Biometrics Deployment of EU-Passports

EU – Passport Specification

Working document (EN) – 28/06/2006

(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 19794-5:2005, 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].

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.

2.1.4 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 19794-4:2005, Biometric Data Interchange Formats – Part 4: Finger Image Data [5]
- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"; FBI: Wavelet Scalar Quantization (WSQ) [15]

[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 either according to full frontal image or token image formats set out in the latest version of ISO 19794-5."

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[2].

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 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 either A or B type RF interfaces, requiring border inspection systems to accommodate both standards for passports.

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.

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.

[2] 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.

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

- International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Draft Sixth Edition, of 2006 [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]
- Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2006 [13]

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 unauthorized access. Does not prevent skimming.	REQUIRED for all data (ICAO mandatory security feature)
2a)	Active Authentication [11, 12]	Proves that the SO_D is not a copy but has been read from	OPTIONAL

No.	Security	Remark	Use
		the authentic chip. Proves that the chip has not been substituted. Does not prove that the content of the LDS is authentic and not changed. Does not prevent eavesdropping on the communications between chip and inspection system	
b)	Chip Authentication [13]	Proves that the SO_D is not a copy and has been read from the authentic chip. Proves that the chip has not been substituted. Prevents eavesdropping on the communications between chip and inspection system.	Additional protection REQUIRED for all data at the time when fingerprint data are introduced or at the latest 36 months after the adoption of the technical specifications. Such a protection MUST NOT be enforced by the chip but EU-Inspection systems MUST use this mechanism, if supported by the chip.
3	Basic Access Control [11, 12]	Prevents skimming. Mitigates the risk of eavesdropping on the communications between chip and inspection system (see 2 b). Does not prevent an exact copy or chip substitution (requires also copying of the conventional document).	REQUIRED for all data
4	Terminal Authentication [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).	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
EAC	Extended Access Control being according to ICAO the combination of chip authentication and terminal authentication

5.3 Inspection Procedure

Deleted

5.4 Public Key Infrastructure for Passports

In order to ensure integrity and authenticity of the digital data stored on the chip, a PKI is introduced: Each Member State MUST set up only a single *Country Signing CA* acting as the national trust point for all receiving states and at least one *Document Signer* issuing passports. Details on this PKI infrastructure (including signature algorithms, key lengths, and validity periods) can be found in [11].

Every Member State MUST notify the name and contact details of the organization responsible for the operation of the *Country Signing CA* and the *Document Signer(s)* to the Commission.

5.5 Public Key Infrastructure for Inspection Systems

To prevent unauthorized inspection systems to access fingerprint data another PKI is introduced: Each Member State MUST set up only a single *Country Verifying CA* acting a the national trust point for the passports issued by this Member State and at least one *Document Verifier* managing a group of authorized inspection systems. Details on this PKI infrastructure can be found in [13].

Every Member State MUST notify the name and contact details of the organization responsible for the operation of the *Country Verifying CA* and the *Document Verifier(s)* to the Commission.

5.5.1 Certificate Validity Periods

The validity of issued certificates MUST be within the following time frames.

Entity	Minimum Validity Period	Maximum Validity Period
Country Verifying CA Certificate	6 months	3 years
Document Verifier Certificate	2 weeks	3 months
Inspection System Certificate	1 day	1 month

These indications may be changed by the Article 6 committee according to the test results presented by BIG.

5.5.2 Certificate Scheduling

To plan the scheduling of certificates the following processing and distribution times MUST be respected. Link certificates for the Country Verifying CA MUST be distributed at least 14 days before the certificate to be replaced expires.

Certification Authority	Maximum Processing Time (Certificate Request)	Maximum Distribution Time (Certificate)
Country Verifying CA	72 hours	24 hours
Document Verifier	24 hours	48 hours

These indications may be changed by the Article 6 committee according to the test results presented by BIG.

5.5.3 Certificate Policies

The "BIG" will develop a common Certificate Policy within one year after the Commission Decision on the technical specifications.

The Country Verifying CA of each Member State SHALL publish a Certificate Policy and may set up a Certification Practice Statement in accordance with the requirements set out by the "BIG", in particular indicating the conditions under which a certificate for a (foreign) Document Verifier will be issued. The Commission shall be informed about the adoption of the Certificate Policy.

6 Conformity Assessment

A technical working group ("Brussels Interoperability Group", BIG) will be established [18] to convey interoperability of passports conforming to the present specification.

6.1 Standard compliance

- ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Parts 2&3 [19]
- ISO/IEC 7816-4, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange [12]
- ISO/IEC 7816-8, Identifications cards – Integrated circuit cards – Part 8: Commands for security operations [20]
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.0 [14]
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Extended Access Control, Version 1.0 [17]

6.2 Functional Evaluation

For the functional evaluation of MRTD chips the appropriate standard [19], which is currently under development, SHALL be used. Additional test cases required for the implementation of [13] MAY be defined by BIG.

Every Member State MUST contract an accredited (national) test laboratory to certify functional compliance to the relevant standards on all ISO/OSI layers. Issued certificates MUST be notified to the Commission.

ISO/OSI Layer	Standard	Scope
1-4	ISO 14443 [7]	Hardware
6	ISO 7816 [12,20]	Software (OS)
7	ICAO Application [10,11]	Software (Application)

6.3 Common Criteria Evaluation

Passport chips MUST be evaluated in accordance with the relevant Common Criteria Protection Profile [14,17].

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] Deleted

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

[4] ISO/IEC 19794-5:2005, Biometric Data Interchange Formats – Part 5: Face Image Data

[5] ISO/IEC19794-4:2005, Biometric Data Interchange Formats – Part 4: Finger Image Data

[6] Deleted

[7] ISO/IEC 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] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 1 Machine Readable Passports, Draft Sixth Edition, of 2006

[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 7816-4:2005, Identifications cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[13] Advanced Security Mechanisms for Machine Readable Travel Documents, Version 1.0, 2005

[14] Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.0

http://www.bsi.bund.de/zertifiz/zert/reporte/PP0017b.pdf

[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] Deleted

[17] Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Extended Access Control, Version 1.0

[18] Brussels Interoperability Group, Terms of Reference

[19] ICAO NTWG, RF Protocol and Application Test Standard for E-Passport; Parts 2&3

[20] ISO/IEC 7816-8:2004, Identifications cards – Integrated circuit cards – Part 8: Commands for security operations