Home Office

THE UNITED KINGDOM'S
National Certificate Policy

for Extended Access Control for Biometric Residence Permits and variants issued and read within the UK

Date

OID: 1.2.826.0.1363

Public Document

DOCUMENT INFORMATION

DOCUMENT HISTORY

Document Reference No:	BRPEAC/NCP3
Version:	2.5
Date of Issue:	08/05/2015
Author:	Home Office
Approver:	Phillip Smith
Status:	Updated Policy supersedes all previous versions.

RELATED DOCUMENTS

Document Name	Issue Status	Owner
Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued By EU Member States. BSI TR-03139. Referred to as [TR-EAC].	Version 2.1	Published by the Bundesamt für Sicherheit in der Informationstechnik.
Technical Guideline 'Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)', Part 1 and Part 3, TR-03110. Referred to as [BSI-EAC]	Version 2.20	Published by the Bundesamt für Sicherheit in der Informationstechnik.
Country Verifying Certification Authority Key Management Protocol for SPOC. ČSN 36 9791. Referred to as [CSN-SPOC]	Version 1.0	Czech Office for Standards, Metrology and Testing
United Kingdom CVCA Certificate Practice Statement.	Version 2.5 08/05/15	Home Office
[Appendix C –SPOC Requirements] – Part of the UK Certificate Practice Statement.	As Above	Home Office
[Appendix D - Registration Form] – Part of the UK Certificate Practice Statement.	As Above	Home Office

1. Introduction

The United Kingdom (UK) Certificate Policy (CP) for Biometric Residence Permits sets out governance arrangements for how the United Kingdom will use digital certificates required to authenticate access to biometric data using Extended Access Control – Public Key Infrastructure (EAC-PKI).

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. The UK CP is owned and administered by the Home Office.

The UK CP is based on the European Common Certificate Policy (CCP)[1]. The UK will not require a Document Verifier (DV) in another Member State to adopt restrictions above those in the CCP as a pre-requisite of issuing a certificate to that DV. However, the UK assumes that all states operate their EAC-PKI in compliance with the general requirements of the CCP. The decision if a certificate is to be issued to any other state or organisation in respect of UK residence permits lies with the Home Office.

The term Machine Readable Document (MRD) is used throughout this CP. For the purposes of this document this refers to Biometric Residence Permits (BRPs) and Biometric Residence Cards (BRCs) and any other variants which may be developed in the future.

The UK implementation of this CP will be as described in the UK Certificate Practice Statement (CPS).

1.1. Overview

UK Visas & Immigration (UKVI) is the Home Office command with responsibility for UK Biometric Residence Permits (BRP) and any variants. The BRP is an EU immigration regulation compliant Residence Permit Document issued by the UK government to all non EU nationals granted permission to stay in the UK for more than 6 months.

BRPs were introduced by the Home Office in November 2008 to replace old style vignettes with a secure card. The UK opted into the European Regulations (EC) 1030/2002 and 380/2008 in relation to uniform format residence permits, and is therefore obliged to implement amendments to the BRP regulations.

BRCs were introduced by the Home Office in April 2015 to replace old style residence cards with a secure standalone card. This meets the provisions of the Immigration Act 2014 and the EEA Regulations.

Under amended EU Regulations the method of Document Verifier (DV) certificate exchange between EU Member States must utilise Single Point of Contact (SPOC) web services conforming to a mandated standard.

For the purposes of this certificate policy the UK Country Verification Certificate Authority (CVCA), DV and SPOC system combination is collectively referred to as the UK EAC-PKI Service.

Within the UK certificates are used for the following purposes:-

Biometric Residence Permits: - Certificates are used to control access to fingerprint biometrics on Residence Permits (as specified in the EU Regulation on Residence Permits) and will only be used for verifying the authenticity of the document and the identity of the holder by means of directly available comparable features.

Biometric Residence Cards:- Certificates are used to control access to fingerprint biometrics on Residence Cards (as specified in the EU Regulation on Residence Permits and in the provisions of the Immigration Act 2014) and will only be used for verifying the authenticity of the document and the identity of the holder by means of directly available comparable features.

1.2. Document Name and Identification

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

1.3. Definitions

A **Member State** is defined to be a state participating in Regulation (EC) No 2252(2004) and Regulation (EC) 1030/2002 in their versions as last amended and concerning this document also ….

- "Domestic" is defined to mean of the same Member State.
- "Foreign" is defined to mean of another Member State or associated country.

[1] Version 2.1, BSI TR-03139, published by the Bundesamt für Sicherheit in der Informationstechnik, referred to as TR-EAC

"Valid Key" is defined to be a key for which the current time is within the validity period of the corresponding Subscriber Certificate and this certificate itself is considered valid.

A **suspension** of a CVCA, DV or IS shall be defined as followed:

There are two registration status of a CVCA, DV or IS. Their default status is not suspended;

- the status of their registration is set by their own registration authority (for CVCA) or domestic/ foreign parental registration authority (for DV or IS) to suspended.
- certificates issued or certificate requests sent by a suspended CVCA, DV or IS SHALL NOT be trusted, processed or forwarded.[2]

This is done because suspension or revocation of certificates is not possible within the EAC-PKI due to technical reasons.

Further definitions and acronyms used in this policy are given in Appendix A Definitions and Acronyms.

1.4. EAC-PKI Participants

This section gives an overview of the UK PKI Co-ordinator, Certification Authorities, Registration Authorities, Subscribers, Relying Parties and technical Single Point of Contact (SPOC) of the Extended Access Control Public Key Infrastructure (EAC-PKI).

	Certification Authority	Registration Authority	Subscriber	Relying Party
National PKI Coordinator		X		
SPOC		X		X
Country Verifying Certification Authority (CVCA)	X	X		X
Document Verifier (DV)	X	X	X	X
Inspection System (IS)			X	X
Machine Readable Document (MRD)				X

Table 1: Overview of the PKI participants of the UK EAC-PKI

1.4.1. National PKI Co-ordinator

Each Member State has one named National PKI Co-ordinator[3], or group of individuals, who are responsible for interacting with Member States with respect to the exchange of Document Verifier (DV) certificates. That means the PKI Co-ordinator is the contact point for, and responsible for facilitating distribution of Residence Permit EAC-PKI certificates from requesting EU Member States.

