Home Office
UK Border Agency

CVCA: THE UNITED KINGDOM'S CERTIFICATE PRACTICE STATEMENT

for Extended Access Control to Fingerprint Biometrics on the United Kingdom's Machine Readable Documents

September 2012

OID: 1.2.826.0.1363
Public Document

CONTENTS

1. INTRODUCTION

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

This document is the public part of the CVCA's Certificate Practice Statement

The UK CPS is owned by the Home Office and administered by the UK Border Agency (UKBA).

BACKGROUND

The Home Office is the lead United Kingdom (UK) government department for immigration and passports, drugs policy, crime, counter-terrorism and police.

The UK Border Agency (UKBA) is an Executive Agency of the Home Office and is responsible for securing the UK border and controlling migration in the United Kingdom (UK). The UK Border Agency manages border control for the UK, enforcing immigration and customs regulations. The Agency also considers applications for permission to enter or stay in the UK, and for citizenship and asylum. The capability to establish and verify a person's identity is crucial to achieving the UK Border Agency's strategic objectives. The Agency issues Biometric Residence Permits (BRPs) and Biometric Travel Documents (BTDs) to non-EU (foreign) nationals.

The Identity and Passport Service (IPS) is an Executive Agency of the Home Office and it incorporates the General Register Office (GRO). The Agency is responsible for issuing UK passports and for the registration of births, marriages and deaths in England and Wales.

The 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 both to Machine Readable Travel Documents (MRTDs); Biometric Residence Permits (BRPs) and any other Machine Readable Documents which may be developed in the future.

The Certificate Practice Statement is based on the UK Certificate Policy and it meets the standards of the Common EU Certificate Policy. In this document the CVCA refers to the UK National CVCA.

The UK Certificate Policy states the purposes for which certificates may be used:-

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

Biometric Residence Permits - Certificates may be used to control access to fingerprint biometrics on Extended Access Control enabled Residence Permits (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 Travel Documents - Certificates may be used to control access to facial biometrics on Basic Access Control enabled Home Office Travel Documents issued to third country nationals (in certain circumstances for example refugees, stateless persons or those who are undocumented) and will only be used for verifying the authenticity of the document and the identity of the holder.

1.1 PURPOSE

The Country Verifying Certification Authorities (CVCA) has been established to protect sensitive biometric data stored on an MRD chip. The CVCA offers the certificate service to parties operating as Document Verifiers (DV). Confidential personal biometric data on an MRD chip can only be accessed if a proper certificate chain is introduced to the chip.

For both CVCAs and DVs this Certificate Practice Statement refers to the UK Certificate Policy.
This Certificate Practice Statement is a statement of the practise that a certification authority employs for issuing, managing, revoking and renewing or re-keying certificates.

1.2 PARTIES

1.2.1 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

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 Document Verifiers. 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 1.3.3).

DOCUMENT VERIFIER CERTIFICATION AUTHORITY (DVCA)

The UK has one or more Document Verifiers (DVs). Each 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.

Each Document Verifier requests and obtains Document Verifier certificates from the CVCA of each country whose MRTDs the Document Verifier is authorised to access.

The UK Document Verifiers (DVs) may include up to 3 International ones (travel, immigration, etc.) and as many domestic ones as appropriate including Border, Police, Other Government Departments (OGDs), local government and trusted commercial customers such as Banks (see 1.3.3 below).

DOCUMENT VERIFIER (DV)

The 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 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.

1.2.2 Registration Authority

As defined in the UK Certificate Policy.

1.2.3 Subscribers to EAC-PKI Service

Subscribers under this CPS include government and public bodies and potentially private sector organisations.

UKBA will initially offer services to operational business areas within UKBA and the wider Home Office. It will be able to expand the service to meet future requirements of other potential users, including other Government departments, police services, and public bodies. In the longer term the service could be strategically released to commercial organisations such as banks, credit checking agencies etc.

Non-governmental organisations and commercial organisations may wish to be subscribers to an EAC-PKI service. An example could be an inspection system to enable verification of document holders against EAC MRDs, such as Biometric Residence Permits, during business transactions (e.g. in banks it could facilitate the process of opening a bank account by a Foreign National). Banks and other financial institutions such as payment service providers like VISA are likely to have the technical and security capability to implement the required technology.

