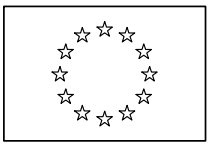


EUROPEAN COMMISSION

Brussels, 4.8.2011
C(2011) 5478 final

COMMISSION DECISION

of 4.8.2011

amending Commission Decision C(2002) 3069 laying down the technical specifications for the uniform format for residence permits for third country nationals

COMMISSION DECISION

of 4.8.2011

amending Commission Decision C(2002) 3069 laying down the technical specifications for the uniform format for residence permits for third country nationals

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third country nationals[1] , and in particular Article 2 (1) (d) and (e) thereof,

Whereas:

(1) Regulation (EC) No 1030/2002 empowers the Commission to adopt further technical specifications for the residence permit for third country nationals in order to prevent counterfeiting and falsification.

(2) Commission decision (EC) No C (2002) 3069 as amended by Commission decision (EC) No C (2009) 3770 has established the technical specifications for the implementation and the protection of the biometric data in residence permits for third country nationals; however more clarification is needed on the fingerprint quality at enrolment as there are no provisions for the handling of bad quality fingerprint images.

(3) The basic access control (BAC) to the biometric data has been further enhanced and specified by the International Civil Aviation Organisation in a technical report entitled "Supplemental Access Control for Machine Readable Travel Documents" and consequently the technical specifications should be upgraded accordingly.

(4) The certificate policy was first applied in connection with the implementation of fingerprints in passports, and a need occurred for practical reasons to change this Certificate policy in order to create a single point of contact (SPOC) in each Member State for the exchange of terminal authentication certificates.

(5) Terminal authentication certificates are necessary to provide authorisation to the reader to access to the fingerprint images of the chip. The issuing procedure of documents is not affected by this change.

(6) It is therefore necessary to introduce SPOC also to the certificate policy for residence permits for third country nationals.

[1] OJ L 157, 15.6.2002, p. 1

(7) Given that Regulation (EC) 1030/2002 builds upon the Schengen *acquis*, in accordance with Article 5 of the Protocol on the Position of Denmark annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark notified by letter of 16 October 2008 the transposition of this *acquis* into its national law. It is therefore bound under international law to implement this Decision.

(8) As regards Iceland and Norway, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis*[2], which fall within the area referred to in Article 1, point C of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement.[3]

(9) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, the United Kingdom gave notice, by letter of 29 December 2003, of its wish to take part in the adoption and application of the Regulation (CE) No 1030/2002.

(10) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and to the Treaty establishing the European Community, Ireland gave notice, by letter of 19 December 2003, of its wish to take part in the adoption and application of Council Regulation (CE) No 1030/2002

(11) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation on the latter's association with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point C of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[4].

(12) As regards Liechtenstein, this Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Protocol signed between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis,* which fall within the area referred to in Article 1, point C of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2011/350/EU[5].

(13) [The measures provided for in this Decision are in accordance with the opinion of the Committee set up by Article 6 of Regulation (EC) No 1683/95.]

---

2 OJ L 176, 10.7.1999, p. 36.
3 OJ L 176, 10.7.1999, p. 31.
4 OJ L 53, 27.2.2008, p. 1.
5 OJ L 160, 18.6.2011, p. 19.

HAS ADOPTED THIS DECISION:

Article 1

Annex II a) to Decision C (2002) 3069 is amended as follows:

1. Point 2.2.2 and 2.2.3 are replaced by the following:

"2.2.2 Type

The primary fingerprints to be incorporated into the residence permit for third country nationals 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 [5] and [6].

The quality of the fingerprint images shall, at the latest on 31 December 2014, be stated in accordance with [5] 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 [6] MUST be used in order to decrease file size."

2. The enrolment guide as attached as Annex I to the present Decision shall be attached to Annex II a) of Decision C(2002) 3069.

3. In point 5.2 the following shall be added to 3):

"PACE v2 according to [14] must be implemented at the latest on 31 December 2014."

