
<th>RSA Exponent</th>
<th>Number of certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>191</td>
</tr>
<tr>
<td>44591</td>
<td>1</td>
</tr>
<tr>
<td>65427</td>
<td>1</td>
</tr>
<tr>
<td>65537</td>
<td>2937</td>
</tr>
<tr>
<td>Total</td>
<td>3130</td>
</tr>
</tbody>
</table>

RSA Exponents in CSCA Certificates

<table>
<thead>
<tr>
<th>RSA Exponent</th>
<th>Number of certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>38129</td>
<td>2</td>
</tr>
<tr>
<td>43459</td>
<td>1</td>
</tr>
<tr>
<td>65537</td>
<td>112</td>
</tr>
<tr>
<td>Total</td>
<td>124</td>
</tr>
<tr>
<td>Country</td>
<td>Nb Revoked Certificates</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>New Zealand</td>
<td>2</td>
</tr>
<tr>
<td>Malaysia</td>
<td>3</td>
</tr>
<tr>
<td>AU</td>
<td>4</td>
</tr>
<tr>
<td>USA</td>
<td>3</td>
</tr>
<tr>
<td>UK</td>
<td>724</td>
</tr>
<tr>
<td>Canada</td>
<td>15</td>
</tr>
<tr>
<td>UNO</td>
<td>3</td>
</tr>
<tr>
<td>Singapore</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>760</td>
</tr>
</tbody>
</table>
The Active Authentication is an optional security mechanism.

Aim is to prove that EF.SOD belongs to the authentic passport, i.e. it is not a cloned one.

Two-pass CR protocol ISO 9796-2 DSS 1 (RSA, DSA, ECDSA).

Passport's public key is stored in DG15 (encoded as RFC 3280).
### Active Authentication Protocol

<table>
<thead>
<tr>
<th>Reader (IFD)</th>
<th>Passport (ICC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate $M_2$</td>
<td>Create $T$</td>
</tr>
<tr>
<td>$M_2$</td>
<td>Generate $M_1$ of $L_{M_1}$ bits $M = M_1</td>
</tr>
<tr>
<td></td>
<td>$H = \text{hash}(M)$</td>
</tr>
<tr>
<td></td>
<td>$F = 6A</td>
</tr>
<tr>
<td></td>
<td>$S = \text{ENC}_{PrK}(F)$</td>
</tr>
<tr>
<td>Decrypt $S'$ with PuK$_{DG15}$</td>
<td></td>
</tr>
<tr>
<td>$D = \text{hash}(M'_1</td>
<td></td>
</tr>
<tr>
<td>Check if $D = H'$</td>
<td></td>
</tr>
</tbody>
</table>

IFD: InterFace Device

ICC: Integrated Circuit Card
Basic Access Control
General View

Passport Number
Expiration Date
Birth Date
MRZ

Basic Access Control
Encryption Key
MAC Key

Secure Messaging
Session Encryption Key
Session MAC Key

Reader
MAC Key
Kr, Kp
Basic Access Control
Secure Messaging
Encryption Key
Session Encryption Key
Session MAC Key

Reader
MAC
Cr, Kr
Encrypted Data
Passport
Cp
Authenticated Query

a = ENC(Cp, Cr, Kr), MAC(a)
b = ENC(Cp, Cr, Kp), MAC(b)
Basic Access Control Protocol

**Reader (IFD)**

- Generate $RND_{IFD}$
- Generate $K_{IFD}$
- $S = RND_{IFD} \| RND_{ICC} \| K_{IFD}$
- $E_{IFD} = ENC_{K_{ENC}}(S)$
- $M_{IFD} = MAC_{K_{MAC}}(E_{IFD})$

**Passport (ICC)**

- $E_{IFD} \| M_{IFD}$
- Check MAC
- Decrypt $E_{IFD}$
- If $RND'_{ICC} = RND_{ICC}$
- Generate $K_{ICC}$
- $R = RND_{ICC} \| RND'_{IFD} \| K_{ICC}$
- $E_{ICC} = ENC_{K_{ENC}}(R)$
- $M_{ICC} = MAC_{K_{MAC}}(E_{ICC})$