The National PKI Co-ordinator ensures that information concerning incidents such as key compromise or misuse, and suspension of CVCA, DVs and IS are shared with Member States.

1.4.2. 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 domestic CVCA are contained in both self-signed CVCA certificates and CVCA link certificates. Both classes are called CVCA certificates. A domestic CVCA determines the access rights to sensitive data stored on domestic MRD chips for all DVs (i.e. domestic DVs as well as foreign Member State's DVs) by issuing DV certificates entitling access control attributes.

A domestic CVCA issues certificates to its Certificate Holders (Subscribers). In this document, a subscriber of a CVCA is called a Document Verifier (DV). A DV is an organisational unit that manages Inspection Systems belonging together.

For the purposes of the remainder of this document the Registration Authority (RA) will be assumed to be part of the CVCA and only the term CVCA will be used.

Within the UK there is one domestic CVCA for the issuance of certificates for the support of the verification of UK Residence Permits: Issuing CVCA Root Certificates to the Biometric Residence Permit (BRP) Signing Service every 3 years to ensure the continued issuance of BRPs.

[2] Except for audit reasons
[3] which should usually be a defined group of persons as a subsection of a governmental office for substitution purposes

Document Verifier Certification Authority

The UK has one DV for the UK CVCA which is

- allowed to sign the DV's certificate requests to foreign CVCAs and
- is stated as "the domestic CVCA" of this DV concerning every rule of this document containing duties for CVCAs and/or DVs

The UK DV operates a CA to issue certificates for UK inspection systems. The inspection system certificates issued by the DV inherit both the access rights and the validity period from the underlying DV certificate. The UK Document Verifier may restrict the validity period of the IS certificates[4] for subscribers to the UK EAC-PKI Service and where apprpriate may choose to further restrict the access rights.

1.4.3. Registration Authorities

Country Verifying Registration Authority

There is one UK CVCA and one Registration Authority (RA), the corresponding UK CVRA. The UK CVRA is operated by the same authority as the CVCA it serves.

The domestic RA is responsible for:-

- the registration of domestic DVs and of foreign Member States CVCAs which shall be authorised to read sensitive data from domestic MRDs;
- provide and change if needed the suspension status of registered DVs and CVCAs
- the listing of foreign DVs including their suspension[5] status;
- performing identification and authentication of certificate requests of Document Verifiers;
- suspension of domestic DVs if they are not longer allowed to request certificates especially from foreign Member States;
- the suspension of the registration of foreign Member States in case of security incidents;
- giving information to all foreign Member States if a domestic DV is not longer allowed to request certificates from those Member States and thus is suspended;
- initiating the issuance of certificates to Document Verifiers;

Document Verifier Registration Authority

The UK has one Registration Authority for each Document Verifier.

DV RAs are responsible for:-

- registration of domestic Inspection Systems;
- performing identification and authentication of certification requests of Inspection Systems;
- suspension of domestic Inspection Systems if they are not longer allowed to request certificates;
- forwarding information about security incidents of the DV itself or its maintained Inspection Systems immediately to the domestic CVCA;
- initiating the issuance of certificates to Inspection Systems;

For the purposes of the remainder of this document the DV RA will be assumed to be part of the DV and only the term DV will be used.

1.4.4. Subscribers

Subscribers under this policy are Document Verifiers (DV) and Inspection Systems (IS). A DV is defined in section 1.4.2 Certification Authorities.

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

---

[4] refer to chapter 4.7 Certificate Validity Periods
[5] refer to chapter 1.1 Definitions for the definition of suspension

1.4.5. Relying Parties

Relying Parties within an EAC-PKI are CVCAs, Document Verifiers, Inspection Systems, SPOC and MRDs. A relying party is an entity who verifies the signature of a certificate or a certificate request using a trusted certification path (see section 4.6 Certificate Usage).

1.4.6. SPOC – Communication between participants

Within the UK a system called SPOC (Single Point of Contact) acts as an interface for communication between Member States. It allows efficient on-line communication to carry out regular key management related tasks.

Technical details of SPOC are defined in ČSN 36 9791, version 1.0, further referred to as [CSN-SPOC].

The UK only operates one SPOC which complies with the additional requirements specified in [Appendix C] of the UK Certificate Practice Statement (UK CPS) and the requirements of [CSN-SPOC].

For communication between Member States the UK CVCA carries out all communication via the UK SPOC except in circumstances where the UK SPOC is unavailable, in which case e-mail will be used.

1.5. Policy Administration

The business owner of the UK EAC-PKI is responsible for the administration of this UK Certificate Policy together with the UK EAC-PKI service supplier.

Any questions regarding this Certificate Policy may be sent to the following e-mail address:

UKPKICoordinator@homeoffice.gsi.gov.uk

2. Publication and Repository Responsibilities

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

The European Commission is responsible for maintaining a list of contact details for National PKI Co-ordinators at the European level; which is distributed and updated regularly at Article 6 Committee forum.

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-HOME) of the European Commission.

2.1. Repositories

The UK CVCA operates a repository containing the certificates and requests signed by this CVCA (CVCA certificates, CVCA link certificates, DV certificates and DV requests) as well as registration data of domestic DVs and foreign Member States and suspension status lists of foreign DVs. The certificates in this repository SHALL be stored for at least the corresponding certificate validity time plus the validity of the MRTDs the certificate may be used by plus six months.

The UK DV operates a repository containing the certificates and requests signed by this DV (DV certificates, DV requests and IS certificates) as well as registration data of the maintained Inspection Systems. The certificates in the DV repositories SHALL be stored for at least corresponding certificate validity time plus one year.

3. Identification and Registration

3.1. Naming

As defined in [BSI-EAC] the Certification Authority Reference (CAR) is used to identify the public key to be used to verify the signature of the certification authority (CVCA or DV).