4. Point 7 shall be amended as follows:

Reference point [2] shall be replaced with:

"[2] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 3 Machine Readable Official Travel Documents, Third Edition, 2008"

Reference point [6] shall be replaced with:

"[6] ANSI/NIST-ITL 1-2007 Standard “Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information”, FBI: Wavelet Scalar Quantization (WSQ), www.itl.nist.gov/iad"

Reference point [10] shall be replaced with:

"[10] Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.10 of 25 March 2009"

and the following reference point [14] shall be added:

"[14] Technical report on Supplemental Access Control for Machine Readable Travel Documents, Version - 1.00 of 23 March 2010."

Article 2

Annex II b) to Decision C (2002) 3069 is hereby amended as follows:

1. in point 1 the following subparagraph shall be added:

"To fulfil the requirements of this Certificate Policy it is required that a robust communication infrastructure be implemented for regular inter-country communication covering DV certificate issuing. The protocol defined in ČSN 36 9791, version 1.0 SHALL be used for routine day to day data exchanges related to EAC PKI.";

2. in point 1.3 the following point 1.3.4a) shall be added

"1.3.4a). SPOC – Single point of contact

SPOC acts as an interface for communication between Member States. It allows efficient on-line communication to carry out regular key management related tasks. Technical details of SPOC are defined in ČSN 36 9791, version 1.0."

3. point 9.11 shall be replaced by the following:

"9.11. All key management tasks MUST be carried out by using robust communication channels.

For communications between countries all CVCA’s and DV’s MUST be able to carry out such communications using SPOC as defined in ČSN 36 9791, version 1.0. Other additional online or offline communication channels MAY be mutually agreed especially to cover situation when SPOC communication channel is not available.

In the event of disruption to a CVCA’s normal communication channels it MUST notify subscribing DVs of an alternate channel by which Certificate Requests can be submitted. This SHALL be done in a timeframe that minimises the risk of current certificates expiring.

SPOC MUST comply with the additional requirements specified in Appendix C.";

4. Appendix C as set out in Annex II to the present Decision shall be added to Annex II b) of Commission Decision C (2002) 3069.

Article 3

This Decision is addressed to the Kingdom of Belgium, the Republic of Bulgaria, the Czech Republic, the Federal Republic of Germany, the Republic of Estonia, Ireland, the Hellenic Republic, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Cyprus, the Republic of Latvia, the Republic of Lithuania, the Grand Duchy of Luxembourg, the Republic of Hungary, the Republic of Malta, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Slovenia, the Slovak Republic, the Republic of Finland, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland. It shall be transmitted to the Kingdom of Denmark, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway and the Swiss Confederation.

