COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.12.2008
C(2008) 8657 final

NOT TO BE PUBLISHED

COMMISSION DECISION

of 22.12.2008

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 and updating the normative reference documents

COMMISSION DECISION

of 22.12.2008

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 and updating the normative reference documents

(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)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to Council Regulation (EC) 2252/04 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, hereafter referred to as "the Regulation", and in particular Article 2 thereof and the technical specifications as laid down in Commission Decision C(2006) 2909 of 28 June 2006,

Whereas:

(1) In accordance with Commission Decision C (2006) 2909 of 28 June 2006 a certificate policy had to be established at a later stage in order to ensure a coherent implementation among all Member States.

(2) At the same time, the Normative References are updated to the latest available versions, which contain no substantial changes to the former versions.

(3) These reference documents were considered as additional reference documents not having an impact on the implementation time frame of Regulation (EC) No 2252/2004 on common security features and biometrics in passports and travel documents issued by Member States.

(4) 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*, the United Kingdom has not taken part in the adoption of the Regulation and is not bound by it or subject to its application as it constitutes a development of provisions of the Schengen *acquis*. The United Kingdom is therefore not addressee of this decision.

(5) 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 the Schengen *acquis;* Ireland has not taken part in the adoption of the Regulation and is not bound by it or subject to its application as it constitutes a development of provisions of the Schengen *acquis*. Ireland is therefore not addressee of this decision.

(6) 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 the Regulation and is therefore not bound by it or subject to its application. However, given that the Regulation 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 under international law to implement this Decision. Consequently, Denmark should receive a copy of this Decision .

(7) As regards Iceland and Norway, the Regulation 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. Norway and Iceland are therefore bound by this Commission decision.

(8) As regards Switzerland, the Regulation 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 4 (1) of the Council decision on the signing, on behalf of the European Community and on the provisional application of certain provision of this Agreement.

(9) The measures provided for in this Decision are in accordance with the opinion of the Committee created by Article 6 of Regulation (EC) 1683/95.

HAS ADOPTED THIS DECISION:

Article 1

(1) According to point 5.5.3 of the Annex to Decision C (2006) 2909 of 28 June 2006 the common certificate policy is established as set out in the annex 1.

(2) The normative references as stated in point 7 of the Annex to Decision C(2006) 2909 of 28 June 2006 are updated as set out in annex 2.

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 Republic of Iceland, Kingdom of Norway and Swiss Confederation.

Article 3

This decision replaces the Commission decision C(2008) 4336 final of 25 September 2008.

Done at Brussels, 22.12.2008.

For the Commission
Jacques BARROT
Vice-President

CERTIFIED COPY
For the Secretary - General

Jordi AYET PUIGARNAU
Director of the Registry

ANNEX

ANNEX I TO COMMISSION DECISION OF ……..C(2008)….
COMMON CERTIFICATE POLICY FOR THE EXTENDED ACCESS CONTROL INFRASTRUCTURE FOR PASSPORTS AND TRAVEL DOCUMENTS ISSUED BY EU MEMBER STATES

Version 1.0

11th March 2008

1. INTRODUCTION

The goal of the Certificate Policy (CP) is to achieve trust and sufficient interoperability between the Country Verifying Certification Authorities (CVCAs) and Document Verifiers (DVs) of different Member States for the EAC-PKI to operate.

This Certificate Policy is established in accordance with Article 5.5.3 of the Technical Specifications on Standards for Security Features and Biometrics in Passports and Travel Documents issued by Member States, set out in Commission Decision C(2006) 2909 of 28.06.2006 [1].

The Certificate Policy only concerns the use of certificates to control access to fingerprint biometrics on Extended Access Control enabled passports and travel documents for the purposes of border control.

This common Certificate Policy provides a common set of minimum requirements upon which each Members State SHALL base a National Certificate Policy for use of certificates for border control purposes.

A National Certificate Policy MUST, as minimum, meet the standards of this common Certificate Policy but MAY place further restrictions on the control and usage of certificates within that Member State. A Member States MUST NOT require a DV in another Member State to adopt restrictions above those in this common Certificate Policy as a pre-requisite of issuing a certificate to that DV.

The issuing of certificates by a CVCA to domestic DV's is outside the scope of this common Certificate Policy.

This Certificate Policy is based on the Technical Guideline 'Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)', Version 1.1.1, TR-03110, published by the Bundesamt fur Sicherheit in der Informationstechnik, further referred to as TR-EAC.

[1] not published in the Official Journal - available on http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm

1.1. Overview

A certificate policy is a set of named rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements.

For both CVCA's and DV's this policy offers the same quality as that offered by the Extended Normalized Certificate Policy (NCP+) as defined in ETSI TS 102 042, version 1.2.2 (2005-06).

This Certificate Policy operates within the Public Key Infrastructure described in TR-EAC paragraph 2.2 "Public Key Infrastructure".

1.2. Documentation Name and Identification

This Common Certificate Policy is identified by its name and version number.

A National CP SHALL contain an OID which MUST identify the document and its version uniquely.

1.3. PKI Participants

This section gives an overview of the Certification Authorities, Certificate Holders, Registration Authorities, and Relying Parties of the Extended Access Control Public Key Infrastructure (EAC-PKI). The EAC-PKI is part of the international security infrastructure to ensure and verify integrity and authenticity of MRTDs issued by a Member State.