Any organisation wishing to subscribe to UKBA's EAC-PKI service will be rigorously vetted both from a business, legal and technical perspective. This will ensure that they are a trusted organisation which has the technical capability and legitimate business reasons to use the service. Subscribers will be required to renew their subscription annually, subject to a subscription fee re-appraisal to ensure that they are complying with the security controls. Any breach of security protocols will be investigated and in such cases subscribers may have their service suspended or withdrawn.

The whole certificate exchange and inspection system infrastructure design employs high levels of security protection to avoid the compromise of signing keys. It also imposes strict limits on digital certificate validity periods to minimise the impact of any breach. When certificates are distributed to inspection systems from subscribing DVs, they will enable identity documents to be read for a specific period of time. Where inspection systems are potentially vulnerable to theft, the certificates issued from the parent DV may be valid for just as little as one day.

1.2.4 Relying Parties

As defined in the UK Certificate Policy.

1.2.5 Single Point of Contact

One of the key principles of exchanging DV certificates with other states is that each country will have a Single Point of Contact (SPOC) via which all international DV certificate requests and DV certificates will be channelled. The SPOC is in essence a communications channel (see also section 9.11).

- SPOCs act as an interface for communication between Member States. A SPOC allows efficient on-line communication to carry out regular key management related tasks.

- A national SPOC collates certificate requests from other SPOCs for delivery and processing by the national CVCA. It also communicates responses back to the requesting SPOC, on behalf of its domestic CVCA.

- The same national SPOC is also responsible for relaying domestic Document Verifier (DV) requests to foreign SPOCs for processing by the foreign DV. It then gathers responses containing certificates from foreign CVCAs for relay to the domestic DV that initiated the request.

UKBA's 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.

1.2.6 Other Participants

As defined in the UK Certificate Policy.

1.3 CERTIFICATE USAGE

CVCA key pairs and certificates, DV key pairs and certificates and certificate trust chains are described in the UK EAC Certificate Policy and in relevant sections of this document.

1.4 POLICY ADMINISTRATION

Any questions regarding this Certificate Practice Statement may be sent to the following address:

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

E-mail: IdentityServices@Homeoffice.gsi.gov.uk

1.5 TERMINOLOGY, DEFINITIONS AND ACRONYMS

As defined in the UK EAC Certificate Policy.

2. PUBLICATION AND DATA SOURCE REQUIREMENTS

The Home Office, and specifically the UK Border Agency, is responsible for maintaining a list of contact details for all UK DVs and groups of 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.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING - HOLDER AND AUTHORITY REFERENCES

CVCA certificates, the holder reference identifies the public key of the CVCA certificate, and the authority reference 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 holder reference identifies the public key of the Document Verifier certificate, and the authority reference identifies the public key of the issuing CVCA certificate.

Inspection System certificates, the holder reference identifies the public key of the Inspection System certificate, and the authority reference identifies the public key of the issuing Document Verifier certificate.

3.1.1 Naming Convention

The Home Office's UK Border Agency has defined the mnemonic that represents the certificate holder as described below.

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

- Country Code - 2 alphanumeric (AN) characters
- Holder Mnemonic - up to 9 alphanumeric (AN) characters
- Sequence number - up to 5 numeric digits

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

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 or 2 letter country code followed by a 3 digit value.

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

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	GB001 GB999 or 00001 -99999	Up to 5 numeric digits or 2 letter country code followed by a 3 digit value.

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

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 Rang	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 INITIAL IDENTITY VALIDATION

Responsibility for the UK CVCA rests with the Home Office and specifically with the UK Border Agency.

COUNTRY VERIFYING CERTIFICATION AUTHORITY SET-UP

UKBA has set up the UK Country Verifying Certification Authority (CVCA) and maintains it so that it can issue DV certificates for UK and foreign DVs for the purpose of reading fingerprint data stored on UK MRDs.

UKBA makes decisions regarding which countries are issued the right to read fingerprint data on UK MRDs. Information, including the necessary technical and administrative contact details (SPOC), are collated by UKBA's EAC-PKI operations team.

DOCUMENT VERIFIER SET-UP

UKBA sets up the UK Document Verifiers (DV) (see 1.3.1) and maintains them so that they can issue IS certificates for subscribers to read fingerprint data stored on MRDs in the UK. The DV administers the DV keys needed to issue IS certificates in order to read data on both UK and foreign MRDs.

