Home Office
UK Border Agency

THE UNITED KINGDOM'S NATIONAL CERTIFICATE POLICY for Extended Access Control Infrastructure for machine readable travel documents and biometric residence permits issued and read within the UK

September 2012

OID: 1.2.826.0.1363
Public Document

1. INTRODUCTION

The United Kingdom (UK) Certificate Policy (CP) sets out governance arrangements for how the United Kingdom will use digital certificates required to open the chip on biometric documents using Extended Access Control – Public Key Infrastructure (EAC-PKI).

The UK CP is owned by the Home Office and is administered by the UK Border Agency. This arrangement is subject to review by the Home Office.

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

BACKGROUND AND ORIGINS OF THE POLICY

The UK CP is based on the Common European Union CPs for i) Passports and Machine Readable Travel Documents (MRTDs) and ii) Biometric Residence Permits (BRPs).

The term Machine Readable Document (MRD) is used throughout this CP. This refers both to Machine Readable Travel Documents, Biometric Residence Permits and any other Machine Readable Documents which may be developed in the future.

a) Passports and MRTDs

The EAC-PKI was developed under auspices of the EU to support free movement of citizens of the EU Schengen States. Commission Decision C(2006) 2909 of 28 06 2006 sets out the Technical Specifications on Standards for Security Features and Biometrics in Passports and Travel Documents issued by Member States. The UK is not party to the travel and border control elements of the Schengen Agreement and is therefore outside the provisions of the regulations governing MRTDs. However, in order to maintain interoperability of travel documents issued by Member States[1] party to the Schengen Agreement, the UK CP mirrors the processes and procedures required by them for EAC-PKI.

b) BRPs

The UK has opted into the European Regulations (EC) 1030/2002 and 380/2008 in relation to BRPs, therefore this Certificate Policy complies with Article 5.4.3 of the Technical Specifications on Standards for Security Features and Biometrics in Residence Permits issued by Member States, set out in Commission Decision C(2009) 3770 final of 20/05/2009. This requires participating Member States to publish a National CP based on the Common EU Certificate Policy. As a minimum, the National Policy must meet the standards of the Common EU Certificate Policy but MAY place further restrictions on the control and usage of certificates within that Member State.

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

COMPLIANCE WITH COMMON EU CERTIFICATE POLICY

In accordance with EU regulations, the UK will not require a Document Verifier (DV) in another Member State to adopt restrictions above those in the Common EU Certificate Policy as a pre-requisite of issuing a certificate to that DV.

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 für Sicherheit in der Informationstechnik, further referred to as TR-EAC

Purposes for which certificates may be used

Passports - As the UK may enter into agreements with states outside the EU and certificates may be used in the UK for purposes other than identification, the UK Certificate Policy has been written to be neutral on the purposes for which certificates relating to passports can be used. Where the purposes fall outside the relevant EU regulations, they will be limited by Memoranda of Understanding or Commercial Agreements between the parties exchanging certificates.

Biometric Residence Permits – Certificates may be used to control access to fingerprint biometrics on Extended Access Control enabled Residence Permits for the purposes of identification and will be only used for verifying the authenticity of the document and the identity of the holder by means of directly available comparable features.

1.1 OVERVIEW

A certificate policy is a set of named rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
For both CVCAs and DVs this policy offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC) requiring the use of a Secure User Device (signing or decrypting).
This Certificate Policy operates within the Public Key Infrastructure described in TR-EAC paragraph 2.2 "Public Key Infrastructure".

1.2 EAC-PKI PARTICIPANTS

This section gives an overview of the Certification Authorities, Certificate Holders, Registration Authorities, and Relying Parties of the EAC-PKI. The EAC-PKI is part of the international security infrastructure which ensures and verifies the integrity and authenticity of MRDs issued by a participating State.

An 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 Document (MRD)				X

TABLE 1 OVERVIEW OF PKI PARTICIPANTS OF AN EAC-PKI

1.2.1 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 MRD 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

Passports - Each State SHOULD have only one certification authority at the level of a Document Verifier (DV) for identification purposes. However, this may not be possible for some 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.

