Home Office

THE UNITED KINGDOM'S CVCA CERTIFICATE PRACTICE STATEMENT

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/CPS
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
The United Kingdom's National Certificate Policy for Extended Access Control for Biometric Residence Permits and variants issued and read within the UK.	Version 2.5 08/05/2015	Home Office
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

1. Introduction

The United Kingdom's (UK) Certificate Practice Statement (CPS) translates certificate policies from the UK's National Certificate Policy (CP) into operational procedures for the UK's Certification Authority (CA) regarding the principles to be followed when issuing certificates.

The UK CPS is owned and administered by the Home Office. This document is the public part of the CVCA's Certificate Practice Statement.

1.1. Background

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. In accordance with EU Regulation BRPs and their variants utilise smartcards containing a contactless chip holding digitally signed data.

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.

This Certificate Practice Statement (CPS) only concerns the use of certificates to control access to fingerprint biometrics on Extended Access Control (EAC) documents for the purposes of identification of the holder. For the purposes of this CPS, the term Machine Readable Document (MRD) is used throughout. This refers to Biometric Residence Permits (BRPs) and variants such as Biometric Residence Cards (BRC) any other variants which may be developed in the future.

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

The UK National Certificate Policy states the purposes for which certificates are used:-

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.

Under EU Regulation the method of Document Verifier (DV) certificate exchange between countries must utilise Single Point of Contact (SPOC) web services conforming to a mandated standard. In the UK the Country Verification Certificate Authority (CVCA), DV and SPOC system has the following functions:-

- The UK Country Verification Certificate Authority (CVCA) digitally signs the BRP Card on behalf of an issuing country (EU Member State) to enable a card reader to gain access to the fingerprint images on a document chip.
- The UK Document Verifier (DV) makes the request for this authority on behalf of a reading country, and when it is received, distributes that authority securely as a verification certificate, to card readers. The minimum infrastructure required to enable access to fingerprints on BRP cards.
- The UK DV is responsible for issuance of certificates to Inspection Systems (IS) which manage certificates on behalf of Extended Access Control (EAC) document reader devices.
- The UK Single Point of Contact (SPOC) component exchanges verification certificates with other EU Member States.

1.2. Document Name and Identification

This UK Certificate Practice Statement 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.

"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 are 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 are NOT be trusted, processed or forwarded.[1]

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. UK 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
UK PKI Coordinator		X		
UK SPOC		X		X
UK Country Verifying Certification Authority (CVCA)	X	X		X
UK Document Verifier (DV)	X	X	X	X
UK Inspection System (IS)			X	X
UK Machine Readable Document (MRD)				X

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

1.4.1. UK PKI Co-ordinator

Within the UK there is one named UK PKI Co-ordinator, or group of individuals, who are responsible for interacting with Member States with respect to the exchange of UK Document Verifier (DV) certificates. That means the UK PKI Co-ordinator is the contact point for, and responsible for facilitating distribution of UK Residence Permit certificates from requesting EU Member States.

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

1.4.2. Certification Authorities

Country Verifying Certification Authority

The UK has a single Country Verifying Certification Authority (CVCA). The CVCA acts as a root of trust for MRDs issued within the UK. The CVCA authorises domestic and foreign Document Verifiers (DVs) to access the biometrics stored in MRDs.

The CVCA issues the following types of certificates:

- **CVCA Root certificates**

[1] Except for audit reasons

When initialising the CVCA or updating the CVCA keys, the CVCA creates a self-signed CVCA certificate, called a root certificate. The initial root CVCA certificate and all link CVCA certificates are sent to each authorised DV.

• CVCA Link certificates

When updating the CVCA keys, the CVCA creates link CVCA certificates. These certificates provide a trust link between the old and new CVCA keys. The initial self-signed CVCA certificate and all link CVCA certificates are sent to each authorised DV.

• Document Verifier certificates

The CVCA creates Document Verifier certificates in response to certificate requests from domestic or foreign DVs. These certificates allow the DVs to access the biometrics stored in UK issued MRDs.

