EN

Annex III

Biometrics Deployment of EU-residence permits
for third country nationals[1]

EU – residence permit specification

[1] SECRET UE/EU SECRET Sans l'(les) annexe(s) jointe(s) – non classifié / When detached from annex(es) – non-classified.

Table of Contents

1 Scope

This Annex sets out technical solutions for chip enabled residence permits, as required by Regulation (EC) No 1030/2002 [1]

The technical solutions are based on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents [4] and the Annex lays down specifications for:

(a) biometric identifiers: face and fingerprints;

(b) storage medium (chip);

(c) logical data structure on the chip;

(d) security of the data stored on the chip and in communication with the reader;

(e) conformity assessment of chip and applications.

This document does not cover:

(a) specifications of the mechanical mounting of the chip in a residence permit card, durability and mechanical testing procedures;

(b) specifications on standard operation procedures (SOP) for the enrolment or the inspection process.

(c) implementation for optional national applications. [This optional implementation, SHALL -if implemented- respect the data protection rules and MUST ensure a complete separation between data for national use and data defined in the scope of Council Regulation (EC) 1030/2002 [1]].

2 Biometrics

2.1 Primary biometric – Face

2.1.1 Standard compliance

ICAO Doc 9303 7th edition, Part 9 [2]

2.1.2 Type

The facial image must be stored as FULL FRONTAL IMAGE, according to [2],[3].

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 [2], JPEG2000 is recommended for residence permits 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 agreed by the committee established by Article 6 of Regulation (EC) 1683/95 according to ICAO recommendations [4]

2.2 Secondary biometric – Fingerprints

2.2.1 Standards compliance

- ICAO Doc 9303 7th edition, Part 9 [2];

- ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information"; FBI: Wavelet Scalar Quantization (WSQ) [7]

2.2.2 Type

The primary fingerprints to be incorporated into the residence permits shall be:

PLAIN IMPRESSIONS OF THE LEFT AND RIGHT INDEX FINGER.

For each hand, if the index finger is injured or missing, or has an ISO/IEC 19794-4 score of 0 to 25, a plain impression of the middle finger, ring finger or thumb of the same hand shall be recorded where a higher ISO score is available. If all fingers on one hand are of the low quality score indicated above, a plain impression of the finger with the best score shall be taken.

2.2.3 Format and Quality

The fingerprints must be stored as IMAGES, according to [2] and [7].

The quality of the fingerprint images shall be stated in accordance with [4] and recorded on the chip in the Biometric Data Block of the individual biometric image using the score of a suitable quality metric, ensuring mapping to the ISO score (0-100).

A compression of the images using the WSQ-algorithm according to [7] 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 Standards compliance

- ICAO Doc 9303 7th edition, Part 9 [2]

- ICAO Doc 9303 7th edition, Parts 10 and 12 [11]

3.2 Chip Interface

Residence permits MUST be equipped with a contactless chip. In addition to the contactless interface, the residence permit MAY also be equipped with a contact-based interface. The contacted-based interface may be provided by a dual-interface chip (one chip that provides both a contactless and a contact-based interface) or by a separate chip.

3.3 Storage capacity

According to the ICAO Doc 9303 7th edition Part 10 [11], alphanumeric data of the machine readable zone (MRZ) of the document and digital document security data (SO_D) 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 in accordance with Regulation (EC) No 1030/2002. See also chapters 2.1.4 and 2.2.4. If, in accordance with Regulation (EC) No 1030/2002 [1], a Member State wishes to include other data, extra storage capacity might be required.

4 Electronic residence permit chip layout (data structure)

4.1 Standards compliance

International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, 7th edition, Part 10, [11]

4.2 Correlation with printed data

The alphanumeric data, printed in the MRZ of the residence permit, according to [4] in Part 1 has to match the data digitally stored in the chip according to ICAO Doc 9303, 7th edition Part 10 [11].

4.3 Chip Logical Data Structure

As defined in ICAO Doc 9303, 7th edition Part 10 [11].

5 Data security and integrity issues

The traditional residence permit document incorporates a number of anti-counterfeiting measures, including security printing and optically variable devices in accordance with Regulation (EC) No 1030/2002 [1]. The integrity, the authenticity and confidentiality of the data, digitally stored in the residence permit chip, have to be equally ensured.