The CAR is equal to the Certificate Holder Reference (CHR) in the corresponding certificate of the certification authority.

The CHR identifies a public key of the certificate holder. It is a unique identifier relative to the issuing certification authority. It consists of the following concatenated elements:

1. The ISO 3166-1 ALPHA-2 country code of the certificate holder's country;
2. An ISO/IEC 8859-1 mnemonic that represents the certificate holder with a length up to 9 characters;
3. An ISO/IEC 8859-1 numeric or alphanumeric sequence number consisting of five characters. The sequence number may be reset if all available sequence numbers are exhausted.

The sequence number starts with the ISO 3166-1 ALPHA-2 country code of the certifying certification authority. If this recommendation is followed, the remaining three characters are assigned as alpha-numeric Sequence Number.

NOTE: It is not guaranteed that the CHR is a unique identifier in general.

The identity of Certificate Authorities and Certificate Holders (Subscribers) is defined as follows:

- CVCA certificate:
  - Certification Authority Reference (CAR): domestic CVCA identity;
  - Certificate Holder Reference (CHR): domestic CVCA identity;
  - The UK CVCA Naming convention is contained in the UK Certificate Practice Statement
- DV certificate:
  - Certification Authority Reference (CAR): domestic CVCA identity or foreign authorised Member State CVCA (see section 3.3) identity;
  - Certificate Holder Reference (CHR): domestic DV identity;
  - The UK DV Naming convention is contained in the UK Certificate Practice Statement
- IS certificate:
  - Certification Authority Reference (CAR): domestic DV identity;
  - Certificate Holder Reference (CHR): domestic IS identity.
  - The UK IS Naming convention is contained in the UK Certificate Practice Statement

3.1.1. UK Naming Convention

- The Country Code for the United Kingdom (UK) is 'GB'.
- For UK DVs, the Home Office will be responsible for defining the mnemonic that represents the Certificate Holders.
- The UK Certificate Practice Statement contains the full Naming Convention for the UK.

3.2. Registration

3.2.1. Domestic CVCA Initial Identity Validation

For the UK responsibility for the authentication and definition of the CVCA identity rests with the Home Office. The Home Office will identify the UK PKI Co-ordinator.

3.2.2. Registration of a foreign Member State

Member State registration is carried out under the supervision of the European Commission. The registration of a Member State's CVCA consists of two steps:

Step 1 – Submitting registration via European Commission

A Member State's National PKI Co-ordinator submits the completed Registration Form [Appendix D Registration form] (part of the Certificate Practice Statement) to the European Commission for distribution to other participating Member States by diplomatic means securing the authenticity and integrity of the information. This part of registration can also be done bilaterally between Member States, but the European Commission should be informed about the registration.

Step 2 – Implementing registration information at domestic CVCA

The registration information is distributed to the Member State's National PKI Co-ordinator and further to its CVCAs and SPOC in a way securing the authenticity and integrity of the data.

When receiving the registration data a Member State's National PKI Co-ordinator and further to its CVCAs and SPOC verifies if the integrity of the information has not been hurt. The digital certificate data of the Member State's CVCA certificate and the SPOC root certificate are checked against the cryptographic fingerprints listed on the registration form.

Only if these checks lead to a positive result the registration data is implemented at the CVCA and hence the registration is completed by requesting all newer CVCA Certificates from the registered Member State via SPOC communication ("GetCACertificates" according to CSN-SPOC).

In event of a change to any of the registration information above, the National PKI Co-ordinator submits the updated version to the European Commission for distribution to other participating Member States. Before performing an update of a registration the Registration Authority verifies if the integrity of the information has not been compromised.

The National PKI Co-ordinator of the Member State having applied for being registered is informed if the registration has been accepted or rejected (including the reason) with in 4 weeks by each Member State having received that application. This message is sent by National PKI Co-ordinators of these Member States.

3.2.3. Registration of a DV

The initial registration of a DV to a CVCA Registration Authority is done by the RA of the domestic CVCA of the DV. This registration process contains an appropriate check of the identity of the DV, authenticity of registration data (including initial certificate request), audit certification, the DV's certificate policy (based on this Certificate Policy) and if applicable the public part of certificate practice statement and the permissions the DV has for applying for certificates.

Only if all these data are correct, the domestic CVCA registers the DV and signs initial DV requests to foreign Member State's CVCAs.

The registration of a DV to a foreign Member State's CVCA is done based on the known CHR of the DV and is finished by accepting the initial request of the DV signed by a known valid CVCA Certificate of its domestic CVCA.

Thereafter the Member State's CVCA lists the DV as valid and not suspended until a notification of an incident concerning the fulfilment of security requirements according to this CP or the termination of the DV is known.

3.2.4. Registration of an IS

DVs have a proper mechanism in place to identify an authenticated Inspection System. The key generation of an Inspection System is processed under consideration of sections 4.4.3, 5 and 6. The initial request of an IS is transmitted to the DV in a secure way. The DV checks if the integrity and authenticity of the request data is uncompromised.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Profile

UK CVCA certificates, UK CVCA link certificates, UK DV certificates and UK IS certificates are produced according to the certificate profile specified in [BSI-EAC "CV Certificates"].

4.2. Initial Certificates and Requests

An initial certificate of a UK DV or UK IS is defined as

- being the first certificate of the same Certificate Holder or
- being the first certificate after a suspension has been cancelled or
- being a new certificate after the previous certificate has been expired before a new request or link certificate could be generated.

An initial certificate of a UK DV or UK IS SHALL be issued based on an initial request of that DV or IS according to [BSI-EAC].

Certificates are not issued without generating a new key pair for the corresponding certificate.

4.3. Successive Certificates and Requests (Re-key)

A successive certificate is every certificate of the same Certificate Holder (Subscriber) except an initial one (see above).

A successive certificate SHALL only be issued conform to the following rules:

a) A new key pair is generated by the Certificate Holder;

b) The certificate contains a different (successive) sequence number in the CHR than the previous certificate(s) of the Certificate Holder;

c) The certificate is issued in accordance with 4.4 Certificate Application and Issuing.

d) In case of a security incident as private key compromise the cause for the incident is detected and the corresponding security problem solved before the issuance of a new **initial** certificate can be performed (see chapter 4.2 Initial Certificates and Requests).