The main functions of the CVCA are:

- Changing to a new root key pair and issuing a new self signed certificate containing the new root public key at least every 3 years.
- Issuing link certificates
- Managing the root private key for DV certificate signing
- Issuing and renewing DV certificates to national and foreign DVs
- Setting the validity period of national and foreign DV certificates
- Authenticating initial certificate requests of national DVs to foreign CVCAs

The CVCA issues certificates to its Certificate Holders (Subscribers – See 1.4.4).

Document Verifier Certification Authority

The UK currently has one Document Verifier for the issuance of certificates for the support of the verification of UK Residence Permits and UK Residence Cards; Issuing DV & IS certificates for BRP & BRC card production service to support quality assurance of the cards.

The UK DV issues Inspection System certificates in response to certificate requests from UK Inspection Systems. These certificates authenticate the Inspection System to MRD chips, and also specify which biometrics the Inspection System can access.

Document Verifier (DV)

The UK Document Verifier

- Imports CVCA certificates from each country CVCA it will submit requests to.
- Creates and manages a key pair for each country it will submit requests to.
- Submits the public key generated for a given country as a signed certificate request to that country's CVCA
- Receives a signed DV Certificate from each country's CVCA it submits a request to.
- Authorises UK Inspection Systems (IS)
- Receives from Inspection Systems their public key as a signed certificate request.
- Creates and distributes back to the submitting IS the IS Certificate
- Communicates with the UK SPOC for foreign DV certificate requests.
- Communicates with the UK CVCA for domestic DV certificate requests,

1.4.3. Registration Authorities

As defined in the UK National Certificate Policy.

1.4.4. Subscribers

The current subscribers to the UK EAC-PKI Service include DVLA, the current BRP Card Producer, and Home Office business assurance areas for quality checking and testing of BRPs and accessing the fingerprints on BRPs for identity verification purposes.

1.4.5. Relying Parties

Relying Parties within the UK EAC-PKI are the UK CVCA, Document Verifiers, Inspection Systems, SPOC and UK issued 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 requirements specified in Appendix C SPOC Requirements and the requirements of [CSN-SPOC]. The UK CVCA uses SPOC to carry out key management tasks and to communicate with foreign Member States. The UK SPOC facilitates access to the fingerprints on Member State issued biometric documents, through the secure exchange of digital certificates.

The UK's EAC-PKI system is capable of registering other SPOCs, receiving, collating and relaying Document Verifying (DV) certificate requests from registered SPOCs for the UK Country Verifying Certification Authority (CVCA). It is also able to relay requests to and receive responses via foreign SPOCs for foreign CVCAs on behalf of UK DVs.

1.5. Policy Administration

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

Any questions regarding this Certificate Practice Statement 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 UK Certification Authority publishes the Certificate Practice Statement, which is a public document. Given its public status detailed description of Information Security is beyond the scope of this document.

2.1. Repositories

As defined in the UK National Certificate Policy.

3. Identification and Registration

3.1. Naming - Holder and authority references

CVCA certificates, the Certificate Holder Reference (CHR) identifies the public key of the CVCA certificate holder, and the Certification Authority Reference (CAR) identifies the public key of the issuing CVCA certificate. If the holder and authority reference match, the CVCA certificate is a root certificate. Otherwise it is a link certificate.

Document Verifier certificates, the Certificate Holder Reference (CHR) identifies the public key of the Document Verifier certificate holder, and the Certification Authority Reference (CAR) identifies the public key of the issuing CVCA certificate.

Inspection System certificates, the Certificate Holder Reference (CHR) identifies the public key of the Inspection System certificate holder, and the Certification Authority Reference (CAR) identifies the public key of the issuing Document Verifier certificate.

3.1.1 Naming Convention

The Home Office has defined the mnemonic that represents the Certificate Holder, as below.

UK devices are named according to a sixteen character, three part naming convention as follows:

a) Country Code - 2 alphanumeric (AN) characters

b) Holder Mnemonic - up to 9 alphanumeric (AN) characters

c) Sequence number - up to 5 numeric digits

1. For the **UK CVCA** the following naming convention will be used:

Mnemonic

Character	Item	Value	Description
1 - 2	Country Code	'GB'	ISO 3166 standard
3 - 6	Authority ID	'cvca'	Lowercase fixed value
7 - 11	Sequence Number	00001 - 99999	Up to 5 numeric digits.