The UK MAY have more than one DV for domestic purposes.

Biometric Residence Permits – Each Member State 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 the Member State MAY operate up to three DVs. 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.

1.2.2 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. States MAY divide/combine the role of CVCA and CVRA as they wish.

Document Verifier Registration Authority Each 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. Participating DVs MAY divide/combine the role of DV and DVRA as they wish.

1.2.3 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 domestic DV, store and manage those certificates, and to obtain fingerprint biometrics from MRDs using those certificates, including mechanisms controlling access to the Inspection Systems.

1.2.4 Relying Parties

Relying Parties within an EAC-PKI are Document Verifiers, Inspection Systems, and MRDs.
A relying party is an entity which verifies the signature of a certificate using a trusted certification path (see section 1.4). A State shall clearly identify which trusted certification path a relying party has to use to verify a certificate (see section 1.4).

1.2.5 Other Participants

Other participants who interact with the EAC-PKI shall be identified within the Agreement (as defined in 1.6 below) governing certificate usage and must not be in conflict with this CP, for the BRP especially the security requirements.

1.3 CERTIFICATE USAGE

To enable read access by Inspection Systems to fingerprint biometrics stored on the MRDs as indicated in the certificates, for the purposes of:

- Verification of the identity of the holder by means of directly available comparable features;
- Demonstration of the MRD by the document issuer, investigation in circumstances where a card holder is not present and quality control.
- Quality assurance during document production.

Key pairs and certificates are used as follows:

- A CVCA private key shall be used to sign UK and external DV certificates and may also be used to sign DV certificate requests submitted to provide to other authorised States' CVCAs (see section 3.3);
- A CVCA certificate shall be used to verify a "Public Key" request from a domestic or international DV;
- A DV private key shall be used to sign national IS certificates;
- A DV certificate shall be used to verify the signature of national of external IS certificates.

These certificates enable read access by Inspection Systems to fingerprint biometrics stored on the MRDs as indicated in the certificates, for the purposes set out in 1.4 above. To do that, it is necessary to have clear identification of which trusted certification path is to be used.

A 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 by the DV.

Relying parties of a trusted certification path are for:

DV	national CVCA certificate and authorised State CVCA certificate;
IS	national DV certificate, national CVCA certificate and authorised State CVCA certificate;
MRD	authorised State IS certificate, authorised State DV certificate and national CVCA certificate and possibly national link CVCA certificate and the corresponding CVCA certificate.

Note: **For Passports only** - national refers to the State who issues the CVCA, DV, IS and MRD. Authorised State refers to a State which is authorised to collect data from the MRD of a national citizen using a DV (and IS) signed by the national CVCA of the State who issues MRD to the citizen.

For BRPs: national refers to the State who issues the CVCA, DV, IS and BRPs. Authorised State refers to a State which is authorised to collect data from the BRPs of third country nationals using a DV (and IS) signed by the national CVCA of Member State issuing BRPs to the third country national

1.4 POLICY ADMINISTRATION

Identity Services
Identity and Data Integrity Directorate,
UK Border Agency
7th Floor
Lunar House
40 Wellesley Road,
Croydon CR9 2BY

1.5 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: Key words to describe requirements].

A "Member State" is a state participating in Regulation (EC) No 2252(2004) passports, Regulation (EC) 1030/2002 in its amended version Regulation (EC) No 380/2008 (BRP)

A "State" is any state whether it participates in Regulation (EC) No 2252(2004), Regulation (EC) No 1030/2002 in its amended version Regulation (EC) No 380/2008 or not.

"Domestic" means "of the same State".

"Foreign" means "of another State."

A "Valid Key" is 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.

"Agreement" is a Memorandum of Understanding between the UK and other States or between the Secretary of State for the Home Office and other UK government agencies; or a Legal Contract between the Home Office and commercial entities stating the specific details of certificate usage between the signatories.

"Participants" are bodies who are signatories to an Agreement, either directly or by their relationship to a signatory.