DV certificates issued by the UK CVCA are valid for periods between 1 and 3 months (depending on agreed business rules).

INSPECTION SYSTEM SET-UP

UKBA sets up Inspection Systems (IS) or allows subscribing parties in the UK to operate ISs that interface to one or more of the UK DVs.

An EAC Concentrator may be a component of the UK's EAC-PKI Service. An EAC Concentrator would act as a conduit for relaying domestic EAC certificate requests and responses for one or more Inspection Systems.

UK National passport inspection authorities (including border services, port authorities and customs) may operate Inspection Systems that are capable of validating MRDs and accessing their biometric data.

Each DV issues signed IS certificates and distributes them along with the current DV certificate in response to certificate requests from domestic Inspection Systems. These certificates, along with a securely held IS private key, authenticate an Inspection System to MRD chips. The certificates also specify which biometrics the Inspection System can access. Each DV must request and obtain DV certificates from the CVCA of each country to whose MRDs the Document Verifier is to authorise to access. For a long term scalable solution much of this process will be automated via online interfaces.

3.2.1 CVCA

The UK Border Agency is responsible for CVCA authentication and CVCA identity definition.
All key management tasks are carried out by using robust communication channels. For communications between states all UK CVCAs and DVs carry out such communications using the UK Single Point of Contact (SPOC) (See 1.3.5).

3.2.2 CVCA to CVCA

In order to authenticate initial foreign country DV requests, the UK CVCA will obtain the CVCA certificate from the foreign country concerned. A pre-condition will be that a bilateral agreement exists between the two countries to exchange certificates; specifying certificate usage and permissions regarding access to biometric data on MRDs. The foreign CVCA certificate will be obtained through the UK SPOC communicating with the foreign country SPOC.

Before a foreign SPOC can communicate with the UK SPOC, a SPOC registration process will need to be undertaken. This will normally follow the Bilateral Agreement so that information about the foreign state's SPOC and CVCA can be registered with the UK and verified as trusted before the automated SPOC messages can be exchanged. The UK SPOC will be similarly registered with the foreign SPOC to provide information about the UK SPOC and CVCA before any SPOC message exchanges can occur.

SPOC/CVCA registration information includes the following:-

- Country Code - country code of the foreign SPOC
- CA Certificate Policy - unique OID identifier
- SPOC Root CA certificate - path and file name
- SPOC URL
- CVCA Identity (see 3.1.1 Naming)

3.2.3 DV to CVCA

In order to read MRDs of a foreign country, a UK Document Verifier will submit a request to the foreign CVCA via SPOC. Prior to the first request the DV should already be registered with the UK CVCA and the UK CVCA should already have received a copy of the foreign CVCA certificate via SPOC. An agreement will also need to be in place concerning the business rules for issuing certificates to read the foreign state documents to UK Inspection Systems.

The DV registration information for UK or foreign CVCA includes the following:-

- Country Code
- DV Holder Identity (see 3.1.1 Naming)
- DV Category (Domestic Government, Domestic Commercial etc.)
- Supervising CVCA Identity
- DV contact details
- DV URL
- Access Rights requested

Once the DV registration is complete a DV certificate request will be sent to the appropriate CVCA. If this is a foreign request it will be sent via the UK SPOC and the SPOC of the foreign state in question.

3.2.4 IS to DV

The DV will process certificate requests from UK Inspection Systems. For the initial request a DV administrator will enrol the IS by adding its identifier (see IS naming convention in section 3.1.1) and assigning its biometric access permissions and permitted certificate lifetime in accordance with UKBA policy. The request (which contains the IS public key) will then be manually authenticated by the DV administrator. This results in an IS certificate signed by the DV which is returned to the IS along with the DV certificate.

Subsequent IS requests will be signed by the previous IS private key which the DV is able to validate using the previous IS public key that it has held in the IS certificate it last issued to the IS concerned.

3.3 IDENTIFICATION AND AUTHENTICATION FOR CERTIFICATE REQUESTS

As specified in the UK Certificate Policy.

3.3.1 DV to CVCA

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 counter signed by the Foreign CVCA for which the foreign CV certificate is provided to the UK CVCA by a CVCA administrator 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.

3.3.2 IS to DV

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. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATIONS

4.1.1 CVCA

The UK Border Agency's EAC-PKI Operations Unit is responsible for the validation and authorisation of certificate applications.