2. For the **UK DVCA** the following naming convention will be used:

Mnemonic

Character	Item	Value	Description
1 – 2	Country Code	'GB'	ISO 3166 standard
3 – 6	Authority ID	'dvca'	Lowercase fixed
7 – 8	Optional DV Type	AA	Two alpha characters to denote type of DV, e.g.: ET – EEA Travel, EN – Non-EEA Travel, DG – Domestic Government DC – Domestic Commercial Values and mapping table to be defined and agreed
9 – 11	Optional DV Ref	1 - 999	Up to 3 alphanumeric characters to further define DV Type Values to be agreed but initially expected to be set to "1"
12 – 16	Sequence Number	00001 - 99999	Up to 5 numeric digits.

3. For **UK Inspection Systems** the following naming convention is expected to be used:

Mnemonic

Character	Item	Value	Description
1 – 2	Country Code	'GB'	ISO 3166 standard
3	IS Type	A	Single character defining type of Inspection System, e.g.: 'I' – Concentrator (standard IS) 'F' – Fixed 'J' – Juxtaposed 'M' - Mobile Others to be defined and agreed
4 – 7	Client and Location	AAAA	Four alpha characters to denote client and location, e.g.: 'EBT5' to represent "E-borders, Terminal 5" Values and mapping table to be defined and agreed
8 – 11	Number Range	9999	4 alphanumeric chars to further define IS Type, e.g. '1000' range to denote Inward travel '5000' range to denote Outward travel Values to be defined and agreed
12 – 16	Sequence Number	99999	Numeric range with leading zeros – will be set to 1 initially, i.e. '00001'

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.

3.2.2. Registration of a foreign Member State

As defined in the UK National Certificate Policy.

3.2.3. Registration of a DV

The UK currently has one Document Verifier registered to the UK CVCA. The Home Office is responsible for ensuring the integrity, authenticity and permissions of the UK DV and ensuring any new or replacement DVs fully meet the security requirements of the UK Certificate Policy and the Common Certificate Policy.

The UK DV's Certificate Holder Reference (CHR) identifies the public key of the UK Document Verifier certificate in accordance with the naming convention at 3.1 above.

3.2.4. Registration of an IS

The UK DV deals with requests to add a new Inspection System, or to re-register an existing one for example should the IS Certificate expire requiring an IS reader to need re-registration. All such requests require approval from the Home Office before subscribers can submit their IS Certificate requests.

In accordance with the UK Certificate Policy, the initial request of a new or re-registered IS is transmitted to the UK DV in a secure way. The DV checks the integrity and authenticity of the IS Request using 'out of band' verification.

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 are 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 is only issued when conforming 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 the case of a security incident, such as private key compromise, the cause for the incident is detected and the corresponding security problem resolved before issuance of a new **initial** certificate is performed (see chapter 4.2 Initial Certificates and Requests).

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

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

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

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

4.4. Certificate Application and Issuing

Certificate Application Processing

The following is a high-level overview of the process steps involved in establishing trust between the CVCA and the DV. In the operational environment, international certificates and certificate requests are sent via SPOC (see Appendix C) and reach the CVCA via the Air gap Proxy and Request Processor. Domestic certificates and certificate requests are currently transferred by a manual process.

At the CVCA

1. The CVCA operator logs into the CVCA and adds the DV holder identity. The CVCA now recognises the DV. If the first two characters (the country code) of the DV holder identity are the same as those of the CVCA, the DV is recognised as domestic; otherwise, the DV is foreign.

2. The CVCA operator exports the CVCA certificate, either by sending email notification to the DV with the CVCA certificate attached, or by saving it and sending it to the DV by other means.

At the Document Verifier

3. The DV operator logs into the DV and adds the CVCA holder identity. The DV now recognises the CVCA.
4. The DV operator imports the CVCA certificate into the DV.
5. The DV operator generates and exports a certificate request, and then sends it to the CVCA operator.