Further definitions and acronyms used in this policy are given in Section 10.1.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The Home Office is responsible for maintaining a list of contact details for all UK DVs and Inspection Systems.

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

The UK implementation of this CP will be as described in the Certificate Practice Statement

3.1 NAMING

As defined in TR-EAC A.4.1, the Certification Authority Reference is used to identify the 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:

- The ISO 3166-1 ALPHA-2 country code of the certificate holder's country;
- A mnemonic that represents the certificate holder, of 1 to 9 characters;
- A five character numeric or alphanumeric sequence number as specified in the Certificate Practice statement.

NOTE: It is not guaranteed that the Certificate Holder Reference is a unique identifier in general. States shall define identity as follows:

- CVCA certificate:
    - Certification Authority Reference: national CVCA identity;
    - Certificate Holder Reference: national CVCA identity;
- DV certificate:
    - Certification Authority Reference: national CVCA identity or other authorised States' 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.

For UK DVs, the Home Office will be responsible for defining the mnemonic that represents the certificate holder.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 National CVCA

Each State SHALL clearly identify who is responsible for the authentication and the definition of the CVCA identity.

For the UK responsibility for the authentication and definition of the CVCA identity rests with the Home Office.

3.2.2 CVCA to CVCA

The CVCA of each Member State SHALL publish a Certificate Policy compliant to [13][2] and may set up a Certification Practice Statement in accordance with the common Certificate Policy [13], in particular indicating the conditions under which a certificate for a (foreign) Document Verifier will be issued. Every Member State SHALL notify the adoption of the Certificate Policy to the Commission.

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

The UK will require other States' CVCAs to provide the following to the Home Office, in order to validate that CVCA: This shall be done by a mutually agreed trusted channel.

- The National Certificate Policy;
- The public part of the CVCAs Certificate Practice Statement, if it exists;
- 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 Home Office.

Prior to DVs submitting certificates requests the participating CVCAs SHALL enter into an Agreement stating the specific details of certificate usage between the signatories.

3.2.3 DV to CVCA

When a DV first submits registration information to the UK CVCA this SHALL be done by a mutually agreed trusted channel

The DV MUST include the following in the registration information:

- The public part of the DVs Certificate Practice Statement;
- The latest Certificate of Conformity with the National Certificate Policy for the DV;
- A list of the organisations using Inspection Systems subscribing to the DV;

A Foreign DV MUST also include the following in the Registration Information:

- 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.

[2] BIG, Common Certificate Policy for the Extended Access Control Infrastructure for Residence permits issued by EU Member States, version 1.0 - 2008

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.

Foreign DVs shall be identified under the Agreement between the UK and foreign CVCA.

Domestic DVs shall make an Agreement with the UK CVCA.

When a UK DV first submits registration information to a foreign CVCA, it SHALL be done by a mutually trusted channel. Information will be provided in accordance with the foreign CVCAs National Certificate Policy.

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. .

Where a UK Inspection System is not already covered by an agreement between the DV and the UK CVCA, an Agreement shall be made between the DV and Inspection System.

An Inspection System first submitting a Certificate Request to a UK DV shall provide the following:

- The Inspection Systems Certificate Practice Statement;
- A Certificate of Conformity with the National Certificate Policy and any additional requirements agreed between the DV and Inspection System, either as part of the DV Certificate of Conformity or as a separate certificate;

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:

- That the request is formatted in accordance with TR-EAC paragraph A.4.2
- That the CVCA for the DVs State continues to list the DV as valid;
- That the DVs Certificate of Conformity is valid;
- 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:

- That the Inspection System remains registered as operational;
- That the Inspection System is not listed as stolen/missing

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 CVCA

The Home Office is responsible for the authorisation of 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.

For UK Inspection Systems, the technical standards for the application SHALL be defined in Agreement between the CVCA and DV or DV and Inspection System.

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 authorised 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.v

For Passports the usage (governmental and non-governmental) of fingerprint biometrics in the MRD is in conformance with the Agreement under which the certificates are being issued.