The overview of all PKI participants is summarised in Table 1.

	Certification Authority	Registration Authority	Subscriber	Relying Party
Country Verifying Certification Authority (CVCA)	X	X		
Document Verifier (DV)	X	X	X	X
Inspection System (IS)			X	X
Machine Readable Travel Document (MRTD)				X

Table 1 Overview of PKI participants of an EAC-PKI

1.3.1. Certification Authorities

Country Verifying Certification Authority The Root Certification Authority (CA) of a national EAC-PKI is called a Country Verifying Certification Authority (CVCA). The public keys of a national CVCA are contained in both self-signed CVCA certificates and link CVCA certificates. Both classes are called CVCA certificates. A national CVCA determines the access rights to sensitive data stored on domestic MRTD chips for all DVs (i.e. domestic DVs as well as foreign DVs) by issuing DV certificates entitling access control attributes.

A national CVCA issues certificates to its Certificate Holders (Subscribers). In this document, a Certificate Holder is called a Document Verifier (DV). A DV is an organisational unit that manages inspections systems belonging together.

Document Verifier Certification Authority Each country SHOULD have only one certification authority at the level of a Document Verifier (DV). However, this may not be possible for some Member States due to the way in which responsibility for border and immigration control is devolved within those states. In such cases, in order to minimise administrative overhead, subject registration SHOULD be carried out in a coordinated manner by the DVs.

A DV operates a CA to issue certificates for its inspection systems. The inspection system certificates issued by a DV usually inherit both the access rights and the validity period from the underlying DV certificate. However, the Document Verifier MAY choose to further restrict the access rights or the validity period.

1.3.2. Registration Authorities

Country Verifying Registration Authority For each national CVCA there is only one Registration Authority, the corresponding national Country Verifying Registration Authority (CVRA). Typically it is operated by the same authority as the CVCA.

The national CVRA is responsible for performing identification and authentication of certification requests of Document Verifiers, that is certification applications for subscriber certificates are only allowed by Document Verifiers. In addition, a CVRA initiates the issuance of certificates to Document Verifiers and it validates the process of revoking and renewing certificates issued by the corresponding CVCA.

For the purposes of the remainder of this document the CVRA will be assumed to be part of the CVCA and only the term CVCA will be used. Member States MAY divide/combine the role of CVCA and CVRA as they wish.

Document Verifier Registration Authority Each Member State SHALL operate only one Registration Authority for each Document Verifier.

DVs are responsible for performing identification and authentication of certification requests of Inspection Systems. In addition, a DV initiates the issuance of certificates to Inspection Systems and it validates the process of revoking and renewing certificates.

For the purposes of the remainder of this document the DVRA will be assumed to be part of the DV and only the term DV will be used. Member States MAY divide/combine the role of DV and DVRA as they wish.

1.3.3. Subscribers

Subscribers under this policy are Document Verifiers (DV) and Inspection Systems (IS). A DV is defined in Section 1.3.1.

For the purposes of this Certificate Policy an Inspection System is defined as the infrastructure, hardware and software required to obtain certificates from a Member States DV, store and manage those certificates, and to obtain fingerprint biometrics from MRTDs using those certificates, including mechanisms controlling access to the inspection systems.

1.3.4. Relying Parties

Relying Parties within an EAC-PKI are Document Verifiers, Inspection Systems, and MRTDs.

A relying party is an entity who verifies the signature of a certificate using a trusted certification path (see section 1.4). A member state shall clearly identify which trusted certification path a relying party has to use to verify a certificate (see section 1.4).

1.3.5. Other Participants

If a member state identify other participants, then this paragraph has to be fulfilled by the member state. Other participants identified by member state, who has role and/or interacts with PKI, doesn't have to be in conflict with the security requirements defined in the present CP.

1.4. Certificate Usage

– To enable read access by Inspection Systems to fingerprint biometrics stored on the MRTDs as indicated in the certificates, for the only purpose of verification of the identity of the holder by means of directly available comparable features.

– For a Member State CVCA, keys pairs and certificates are used for the following purpose:

– CVCA private key shall be used to sign national and external DV certificate and may be used to signs DV certificate request to provide to other authorized Member state CVCA (see section 3.4);

– CVCA certificate shall be used to verify signatures realized by a national or other Member State DV;

– DV private key shall be used to sign national IS certificates;

– DV certificate shall be used to verify signature of national or external IS certificate.

Those certificates enable to read access by Inspection Systems to fingerprint biometrics stored on the MRTDs as indicated in the certificates, for the only purpose of verification of the identity of the holder by means of directly available comparable features. To do that, it is necessary to have clear identification of which trusted certification path to be used.

Trusted certification path managed by a CVCA shall be composed of the following certificates:

– CVCA certificate: self-signed certificate;

– If needed, intermediate link CVCA certificate;

– DV certificate: DV certificates are signed by at least the national CVCA;

– IS certificate: IS certificates are signed DV.