4.1.2 DV to CVCA

Following successful Initial Identity Validation as per 3.2.3 above, DV certificate requests are carried out in accordance with section 4.2 "Certificate Application Processing" below.

4.1.3 IS to DV

Inspection Systems submits IS certificate requests upon completion of successful Initial Identity Validation as per 3.2.4. IS certificate request are carried out in accordance with section 4.2 below.

4.2 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 sections 1.3.5) 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 administrator 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 administrator 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 administrator logs into the DV and adds the CVCA holder identity. The DV now recognises the CVCA.
4. The DV administrator imports the CVCA certificate into the DV.
5. The DV administrator generates and exports a certificate request, and then sends it to the CVCA administrator.

At the CVCA

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

At the Document Verifier

9. The DV administrator imports the certificate.

4.2.1 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 (see 4.6.1)

4.2.2 Certificates issued by CVCA to DV

The UK CVCA only issues a certificate to a DV that is complying with its own (the DVs) Certificate Practice Statement. The UK CVCA processes a certificate request as follows:-

- UK CVCA checks that a certificate request is valid.
- UK CVCA acknowledges a certificate request upon its receipt.
- UK CVCA processes the certificate request within 72 hours.

In event the UK CVCA system is non-operational for more than 72 hours it will inform all subscribing DVs no later than 7 days before the loss of service, if planned, and as soon as is reasonably possible in the event of an unplanned loss of service.

4.2.3 Certificates issued by DV to IS

A UK DV will only issue a certificate to an IS that is complying with the UK Certificate Policy and UK Certificate Practice Statement. DVs automatically check that a certificate request is valid prior to issuing a certificate.

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

4.3 CERTIFICATE ACQUISITION, STORAGE & DISTRIBUTION

4.3.1 Certificate Acquisition Overview

One of the primary functions of UKBA is to obtain certificates from the appropriate Certification Authority (CA) before the currently issued certificates expire. Acquired certificates are held in a repository on the relevant server which is interrogated at regular intervals to ensure a replacement certificate is requested before the stored certificate expires.

Certificates will be provided to Inspection Systems (IS) upon request if the IS meets the policy and security thresholds set for the IS. The onus is on the Inspection System to request a certificate before the expiry of an existing certificate.

UKBA will acquire EAC certificates from the following sources:

- UK Country Verifying Certification Authority (CVCA)
- Foreign CVCAs via the Single Point Of Contact (SPOC)
- Foreign SPOCs by out of band means e.g. CD from a known foreign government official.

4.3.2 Certificate Acquisition Process

A first generation document (containing non-sensitive data) is opened using the Basic Access Control protocol and the encoded data is verified at the border by checking the digital signatures on the document chip against the country signing public key (CSCA) certificates or against the Document Signer Certificate stored in the PKD Store.

These checks are extended for second generation Machine Readable Documents (MRDs) to allow Inspection Systems to access sensitive data on the chip (i.e. fingerprints) using the EAC access protocol which combines Terminal Authentication (TA) and Chip Authentication (CA) protocols. For EAC additional certificates must be provided to the Inspection System so that it may prove to the chip that it has the authority to 'unlock' and access the sensitive information on the chip.

The basic certificate acquisition flow for second generation documents is as follows:

- A second generation MRD is presented at the border to an immigration officer who uses a reader to confirm that the document and contents are valid (as part of the BAC, CA and TA checking process).

- The reader first starts an encrypted channel using BAC and then performs validation of document signing signatures (Passive authentication) and reads the MRZ and facial image data from the chip.

- The reader then moves into EAC. It first checks the chip is genuine by using the Chip Authentication protocol and establishes a strongly encrypted communication channel with the chip. If this is successful it then moves on to the Terminal Authentication phase of EAC.

- The reader is controlled by an Inspection System which potentially will be controlling a group of readers. In order to open the chip on the travel document, the reader will need to prove to the chip that it is a trusted device with authority to read the contents of the chip (Terminal Authentication). The reader first queries the chip for the identity of the CVCA which issued the CVCA certificate it holds which it then relays to its associated Inspection System.

- If it holds certificates issued by the identified CVCA the Inspection System will respond by passing the relevant DV Certificate and the IS Certificate to the querying reader.