For Biometric Residence Permits – In accordance with EC Regulation (EC) No 1030/2002 last amended by Regulation (EC) No 380/2008, certificates may be used to control access to fingerprint biometrics on Extended Access Control enabled Residence Permits for the purposes of identification.

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 72 hours.

If required by the Agreement, the CVCA SHALL issue a Certificate Thumbprint to the DV.

In the event that a Foreign CVCA system is non-operational for more than this time frame, it MUST inform all subscribing UK 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.

In event the UK CVCA system is non-operational for more than 72 hours it SHALL 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 with its domestic 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.

For UK Inspections Systems, notification periods for loss of service shall be defined in the Agreement between the DV and Inspection System.

If required by the Agreement, the DV SHALL issue a Certificate Thumbprint to the IS.

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 certificates 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

CVCA, DV and IS 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 and the Agreement between the participants
- 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 DVs Private Key has been compromised and certificates signed by these Private Keys SHOULD NOT be relied upon and Relying Parties 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

- The purpose as described in Section 1.3 '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:

- The DV or IS certificate is about to expire.
- A DV certificate is revoked;
- An IS key is compromised;
- 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:

- 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;
- 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.

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 for foreign DVs subscribing to the UK CVCA.

UK DVs shall notify all CVCAs to which they subscribe that they are intending to end their subscription.

UK Inspection Systems shall notify all DVs to which they subscribe that they are intending to end their subscription.

4.12 KEY ESCROW AND RECOVERY

MUST NOT be used.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

Within the UK the following documents will have the following protective markings, as defined in the Cabinet Office Security Policy Framework v1.0 December 2008.

CVCA Private Key:	SECRET
CVCA Public Key:	NOT PROTECTIVELY MARKED
DV Certificate:	CONFIDENTIAL
DV Certificate Request:	RESTRICTED
DVCA Private Key:	SECRET
DVCA Public Key:	NOT PROTECTIVELY MARKED
IS Certificate:	RESTRICTED
IS Certificate Request:	RESTRICTED
IS Private Key:	SECRET

5.1 PHYSICAL CONTROLS

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

- Site location and construction: The CVCA/DV are operated in a physically protected area.
- Physical access: Access to the CVCA/DV is controlled and audited. Only authorised persons have physical access to the CVCA/DV environment.
- 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).
- Waste disposal: Procedures for the disposal of waste are implemented in order to avoid unauthorised use, access, or disclosure of sensitive data.
- 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:

- Controls (e.g. firewalls) SHALL be implemented to protect the CV internal network domains from external network domains accessible by third parties.
- Sensitive data SHALL be protected against unauthorised access or modification.
- Sensitive data SHALL be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.
- Each CVCA, DV, and IS SHALL ensure effective administration of users' access to maintain system security, including user account management, auditing and timely modification or removal of access (this includes operators, administrators and any users given direct access to the system).
- 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. In particular, 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.
- CVCA, DV, and IS personnel SHALL be successfully identified and authenticated before using EAC-PKI applications related to certificate management or access to MRDs.
- CVCA, DV, and IS personnel SHALL be accountable for their activities, for example by retaining event logs as defined in Section 5.4.
- 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:

- 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;
- Personnel SHALL undergo domestic security screening appropriate to the role(s) they are carrying out;
- Appropriate disciplinary sanctions SHALL be applied to personnel violating CVCA, DV or IS policies or procedures;
- 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;
- All personnel (both temporary and permanent) SHALL have job descriptions defined from the view point of separation of duties and least privilege.
- Personnel SHALL exercise administrative and management procedures and processes that are in line with the Procedural Controls described in 5.2 above;
- 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;
- 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;
- 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:

- The confidentiality and integrity of current and archived records concerning certificates is maintained;
- Records concerning certificates are completely and confidentially archived;
- The precise time of significant environmental, key management and certificate management events is recorded
- All events relating to the life-cycle of keys are logged;
- All events relating to the life-cycle of certificates are logged;
- All events relating to registration are logged;
- All requests and reports relating to revocation, as well as the resulting actions, are logged;
- The specific events and data to be logged are documented;
- 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:

- 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.
- Protection against modification or deletion of logs.
- 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 authorised 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 MRDs. These biometrics SHALL be deleted immediately after finishing the comparison process between fingerprints acquired from of the bearer and fingerprints read from the MRD.