- $K_{seed} = K_{IFD} \oplus K_{ICC}$
- Calculate $K_{S_{ENC}}$
- Calculate $K_{S_{MAC}}$
- Calculate SSC

- $K_{seed} = K_{IFD} \oplus K_{ICC}$
- Calculate $K_{S_{ENC}}$
- Calculate $K_{S_{MAC}}$
- Calculate SSC
Basic Access Control
Standards

- Three-pass CR protocol according to ISO 11770-2 Key Establishment Mechanism 6, 2-key 3DES as block cipher.

- Nonces should be 8-byte long.

- Encryption done using 3DES in CBC mode with zero-IV according to ISO 11568-2.

- A cryptographic checksum is calculated over: ISO 9797-1 MAC Algorithm 3 (i.e. Retail-MAC), based on DES, zero-IV, ISO 9797-1 Padding Method 2.

- Encryption and MAC keys derived from the MRZ using SHA-1.
The encryption uses 3DES in CBC mode with a zero IV, and a padding compliant with ISO/IEC 9797-1 padding method 2.

The MAC is computed using ISO/IEC 9797-1 MAC algorithm 3 with DES, a zero IV, and the ISO/IEC 9797-1 padding method 2.

Before the MAC is computed, the Send Sequence Number is incremented and prepended to the ciphertext.

The original value for SSD is the concatenation of the 4 less significant bytes of each RND_{ICC} and RND_{IFD}.
**Basic Access Control and Secure Messaging**

**Key Derivation**

- \( K_{seed} = \text{trunc}_{16}(\text{SHA-1} (\text{MRZ_info})) \) or \((Kr \oplus Kp)\).

- Set \( D = K_{seed} || 00000001 \).

- Compute \( H = \text{SHA-1}(D) \).

- First 16 bytes of \( H \) are set to the 2-key 3DES \( K_{ENC} \).

- Set \( D = K_{seed} || 00000002 \).

- Compute \( H = \text{SHA-1}(D) \).

- First 16 bytes of \( H \) are set to the 2 DES keys \( K_{MAC} \).

- Adjust the parity bits of DES keys.
ADDITIONAL CRYPTOGRAPHIC MECHANISMS

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
2004: Basic Access Control (BAC)

2009: Extended Access Control (EAC)
- EACv1, EACv2.
- EAC provides terminal authentication (TA) with a stronger session key than BAC.
- EAC provides chip authentication (CA) without the AA semantic problem.

2010: Supplemental Access Control (SAC)
- SAC improves BAC with more entropy.
- SAC uses PACE as an additional security mechanism.
- SAC must be implemented by EU countries by the end of 2014.
- By the end of 2017 only passports supporting SAC will be considered to be ICAO-compliant.
Extended Access Control

- EAC uses Extended Access Keys, which can be either symmetric or asymmetric, which cannot be derived from the MRZ.

- Each country needs a Country Verifying CA (CVCA), which issues Document Verifier (DV) Certificates. The public key of the CVCA is stored in the passport.

- CA enables the terminal (reader, inspection system) to authenticate the passport and to establish a secure channel.

- TA enables the chip (passport) to verify that the terminal is allowed to access sensitive information such as biometric data. TA may only be used together with CA.
Terminal Authentication

Reader (IFD)  Passport (ICC)

Certificate chain

Verify_{PuK_{CVCA}}(DV_c)
Verify_{DV_c}(IS_c)
Extract PuK_{IS} from IS_c
Generate RND_{ICC}

Generate PrK_{IFD}, PuK_{IFD} (DH Keys)
C := hash(PuK_{IFD})

S := ID_{ICC}||RND_{ICC}||PuK_{IFD}
\text{sign}_{PrK_{IS}}(S) = s_{IFD}

Verify_{PuK_{IS}}(s_{IFD})

\text{Store } C'

Gildas Avoine  Biometric Passport from a Security Perspective 28
Chip Authentication