- The reader presents the Document Verifying (DV) Certificate and an IS Certificate provided by IS to the document. If the chip is able to authenticate the DV certificate signature using the CVCA certificate it holds and then use the DV certificate to authenticate the IS certificate presented it is able to confirm a chain of trust back to its issuer. If this step fails the read ceases at this point.

- With the trust chain to its CVCA confirmed the chip sends a challenge for the IS back to reader. The reader must relay the challenge back to its managing IS to sign. The IS signs the challenge with the private key it holds that is associated with the IS certificate provided to the chip. The signed response is sent to the reader for relay on to the MRD chip.

- If the MRD chip is able to authenticate the signed response to its challenge using the IS cert just received this authenticates live communication with the IS authorised to use the IS certificate presented. If not either the response is not live or the IS is unable to prove rightful ownership of the IS certificate presented so read access is refused and the read process ceases.

- Upon successful validation, the chip will allow the reader access to the stored information on the chip including fingerprints for comparison with fingerprints of the document holder. The Inspection System (IS) relies on the established trust chain that the DV Certificate obtained from the DVCA in the DRA is authentic.

- Compliance with UKBA policy and data protection legislation will require that the extracted information is not subsequently retained by the reader.

4.3.3 Certificate Storage

UKBA stores and catalogues all certificates acquired or issued by each respective Certificate Authority in the DRA.

A business rules table exists and is maintained to ensure that certificates are only issued by UKBA in accordance with agreements with each provider.

4.3.4 Certificate Distribution

In order to deliver certificates to recipients (Inspection Systems), the recipient must be approved by UKBA and a trust relationship established between UKBA's system and the recipient's system.

Having established trust, UKBA's system transmits certificates (for that recipient) in accordance with relevant business rules.

UKBA's EAC-PKI system receives requests from various subscribing customers for appropriate certificates to allow the customer's system to access and interrogate second generation travel documents including Biometric Residents Permits (BRPs)

The most common occurrence is a request from a UK based Inspection System (Terminal) for a verification certificate. This certificate allows an IS or attached reader to access the sensitive data protected by Extended Access Control (EAC) stored on the chip. It is anticipated that as the number of EAC protected identification products in circulation increases, demand to read the sensitive data groups will grow. This would eventually result in UKBA receiving certificate requests from more users of these products including commercial organisations.

UKBA will also receive requests for certificates to allow access to foreign travel documents (i.e. to enable Inspection Systems to read non-UK passports and EU Identity documents). The acquisition of foreign certificates is undertaken by UK DVCAs via the UK SPOC function. However to facilitate this, a trust relationship will need to be established with each foreign issuer of travel documents with whom UKBA has a defined policy.

The distribution of certificates by UKBA is undertaken on a predefined scheduled basis to Inspection Systems as real time distribution is impractical owing to the logistics and inherent time delays. The onus is on Inspection Systems to request a new certificate in a timely manner before the expiry of an existing certificate.

The validity period of certificates will vary as it is dependent on the certificate policy agreed with the end customer and is based on the security risk profile of the end user. Typically, the expiry period for DV certificates is one to three months and for IS Certificates one day to thirty days. The maximum is governed by the EU EAC certificate policy

UKBA's EAC-PKI system will distribute certificates to Inspection Systems as follows:

- Inspection System ascertains requirement for new IS and or Document Verifier certificate as the existing certificates are due to expire (in x days, where x is based on agreed rules/policy).

- IS sends a request to the UK system for a new certificate.

- UK system receives request from IS for a new IS certificate.

- UK system will ensure the Inspection System is a known device (using predefined rules) and ensure it is active and authorised to receive the requested certificate.

- If it is authorised the DV will process the IS certificate request signing the IS certificate and return this certificate to the IS. If the IS certificate is signed using later DV keys than the previous IS certificate then the latest DV certificate will also be distributed to the requesting IS from the DVs certificate store..

- The result of this request and response process is logged by the DVCA.

- Each time a MRD requiring this certificate chain is accessed by a reader the IS will query the IS for the relevant certificate chain and the IS will respond with the latest DV and IS certificate it holds under the relevant CVCA.

Once the Inspection System receives the signed IS and DV certificate from the DV, these will be stored internally as a chain for the respective country's CVAC. Hence when a request is received from a reader, the IS will provide the relevant country DV & IS Certificates to the reader.