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 Procedural Controls and System Access Management.

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:

- Measures to minimise the impact of disruption to power services;
- Measures to minimise the impact of events such as flooding or fire;
- 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:

- Each CVCA, DV and IS SHALL define and maintain an EAC-PKI business continuity plan to enact in case of disaster (see also Section 5.7.4).
- 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 quickly resume operations in case of incident/disaster.
- Back up and restore functions SHALL be performed by the relevant trusted roles.
- 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 5.7.4).

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 5.7 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. The method of notification shall be defined by the Agreement between the participants.

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.

The process for notifying CVCAs of key compromise shall be detailed in the Agreement between the participants.

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 UK 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;
- destroy, or withdraw from use, its private keys;

Any replacement UK CVCA MUST continue to provide certificates for MRDs issued under the original CVCA.

In the event of a foreign CVCA registered with the UK terminating its operations it SHALL:

- Notify the UK CVCA of the termination
- Notify the UK CVCA of the CVCA, if any, which will be issuing certificates in its place;
- Notify all UK DVs which it supplies of the termination;
- Notify all UK DVs which it supplies with certificates, of the CVCA, if any, which will be issuing certificates in its place;
- Destroy , or withdraw from use, its private keys;

Any replacement CVCA MUST continue to provide certificates for MRDs issued under the original CVCA.

In the event of a foreign CVCA registered with the UK terminating its operations it SHALL:

- Notify the UK CVCA of the termination
- Notify the UK CVCA of the CVCA, if any, which will be issuing certificates in its place;
- Notify all UK DVs which it supplies of the termination;
- Notify all UK DVs which it supplies with certificates, of the CVCA, if any, which will be issuing certificates in its place;
- Destroy , or withdraw from use, its private keys;

Any replacement CVCA MUST continue to provide certificates for MRDs issued under the original CVCA.

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. Any replacement DV will then complete initial identity validation as in 3.2 Initial Identity Validation.

A UK DV MUST ensure that all subscribing ISs are notified that the Termination Notice Periods will be as defined in any Agreement between the DV and the IS.

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 A.

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 A.

CVCAs SHALL implement technical and procedural mechanisms that require the participation of multiple trusted individual authorisations 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 authorisations 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 authorised 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 and in accordance with appropriate protective markings for that key.

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 CVCA private key MUST be destroyed or put beyond use once it has been used to sign a link certificate.

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 for the CVCA and DV are as shown below. Inspection System Certificates for Inspection Systems carrying out verification of identity WILL have operational periods as shown below.[3]

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

In circumstances where an Inspection System is used for Quality Assurance during document production and the production environment is considered sufficiently secure, an Inspection System Certificate MAY be issued with a validity period of up to a maximum of three months.

Where an Inspection System is used by an Issuer for the purposes of demonstration, investigation or quality assurance, Inspection System Certificates WILL have operational periods as defined in point 5.5.1 of Commission Decision C(2006) 2909 of 28.06.2006.

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.

[3] Both as defined in point 5.5.1 of Commission Decision C(2006) 2909 of 28.6.2006

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 control 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 CERTIFICATE REVOCATION LIST (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 (ONLINE CERTIFICATE STATUS PROTOCOL)

Not applicable

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

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

The Auditing Body MUST be accredited for this purpose by its national accreditation body. For UK DVs this body will each time be specified through a specific call for tender. 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.

When a new Inspection System is added to the subscribers to a UK DV, it shall be audited to the same standard as the DV, prior to its inclusion in the next three yearly review.