Relying parties trusted certification path are for:

– DV:

  - national CVCA certificate and authorized Member State CVCA certificate;

– IS:

  - national DV certificate, national CVCA certificate and authorized Member State CVCA certificate;

– MRTD: authorized Member State IS certificate, authorized Member State DV certificate and national CVCA certificate and possibly national link CVCA certificate and the corresponding CVCA certificate.

Note: national refers to the Member State who issues the CVCA, DV, IS and MRTD. Authorized Member State refers to a Member State which is authorized to collect data from MRTD of national citizen using a DV (and IS) signed by the national CVCA of the citizen.

1.5. Policy Administration

European Commission
Directorate General for Justice, Freedom and Security
Directorate B, Unit B1
1049 Brussels
Belgium

1.6. Terminology, Definitions and Acronyms

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

A “Member State” is defined to be a state participating in Regulation 2252(2004).

“Domestic” is defined to mean of the same Member State.

“Foreign” is defined to mean of another Member State.

A “Valid Key” is defined to be a key for which the current time is within the validity period of the corresponding Subscriber Certificate and for which the corresponding Subscriber Certificate has not been revoked.

Further definitions and acronyms used in this policy are given in Appendix A.1.**2.**

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The European Commission is responsible for maintaining a list of contact details for CVCAs and DVs at the European level. The content and integrity of this list is preserved by diplomatic means. The corresponding information is available on the web site of the Directorate General for Justice, Freedom and Security (DG-JLS) of the European Commission.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

As defined in TR-EAC A.4.1, the Certification Authority Reference is used to identify to public key to be used to verify the signature of the certification authority (CVCA or DV).

The Certificate Authority Reference MUST be equal to the Certificate Holder Reference in the corresponding certificate of the certification authority (CVCA Link Certificate or DV Certificate).

The Certificate Holder Reference SHALL identify a public key of the certificate holder. It MUST be a unique identifier relative to the issuing certification authority. It SHALL consist of the following concatenated elements:

– 1) The ISO 3166-1 ALPHA-2 country code of the certificate holder's country;

– 2) A mnemonic that represents the certificate holder;

– 3) A numeric or alphanumeric sequence number.

NOTE: It is not guaranteed that the Certificate Holder Reference is a unique identifier in general.

Members State shall defined identity as follow:

– CVCA certificate:

- Certification Authority Reference: national CVCA identity;
- Certificate Holder Reference: national CVCA identity;

– DV certificate:

- Certification Authority Reference: national CVCA identity or other authorized Member State CVCA (see section 3.3) identity;
- Certificate Holder Reference: national DV identity;

– IS certificate:

- Certification Authority Reference: national DV identity;
- Certificate Holder Reference: national IS identity.

3.2. Initial Identity Validation

3.2.1. National CVCA

Each Member State SHALL clearly identified who is responsible of the authentication and the definition of the CVCA identity.

3.2.2. CVCA to CVCA

In order to validate requests from DVs, a CVCA must be able to confirm the identity of the DV with that Member States CVCA. Therefore prior to DVs submitting certificate requests the CVCAs of participating states MUST validate each other's identity.

CVCA identity validation SHALL be carried out under the supervision of the European Commission. CVCAs SHALL submit the following information to the European Commission for distribution to other participating CVCAs:

(a) The National Certificate Policy;

(b) The public part of the CVCA's Certificate Practice Statement, if it exists;

(c) A copy of the CVCA Public Key;

In event of a change to any of the above, CVCAs SHALL submit the updated version to the European Commission for distribution to other participating CVCAs.

3.2.3. DV to CVCA

When a DV from one Member State first submits registration information to a CVCA in another Member State this SHALL be done by a mutually agreed trusted channel

The DV MUST include the following in the registration information:

(a) The public part of the DVs Certificate Practice Statement;

(b) The latest Certificate of Conformity with the National Certificate Policy for the DV;

(c) A list of the organisations using Inspection Systems subscribing to the DV;

(d) A Certificate Request as specified in TR-EAC, paragraph A.4.2. This Certificate Request MUST include an Outer Signature, as defined in TR-EAC paragraph A.4.2.4, signed by the DVs supervising CVCA.

In the event of a non-trivial change to any of the above, the DV SHALL submit details of the change to the CVCA to allow it to make an assessment as to whether a new Initial Identity Validation is required.

3.2.4. IS to DV

DVs SHALL have a proper mechanism in place to identify an authenticated inspection system. When the initial key material is generated and the Certificate Request is compiled, staff authorised by the DV SHALL be physically present.

3.3. Identification and Authentication for Re-key Requests

As specified in TR-EAC, paragraph A.4.2.

3.3.1. DV to CVCA

The CVCA SHALL ensure the validity of the request by confirming:

(a) That the request is formatted in accordance with TR-EAC paragraph A.4.2

(b) That the CVCA for the DV's Member State continues to list the DV as valid;

(c) That the DV's Certificate of Conformity is valid;

(d) That the outer signature of the request is created with a key which is valid with respect to a certificate of that DV, issued by the CVCA

3.3.2. IS to DV

The DV SHALL only issue a certificate once it has confirmed:

(a) That the Inspection System remains registered as operational;

(b) That the Inspection System is not listed as stolen/missing;

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. CVCA

Each Member State shall define which entity is responsible to authorize the CVCA creation.