At the CVCA

6. The CVCA operator accepts the certificate request and imports it.
7. The CVCA processes the certificate request and generates a certificate for the DV.
8. The CVCA operator exports the DV certificate and sends it to the DV operator.

At the Document Verifier

9. The DV operator imports the certificate.

4.4.1. Certificates issued by CVCA to CVCA

The UK CVCA issues a self-signed CVCA certificate and corresponding link certificate approximately every 3 years. It is timed to ensure a new certificate is created prior to the end of the 3 year validity period of the current certificate.

CVCA Rollover

The UK CVCA root key will expires every 3 years and was last renewed June 2014. The Home Office will ensure that the CVCA key rollover works properly so that EAC MRDs will read correctly even when the MRD contains an old CVCA certificate and the IS holds certificates signed by the new CVCA root keys.

The Home Office will prove end-to-end that systems and cards will handle rollover of country verification root key (including use of link certificates for chips encountering chains signed by the new key when they contain an earlier CVCA certificate); and then introduce the key change.

The transitional arrangements and completion of testing will be done before bringing the new CVCA/DV keys into live operation. This will involve the Home Office and its delivery partners and will include production of a test batch of new cards.

CVCA New Root and Link Certificate

When moved or “rolled” to new keys the CVCA produces both a new root and link CVCA certificate. The new Root certificate will be supplied to the personalisation system for new cards and to newly subscribing foreign DVs. The link CVCA link certificate is provided to IS systems and subscribing DVs alongside the new Root certificate. It is used to provide a chain of trust between the old and new CVCA certificates. This allows DV, IS and subsequently MRD chips containing old CVCA certificates to trust the new CVCA Root. When this is done by an MRD chip updates the CVCA certificate public key it holds internally to the latest version after which point the link certificate is no longer required to EAC read that particular document chip.

4.4.2. Certificates issued by CVCA to DV

The UK CVCA only issues a certificate to an authorised DV; processing a certificate request as follows:-

- UK CVCA processes DV Certificate Requests from foreign Member States within 7 days.
- UK CVCA processes domestic DV Certificate Requests within 2 working days.

In event the UK CVCA system is non-operational for more than 72 hours it will inform all subscribing DVs and foreign Member States 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 domestic DV Certificate, UK subscribers must submit their Certificate Requests 15 working days before the certificate expiry date.

For UK DVs that submit requests, the UK CVCA ensures the validity of the certificate request by confirming that the:

- DV is registered with the CVCA
- CVCA recognises the DV Holder Identity including domestic country code of GB
- The DV certificate request is valid with an authentic signature from that DV. If this is an initial request where no previous DV cert has been issued this authentication is manual rather than a digital signature check.

The CV also ensures new DV certificates are issued in accordance with the biometric access rights and validity period configured for that DV.

For Foreign DVs that submit requests via a foreign SPOC, the UK CVCA ensures the validity of the certificate request by confirming that the:

- Initial request is countersigned by the Foreign CVCA for which the foreign CV certificate is provided to the UK CVCA by a CVCA operator as part of the foreign DV registration process.
- CVCA recognises the Foreign CVCA Holder Identity
- CVCA recognises the Foreign DV Holder Identity
- The DV certificate request is valid with an authentic signature from that DV. If this is an initial request where no previous DV cert has been issued this authentication is manual rather than a digital signature check.

The CV also ensures new DV certificates are issued in accordance with the biometric access rights and validity period configured for that DV.

4.4.2.1. Certificate application

As defined in the UK National Certificate Policy for requests from foreign Member States CVCAs.

4.4.2.2. Application period and response time

As defined in the UK National Certificate Policy for requests from foreign Member States CVCAs.

4.4.3. Certificates issued by DV to IS

A UK DV will only issue a certificate to an IS that is complying with the UK Certificate Policy and UK Certificate Practice Statement. The UK DV automatically checks that a certificate request is valid prior to issuing a certificate. The UK DV processes IS Certificate Requests within 2 working days.