A successive certificate for a DV or IS are only be issued conform to the following rules:

a) The DV or IS certificate is about to expire, in this case BSI-EAC chapter "Certificate Requests" is followed.

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

Certificates cannot be issued without generating a new key pair for the corresponding certificate.

4.4. Certificate Application and Issuing

Certificate Authorities (CVCA and DV) take measures against the forgery of certificates and ensure that the procedure of issuing the certificate is securely linked to the associated registration.

4.4.1. Certificates issued by CVCA to CVCA

The Home Office will define which entity is responsible to authorise the CVCA creation.

A CVCA SHALL only issue a self signed CVCA certificate or a CVCA link certificate to a former CVCA certificate of the same CVCA[6]. This is done during a key ceremony which fulfils at least the security requirements in chapters 5 and 6 of this Certificate Policy. CVCAs check that a certificate request is authorised and valid.

---

[6] *or a new CVCA being the replacement for a terminated CVCA according to chapter 5.4.*

When the validity of a CVCA certificate is going to end the CVCA SHALL generate a new key pair and issue a self-signed CVCA certificate and a CVCA link certificate[7].

The CVCA link certificate SHALL contain

- the public key of the new key pair,
- a signature generated with the private key of the previous CVCA certificate ,
- the same validity period as the new CVCA certificate holding the same public key

according to [BSI-EAC]. The CVCA certificate and the CVCA link certificate SHALL be distributed to all foreign Member States registered at the CVCA via “SendCertificates” message according to CSN-SPOC.

The CVCAs / SPOCs receiving a new CVCA certificate and a corresponding CVCA link certificate SHALL check the validity and authenticity of the certificate:

- if the certificate is correct according to syntax, authenticity and validity the receiving CVCA SHALL update its registration information on the issuing CVCA with CVCA certificate and CVCA link certificate as new trusted CVCA certificate;

- if the certificate is not correct the receiving Member State SHALL inform the issuing CVCA of the CVCA (link) certificate. This MAY be done by response on “SendCertificate” message according to CSN-SPOC automatically.

4.4.2. Certificates issued by CVCA to DV

Following successful registration as per 3.2.3 above, DV Certificate Application SHALL be carried out in accordance with BSI-EAC (chapters “Certificate Requests” and BSI-EAC “Document Verifiers”).

The DV certificate request SHALL always contain the inner CAR (this is in BSI-EAC only recommended) in order to distinguish between the different CVCAs if there are more than one CVCA in the Member State receiving the certificate request.

4.4.2.1. Certificate application

The following steps are processed if a certificate is to be issued by a foreign Member State's CVCA to a domestic DV:

<table>
<tr><th>Step no.</th><th>Indication</th><th>Initial Request</th><th>Successive Request[8]</th><th>Party involved</th></tr>
<tr><td>1</td><td>Generate key pair</td><td colspan="2">the DV generates a key pair according to BSI-EAC and in consideration of the security requirements of chapters 5 and 6 of this document;</td><td>DV</td></tr>
<tr><td>2</td><td>Generate certificate request</td><td colspan="2">the DV generates a certificate request out of the new generated public key considering the naming scheme of chapter 3.1 and BSI-EAC and generates the inner signature (see BSI-EAC) with the corresponding private key;</td><td>DV</td></tr>
<tr><td>3</td><td>Generate outer signature (successive request)</td><td>N/A</td><td>The request MUST be signed with the private key corresponding to a still valid DV certificate which has been issued by the same Member State the request shall be sent to [9]</td><td>DV</td></tr>
</table>

[7] The CVCA link-certificate will be used as part of the trusted path for the MRTDs to be read and to proof the authenticity of the new CVCA certificate and the self-signed CVCA certificate is used to proof the possession and operational reliability of the corresponding private key.
[8] Initial / Successive Request concerning the Member State's CVCA which shall sign the DV certificate.
[9] If a private CVCA, DV or IS key is unusable for non-critical reasons, as a delayed successive request, a new initial request SHALL be produced (see also chapter 5.3.3).

4	**Send Request to CVCA/ SPOC**	The request MUST be submitted to the corresponding domestic [10] CVCA of the DV in a secure way.	The signed request MUST be submitted to the domestic CVCA/SPOC.	DV
5	**Check suspension status (domestic)**	The domestic CVCA/SPOC MUST check if the DV is still allowed to request certificates from foreign Member States i.e. it is not suspended before processing the Request. A request of a suspended DV MUST be refused.		Domestic CVCA/ SPOC
6	**Check integrity**	The CVCA MUST check if the authenticity and integrity of the DV request is correct, otherwise the request MUST be refused.	It is RECOMMENDED to check the authenticity and integrity of the request within the CVCA/SPOC by automatic means.	Domestic CVCA/ SPOC
7	**Generate outer signature (initial request)**	An outer signature has to be added to the request by the corresponding domestic CVCA. Then forward the request to the domestic SPOC.	N/A	Domestic CVCA
8	**Submit request to foreign SPOC**	The request SHALL be submitted to the foreign SPOC following the requirements of CSN-SPOC.		Domestic SPOC
9	**Check outer signature**	The foreign SPOC/CVCA MUST check if the outer signature of the request is created with a key which is valid with respect to:		Foreign CVCA/ SPOC
		A still valid certificate of that DV, issued by the foreign Member State's CVCA itself.	A still valid certificate of that DV, issued by the foreign Member State's CVCA itself.	
10	**Check suspension status (foreign)**	The foreign Member State's CVCA MUST check if the DV is still allowed to apply for certificates concerning the information provided by the DV's domestic CVCA or if the foreign Member State has suspended the DV itself, i.e. checking registration status of the DV.		Foreign CVCA/ SPOC
11	**Issue certificate?**	If both checks of the two previous steps lead to a positive result the foreign CVCA MUST generate a certificate corresponding to the received request. Otherwise the request MUST be rejected.		Foreign CVCA
12	**Send response**	The foreign Member State's SPOC sends a response message to the DV's domestic SPOC, containing either the DV certificate or the refusal of the certificate application.		Foreign SPOC
13	**Check certificate**	The domestic SPOC checks the syntax of the certificate by automatic means and sends the result of this check as response to the foreign SPOC (see CSN-SPOC)		Domestic SPOC
14	**Forward response**	The domestic SPOC of the DV forwards the response of the Member State's CVCA to the DV		Domestic SPOC
15	**Implement certificate**	DV implements the certificate		DV

[10] Domestic/foreign means in the context of this table same/other Member State than the DV

Table 2: Generating and processing a DV Request

4.4.2.2. Application period and response time

The CVCA MUST process the certificate request within a timeframe of 7 days.