4.1.2. DV to CVCA

Following successful Initial Identity Validation as per 3.2.3 above, DV Certificate Application SHALL be carried out in accordance with TR-EAC A.4.2 Certificate Requests and TR-EAC 2.2.2 Document Verifiers.

4.1.3. IS to DV

Inspection Systems MAY submit Certificate Applications upon completion of successful Initial Identity Validation as per 3.2.4 above.

4.2. Certificate Application Processing

4.2.1. Certificates issued by CVCA to CVCA

A CVCA SHALL only issue a self signed CVCA certificate or a link certificate to a former CVCA certificate, during the key ceremony that complies with its own National Certificate Policy.

CVCAs MUST check that a certificate request is authorized and valid (see section 4.1.1).

4.2.2. Certificates issued by CVCA to DV

A CVCA SHALL only issue a certificate to a DV that is complying with its own (the DVs) National Certificate Policy that is, at minimum, in accordance with this Certificate Policy and the usage (governmental and non-governmental) of fingerprint biometrics in the Travel Document is in conformance with Section 1.4 of this document.

CVCAs MUST check that a certificate request is valid.

CVCAs MUST acknowledge a certificate request upon its receipt.

The CVCA MUST process the certificate request within the timeframe of 72 hours set out in point 5.5.2 of Commission Decision C(2006) 2909 of 28.06.2006.

In the event that a CVCA system is non-operational for more than this time frame, it MUST inform all subscribing DVs no later than 7 days before the loss of service, if planned, and as soon as is reasonably possible in the event of an unplanned loss of service.

4.2.3. Certificates issued by DV to IS

A DV SHALL only issue a certificate to an IS that is complying to its own National Certificate Policy and that is using the certificates in accordance with part 1.4 of this document.

DVs MUST check that a certificate request is valid prior to issuing a certificate.

4.3. Certificate Issuance

4.3.1. CV Issued Certificates

CVCAs SHALL take measures against the forgery of certificates and ensure that the procedures of issuing the certificate is securely linked to the associated registration, certificate renewal or re-key, including the provision of any subject generated public key.

Certificates SHALL be generated and issued in accordance with TR-EAC A.4 CV Certificates.

4.3.2. DV Issued Certificates

DVs SHALL ensure they issue certificates securely to maintain their authenticity.

DVs SHALL take measures against the forgery of certificates and ensure that the procedures of issuing the certificate is securely linked to the associated registration, certificate renewal or re-key, including the provision of any subject generated public key.

Certificates SHALL be generated and issued in accordance with TR-EAC A.4 CV Certificates.

4.4. Certificate Acceptance

CVCA self signed certificate SHALL be accepted by the entity responsible for the CVCA after its creation at the end of the key ceremony.

A DV or IS SHALL be deemed to have accepted a certificate upon its receipt.

4.5. Key Pair and Certificate Security Rules

CVCAs, DVs and ISs and MUST fulfil the following requirements as appropriate.

- Ensure that accurate and complete information is submitted to the CVCA/DV in accordance with the requirements of this policy, particularly with regards to registration;
- The key pair is only used in accordance with the limitations imposed by this CP;
- Ensure there is no unauthorised use of the private key;
- Keys are generated in accordance with TR-EAC.
- Only use private keys for signing or decrypting within a secure cryptographic device as described in section 6.2;
- Notify a CVCA/DV without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - A private key has been lost, stolen, potentially compromised; or
    - Control over the private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or
    - Inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;
- Following compromise, the use of a private key is immediately and permanently discontinued;
- In the case of being informed that a CVCA or DV's Private Key has been compromised and certificates signed by these Private Keys SHOULD NOT be relied upon and SHOULD act appropriately.

Key pair and certificate usage SHALL be as indicated by the certificate issuer (CVCA or DV) in the Certificate Holder Authorisation Field of the Certificate.

DVs and ISs SHALL only use the private key corresponding to the received DV and IS certificate for the following purposes only;

- The purpose as described in Section 1.4 'Certificate Usage' of this CP;
- In accordance with the content of the issued certificates.

4.6. Certificate Renewal

Not allowed

4.7. Certificate Re-key

Certificate re-key MAY only take place where:

(a) The DV or IS certificate is about to expire.

(b) A DV certificate is revoked;

(c) An IS key is compromised;

(d) Where a DV\IS certificate requires modification due to changes in the DV\IS attributes;

The CVCA\DV SHALL ensure that requests for certificates issued to a previously registered DV\IS are complete, accurate and duly authorised. The CVCA\DV SHALL:

(a) Check the existence and validity of the certificate to be re-keyed and that the information used to verify the identity and attributes of the DV\IS is still valid;

(b) Issue a new certificate based on verification of the subject's signature on the request only if the cryptographic security of that signature key is still sufficient for the new certificate's validity period and no indications exist that the key used to generate the subject's signature on the request has been compromised

Certificates SHALL be issued in accordance with 4.3 Certificate Issuance above.

In the case where a DV certificate is about to expire (see 4.7a above), TR-EAC A.4.2 Certificate Requests MUST be followed.

In the case where a DV certificate is revoked, expired or requires modification (see 4.7b,c,d above), re-keying is equal to the procedures when a DV applies for a DV certificate for the first time.