Reader (IFD)

\[ K = \text{DH}(\text{PrK}_{\text{IFD}}, \text{PuK}_{\text{ICC}}, D') \]

\[ \text{PuK}_{\text{ICC}} + D \]

\[ \text{PuK}_{\text{IFD}} \]

\[ \text{K}_{\text{ENC}} = \text{KDF}_{\text{ENC}}(K, \text{RND}_{\text{ICC}}) \]

\[ \text{K}_{\text{MAC}} = \text{KDF}_{\text{MAC}}(K, \text{RND}_{\text{ICC}}) \]

\[ \text{T}_{\text{ICC}} = \text{MAC}_{\text{K}_{\text{MAC}}}(\text{PuK}_{\text{IFD}}) \]

Passport (ICC)

\[ \text{Check if hashPuK}'_{\text{IFD}} = C' \]

\[ K = \text{DH}(\text{PrK}_{\text{ICC}}, \text{PuK}_{\text{IFD}}, D') \]

Generate RND\(_{\text{ICC}}\)

\[ \text{K}_{\text{ENC}} = \text{KDF}_{\text{ENC}}(K, \text{RND}_{\text{ICC}}) \]

\[ \text{K}_{\text{MAC}} = \text{KDF}_{\text{MAC}}(K, \text{RND}_{\text{ICC}}) \]

\[ \text{T}_{\text{ICC}} = \text{MAC}_{\text{K}_{\text{MAC}}}(\text{PuK}_{\text{IFD}}) \]
As for the BAC, the shared secret ($\pi$) is printed on the passport.

The secret $\pi$ is a Card Access Number or a MRZ-Password.

Reader and passport compute the key $K_\pi = \text{SHA-1}(\pi\|3)$.

Passport and reader are authenticated using $K_\pi$.

A DH key agreement protocol is performed to generate encryption and mac keys.

The keys are no longer static (contrarily to BAC).
Password Authenticated Connection Establishment

**Reader (IFD)**

- $RND'_{ICC} = \text{DEC}_{K_{\pi}}(z)$
- Compute $D_e$ from $RND_{ICC}$ and $D_c$
- Generate $PrK_{IFD}$, $PuK_{IFD}$

**Passport (ICC)**

- Generate $RND_{ICC}$
  - $z = \text{ENC}_{K_{\pi}}(RND_{ICC})$

**Steps**

1. $K = KA(PrK_{IFD}, PuK_{ICC}, D')$
2. $K_{ENC} = 128\text{msb of SHA-1}(K\|1)$
3. $K_{MAC} = 128\text{msb of SHA-1}(K\|2)$
4. $T_{IFD} = MAC_{K_{MAC}}(PuK_{ICC})$
5. $T_{ICC} = MAC_{K_{MAC}}(PuK_{IFD})$
6. Verify $T_{ICC}$
VULNERABILITIES

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
Vulnerabilities

Five vulnerabilities were identified so far in the literature.

Vulnerabilities on the protocol designs or their implementation.

Issues related to the certificates are not discussed here.

None of them allows an adversary to forge a passport.
  - Recognition of a batch of passports (e.g., country).
  - Recognition of an individual passport.
  - Obtaining a proof of presence.
  - Obtaining the data contained in the passport.
<table>
<thead>
<tr>
<th>Fields</th>
<th>No information</th>
<th>Country known</th>
<th>Visual access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document number</td>
<td>1.02 × 10^{14}</td>
<td>from 6.76 × 10^8 to 10^4</td>
<td>–</td>
</tr>
<tr>
<td>Date of birth</td>
<td>36525 days</td>
<td>–</td>
<td>1825 days</td>
</tr>
<tr>
<td>Date of expiration</td>
<td>3652.5 days</td>
<td>from 3652.5 days to 1250 days</td>
<td>–</td>
</tr>
</tbody>
</table>

**Total**

<table>
<thead>
<tr>
<th>No information</th>
<th>Country known</th>
<th>Visual access</th>
<th>Country+Visual</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.36 × 10^{22}</td>
<td>from 9.02 × 10^{16} to 4.57 × 10^{11}</td>
<td>6.8 × 10^{20}</td>
<td>from 4.51 × 10^{15} to 2.28 × 10^{10}</td>
</tr>
<tr>
<td>73.52 bits</td>
<td>from 56.32 bits to 38.73 bits</td>
<td>69.20 bits</td>
<td>from 52.00 bits to 34.41 bits</td>
</tr>
</tbody>
</table>
When the reader sends (Ciphertext, MAC) during BAC, the passport recomputes MAC and compares it to the received one.