In the event that a CVCA system is non-operational for more than this time frame, it MUST inform all subscribing domestic DVs and foreign Member State CVCAs 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.

For getting a new DV certificate at least 11 days SHOULD be scheduled, if there is need for a fall back to communication via email 3 additional days SHOULD be considered.

This time frame has been calculated as follows:

- the key ceremony and internal quality assurance(1/2 day)
- generating the corresponding certificate request (1/2 day)
- submitting the request to signing authority via domestic SPOC (1 day)
- response time of signing authority (7 days)
- getting the certificate via domestic SPOC (1 day)
- import of the certificate (1 day)

If the kind of installation of a DV's infrastructure requires a greater amount of time for one of the steps above, the DV SHOULD increase the time frame for generating a new DV Certificate Request accordingly.

4.4.3. Certificates issued by DV to IS

Inspection Systems MAY submit certificate requests upon completion of successful registration as per 3.2.4 above.

A DV SHALL only issue a certificate to an IS that is complying with this Certificate Policy and that is using the certificates in accordance with part 4.6 of this document.

Step no.	Indication	Initial Request	Successive Request[11]	Party involved
1	**Generate key pair**	The IS generates a key pair according to BSI-EAC and in consideration of the security requirements of chapters 5 and 6 of this document.		Inspection System
2	**Generate certificate request**	The IS generates a certificate request out of the new generated public key considering the naming scheme of chapter 3.1 and BSI-EAC and generates the inner signature (see BSI-EAC) with the corresponding private key;		Inspection System
3	**Generate outer signature**	N/A	The request SHOULD contain an outer signature generated with the private key corresponding to a still valid IS certificate. If this mechanism is not used, then another mechanism of equivalent security MUST be used.	Inspection System
4	**Submit request**	The request MUST be submitted to the corresponding DV in a way ensuring any compromise of the authenticity or integrity of the request can	The request MUST be submitted to the DV.	Inspection System

11 Initial / Successive Request concerning the Member State's CVCA which shall sign the DV certificate.

		be detected. E.g. by submitting a cryptographic fingerprint of the request via a different channel.		
5	**Check request**	The DV MUST check if the authenticity and integrity of the IS request is not compromised and if the request is conformant to BSI-EAC and chapter 3.1 of this CP;	The DV MUST check if the outer signature is correct and generated with the private key corresponding to a still valid IS certificate and if the request is conformant to BSI-EAC and chapter 3.1 of this CP;	DV
6	**Check registration status**	The DV MUST check if the IS is still allowed to request certificates i.e. the registration of the IS is not suspended.		DV
7	**Issue certificate?**	The DV MAY issue a certificate corresponding to the request if the checks of the previous two steps lead to a positive result otherwise the IS request MUST be refused;		DV
8	**Send response**	The DV SHALL send a response message to the IS containing either the IS certificate or the refusal of the certificate application.		DV
9	**Implement certificate**	The IS implements the certificate.		IS

Table 3: Generating and processing an IS Request

4.5. Certificate Acceptance

A UK CVCA self signed certificate is accepted by the entity responsible for the CVCA after its creation at the end of the key ceremony.

A UK DV or IS is deemed to have accepted a certificate upon its receipt.

4.6. Certificate Usage

UK Inspection System Certificates are used to enable read access to fingerprint biometrics stored on UK issued MRDs including Biometric Residence Permits (BRPs) and Biometric Residence Cards (BRCs).

The UK CVCA, keys pairs and certificates are used for the following purpose:

- CVCA private key SHALL be used to sign CVCA certificates, CVCA link certificates and UK and foreign DV certificates and DV certificate requests to be provided to foreign authorised Member State's CVCAs;
- CVCA certificate SHALL be used to verify signatures of UK or foreign Member State DV certificates and CVCA link certificates issued by this CVCA and DV requests signed by this CVCA;
- DV private keys SHALL be used to sign UK IS certificates and successive DV requests;
- DV certificates SHALL be used to verify signatures of IS certificates issued by this DV.

Note: Every DV and IS holds several key pairs (and certificates) in use at the same time as needing one key pair for each Member State (including own domestic one) issuing MRDs. A CVCA holds only one key pair in use at the same time excluding the short interval needed for signing the CVCA link certificate.

The trusted certification path for a domestic MRD being read by an IS of an authorised foreign Member State:

- authorised foreign Member State IS certificate,
- corresponding authorised foreign Member State DV certificate signed by the domestic CVCA certificate corresponding to the MRD and
- consists of zero or more domestic CVCA link certificates completing a certificate chain up to the domestic CVCA public key stored on the MRTD.

Certificates and paths of certificates SHALL be validated and interpreted by relying parties according to ISO 7816-4 and BSI-EAC.

4.7. Certificate Validity Periods

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
CVCA certificate	6 months	3 years
Document Verifier certificate	2 weeks	3 months
Inspection System certificate	1 day	1 month*

*There may be exceptionally circumstances where the validly of IS Certificates is extended where exceptions have been authorised.