In the case where an IS private key is compromised or expired, re-keying is equal to the procedures when an IS appliers for an IS certificate for the first time.

4.8. Certificate Modification

This is covered by section 4.7, 'Certificate Re-Key', of this document.

4.9. Certificate Revocation and Suspension

See section 5.7, 'Compromise and Disaster Recovery', of this document.

4.10. Certificate Status Services

See section 5.7, 'Compromise and Disaster Recovery', of this document.

4.11. End of Subscription

Not applicable.

4.12. Key Escrow and Recovery

MUST NOT be used.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1. Physical Controls

Each CVCA and DV SHALL ensure that it operates of its services in a secure environment. This SHALL include:

(a) Site location and construction: The CVCA/DV are operated in a physically protected area.

(b) Physical access: Access to the CVCA/DV is controlled and audited. Only authorised persons have physical access to the CVCA/DV environment.

(c) Media storage: The storage media are protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).

(d) Waste disposal: Procedures for the disposal of waste are implemented in order to avoid unauthorised use, access, or disclosure of sensitive data.

(e) Off-site backup: An off-site backup of critical data MAY be installed.

5.2. Procedural Controls and System Access Management

Procedural controls SHALL be implemented, especially the separation of duties by implementing a two person principle for critical tasks.

Each CVCA, DV, and IS SHALL ensure that system access to any EAC-PKI device is limited to individuals who are properly authorised on a need to know basis. In particular, the following requirements apply:

(a) Controls (e.g. firewalls) SHALL be implemented to protect the CV internal network domains from external network domains accessible by third parties.

(b) Sensitive data SHALL be protected against unauthorised access or modification.

(c) Sensitive data SHALL be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.

(d) Each CVCA, DV, and IS SHALL ensure effective administration of users (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.

(e) The CVCA, DV, and IS SHALL ensure access to information and application system functions are restricted to authorised staff and that the EAC-PKI systems provide sufficient computer security controls for the separation of

trusted roles, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled. Access SHALL be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user.

(f) CVCA, DV, and IS personnel SHALL be successfully identified and authenticated before using EAC-PKI applications related to certificate management or access to MRTDs.

(g) CVCA, DV, and IS personnel SHALL be accountable for their activities, for example by retaining event logs as defined in Section 5.4.

(h) Sensitive data SHALL be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorised users.

5.3. Personnel Controls

All EAC-PKI systems, that is the CVCA, DV and IS systems, SHALL be operated by qualified and experienced staff.. In particular, the following requirements hold:

(a) Each CVCA, DV and IS SHALL employ a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;

(b) Personnel SHALL undergo domestic security screening appropriate to the role(s) they are carrying out;

(c) Appropriate disciplinary sanctions SHALL be applied to personnel violating CVCA, DV or IS policies or procedures;

(d) Security roles and responsibilities, as specified in the system's security policy, SHALL be documented in job descriptions. Trusted roles, on which security of the system's operations are dependent SHALL be clearly identified;

(e) All personnel (both temporary and permanent) SHALL have job descriptions defined from the view point of separation of duties and least privilege.

(f) Personnel SHALL exercise administrative and management procedures and processes that are in line with the Procedural Controls described in 5.2 above;

(g) All CVCA, DV and IS personnel in trusted roles SHALL be free from conflicting interests that might prejudice the impartiality of the system's operations;

(h) Personnel with access to private keys within the EAC PKI SHALL be formally appointed to trusted roles by a senior management responsible for security of the IS;

(i) CVCAs, DVs and ISs SHALL NOT appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel SHALL

NOT have access to the trusted functions until any necessary checks are completed;

5.4. Audit Logging Procedures

Each CVCA, DV, and IS MUST implement appropriate logging procedures to analyze and recognize any proper and improper use of its system within the EAC-PKI.

CVCAs, DVs and ISs SHALL ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, at minimum to ensure compliance with audit requirements as described in 8. Compliance Audit and Other Assessment.

CVCAs and DVs SHALL ensure that:

(a) The confidentiality and integrity of current and archived records concerning certificates is maintained;

(b) Records concerning certificates are completely and confidentially archived;

(c) The precise time of significant environmental, key management and certificate management events is recorded

(d) All events relating to the life-cycle of keys are logged;

(e) All events relating to the life-cycle of certificates are logged;

(f) All events relating to registration are logged;

(g) All requests and reports relating to revocation, as well as the resulting actions, are logged;

(h) The specific events and data to be logged are documented;

(i) Events are logged in a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the time period they are REQUIRED to be held;

ISs SHALL maintain a log including:

(a) The logging of the key management part of the Inspection System SHALL be done in such a way that the responsible DV can detect misuse of the system and apply appropriate countermeasures.

(b) Protection against modification or deletion of logs.

(c) Records SHALL be kept to enable the auditor to confirm that misuse can be detected.

5.5. Records Archival Procedures

Each CVCA, DV, and IS SHALL implement appropriate records archival procedures for its system within the EAC-PKI. Procedures SHALL ensure the integrity, authenticity and confidentiality of the data.

The archives SHALL be created in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Access to archives SHALL be restricted to authorized operators only.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

Inspection Systems SHALL NOT log or transmit fingerprints obtained from MRTDs. These biometrics SHALL be deleted immediately after finishing the comparison process between fingerprints acquired from of the bearer and fingerprints read from the MRTD.