For getting a new IS Certificate, UK subscribers must submit their IS Certificate Requests 15 working days before the certificate expiry date.

A UK DV only issues a certificate to a UK Inspection System once it has confirmed that the:

- IS Holder Identity is registered
- IS is currently operational
- Administrator manually approves the initial request or, for subsequent requests, the request can be authenticated as signed by the IS concerned using its previous key. To do this the DV uses the public key held in the previous IS certificate.

The DV also ensures new IS certificates are issued in accordance with the biometric access rights and validity period configured for that IS or that IS grouping.

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 are 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 are 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 are used to sign UK IS certificates and successive DV requests;
- DV certificates are 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.

4.7. UK Certificate Validity Periods

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	3 months*

*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 their services in a secure environment.

All physical security controls for the UK's EAC-PKI system comply with the physical security requirements of UK Standards. These measures include vetting of operational personnel with access to the operational environment, physical access control of the operational environment and physical handling/storage of key material in line with HMG Information Assurance Standards (IAS4).

5.1.1. CVCA Keys

CVCA key material is generated and supplied by the UK Key Production Authority (UK KPA). The private key is only ever utilised for signing inside an approved Hardware Security Module (HSM) device.

Technical configurations and procedural rules protect the key material from exposure by unauthorised activities.

5.1.2. DV Keys

HSM devices, separate to that used to protect the CVCA are used to protect the DV related key material during storage. The HSM capabilities used include the ability to securely generate new keys and sign certificates.

Technical configurations and procedural rules protect the key material from exposure by unauthorised activities.

5.2. Procedural Controls and System Access Management

Procedural controls are implemented, including the use of a two-person principle for critical tasks. Each UK CVCA, DV, and IS ensure that system access to any UK EAC-PKI device is limited to individuals who are properly authorised. The CVCA, DV, and IS ensure access to information and application system functions are restricted to staff with valid access credentials.

The UK CVCA and DV employ security measures in order to protect the authenticity, integrity and confidentiality of their data and the accurate functionality of their IT systems. Within the UK the Security Concept is in the form of a Security Case which has been written covering the SPOC, CVCA and DV components of the UK EAC-PKI Service and which is fully complied with by the UK's EAC-PKI Service Providers.

5.2.1. Logging

Each CVCA and DV within the UK EAC-PKI service will retain an audit log which can be used to audit for improper usage of the system. Firewall alerting and alerts from an inspection gateway monitoring all traffic to the UK SPOC are in use to inform system administrators of network activity that may be of concern to the UK SPOC.

Due to device limitations IS systems run more limited audit logging functionality. However, physical and logical access to IS systems is restricted to authorised users.

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

Backups are stored both locally and remotely. Where backups are removed from site, transportation mechanisms are appropriately secure – using the two-person-rule. Backups are stored both on site and off site (for disaster recovery purposes).

Backups are stored in fireproof safes and kept for a period of time that ensures the effort required to recover from a data loss will not jeopardise the agreed 72 hour outage as described in section 4.4.2.

5.2.2. Personnel

All of the UK's EAC-PKI systems (CVCA, DV and IS systems) are operated by suitably qualified and trained staff. All staff working with the UK EAC-PKI systems will be security cleared to SC level as a minimum.

5.2.3. Life-Cycle of security measures

As defined in the UK Certificate Policy.

5.3. Incident Handling

5.3.1. Subscriber Suspension

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

- any incidents such as key compromise or other security vulnerabilities
- being no longer conformant to this Certificate Practice Statement and the UK Certificate Policy

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

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

5.3.2. Compromise and Disaster Recovery

The UK EAC-PKI Service takes reasonable measures to ensure that service continuity is maintained through the use of disaster recovery infrastructure that can be brought on-line within a period of time in compliance with the acceptable outage period described in section 4.4.2 above. Regular backups of CVCA, DVCA and SPOC are taken and a process to restore them in case of failure has been proven.

Should the main operational site become unusable, a capability exists to bring a reserve CVCA and DVCA into operation from offsite backups. This is designed to ensure continued capability to read UK documents on a small scale and meet EU obligations for renewal of foreign DV certificate requests. Foreign states will have to be notified to send certificate requests to the UK EAC- PKI Service by email until a new UK SPOC can be established.