5. Security Requirements

5.1. Physical Controls

The UK CVCA and DV operate its services in a secure environment. This SHALL include:

- **Site location and construction:** The UK CVCA/DV is operated in a physically protected area.
- **Physical access:** Access to the UK CVCA/DV is controlled and audited. Only authorised persons have physical access to the UK 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

The UK CVCA and DV SHALL implement security measures in order to protect the authenticity, integrity and confidentiality of their data and the accurate functionality of their IT systems. A **Security Concept** SHALL be written for each CVCA and DV which:

- lists any IT systems being part of the Certificate Authority, Registration Authority or SPOC, being directly connected to one of these or handles data for the registration or certification process;
- describes any process being part of the tasks of CVCA, DV or SPOC;
- describes the roles needed (see below);
- describes security measures and incident handling.

The following items SHALL be concerned:

- **Protection of the IT system:** IT security mechanisms (e.g. firewalls) have been implemented to protect the internal network domains from external network domains accessible by third parties. Each interface of the used IT systems has been considered for implementing appropriate security measures;
- **Trusted roles:** Within the UK Processes of SPOC, DV and IS tasks are attached to trusted roles. At least the following roles are available: system administrator, auditor, PKI Coordinator, SPOC operator, DV Operator, IS operator. This is realised by organisational measures as well as IT controls and includes user account management, auditing and timely modification or removal of access.
- **Separation of trusted roles:** the IT systems provide sufficient computer security controls for the separation of trusted roles. Distinct trusted roles are not adopted by the same person.
- **Access Control:** authentication of roles is enforced by the IT system for system access. Access to data or functionalities is only granted to trusted roles allocated to the corresponding task.
- **Two person principle:** Separation of duties has been implemented for critical tasks by a two person principle.
- **Substitution concept:** for the case of inactivity of personnel covering trusted roles the substitution is planned. Also in case of substitution a person cannot have the possibility to cover separated roles.
- **Separated systems:** communication between separated IT systems has been secured against manipulation and access of third parties. IT systems are separated according to their need of availability, internet communication (e.g. SPOC) and confidentiality, integrity of data (e.g. CA).
- **Sensitive data:** Sensitive data is protected against unauthorised access or modification. Sensitive data is protected (e.g. using encryption and an authenticity/integrity protecting mechanism) when exchanged over networks which are not secure.
- **Suspension of subscribers:** each CVCA and DV provides adequate mechanisms for suspension of registered subscribers (foreign CVCAs, DVs resp. IS). These mechanisms prevent the issuing of certificates or signing of certificate requests of suspended subscribers.

- **Logging:** each modification of sensitive data is logged which includes private key operations as well as registration information and status. Subchapter 5.2.1 defines the details on the logging requirement.
- **Archival:** archived records are held for a period of time as appropriate for providing necessary legal evidence in accordance with the applicable legislation of the Member State.
- **Personnel:** IT systems are operated by qualified and experienced staff. Subchapter 5.2.2 defines the details on the personnel requirement.
- **Life-Cycle of security measures:** security measures are reviewed and updated regularly during the life-cycle of the PKI. Subchapter 5.2.3 defines the details on the life-cycle requirement.
- **Testing system:** a testing system (pre-production) has been constructed to replicate the real (Live) SPOC, registration and certification systems in order to test new security measures, software updates and interoperability with IT systems of foreign Member States;

For each IS a **Security Concept** SHALL be written which describes

- the type and structure of the IS,
- describes every IT system being part or hosting parts of the IS,
- the security measures and incident handling.

The following items SHALL be concerned for the **Security Concept** of an IS:

- **Protection of the IS:** IT security mechanisms (e.g. firewalls, Anti-Virus Software) SHALL be implemented on each IT system being part or hosting parts of the IS[12]. Each interface of the used IT systems SHALL be considered for implementing appropriate security measures.
- **Access Control:** authentication of roles SHALL be enforced by the IT system for system access. Access to data or functionalities SHALL only be granted to trusted roles allocated to the corresponding task.
- **Separated systems:** If applicable the communication between separated IT systems MUST be secured against manipulation and access of third parties. IT systems SHOULD be separated according to their need of availability, internet communication and confidentiality, integrity of data.
- **Sensitive data:** Sensitive data SHALL be protected against unauthorised access or modification. Sensitive data SHALL be protected (e.g. using encryption and an authenticity/integrity protecting mechanism) when exchanged over networks which are not secure.
- **Logging:** Subchapter 5.2.1 defines the details on the logging requirement for IS.
- **Archival:** 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.
- **Personnel:** Inspection Systems SHALL be operated and administrated by qualified and experienced staff. Subchapter 5.2.2 defines the details on the personnel requirement.
- **Life-Cycle of security measures:** security measures SHALL be updated regularly during the life-cycle of the IS. Subchapter 5.2.3 defines the details on the life-cycle requirement.

5.2.1. Logging

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

UK SPOC, CVCA and DVs SHALL ensure that:

- **Events to be logged:** the following events are logged:
    - creation, use and destruction of **keys and certificates,**
    - creation and modification of **registration entries**;

[12] The security mechanisms depend on type and structure of the IS.

- all requests and reports relating to **incident notification and suspension** of registrations, as well as the resulting actions;

- **Logging mode:** the precise time of the concerning event and if applicable the trusted role having triggered or executed the event is recorded;
- **Integrity and confidentiality:** the confidentiality and integrity of current and archived records is maintained. 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;
- **Archival:** The logs SHALL be archived at least until the next full audit according to chapter 7 “Compliance Audit and Other Assessment“ has been completed. 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. Access to archives SHALL be restricted to authorised operators only.
- **Documentation:** The specific events and data to be logged are documented;

UK ISs SHALL fulfil the following requirements for logging; except those used for document production where this is part of the service provision:

Key management: an IS SHALL log each key management event as generating and deleting private keys;

- **Certificate Management:** an IS SHALL log the issuing of certificate requests and if corresponding certificates are received;
- **Access control:** an IS SHALL log each attempt of getting access to the IS functionalities;
- **Protection:** The log is protected against modification or deletion;
- **Audit trail:** Records SHALL be kept to enable the auditor to confirm that misuse can be detected;
- **Prohibited logging:** Inspection Systems SHALL NOT log or transmit fingerprints obtained from MRTDs. Any traces of these biometrics SHALL be explicitly deleted immediately after finishing the comparison process between fingerprints acquired from the bearer and fingerprints read from the MRD.