Archived records SHALL be held for a period of time as appropriate for providing necessary legal evidence in accordance with the applicable legislation of the Member State.

5.6. Key Changeover

CVCAs and DVs SHALL ensure that keys are generated in controlled circumstances and in accordance with the procedures defined in Section 5.2 Management, Operational, and Physical Controls.

Full self-signed certificates plus link certificates SHALL be provided by the CVCA

5.7. Compromise and Disaster Recovery

CVCAs SHALL take reasonable measures to ensure that continuity of service is maintained, including:

(a) Measures to minimise the impact of disruption to power services;

(b) Measures to minimise the impact of events such as flooding or fire;

(c) Measures to minimise the impact of the loss of availability of key staff;

5.7.1. Incident and Compromise Handling Procedures

Any CVCA, DV and IS SHALL ensure in the event of a disaster, including compromise of the participant's private key, that operations are restored as soon as possible. In particular, the following requirements hold:

1. Each CVCA, DV and IS SHALL define and maintain a continuity plan to enact in case of disaster (see also Section 5.7.4).

2. CVCA and DV systems data necessary to resume CVCA and DV operations SHALL be backed up and stored in safe places suitable to allow the CVCA and DV to timely go back to operations in case of incident/disasters.

3. Back up and restore functions SHALL be performed by the relevant trusted roles.

4. The EAC-PKI business continuity plan (or disaster recovery plan) SHALL address the compromise or suspected compromise of a private key as a disaster and the planned processes SHALL be in place (see also Section 5.7.3).

5.7.2. Computing Resources, Software, and/or Data are Corrupted

If a private CVCA key is unusable for non-critical reasons, the procedure described in Section 5.6 is processed.

5.7.3. Entity Private Key Compromise Procedures

A Document Verifier SHALL immediately inform all CVCAs that have issued certificates for this DV about DV or IS private key compromise or misuse.

If an Inspection System is lost or stolen, the responsible Document Verifier SHALL inform all CVCAs that have issued certificates for this DV about the corresponding incident as soon as possible, but not later than the next certificate request.

Each country SHOULD publish to all other countries in which way the requested information is made available.

5.7.4. Business Continuity Capabilities after a Disaster

Each CVCA SHALL maintain a Business Continuity Plan detailing how it will maintain its CVCA services in the event of an incident that affects its normal capability.

5.8. CVCA or DV Termination

In the event of a CVCA terminating its operations it SHALL:

- Notify all CVCAs with which it is registered of the termination;
- Notify all CVCAs, with which it is registered, of the CVCA, if any, which will be taking over responsibility for national DVs;
- Notify all DVs which it supplies with certificates of the termination;
- Notify all DVs, which it supplies with certificates, of the CVCA, if any, which will be issuing certificates in its place;
- Any replacement CVCA MUST continue to provide certificates for MRTDS issued under the original CVCA;
- The CVCA SHALL destroy, or withdraw from use, its private keys;

In the event of a DV terminating its operations, it SHALL notify its national CVCA which will then notify all CVCAs issuing certificates to that DV.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation

CVCAs and DVs SHALL ensure that CA keys are generated in controlled circumstances according to Section 5 Management, Procedural and Physical Controls of this document.

Key generation SHALL be carried out within a trustworthy device which is compliant with Appendix B.

Before expiration of a CVCA or DV signing key, the CVCA or DV SHALL generate a new certificate-signing key pair and SHALL apply all necessary actions to avoid disruption to the operations of any CVCA, DV or IS which may rely on that key. The new key SHALL be generated and distributed in accordance with TR-EAC and this policy.

CVCAs and DVs SHALL ensure that the integrity and authentication of their public keys and any associated parameters are maintained during distribution to DVs and ISs.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Private signing keys SHALL be held and used within a trustworthy device which is compliant with Appendix B.

CVCAs SHALL implement technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive CVCA key operations (such as creation, back-up, restore, destruction and use).

DVs SHALL implement technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive DV key operations (such as creation, back-up, restore and destruction). DV must implement trusted role authentication process with the DV HSM to allow DV key usage.

IS key operations (such as creation, back-up, restore, destruction and use) MUST be restricted to authorized personnel appointed to this role.

When outside the signature–creation device, private signing keys SHALL be protected in a way that ensures the same level of protection as provided by the signature creation device.

If private keys are backed up, they SHALL be stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorised to carry out this function SHOULD be kept to a minimum.

Backup copies of the private signing keys SHALL be subject to the same or greater level of security as keys currently in use.

Where keys are stored in a dedicated key processing hardware module, access controls SHALL be in place to ensure keys are not accessible outside the hardware module.

Private signing keys MUST NOT be used beyond the end of their lifecycle and all copies of the key SHALL be destroyed or put beyond use at the end of their life.

The security of cryptographic devices MUST be ensured throughout their lifecycle including ensuring that certificate and revocation status signing cryptographic hardware is not tampered with during shipment or storage, functions correctly when in operation and any private keys stored on the equipment is destroyed upon device retirement.

