Biometrics Deployment of EU-Passports

EU – Passport Specification

Working document (EN)

(As the United Kingdom and Ireland have not taken part in the adoption of this measure, an authentic English version of the whole specifications has not been established)

Table Of Contents

1 Scope and Limitations

This document describes solutions for chip enabled EU passports, based on the EU document [1] titled

> *„Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States"*

The document is based on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents, and accommodates:

- Specifications for biometric identifiers: face and fingerprints
- Storage medium (chip)
- Logical data structure on the chip
- Specifications for the security of the digitally stored data on the chip
- Conformity assessment of chip and applications
- RF compatibility with other electronic travel documents

The following considerations are out of scope of this document:

- Specifications of the mechanical mounting of the chip in a passport book, durability and mechanical testing procedures.
- Specifications on standard operation procedures (SOP) for the enrolment or the inspection process.

2 Biometrics

2.1 Primary biometric – Face

2.1.1 Standard compliance

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004 [3]
- ISO/IEC FCD 19794-5: Biometric Data Interchange Formats – Part 5: Face Image Data [4]

2.1.2 Type

The facial image must be stored as FRONTAL IMAGE[1], according to [3, 4].

[1] According to ICAO standards, the
"Face biometric data interchange image recorded in Datagroup 2 [of the LDS] shall be derived from the passport photo used to create the displayed portrait printed on the data page of the Machine Readable Passport; and shall be encoded

2.1.3 Format

The face is to be stored as a compressed IMAGE FILE, not as vendor specific template.

Although both JPEG and JPEG2000 compression is standard compliant [3], JPEG2000 is recommended for EU-Passports because it results in smaller file sizes compared to JPEG compressed images.[2]

2.1.4 Storage requirements

No.	Option	Remark	Recommendation
1	JPEG compression	approx. 12-20 KByte per photo	
2	JPEG2000 compression	approx. 6-10 KByte per photo	recommended (see 2.1.3)

2.1.5 Other issues

- Photograph Taking Guidelines taking into account the requirements of facial recognition technology have to be adopted according to ICAO standards [3]

2.2 Secondary biometric – Fingerprints

2.2.1 Standard compliance

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004 [3]
- ISO/IEC FCD 19794-4, Biometric Data Interchange Formats – Part 4: Finger Image Data [5]
- ISO/IEC FCD 19794-2, Biometric Data Interchange Formats – Part 2: Finger Minutiae Data [6]
- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"; FBI: Wavelet Scalar Quantization (WSQ) [15]

either according to type 2 (full frontal image) or type 3 (token image) formats set out in the latest version of ISO 19794-5."

[2] The commercial use of JPEG2000 may result in one-time cost up to € 7.000 for SDK and support.

2.2.2 Type

The primary fingerprints to be incorporated into the European Passport shall be

PLAIN IMPRESSIONS OF THE LEFT AND RIGHT INDEX FINGER.

In the case of insufficient quality of the fingerprints and/or injuries of the index fingers, good quality, plain impressions of middle fingers, ring fingers or thumbs shall be recorded[3].

2.2.3 Format and Quality

The fingerprints must be stored as IMAGES, according to [5].

The quality of the fingerprint images shall be according to [5] and [15].

A compression of the images using the WSQ-algorithm according to [15] MUST be used in order to decrease file size.

2.2.4 Storage requirements

The use of fingerprint IMAGES requires approximately 12 – 15 KByte per finger.

3 Storage medium (RF-Chip architecture)

3.1 Standard compliance

- ICAO NTWG, Biometrics Deployment of Machine Readable Travel Document, Technical Report, Version 2.0, 05 May 2004 [3]
- ISO/IEC FDIS 14443, Identification cards - Contactless integrated circuit(s) cards - Proximity cards [7]
- ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 April 2003 [8]

3.2 RF-Interface

According to [3,7,8], both type A and type B RF-interfaces are considered to be ICAO standard compliant.

ICAO compliant passports will be equipped with both A and B type RF interfaces, requiring border inspection systems to accommodate both standards for passports and visa.

3.3 Storage capacity

According to the ICAO Logical Data Structure [10], alphanumeric data of the machine readable zone (MRZ) of the document and digital document security data (PKI) must be stored on the chip together with the biometric identifiers.

[3] The storage format (CBEFF – Common Biometric Exchange File Format) will record the type of fingers used (left index, right middle etc) in order to ensure verification with the correct finger.

Member States are required to use appropriately sized RF chips to hold the personal data and biometric features according to the EU regulation [1]. See also chapter 2.1.4 and 2.2.4.

If, in accordance to the EU Regulation [1], a Member State wishes to include other data, extra storage capacity might be required.

4 Electronic Passport chip layout (data structure)

4.1 Standard compliance

- ICAO Doc 9303, Part 1, Machine Readable Passports, Fifth Edition, 2003 [9]
- Common Consular Instructions (CCI), Chapter VI No. 4 and Annex 10
- ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004 [10]

4.2 Correlation with printed data

The alphanumeric data, printed in the MRZ of the passport, according to [9], have to correlate to the data digitally stored in the chip according to [10].