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

In the event that an audit indicates that a DV, including subscribing Inspection Systems, 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, CVCAs 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 Registration Authority (RA) functionality in accordance to ISO/IEC 27001. The ISMS is based on an ISMS policy of which its scope is defined by this National Certificate Policy and the associated Certificate Practise Statement.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

There shall be no fees charged to other States for provision of certificates. Provision of certificates within the UK shall be subject to the Agreement between the CVCA and DVs and between DVs and Inspection Systems.

9.2 FINANCIAL RESPONSIBILITY

Foreign and domestic State bodies are not required to make any disclosures on their financial state or ability to meet liabilities arising from the EAC-PKI.
Where commercial parties are involved in the use of EAC-PKI, financial responsibilities will be defined in the Agreement between the participants.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Not applicable to relationships between States.
Where commercial parties are involved in the use of EAC-PKI, confidentiality of business information requirements will be defined in the Agreement between the participants.

9.4 PRIVACY OF PERSONAL INFORMATION

ISs are not permitted to log or transmit fingerprint biometrics obtained from MRDs. 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 MRD.

Logging or transmitting of fingerprint data obtained from the bearer by Inspection Systems at identification is permitted but data must be deleted as soon as practicable after facilitating the transaction.

9.5 INTELLECTUAL PROPERTY RIGHTS

Not applicable.

9.6 REPRESENTATIONS AND WARRANTIES

Where representations and warranties are required these will be stated in the Agreement between the participants.

9.7 DISCLAIMERS OF WARRANTIES

Where disclaimers of warranties are required these will be stated in the Agreement between the participants.

9.8 LIMITATIONS OF LIABILITY

Where limitations of liability are required these will be stated in the Agreement between the participants.

9.9 INDEMNITIES

Where indemnities are required these will be stated in the Agreement between the participants.

9.10 TERM AND TERMINATION

Not applicable.

9.11 INDIVIDUAL NOTICES AND COMMUNICATING WITH PARTICIPANTS

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

For communications between states all CVCAs and DVs MUST be able to carry out such communications using a Single Point of Contact (SPOC) as defined in ČSN 36 9791. Other additional online or offline communication channels MAY be mutually agreed especially to cover situation when a 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.

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

9.12 AMENDMENTS

States may revise their National CP. Additional reviews may be enacted at any time at the discretion of the 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 foreign States SHOULD inform the UK CVCA. Prior to approving any major security changes to their National CP, foreign States SHALL notify the UK CVCA.

Correction of spelling and typographical errors which do not change the meaning of this CP are allowed without prior notification. After the changes the UK CVCA SHALL inform all foreign CVCAs with subscribing DVs of the changes. Prior to approving any major security changes to this CP, the UK CVCA shall notify all foreign CVCAs with subscribing DVs.

Notification of a CVCAs intention to modify the CP SHALL be no less than 3 months before entering in a modification process on the CP and include the scope of modification.

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

9.13 DISPUTE RESOLUTION PROCEDURES

SHALL be defined in the Agreement between participants or in case of the BRP be referred to the European Commission.

9.14 GOVERNING LAW

This SHALL be defined in the Agreement between participants.

9.15 COMPLIANCE WITH APPLICABLE LAW

Not applicable.

9.16 MISCELLANEOUS PROVISIONS

Not applicable

9.17 OTHER PROVISIONS

Not applicable

10. GLOSSARY AND REFERENCES

10.1 GLOSSARY

Abbreviation / Term	Description / Definition
Certification Authority (CA)	An entity that issue certificates
Certificate Revocation List (CRL)	A list of revoked certificates
Certificate Policy (CP)	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;
Certificate Practice Statement (CPS)	A statement of the practise that a certification authority employs in issuing, managing, revoking and renewing or re-keying certificates;
Certificate Thumbnail	Hash Value of the Certificate Public Key;
CESG	CESG is the Information Assurance (IA) arm of GCHQ and we are based in Cheltenham, Gloucestershire, UK. We are the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help our customers achieve their business aims.
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.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.
Country Signing Certification Authority (CSCA)	The Certificate Authority responsible for issuing Country Signing Certificates. These are used to validate the Document Signing Certificate.
Extended Access Control Public Key Infrastructure (EAC-PKI)	The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control