6.3. Other Aspects of Key Pair Management

Operational periods as specified in point 5.5.1 of Commission Decision C(2006) 2909 of 28.06.2006:

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

6.4. Activation Data

The requirements applicable to the activation data SHOULD be determined by the DV itself based on a risk analysis.

It MAY make use of de-blocking the activation data, but this MUST be in line with the security level offered by the activation data.

6.5. Computer Security Controls

CVCAs, DVs and ISs SHALL comply with the procedures for computer security controls described in Section 5 Management, Operational and Physical Controls.

CVCA/DV/IS components MAY include the following functionalities:

– Require authenticated logins for trusted roles;

– Provide Discretionary Access Control;

– Provide a security audit capability (protected in integrity);

– Prohibit object re-use;

– Require use of cryptography for session communication and database security;

– Require a trusted path for identification and authentication;

– Provide domain isolation for process;

– Provide self-protection for the operating system.

6.6. Life Cycle Security Controls

The trustworthy devices used by CVCAs, DVs and ISs SHALL be protected against modification.

An analysis of security requirements SHALL be carried out at the design and requirements specification stage of any systems development project undertaken by the CVCA, DV or IS

that impacts on trustworthy systems or products to ensure that security is built into IT systems.

Change controls procedures MUST exist, and be documented, and used for releases, modifications and emergency software fixes for any operational software of CVCAs, DVs and ISs.

6.7. Network Security Controls

CVCAs and DVs SHALL comply with the procedures for network security controls described in Section 5 Management, Operational and Physical Controls.

6.8. Time-stamping

Not applicable

7. CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

CV Certificates as specified in TR-EAC A 4.1 CV Certificates.

7.2. CRL Profile

Not applicable

7.3. OCSP Profile

Not applicable

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

A DV can only claim conformance with this CP if it is able to show it is conformant with a National Certificate Policy that meets the standard of this document. Other CVCAs must assess whether the National Certificate Policy is compliant with this Certificate Policy, prior to issuing certificates to DV operating under that policy. In the event of a dispute, arbitration SHALL be carried out under the supervision of the European Commission.

DVs MUST select an independent accredited company/organisation ("Auditing Body") to audit the DV according to their National Certificate Policy and their Certificate Practice Statement.

The Auditing Body MUST be accredited for this purpose by its national accreditation body. The audit MUST not only check that procedural security controls are specified but also that they are adhered to in practice. This also includes the operation and management of Inspection Systems subscribing to the DV. Audits MUST be performed at least every three years.

The Auditing Body SHALL carry out a review at least once a year by a team of one or more auditors to ensure ongoing compliance with this CP.

Proof of conformity with the CP is only recognised if the DV can show a 'certificate of conformity' issued by the Auditing Body stating that the DV is compliant with this CP by way of being compliant its National Certificate Policy.

In the event that an audit indicates that a DV is not conforming to its National Certificate Policy, the DV is REQUIRED to notify all CVCAs from which it receives certificates.

In the event a DV is not certified to be compliant with its National Certificate Policy, or its certification becomes invalid or expires, other Member States MUST not issue any further DV Certificates to this DV.

It is recommended that a DV implement an Information Security Management System (ISMS) for its CA and RA functionality in accordance to ISO/IEC 27001. The ISMS is based on an ISMS policy of which its scope is defined by the National Certificate Policy and the associated Certificate Practise Statement.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Not applicable.

9.2. Financial Responsibility

Not applicable.

9.3. Confidentiality of Business Information

Not applicable.

9.4. Privacy of Personal Information

ISs are not permitted to log or transmit fingerprint biometrics obtained from MRTDs. These biometrics MUST be deleted immediately after finishing the comparison process between the fingerprint biometric collected by the IS from the bearer and the fingerprint biometric read from the MRTD.

9.5. Intellectual Property Rights

Not applicable.

9.6. Representations and Warranties

Not applicable.

9.7. Disclaimers of Warranties

Not applicable.

9.8. Limitations of Liability

Not applicable.

9.9. Indemnities

Not applicable.

9.10. Term and Termination

Not applicable.

9.11. Individual Notices and Communicating With Participants

All key management tasks MUST be carried out by robust communications channels.

All CVCAs and DVs MUST be able to carry out such communications by Email at minimum, although other additional online or offline communication channels MAY be mutually agreed.

In the event of disruption to a CVCAs 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

Email messages MUST conform to the following format and, where appropriate, MIME compliant attachments MUST be used.

9.11.1. Register

Subject:	Register
Body:	URLs to be used to contact this state
Attachments:	none

9.11.2. CVCA Certificate

Subject:	CVCA Certificate
Body:	Unspecified
Attachments:	CVCA Link Certificate(s)

9.11.3. DV Certificate Request

Subject:	DV Certification Request
Body:	Unspecified
Attachments:	Certificate Request(s)

9.11.4. DV Certification Receipt Acknowledgement

Subject:	DV Certification Request Receipt Acknowledgement
Body:	Unspecified
Attachments:	Certificate Request(s)

9.11.5. DV Certificate

Subject:	[Reply to] DV Certification Request
Body:	If a DV certificate is not to be issued, the reason why.