4.3 Chip Logical Data Structure

According to [10].

5 Data security and integrity issues

The traditional passport document incorporates a number of anti-counterfeiting measures, including security printing and optically variable devices according to [1]. The integrity, the authenticity and confidentiality of the data, digitally stored in the passport's chip, have to be equally secured.

5.1 Standard Compliance

- ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004 [11]
- ISO/IEC 7816-4, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange [12]
- Access Control for Machine Readable Travel Documents, Preliminary Draft, 2004 [13]
- CWA 14890-1:2004, Application Interface for smart cards used as Secure Signature Creation Devices , Part 1 - Basic requirements, Version 1.09 rev2 [16]

5.2 Digital data security

No.	Security	Remark	Use
1	Passive Authentication [11, 12]	Proves that the contents of the SO_D and the LDS are authentic and not changed. Does not prevent an exact copy or chip substitution. Does not prevent unauthor-	REQUIRED for all data (ICAO mandatory security feature)

No.	Security	Remark	Use
		ized access. Does not prevent skimming.	
2	Active Authentication [11, 12]	Proves that the SO_D is not a copy but has been read from the authentic chip. Proves that the chip has not been substituted. Requires processor-chips.	OPTIONAL
3	Basic Access Control [11, 12, 16]	Prevents skimming. Prevents eavesdropping on the communications between MRTD and inspection system (when used to set up encrypted session channel). Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Requires processor-chips.	REQUIRED for all data
4	Extended Access Control [11, 12, 13]	Prevents unauthorized access to fingerprint data. Prevents skimming of fingerprint data. Requires additional key management. Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Requires processor-chips.	Additional protection REQUIRED for fingerprint data

SO_D Document Security Object (SO_D). This object is digitally signed by the issuing State and contains hash representations of the LDS contents.

LDS Logical Data Structure

MRTD Machine Readable Travel Document

MRZ Machine Readable Zone

The specifications on Extended Access Control and PKI will be set out in a separate Commission Decision.

5.3 Security Infrastructure

In order to ensure integrity and authenticity of the digital data stored on the chip, a "flat" PKI is introduced.

Country Signing CA Certificate:

- Highest level certificate acts as the trust point for the receiving State, self-signed and issued by the country Signing CA.
- The Country Signing CA Private Key is used to sign Document Signer Certificates.
- The Country Signing CA Certificates must be distributed initially via "diplomatic channel". A later update by electronic means has to be specified.

Document Signer Certificate:

- The Document Signer Private Key is used to sign Document Security Objects.
- Document Signer Certificates, generated by each State in a National Document Signing Authority, MUST be stored on the passports chip.

Relation between Electronic Passport and Electronic Visa Certificates:

Member States will most likely issue ICAO compliant electronic passports and electronic visa.

- It is recommended to use the same Country Signing CA certificate for both passports and visa.
- Document Signer Certificates for visa will be different from Document Signer Certificates for passports because of the decentralised personalisation of visa documents. A naming convention has to be developed to distinguish between Document Signer Certificates for visa and those for electronic passports.

For Details, see [11].

6 Conformity Assessment

Conformity according to [14] of biometrically enhanced travel documents will be assessed.

Protection profiles for biometrically enhanced travel documents will be developed.

7 Normative References

[1] "Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States"

[2] "Proposal for a Council Regulation amending Regulation (EC) No 1683/95 laying down a uniform format for visas"
"Proposal for a Council Regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals"
EU Document 14969/1/03 REV1, 21 November 2003

[3] ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004 [ICAO Bio]

[4] ISO/IEC FCD 19794-5: Biometric Data Interchange Formats – Part 5: Face Image Data

[5] ISO/IEC FCD 19794-4, Biometric Data Interchange Formats – Part 4: Finger Image Data

[6] ISO/IEC FCD 19794-2, Biometric Data Interchange Formats – Part 2: Finger Minutiae Data

[7] ISO/IEC FDIS 14443, Identification cards – Contactless integrated circuit(s) cards - Proximity cards

[8] ICAO NTWG, Use of Contactless Integrated Circuits In Machine Readable Travel Documents, Technical Report, Version 3.1, 16 April 2003

[9] ICAO Doc 9303, Part 1, Machine Readable Passports, Fifth Edition, 2003

[10] ICAO NTWG, Development of a Logical Data Structure – LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004

[11] ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004

[12] ISO/IEC 7816-4, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[13] Access Control for Machine Readable Travel Documents, Preliminary Draft, 2004

[14] Common Criteria

[15] ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"
FBI: Wavelet Scalar Quantization (WSQ)

www.itl.nist.gov/iad

[16] CWA 14890-1:2004, Application Interface for smart cards used as Secure Signature Creation Devices , Part 1 - Basic requirements, Version 1.09 rev2
http://www.uninfo.polito.it/ws_esign/docs.htm