5.2.2. Personnel

The following requirements SHALL be maintained concerning personnel of the UK EAC-PKI Service:

- **Knowledge**: Personnel SHALL possess of the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;
- **Reliability:** Personnel SHALL undergo domestic security screening appropriate to the role(s) they are carrying out.
- **Conflicts of interest:** Personnel SHALL be free from conflicts of interest;
- **Completing checks:** Personnel SHALL NOT have access to the trusted functions until any necessary checks are completed;
- **Clear instructions:** Personnel SHALL be clearly instructed on their duties and tasks;
- **Accountability:** Personnel SHALL be accountable for their activities.

5.2.3. Life-Cycle of security measures

Security of the UK SPOC, CVCA, DV and IS SHALL be sustained by fulfilling the following requirements:

- **Searching for security news:** Administrators SHALL search for news on security risks, attacks and countermeasures concerning the used hardware, software, algorithms and protocols at least once per month;
- **Up-to-date security:** New security patches for software, algorithms or protocols SHOULD be promptly implemented after being tested appropriately;

- **Closing gaps:** Security measures SHALL be updated immediately if a security gap is known;
- **Change control:** change control procedures MUST be part of the Security Concept, and be documented, and used for releases, modifications and emergency software fixes for any operational software of CVCAs, DVs and ISs.
- **Security training:** Personnel SHALL be trained on new security risks and countermeasures at least once every six months;
- **Retraining on duties:** Personnel SHALL be retrained on duties and tasks at least once per year;
- **Review Security Concept:** The Security Concept SHALL be reviewed and updated and be compared with its realisation at least once per year;

5.3. Incident Handling

5.3.1. Subscriber Suspension

The UK CVCA, DV or IS SHALL be suspended in case of

- any incidents as key compromise or other security vulnerabilities
- being no longer conformant to this National Certificate Policy and the EU Common Certificate Policy

The UK DV or IS SHALL be also suspended if it is no longer allowed to apply for certificates of foreign Member States.

The suspension MUST be processed by all SPOCs, CVCAs and DVs having registered the suspended CVCA, DV or IS.

5.3.2. Compromise and Disaster Recovery

The UK CVCA 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;

5.3.3. Incident and Compromise Handling Procedures

The UK CVCA, DV and ISs 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:

- The UK CVCA SHALL define and maintain a continuity plan to enact in case of disaster.
- UK CVCA systems data necessary to resume CVCA operations SHALL be backed up and stored in safe places suitable to allow the UK CVCA to timely go back to operations in case of incidents/disasters.
- Back up and restore functions SHALL be performed by the relevant trusted roles.
- The UK 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 5.3.4).

If a private UK CVCA, DV or IS key is unusable for non-critical reasons, as a delayed successive request, a new initial request SHALL be produced as described in chapter 4.2 Initial Certificates and Requests.

If a private UK CVCA, DV or IS key is unusable for critical reasons as e.g. key compromise the security problem having caused the compromise MUST be solved first, before a new initial request SHALL be produced as described in chapter 4.2 Initial Certificates and Requests.

5.3.4. Entity Private Key Compromise Procedures

A Document Verifier SHALL immediately inform its National PKI Co-ordinator which informs all foreign Member State's National PKI Co-ordinators that have issued certificates for this DV about private key compromise or misuse. Domestic and foreign CVCAs SHALL immediately suspend that DV.

Following suspension of a CVCA or DV by its domestic CVCA the use of a private key is immediately and permanently discontinued.

If an Inspection System is lost, stolen or its private key is compromised or control over the private key has been lost, the responsible Document Verifier SHALL be informed. The DV SHALL immediately suspend the IS in order to prevent the issuance of new certificates for this IS. In case of key compromise which includes the possibility of unauthorised private key use on lost or stolen Inspection Systems the Member States involved MUST be informed.

Following suspension of an IS the use of a private key is immediately and permanently discontinued.

The incident information to foreign Member States SHALL be distributed via SPOC and via the National PKI Co-ordinator using the wording of section C.4 Sending notifications.

The incident report and the solution of the security problem having caused the incident SHOULD be shared with all Member States.

5.4. CVCA or DV Termination

In the event of a CVCA terminating its operations the following requirements SHALL be fulfilled:

- **Notification of foreign National PKI-Coordinators:** the terminating CVCA SHALL notify each registered foreign National PKI Co-ordinator, and those being registered at, of the termination and, if any, which CVCA will take over its tasks;
- **Notification of European Commission:** the European Commission SHALL be notified by the belonging Member State's National PKI Co-ordinator about the termination of the CVCA;
- **Continuity of certificate path:** Any replacement of a CVCA MUST continue to provide certificates for MRTDs issued under the original CVCA. For this reason a link certificate MUST be issued which contains the first public key of the new CVCA and is signed by a valid private key of the replaced CVCA;
- **Destruction of keys:** The CVCA SHALL destroy, or withdraw from use, its private keys;

In the event of a DV terminating its operations

- **Notify domestic CVCA:** The DV SHALL notify its domestic CVCA
- **Notify foreign CVCAs:** The domestic CVCA/SPOC of the DV notify all foreign National PKI Co-ordinators the CVCA is registered at13.
- **Suspend DV's registration:** All notified CVCAs SHALL suspend the DV's registration for the further issuance of certificates.
- **Destruction of keys:** The DV SHALL destroy, or withdraw from use, its private keys.