Abbreviation / Term	Description / Definition
Document Signing Certificate	A digital certificate held on the chip, and also distributed by the Document Signer, used in Passive Authentication to validate the data held on the chip.
Document Signer	The entity signing the original document, in this case the organisation that issues the MRD
Document Verifier (DV)	An entity within the EAC-PKI that requests certificates from CVCAs and, on the basis of those certificates, issues certificates to Inspection Systems;
Evaluation Assurance Level	A numeric grade assigned to an IT system or product following the completion of a Common Criteria security evaluation
Extended Access Control (EAC)	A means of accessing and authenticating the chip and the data thereon, incorporating Basic Access Control (reads the chip), Chip Authentication (verifies the chip ensuring it has not been cloned), Passive Authentication (verifies the data is unchanged) and Terminal Authentication (verifying that the reader has the authority to read the chip)
Inspection System (IS)	The operational system that reads fingerprint biometrics from MRDs
International Civil Aviation Organisation (ICAO)	A UN organisation tasked with fostering the planning and development of international air transport. In this role it sets international standards for MRTDs
Key ceremony	A procedure whereby a key pair is generated using a cryptographic module and where the public key is certified.
Link Certificate	Link certificates ensure business continuity without exchanging a new trusted self-signed root CVCA certificate out-of-band.
Machine Readable Travel Document (MRTD)	An international travel document containing eye- and machine-readable data
MRD	Machine Readable Document. Used as not all documents issued under this policy will be travel documents although they will conform to the MRTD standards for EAC.

Abbreviation / Term	Description / Definition
Memorandum of Understanding (MoU)	A legal document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action and may not imply a legal commitment. In the case of this CP they will be used where a commercial contract would be inappropriate, for example between UK government departments or between the UK and other States.
National Certificate Policy	A Members State's Certificate Policy for management of the process of issuing and receiving certificates too and from other Member States
Public Part of the Certification Practice Statement	A subset of the provisions of a complete CPS that is made public by a CA
Registration Authority(RA)	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
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

10.2 REFERENCES

References

Reference	**Description / Title**	**Location**
TR-EAC	Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)', Version 1.1.1, TR-03110	Published by Bundesamt fur Sicherheit in der Informationstechnik
	Commission Decisions: Commission Decision C(2006) 2909 of 28 06 2006 and Commission Decision C(2009) 3770 final of 20/05/2009.	
	Qualified Certificate Policy (QCP) as defined in TS 101 456	
	Electronic Signature Directive (1999/93/EC)	

APPENDIX A SECURITY REQUIREMENTS

A1 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 [4]
- FIPS PUB 140-2 level 3 or higher [5]
- PP-SSCD [6,7,8]
- BSI Cryptographic Modules Security Level "Enhanced" [9]

These standards are approved by the EU Common Certificate Policy. If in the course of reaching a bilateral agreement with a non-EU State a further standard is proposed, the UK will assess that standard. If the standard meets the UK's requirements for trustworthy devices, it will be accepted as part of the bilateral agreement between the UK and the other State.

A2 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

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

APPENDIX B COMMUNICATIONS

B1 SINGLE POINT OF CONTACT

B1.1 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 for 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 for details)

B1.2 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 A1.

B1.3 SPOC CA REQUIREMENTS

B1.3.1 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. The SPOC CA policy MUST assure the OIDs identifying SPOC certificates are assigned only to certificates belonging to the SPOC.

B1.3.2 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 a maximum of 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 period of time.

B1.3.3 Technical and organisational 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".

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].
[EUCP] sec. 8.	DV not compliant	The DV [CHR] is no longer compliant to EU CP requirements.

B1.3.4 Validity periods

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

B1.4 Request received via 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 (in accordance with 3.3.1 b) of this document.

B1.5 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.

B1.6 Sending notifications

To send the notification SPOC SHALL be used. GeneralMessage as defined in ČSN 36 9791 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.