5.3.3. Incident and Compromise Handling Procedures

The UK CVCA, DV and ISs will ensure that in the event of a disaster, including key compromise, that operations are restored as soon as possible. In particular, the following:

- The UK CVCA has defined and will maintain a continuity/disaster recovery plan to enact in case of disaster/serious outage.
- UK CVCA systems data necessary to resume CVCA operations will be backed up and stored in safe places suitable to allow the UK CVCA to timely return to operations in case of incidents/disasters.
- Back up and restore functions will be performed by the relevant trusted roles.
- The UK EAC-PKI continuity/disaster recovery plan will address the compromise or suspected compromise of a private key as a disaster and the planned processes will 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 are 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 is resolved first, before a new initial request can be produced as described in chapter 4.2 Initial Certificates and Requests.

5.3.4. Entity Private Key Compromise Procedures

Where the UK Document Verifier (the UK currently has one DV) private key has been compromised or misused, the UK PKI Coordinator is informed immediately. The UK PKI coordinator will inform all foreign Member States National PKI Coordinators who have issued certificates to the UK DV.

The UK CVCA and foreign CVCAs take immediate action to suspend that UK DV. This should be done within 24 hours of being notified and where this is not possible due to a weekend or public holiday it must be done within 72 hours.

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

If a UK Inspection System is lost, stolen or its private key is compromised or control over the private key has been lost, the UK Document Verifier must be informed. The UK DV will take immediate action to suspend the IS in order to prevent the issuance of new certificates for this IS. This should be done within 24 hours of being notified and where this is not possible due to a weekend or public holiday it must be done within 72 hours.

In case of key compromise which includes the possibility of unauthorised private key use on lost or stolen Inspection Systems the foreign Member States involved are informed by the UK PKI Coordinator.

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

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

The UK PKI Coordinator will ensure that the UK EAC-PKI Supplier provides the incident report (and explanation of the solution to the security problem that caused the incident) and that this is shared with all subscribing foreign Member States.

5.4. CVCA or DV Termination

In the event of a UK CVCA terminating its operations the administrators of any dependent DVs (foreign or domestic) must be notified. The CVCA will close down and be unable to sign any further DV certificate requests. The ability to continue issuing updated certificates for EAC reads of MRDs issued under that CVCA will then cease.

In the event of a UK DV terminating its operations the UK CVCA administrators should be notified so its entry can be removed from the UK CVCA. The administration authorities for any foreign state CVCAs that the DV holds certificates for must also be notified. The DV will then cease to request certificate renewals. This will mean that once the last DV certificate issued to that DV expires it is no longer live. Any ISs that this DV was responsible for must be migrated to an alternative Domestic DV if they are to continue live operation.

6. Key Pair Security

6.1. Key Pair Generation

The UK ensures that CA keys, including those for CVCA and DVCA, are generated in controlled circumstances according to Section 5.2 Procedural Controls and System Access Management

Before expiration of a UK CVCA or DV certificate, the UK CVCA or DV moves to a new pair and generates or acquires a new certificate. This is done in a timely manner to avoid disruption to the operations of the UK CVCA, DV or ISs which may rely on that key. The new key material is generated, utilised and protected in accordance with this CPS (see 5.1.1, 5.1.2 and 5.1.3). Public keys are distributed in signed certificate requests and card verifiable CVCA Root, CVCA Link, DVCA and IS certificates; or in the case of SPOC signed x509 certificates.

UK CVCAs and DVs make use of Hardware Security Modules to protect all private keys. The integrity and authenticity of all certificate requests and certificates they receive is also verified. In the case of initial certificate requests this will involve an out of band operator process but for subsequent exchanges it will be via automated cryptographic check.

Within the UK all CVCA Keys and their respective Key Encryption Keys (KEKs) originate from the UK Key Production Authority (UK KPA) are handled only by personnel holding the status of UK KPA Approved Crypto Custodian.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

CVCA, DVCA and Root SPOC Private Keys are held and used within dedicated trusted Hardware Security Modules (HSMs). These HSMs are connected in a manner to assure that only the connected CA has access to the functionality of the HSM involving its private key.