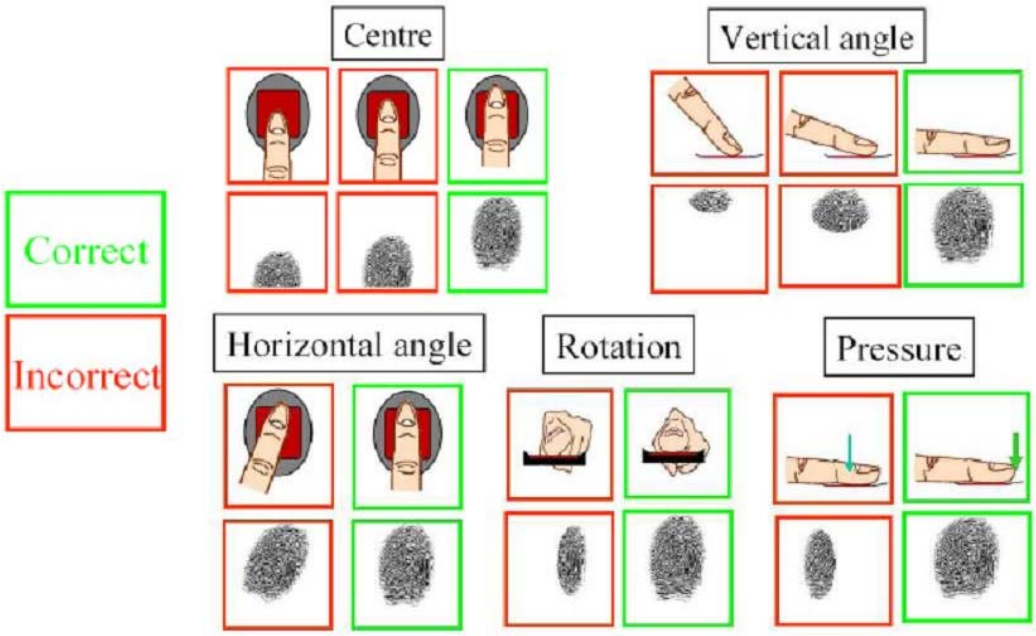
Done at Brussels, 4.8.2011

For the Commission
Cecilia MALMSTRÖM
Member of the Commission

CERTIFIED COPY
For the Secretary - General

Jordi AYET PUIGARNAU
Director of the Registry

ANNEX I



Enrolment guide

ANNEX II

APPENDIX C – SPOC REQUIREMENTS

1.1 SPOC Initial registration

Before inter-SPOC communication starts a SPOC SHALL register at the other SPOCs. The registration information SHALL be exchanged by trusted channel in the same way as initial DV registration is done. Following data must be presented during the registration:

- physical contact details of the organization responsible for SPOC operation;
- organization name;
- postal address;
- telephone number;
- fax number (OPTIONAL);
- SPOC root CA certification policy.
- SPOC root CA certificate
- SPOC e-mail address
- SPOC URL (see ČSN 36 9791, version 1.0 for details)

1.2 SPOC private keys storage requirements

Private key used for SPOC communication SHALL be stored in a secure cryptographic module. The module SHALL fulfil requirements specified in Appendix B.1.

1.3 SPOC CA requirements

1.3.1 Certificate assurance and content

The CA issuing SPOC communication certificates SHALL be under governmental control. The certificates issued by the SPOC CA SHALL fulfil requirements (naming, key usage, extensions) defined in ČSN 36 9791 version 1. The SPOC CA policy MUST assure the OIDs identifying SPOC certificates are assigned only to certificates belonging to the SPOC.

1.3.2 Certificate revocation information

The certificates SHALL contain valid CDP extension. At least one distribution point SHALL be reachable via HTTP. CRL regular issuing period MUST be max 3 months; in case a certificate is revoked, the CRL including the revoked certificate MUST be published no later than 72 hours after the certificate revocation. It is not advised to cache the CRL for a long period of time.

1.3.3 Technical and organizational requirements

The SPOC CA SHALL fulfil the same level of requirements as specified for CVCA in section "5. Management, Operational, and Physical Controls" and section "6. Technical Security Controls".

1.3.4 Validity periods

- CA certificate validity period: 5-10 years
- SPOC certificates validity period: 6-18 months

1.4 Request received vie SPOC is trusted

If the originator of the message is successfully validated (TLS client authentication) the received DV certification request SHALL be considered as approved by the originator as belonging to the DV which is allowed to request for a certificate abroad (according to 3.3.1 b) of this document).

1.5 Communication priorities

Whenever possible an automated web service interface SHALL be used to exchange data. When the web service interface of respective SPOC is not available for more than 72 hours, the client (initiator of the TCP connection) SHALL contact SPOC using registration information to find the solution for urgent communication requests.

1.6 Sending notifications

To send the notification SPOC SHALL be used. General Message as defined in ČSN 36 9791 version 1.0 SHALL be used to transport notification. It is RECOMMENDED to use wording as specified in the following table for subject and body part of the message.

Reference to CP	Subject	Body
[EUCP] sec. 9.11	Disruption of CVCA communication channel	Country SPOC webservice interface will not be operational from [date,time] to [date, time]. During the period use email.
[EUCP] sec. 9.11.6	Suspension of CVCA Service	CVCA service will be suspended from [date] to [date].
[EUCP] sec. 4.5, 5.7.3	[IS|DV|CVCA] private key [lost/stolen/compromised]	Private key belonging to [CHR] was [lost/stolen/compromised] on [date].
[EUCP] sec. 4.5	[DV|CVCA] private key activation data compromised	Activation data of the private key belonging to [CHR] was compromised on [date].
[EUCP] sec. 4.5	Certificate inaccurate	Attached certificate was found inaccurate.
[EUCP] sec. 5.8	[CVCA|DV] Termination	[CVCA|DV] identified by [CHR] will terminate operation from [date]. For further information contact [contact details].

Reference to CP	Subject	Body
[EUCP] sec. 8.	DV not compliant	The DV [CHR] is no more compliant to EU CP requirements.