Attachments:	DV Certificate (if at least one is issued)

9.11.6. Suspension of CVCA Service

Subject:	{Nation States} CVCA Suspension
Body:	Details of start and end date of CVCA service suspension
Attachments:	Unspecified

9.12. Amendments

Member States may revise their National CP. Additional reviews may be enacted at any time at the discretion of the Member State. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without prior notification, but after the changes have been made Member States and the European Commission should be informed. Prior to approving any major security changes to the CP, the Member State SHALL notify the European Commission and other Member States that have DVs signed by national CVCA.

A Member State SHALL notify other authorized Member States and the European Commission and CVCA/DVs on its intention to modify the CP no less than 3 months before entering in a modification process on the CP and the scope of modification.

CP OIDs SHALL be changed if a Member State determines that a change in the CP modifies the level of trust provided by the CP.

9.13. Dispute Resolution Procedures

Not applicable.

9.14. Governing Law

Not applicable.

9.15. Compliance with Applicable Law

Not applicable.

9.16. Miscellaneous Provisions

Not applicable

9.17. Other Provisions

Not applicable

APPENDIX A.1. DEFINITIONS

1. *Certification Authority* – An entity that issue certificates

2. *Certificate Revocation List* – A list of revoked certificates;

3. *Certificate Policy* – A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirement;

4. *Certificate Practice Statement* – A statement of the practise that a certification authority employs in issuing, managing, revoking and renewing or re-keying certificates;

5. *Common Certificate Policy* – The outline Certificate Policy published by the Commission which sets the minimum requirements for Member States National Certificate Policies to meet, in order to be included within the EAC-PKI.

6. *Common Criteria* - Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

7. *Extended Access Control Public Key Infrastructure* – The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control.

8. *Document Signer* – the entity signing the original document, in this case the organisation that issues the MRTD;

9. *Document Verifier* – an entity within the EAC-PKI that requests certificates from CVCAs and, on the basis of those certificates, issues certificates to Inspection Systems;

10. *Evaluation Assurance Level* – a numeric grade assigned to an IT system or product following the completion of a Common Criteria security evaluation

11. *Inspection System* – the operational system that reads fingerprint biometrics from MRTDs.

12. *International Civil Aviation Organisation* – A UN organisation tasked with fostering the planning and development of international air transport. In this role it sets international standards for MRTDs

13. *Key ceremony* - A procedure whereby a key pair is generated using a cryptographic module and where the public key is certified.

14. *Link Certificate* – Link certificates ensure business continuity without exchanging a new trusted self-signed root CVCA certificate out-of-band.

15. *Machine Readable Travel Document* – An international travel document containing eye- and machine-readable data;

16. *National Certificate Policy* – a Members States Certificate Policy for management of the process of issuing and receiving certificates too and from other Members States;

17. *Object Identifier* – a unique numerical sequence allowing a document to be identified;

18. *Public Part of the Certification Practice Statement* – A subset of the provisions of a complete CPS that is made public by a CA

19. *Registration Authority* – An entity that establishes enrolment procedures for certificate applicants, performs identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA

20. *Trusted certification path* – A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of one or more CVCA-certificates, link certificates as appropriate, a DV-certificate and the IS certificate.

APPENDIX A.2 ACRONYMS

CA	Certification Authority
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSPKI	Country Signing Public Key Infrastructure
CVRA	Country Verifying Registration Authority
CVCA	Country Verifying Certification Authority
EAC-PKI	Extended Access Control Public Key Infrastructure
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organisation
IS	Inspection System
MRTD	Machine-Readable Travel Document
OID	Object Identifier
RA	Registration Authority

APPENDIX B.1 – REQUIREMENTS FOR CERTIFICATION AUTHORITIES

The crypto modules used by certificate authorities SHALL be evaluated and certified in accordance with one of the following standards:

- FIPS PUB 140-1 level 3 or higher [2]
- FIPS PUB 140-2 level 3 or higher [3]
- PP-SSCD [4,5,6]
- BSI Cryptographic Modules Security Level "Enhanced"[7]

APPENDIX B.2 – REQUIREMENTS FOR INSPECTION SYSTEMS

Member States SHALL adopt security targets for their inspection systems in accordance with Section 6. The inspection system SHALL be evaluated at a minimum level 2 and the key management component SHALL be evaluated at Level 4, augmented by VLA4 or VAN5.

2 Security Requirements for Cryptographic Modules (FIPS PUB 140-1).
3 Security Requirements for Cryptographic Modules (FIPS PUB 140-2).
4 BSI-PP-0004-2002T Protection Profile – Secure Signature-Creation Device Type 1, Version 1.05
5 BSI-PP-0005-2002T Protection Profile – Secure Signature-Creation Device Type 2, Version 1.04
6 BSI-PP-0006-2002T Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05
7 BSI-PP-0036-2008: Cryptographic Modules Security Level "Enhanced" Version 1.01

ANNEX II TO COMMISSION DECISION OF……C(2008) …..CHANGES TO THE NORMATIVE REFERENCES AS STATED IN POINT 7 OF THE ANNEX TO DECISION C(2006) 2909 OF 28 JUNE 2006

1. Reference No 13 is changed as follows:

"Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) Version 1.11"

2. Reference No 17 is changed as follows:

"Common Criteria Protection Profile for Machine Readable Travel Document with “ICAO Application”, Extended Access Control, Version 1.2"