COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 5.10.2009
C(2009) 7476 final

COMMISSION DECISION

of 5.10.2009

amending Commission Decision (C(2008) 8657 final) laying down a certificate policy as required in the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States

(Only the Bulgarian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Swedish, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovakian, Slovenian and Spanish texts are authentic)

COMMISSION DECISION

of 5.10.2009

amending Commission Decision (C(2008) 8657 final) laying down a certificate policy as required in the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States[1],, and in particular Article 2 (b) thereof, ,

Whereas:

(1) In accordance with Commission Decision C (2006) 2909 of 28 June 2006 a certificate policy was adopted on 22 December 2008[2].

(2) The certificate policy took the form of additional reference documents not having an impact on the implementation time frame of Regulation (EC) No 2252/2004 as regards common security features and biometrics in passports and travel documents issued by Member States.

(3) When the certificate policy was first applied in connection with the implementation of fingerprints in passports, 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.

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

(5) This Decision constitutes a development of provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*[3]. The United Kingdom is not therefore taking part in its adoption and is not bound by it or subject to its application.

(6) This Decision constitutes a development of provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of

---

1 OJ L 385, 29.12.2004, p. 1.
2 C(2008) 8657 final
3 OJ L 131, 1.6.2000, p. 43.

the Schengen *acquis*[4]. Ireland is not taking part in its adoption and is not bound by it or subject to its application

(7) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark, annexed to the Treaty on European Union and to the Treaty establishing the European Community, Denmark has not taken part in the adoption of Regulation (EC) No 2252/2004 and is therefore not bound by it or subject to its application. However, given that Regulation (EC) No 2252/2004 aims to build upon the Schengen *acquis* under the provisions of Title IV of Part Three of the Treaty establishing the European Community, Denmark has, in accordance with Article 5 of the said Protocol, notified with letter of 6 June 2005 that it has transposed it into its national law. It is therefore bound to implement this Decision. Consequently, Denmark should receive a copy of this Decision.

(8) As regards Iceland and Norway, this Decision constitutes a development of 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 association of those two States with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1, point B of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[5].

(9) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the agreement concluded 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(A) of Decision 1999/437/EC read in conjunction with Article 3 of Council Decisions 2008/146/EC[6] and 2008/149/JHA[7].

(10) 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(A) of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/261/EC of 28 February 2008 on the signature, on behalf of the European Community, and on the provisional application of certain provisions of the Protocol 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[8].

---

4 OJ L 64, 7.3.2002, p. 20.
5 OJ L 176, 10.7.1999, p. 1.
6 OJ L 53, 27.2.2008, p. 1.
7 OJ L 53, 27.2.2008, p. 50.
8 OJ L 83, 26.3.2008, p. 3.

(10) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 6 of Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas[9],

HAS ADOPTED THIS DECISION:

Article 1

Annex I to Decision C(2008) 8657 final is amended as follows:

(1) in point 1 the following subparagraph is 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) is 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 is 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 the Annex to this Decision shall be added.

[9] OJ L 164, 14.7.1995, p. 1.

Article 2

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

Done at Brussels, 5.10.2009.

For the Commission
Jacques BARROT
Vice-President

CERTIFIED COPY
For the Secretary - General

Jordi AYET PUIGARNAU
Director of the Registry

ANNEX

1. "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 revoked certificate MUST be published no later than 72 hours after the certificate revocation. It is not advised to cache the CRL for long periond 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.