If they do not match, the passport sends an error message.

Otherwise it decrypts Ciphertext and check if $\text{RND}_{\text{ICC}}' = \text{RND}_{\text{ICC}}$

If they do not match the passport sends an error message.

Otherwise the BAC process continues.

Decrypting ciphertext and comparing nonces takes milliseconds.

This discloses if BAC failed at the MAC comparison (wrong key) or at nonces comparison (correct key but unexpected nonce).

Chothia and Smirnov also noticed that old French passports send a different error message when the BAC failed.
Error messages.

Result of the `select` command (can be used before BAC).

Answer to select (ATS) depends on the implementation.

UID (random or not).

Response time to APDUs depends on the implementation.

Physical layer characteristics.
A vulnerability pointed out by Sportiello targets old generations of Italian passports.

By manipulating the `get challenge` command ($L_E$ set to 01), it is possible to force the passport to send a 8-byte challenge with the 7 less significant bytes set to 00.

Probability that a given nonce appears is $1/2^8$.

Perform a brute force attack on the MRZ space (CPA).

Precomputations are possible because it is a chosen plaintext attack, encrypted with 3DES in CBC mode with an $IV = 0$ and a key $K_{ENC}$ derived from the MRZ.
### MRZ Lookup Table (Italian Passport)

<table>
<thead>
<tr>
<th>Reader</th>
<th>MITM</th>
<th>ePassport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get 8-byte challenge</td>
<td>1</td>
<td>Get 1-byte challenge</td>
</tr>
<tr>
<td>RND&lt;sub&gt;ICC&lt;/sub&gt; = NN∥{0x00}^7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>if RND&lt;sub&gt;ICC&lt;/sub&gt;[0] ≠ 0x00: jump to 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E&lt;sub&gt;IFD&lt;/sub&gt; = ENC&lt;sub&gt;KEnc&lt;/sub&gt;(S)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M&lt;sub&gt;IFD&lt;/sub&gt; = MAC&lt;sub&gt;KMAC&lt;/sub&gt;(E&lt;sub&gt;IFD&lt;/sub&gt;)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E&lt;sub&gt;IFD&lt;/sub&gt;∥M&lt;sub&gt;IFD&lt;/sub&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E&lt;sub&gt;ICC&lt;/sub&gt; = ENC&lt;sub&gt;KEnc&lt;/sub&gt;(R)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M&lt;sub&gt;ICC&lt;/sub&gt; = MAC&lt;sub&gt;KMAC&lt;/sub&gt;(E&lt;sub&gt;ICC&lt;/sub&gt;)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E&lt;sub&gt;ICC&lt;/sub&gt;∥M&lt;sub&gt;ICC&lt;/sub&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lookup for K&lt;sub&gt;ENC&lt;/sub&gt; where:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENC&lt;sub&gt;KEnc&lt;/sub&gt;({0x00}^8) = E&lt;sub&gt;ICC&lt;/sub&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E&lt;sub&gt;ICC&lt;/sub&gt;∥M&lt;sub&gt;ICC&lt;/sub&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...
There exists passports that accept to execute AA before BAC.

Signature evidence.

Traceability attacks due to the RSA modulus.
CONCLUSION AND FURTHER READING

- Passport Primer
- Memory Content
- Cryptographic Mechanisms defined by ICAO
- Additional Cryptographic Mechanisms
- Vulnerabilities
- Conclusion and Further Reading
ICAO’s passport is a pretty well-defined secure application.

Complex security mechanisms.

Security weaknesses due to misuse and short time-to-market.

Security level is improved over time.