The UK EAC-PKI Service obeys a two-person rule for all sensitive CVCA and DVCA key operations e.g. request processing, backup, restore and destruction.

The UK EAC-PKI IS key operations such as certificate request generation and key use are restricted to authorised personnel appointed to this role. IS private keys are protected in a HSM or cryptographic smartcard device.

Where required, we will install/introduce Key Material from the original media (securely held away from the UK EAC-PKI systems and supplier).

Private keys are not used beyond the validity period assigned to their corresponding certificates. Once their certificate has expired private keys are destroyed or put into a non usable state.

The UK EAC-PKI Service ensures that HSMs are not tampered with during their active life and that in the case of retirement all private key data is wiped from the HSM. In the case of an HSM failure that results in an inability to delete private keys the HSM will be securely destroyed by an HMG approved destruction mechanism.

6.3. Backup and Recovery

As defined in the UK Certificate Policy.

7. Compliance Audit and Other Assessment

The UK EAC-PKI system will be subject to security review activity, conducted on a quarterly basis. Further, in line with UK government practice, the UK EAC-PKI system will be subject to a process of reaccreditation. This will ensure that assessed risks and consequent controls are still relevant. This re-accreditation process includes an IT Health Check, conducted by an independent UK government approved organisation. This will ensure the soundness of technical implementation of designed countermeasures.

Routing auditing of the UK CVCA and DV will be done as part of the EAC-PKI Service Providers activity.

Periodically, the Audit information generated by the UK EAC-PKI will be reviewed periodically to ensure EAC-PKI activity corresponds with genuine business transactions.

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

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 MRTDs

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 passes along incident and suspends information of Subscribers, and approves 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	Certificate 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
KPA	Key Production Authority
MRD	Machine-Readable Document
MRTD	Machine-Readable Travel Document
OID	Object Identifier
RA	Registration Authority
SPOC	Single Point of Contact

Appendix B Hardware Requirements

The cryptographic modules used by Certificate Authorities or Inspection Systems are 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

Appendix C SPOC REQUIREMENTS

C.1 SPOC Initial registration

SPOC initial registration together with the Member State's CVCA registration is carried out as defined in section 3.2 and Appendix D.

C.2 SPOC CA requirements

C.2.1 Certificate assurance and content

The CA issuing SPOC communication certificates are under governmental control. The certificates issued by the SPOC CA are fulfil requirements (naming, key usage, extensions) defined in CSN-SPOC. The SPOC Root CA Certificate Policy assures the OIDs identifying SPOC certificates are assigned only to certificates belonging to the SPOC.

C.2.2 Certificate revocation information

The certificates contain valid CDP extension. At least one distribution point is reachable via HTTP. CRL regular issuing period MUST be max. 90 days, in case a certificate is revoked, the CRL including revoked certificate MUST be published no later than 72 hours after the certificate revocation. The corresponding CRL are checked at each TLS connection establishment using SPOC communication.

UK SPOC CRLS are only made available to IP addresses specified in Member State SPOC Registrations forms received by the Home Office and supplied to the UK EAC-PKI Supplier.

C.2.3 Technical and organizational requirements

The SPOC CA are fulfil the same level of requirements as specified for CVCA in chapters 5 Security Requirements and 6 Key Pair Security.

Private keys used for SPOC communication are stored in a secure cryptographic module. The module containing the SPOC root CA private key fulfils the requirements specified in Appendix B.

C.2.4 Validity periods

The certificates used for SPOC communication have the following private key usages and validity periods:

- SPOC root CA certificate validity period:
  - up to 13 years if the CSCA certificate is used as SPOC root CA certificate
  - 5-7 years if any other CA certificate is used as SPOC root CA certificate
- SPOC root CA private key usage: up to 3.5 years
- SPOC client and server certificates validity period: 6-18 months

C.2.5 Distribution of successive SPOC root certificates

The issuance of a successive SPOC root CA certificate comprises the issuance of a link certificate between the actual SPOC root CA certificate and the successive SPOC root CA certificate.