4.4 KEY PAIR AND CERTIFICATE SECURITY RULES

The UK CVCAs, DVs and ISs fulfil the requirements of the UK National EAC Certificate Policy.

The UK CVCAs, DVs and ISs all hold their own key pair the public key of which is contained within the respective CVCA, DV or IS certificate. The mechanism for generating, protecting, holding and renewing these keys is outside the scope of this document for reasons of security.

4.5 CERTIFICATE RENEWAL

Not allowed See 4.6 Re-Key

4.6 CERTIFICATE RE-KEY

The UK CVCAs, DVs and ISs must all renew their key pairs whenever they require a new certificate. The mechanisms for generating, protecting, holding and renewing these keys are outside the scope of this document for reasons of security. The frequency of rekeying increases as the trust chain is descended from CVCA to DVCA and again from DVCA to IS. This follows the EU certificate policy requirements.

4.6.1 CVCA Certificates

CVCA Rollover

The UK CVCA root key will expires every 3 years and was last renewed September 2011. The UK Border Agency 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.

UKBA 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 UKBA 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.

4.7 CERTIFICATE MODIFICATION

This is covered by section 4.6, "Certificate Re-Key", of this CPS.

4.8 CERTIFICATE STATUS SERVICES

EAC certificates contain an effective date and expiration date. These dates determine the current state of the certificate. A certificate can have one of the following states:

- **Not yet valid** - A certificate may have this state if the clock difference between a CVCA and a DV is significant. This state is not seen very often.
- **Valid** - A certificate with a 'Valid' state indicates that the certificate is within its validity period i.e. between its effective and expiration date. A certificate should not be used outside of its validity period.
- **Expired** - This state indicates that the expiry date in the certificate has passed so it has reached the end of its lifetime and is no longer valid.
- **Nearing expiry** - This state indicates that the certificate is nearing its expiration date and should be renewed.

4.9 END OF SUBSCRIPTION

Governmental, commercial and other organisations that have subscribed to EAC-PKI certificate services will notify UKBA within an agreed timeframe (as stipulated in MOUs/SLAs) that they are intending to end their subscription.

4.10 KEY ESCROW AND RECOVERY

Not used.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

UKBA's EAC-PKI systems, equipment and processes are designed to ensure the security and integrity of the UKBA EAC-PKI system. This will include putting in place the following measures:

- Public Key Infrastructure to allow safe transmission and validation of Certificates
- Appropriate Hardware Security Modules (HSM) for secure storage of Private Keys
- A minimum of SC clearance for staff administering the equipment
- Accreditation of solutions by SACU, DSU and CESG as appropriate
- A secure physical location to house the infrastructure
- A securely defined process for managing certificate distribution
- Firewalls & Virus protection
- Authentication of certificate requests and initial registration of Inspection Systems and DVs
- Logging
- Secure transmission

5.1 PHYSICAL CONTROLS

The UK CVCA and DVs operate their services in a secure environment.

All physical security controls for UKBA's EAC-PKI systems comply with the physical security requirements of SACU and CESG. These measures include vetting of operational personnel, physical access control of the operational environment and physical handling/storage of key material in line with CESG guidance (IS4).

5.1.1 CVCA Keys

CVCA key material is created via a CESG mechanism. The private key is only ever utilised for signing inside a CESG fit for purpose (FFP) approved Hardware Security Module (HSM) device.

CESG approved network security rules configured in a manner compliant with GPG 13 and GPG 8 are employed to protect the key material from exposure from unapproved access.

5.1.2 DV Keys

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

CESG approved network security rules and devices configured in a manner compliant with GPG 13 and GPG 8 are employed to protect the key material from exposure from unapproved access.

5.1.3 IS Keys

IS private keys are generated and held within a local HSM device assoiled with the IS devices themselves.

5.2 PROCEDURAL CONTROLS AND SYSTEM ACCESS MANAGEMENT

Procedural controls are implemented, especially the separation of duties by implementing a two person principle for critical tasks. Each CVCA, DV, and IS ensure that system access to any 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.

5.3 PERSONNEL CONTROLS

All of the UK's EAC-PKI systems (CVCA, DV and IS systems) are operated by suitably qualified and experienced staff.

Like all Home Office Staff, those responsible for operating UKBA's EAC-PKI infrastructure undergo security checks and vetting at the appropriate level for the job they do.