5.1 Standards Compliance

- ICAO Doc 9303, 7th edition Part 11 [10]
- Advanced Security Mechanisms for Machine Readable Travel Documents, BSI TR03110 Part 1 and 3, Version 2.10 of 20 March 2012[5]

5.2 Digital data security

No.	Security	Remark	Use
1	Passive Authentication [10]	Proves that the contents of the SO_D and the LDS are authentic and not changed. Does not prevent an exact	**REQUIRED** for all data (ICAO mandatory security feature)

No.	Security	Remark	Use
		copy or chip substitution. Does not prevent unauthorized access. Does not prevent skimming.	
2a)	Active Authentication [10]	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. 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	OPTIONAL
2b)	Chip Authentication [5]	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. 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 (BAC) Password Authenticated Connection Establishment (PACE) [10]	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 PACE MUST be implemented. Implementation of BAC is OPTIONAL.
4	Terminal Authentication [5]	Prevents unauthorized access to fingerprint data. Prevents skimming of fingerprint data. Requires additional key management. Does not prevent an exact	Additional protection **REQUIRED** for fingerprint data

No.	Security	Remark	Use
		copy or chip substitution (requires also copying of the conventional document).	

SO_D Document Security Object (SO_D) defined in Doc 9303 7th edition Part 10. This security object is digitally signed by the issuing State and contains hash representations of the LDS contents. It is recommended to use the SOD version laid down in LDS version 1.8.

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 Public Key Infrastructure for Passive Authentication

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 residence permits. Details on this PKI infrastructure (including validity periods, certificate profiles, etc.) are defined in ICAO Doc 9303, 7th Edition Part 12 [11]. Cryptographic algorithms defined in [14] are recommended.

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.

5.4 Public Key Infrastructure for Extended Access Control

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 as the national trust point for the residence permits issued by this Member State and at least one *Document Verifier* managing a group of authorized inspection systems. Details on this PKI are defined in [5].

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. Member States MUST exchange access certificates using the forms provided in the Common Certificate Policy [13].

5.4.1 Certificate Validity Periods

Refer to the Common Certificate Policy [13].

5.4.2 Certificate Scheduling

Refer to the Common Certificate Policy [13].

5.4.3 Certificate Policies

Refer to the Common Certificate Policy [13].

6 Conformity Assessment

6.1 Standards compliance

- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control, Version 1.10 [6]

-Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Extended Access Control, Version 1.3 [8]

- Chapters 6 and 7 in ICAO Doc 9303 7th edition, Part 9 [2]

-BSI TR-03105 Part 3.2: Test plan for eMRTDs with EACv1 [12]

6.2 Common Criteria Certification

Residence permit chips MUST be evaluated and certified in accordance with the relevant Common Criteria Protection Profile [8] and, if Basic Access Control is implemented, Common Criteria Protection Profile [8].

6.3 Functional Evaluation

For the functional evaluation of MRTD chips the following standards MUST be used:

- Chapters 6 and 7 in ICAO Doc 9303 7th edition, Part 9 [2]

-BSI TR-03105 Part 3.2: Test plan for eMRTDs with EACv1 [12]

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.

7 [Normative References

[1] Council Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals", OJ L 157, 15.06.2002, p. 1 as last amended.

[2] ICAO Doc 9303 7th edition, Part 9

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

[4] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, 7th edition, 2015

[5] Advanced Security Mechanisms for Machine Readable Travel Documents, BSI TR-03110-Part 1 and 3 Version 2.10

[6] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009 (https://www.bsi.bund.de) http://www.bsi.bund.de/zertifiz/zert/reporte/PP0017b.pdf [14]

[7] ANSI/NIST-ITL 1-2007 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information", FBI: Wavelet Scalar Quantization (WSQ), [https://www.nist.gov/sites/default/files/documents/itl/ansi/sp500-245-a16.pdf, 10-04-2018]

[8] Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, BSI-CC-PP-0056-V2-2012

[9] (Deleted)

[10] ICAO Doc 9303, 7th edition, Part 11

[11] ICAO Doc 9303 7th edition, Parts 10 and 12

[12] BSI TR-03105 Part 3.2: Test plan for eMRTDs with EACv1

[13] BSI TR-03139 Common Certificate Policy for the Extended Access Control Infrastructure for Travel and Residence Documents issued by EU Member States, v2.2

[14] SOGIS, Agreed Cryptographic Mechanisms Version 1.0, May 2016, http://www.sogisportal.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf

8 Appendix

8.1 Enrolment guide for fingerprints