6. Key Pair Security

6.1. Key Pair Generation

The UK CVCA and DVs SHALL ensure that their keys are generated

- in controlled circumstances according to Section 5.2 “Procedural Controls and System Access Management” of this document;
- within a cryptographic module which is compliant with Appendix B;
- and distributed in accordance with BSI-EAC and this policy;
- CVCAs and DVs SHALL ensure that the integrity and authenticity of their public keys and any associated parameters are maintained during distribution to DVs and IS.
- Within the UK all CVCA Keys and their respective Key Encryption Keys (KEKs) originate from the UK Key Production Authority (UK KPA) shall be handled only by personnel holding the status of UK KPA Approved Crypto Custodian.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Private keys of the UK CVCA, DVs and IS SHALL be held and used adhering the following rules:

- **Trustworthy device:** Private keys SHALL be held and used within a cryptographic module which is compliant with Appendix B Hardware Requirements and SHALL only leave the cryptographic module for back-up purposes according to 6.3 Key Backup and Recovery.
- **Lifecycle of trustworthy device:** The security of trustworthy devices MUST be ensured throughout their lifecycle including ensuring that the cryptographic module is not tampered with during shipment or storage, functions correctly when in operation and any private keys stored on the equipment is destroyed upon module retirement.
- **Access control of trustworthy device:** Where keys are stored in a cryptographic module, access controls SHALL be in place to ensure keys are not accessible outside the cryptographic module. Measures SHALL be in place to prevent unauthorised use of private keys.
- **Key destruction:** 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.

6.3. Key Backup and Recovery

If key back-up for CVCA or DV private keys is done this MUST be executed according to the processes described in chapter 6.2 Private Key Protection and Cryptographic Module Engineering Controls in this Certificate Policy and the following rules:

- Backup copies of the private key 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 keys SHALL be protected in a way that ensures the same or greater level of protection as provided by the cryptographic module.
- Backup copies of the private keys of the domestic CVCA MUST NOT be used anywhere except for restoration of the service of the domestic cryptographic module.

Private keys of IS SHALL not be backed up. Private keys of DV SHOULD NOT be backed up and/or recovered. As shown in the following table:

	CVCA	**DV**	**IS**
Back-up	SHOULD	SHOULD NOT	SHALL NOT

If a private key of a DV or IS is unusable for non-critical reasons, the DV or IS SHOULD generate a new key pair and request for a new certificate at its signing authority (see chapter 5.3.3).

A CVCA private key SHOULD be backed up in order to secure the certificate chain needed to get read access to the MRDs.

7. Compliance Audit and Other Assessment

Each CVCA and DV SHALL be audited according to the following requirements:

- **Auditor qualification (only DV):** DVs MUST select an independently acting and accredited company/organisation ("Auditing Body") or certified auditors to audit the DV according to this Certificate Policy. The Auditing Body MUST either be accredited for this purpose by its national accreditation body or authorised by a responsible government office.
- **Control by authority (CVCA and DV):** the Security Concept, its realisation and the conformity to this CP of CVCAs and DVs SHALL be (additionally) controlled by a domestic authority.
- **Audit basis:** The Audit SHALL be based on ISO/IEC 27001 and 27002.
- **Checking requirement realisation:** The audit and control MUST not only check that procedural security controls are specified but also that they are adhered to in practice. This also includes the registration process, the receipt of the initial certificate request and the suspension procedure for Inspection Systems subscribing to the DV.
- **Iteration of audits and controls:** Audits and controls MUST be performed at least every three years. The Auditing Body and the controlling authority SHALL carry out a review at least once a year by a team of one or more auditors to ensure on going compliance with this CP.
- **Being not conformant:** In the event that an audit indicates that a DV does not comply with this CP, or its certificate becomes invalid or expires, the DV MUST notify its domestic National PKI Co-ordinator who SHALL notify all foreign Member State's National PKI Co-ordinators [13] to suspend the DV for requesting certificates. The Member States MUST NOT issue any further DV certificates to this DV.
- **Availability of audit results:** The certificate of conformity MUST be made available to other Member States and the Commission.
- **Reuse of audit results:** The conformity of the DV to its national Certificate Policy and its Certificate Practice Statement if applicable MAY also be proven by this audit, for this those documents have to be considered additionally.

The operational environment supporting the UK EAC-PKI is ISO 27001 accredited and tScheme compliant.

The UK EAC-PKI, comprising the CV, DV and SPOC is subject to annual reaccreditation activity, regarding Information Assurance risks. Further detail can be found in the Certification Practice Statement.

[13] This means all foreign Member States the DV's Member State is registered at.

Appendix A Definitions and Acronyms

A.1 Definitions

1. *Certification Authority (CA)* – An entity that issues certificates

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

3. *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;

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

5. *Common Certificate Policy (CCP)* – 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 (CC)* - 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 (EAC-PKI)* – The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control.

8. *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;

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

10. *Inspection System (IS)* – the operational system that reads fingerprint biometrics from MRTDs.

11. *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 MRTD’s

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

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

14. *Machine Readable Travel Document (MRTD)* – An international travel document containing eye- and machine-readable data;

15. *National Certificate Policy* – a Members States Certificate Policy for management of the process of issuing and receiving certificates to domestic DVs;

16. *National PKI Co-ordinator* – Person or group of persons which is fully responsible for interacting with foreign Member States with respect to exchange of DV certificates and this Certificate Policy

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 (RA)* – An entity that establishes enrolment procedures for certificate applicants, performs identification and authentication of certificate applicants, initiate or pass along incident and suspend information of Subscribers, and approve applications for re-keying certificates on behalf of a CA

20. *Security Concept* – A Security Concept is a documentation of all tasks, duties, involved personnel and IT-Systems, and the interfaces of IT-Systems of a CA/RA. Further a Security Concept describes in detail the countermeasures against threats and (organisational and technical) security measures to be realised.

21. Single Point of Contact (SPOC) – Technical communication interface according to CSN SPOC.

22. 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.

A.2 Acronyms

BRC	Biometric Residence Card
BRP	Biometric Residence Permit
CA	Certification Authority
CC	Common Criteria
CDP	Certificate Revocation List Distribution Point
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
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
MRD	Machine-Readable Document
MRTD	Machine-Readable Travel Document
OID	Object Identifier
RA	Registration Authority
SPOC	Single Point of Contact
UK	United Kingdom

Appendix B Hardware Requirements

The cryptographic modules used by Certificate Authorities or Inspection Systems SHALL be evaluated and certified in accordance with one of the following standards:

- FIPS PUB 140-2 level 3 or higher 15
- PP-SSCD 16
- BSI Cryptographic Modules Security Level “Enhanced”17