The issuance of a successive SPOC root CA certificate are announced 90 days before TLS certificates signed by this certificate will be used for communication. The announcement includes the last date of use for the old certificates and the first date of use of the new ones.

The announcement of a successive SPOC root CA certificate are done via SPOC General Message and additional be sent to European Commission.

The successive SPOC root CA certificate and the corresponding link certificate are distributed by email using the addresses from the registration form at least 10 days before first day of use for SPOC communication. Additionally part II of the registration form MUST be filled in with the new certificate data and be delivered to the European Commission.

If the issuance of a link certificate is not possible e.g. after a security incident, the new SPOC root CA certificate MUST be distributed as an initial SPOC root CA certificate according to chapter 3.2.2 Registration of a foreign Member State.

C.3 Communication priorities

Whenever possible an automated web service interface is 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) contacts SPOC using registration information to find the solution for urgent communication requests.

C.4 Sending notifications

To send the notification SPOC are used. General Message as defined in CSN-SPOC is used to transport notification. It is RECOMMENDED to use wording as specified in the following table for subject and body part of the message. For additional purposes of General Messages individual wording MAY be used as needed.

Reference to CP	**Subject**	**Body**
[EUCP] sec. 1.4.6	Disruption of CVCA communication channel	Country SPOC Web-service interface will not be operational from [date, time] to [date, time]. During the period use email.
[EUCP] sec. 1.4.6	Suspension of CVCA service	CVCA service will be suspended from [date] to [date].
[EUCP] sec. 1.4.6	Reactivation of SPOC service	Country SPOC Web-service interface has been reactivated
[EUCP] sec. 5.3.4	[IS|DV|CVCA] private key [lost/stolen/ compromised]	Private key belonging to [CHR] was [lost/stolen/compromised] on [date].
[EUCP] sec. 4.5	Certificate inaccurate	Attached certificate was found inaccurate.
[EUCP] sec. 5.4	[CVCA|DV] Termination	[CVCA|DV] identified by [CHR] will terminate operation from [date]. For further information contact [contact details].
[EUCP] sec. 7	DV not compliant	The DV [CHR] is no more compliant to Common CP requirements.

Appendix D Registration form

The Registration Forms are used for registration of a Member State's CVCA at foreign Member State's CVCAs according to section 3.2. The registration form consists of three parts:

- the first part contains the registration information of the Member State, its National PKI Co-ordinator and the declaration of being conformant to this Certificate Policy,
- the second part contains the information on technical SPOC and
- the third part contains information on the CVCA Certificate. If a Member State wants to register more than one CVCA it are fill in (only) this part of the registration form once per CVCA.
- the fourth part contains information on the Document Verifiers. If a Member State wants to register more than one DV it are fill in (only) this part of the registration form once per DV.

D.1 Registration form commentary

CVCA certificate:

The CVCA certificate used for registration SHOULD be the oldest CVCA certificate of that CVCA which might be stored as trust anchor in a still valid travel document. Which means the CVCA certificate been valid at the day x:

- x = actual date – (travel document validity + CVCA certificate validity)

or the earliest CVCA certificate after day x[2].

Certificate encoding:

The CVCA certificate MUST be binary and the SPOC root certificate MUST be DER encoded for certificate exchange and generating cryptographic fingerprints.

Hash algorithm:

The hash values needed for the registration form are SHA-1 but additional hash values and algorithms MAY be added.

D.2 UK Registration Forms

The UK SPOC Registration Forms can be obtained from the UK PKI Coordinator:-

UKPKICoordinator@homeoffice.gsi.gov.uk

[2] E.g. *actual date = 12.10.2012, max. validity of German ePassport = 10 years, max. validity of CVCA Certificate = 3 years, so 12.10.2012 – (10+3 years) = 12.10.1999, earliest CVCA Certificate of Germany issued in 2008. Until 2021 this will be the German CVCA Certificate for initial registration, but not for signing certificates.*