All staff working with UK Border Agency EAC-PKI infrastructure will be security cleared to SC level as a minimum. Project staff, consultants and agency staff are all cleared to at least BC level and higher where necessary. All staff are also issued with a security pass which they must clearly display and access to EAC-PKI equipment is limited to those who require access as part of their duties.

5.4 AUDIT LOGGING PROCEDURES

Each CVCA and DV within UKBAs infrastructure 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 for 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 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-man-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 4.2.2.

5.6 KEY CHANGEOVER

UK CVCAs and DVs ensure that keys are generated in controlled circumstances and in accordance with the procedures defined in Section 5.2 Procedural Controls and System Access Management.
Full, self-signed certificates plus link certificates are provided by the CVCA (see section 4.6.1).

5.7 COMPROMISE AND DISASTER RECOVERY

The UK CVCA take reasonable measures to ensure that continuity of service 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 4.2.2 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 to bring a reserve CVCA and DVCA into operation from offsite backups and a pre loaded HSM is available. 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 UKBA by email until a new UK SPOC can be established.

5.8 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. TECHNICAL SECURITY CONTROLS

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 Management, Procedural and Physical Controls of this document.

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 administrator process but for subsequent exchanges it will be via automated cryptographic check.

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). In the case of the CVCA this is an HSM accredited as Fit for Purpose (FFP) by CESG. 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.

UKBA obey a two man rule for all sensitive CVCA and DVCA key operations e.g. request processing, backup, restore and destruction.

UKBA IS key operations such as certificate request generation and key use will be restricted to authorised personnel appointed to this role. IS private keys are protected in a HSM or cryptographic smartcard device.

If private key material is ever exported from a CVCA or DVCA HSM, e.g. to provide a backup in another HSM, it will be strongly encrypted and meet the requirements of the protective marking. All handling will be undertaken under a procedurally controlled two man rule and where possible this will be enforced by technical constraints. The protection provided will be suitable for the protective marking assigned to that key. The number of personnel able to perform this function should be kept to a minimum and must hold a minimum of SC clearance.

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.

UKBA 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 first. 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 OTHER ASPECTS OF KEY PAIR MANAGEMENT

As defined in the UK National EAC Certificate Policy.

6.4 ACTIVATION DATA

As defined in the UK National EAC Certificate Policy.

6.5 COMPUTER SECURITY CONTROLS

- Dedicated Windows User Accounts
- Audit Logs
- CA Role Separation
- CA User Accounts

6.6 LIFE CYCLE SECURITY CONTROLS

As defined in the UK National EAC Certificate Policy.

6.7 NETWORK SECURITY CONTROLS

- Infrastructure compliant with CESG GPG 8
- Firewall White Lists
- Air-gap where appropriate and practicable
- Host Firewalls

7. CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILES

7.1 CERTIFICATE PROFILE

CV Certificates as specified in Technical Guideline TR-03110, "Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)" Version 1.11 section A 4.1, "CV Certificates".

7.2 CRL PROFILE

Not applicable

7.3 OCSP PROFILE (ONLINE CERTIFICATE STATUS PROTOCOL)

Not applicable

8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS

The UKBA EAC-PKI infrastructure will be subject to re-accreditation procedures in line with standard UK government best practice. This will ensure good security practices and infrastructure protection remain in place along with ensuring continued compliance with the UKBA EAC-PKI Risk Management and Accreditation Documentation Set (RMADS).

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The UK does not charge a fee to foreign countries for provision of DV certificates. UKBA does not charge UK government departments who may subscribe to the UK EAC-PKI service for the purposes of verifying identity of individuals accessing UK government services.

There may be a set-up fee and annual operational charge for non-governmental organisations and commercial organisations who wish to subscribe to the UK EAC-PKI service. For example some commercial organisations may wish to operate an inspection system to enable them to verify MRDs during business transactions e.g. in a bank this could facilitate the process of opening a bank account by a Foreign National holding a BRP card.

9.2 FINANCIAL RESPONSIBILITY

Where commercial organisations subscribe to the UK's EAC-PKI service, financial responsibilities are defined in the agreements between the parties.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Where commercial organisations subscribe to the UK's EAC-PKI service, confidentiality of business and technical information is defined in the agreements between the parties.

9.4 PRIVACY OF PERSONAL INFORMATION

UK ISs are not permitted to log or transmit fingerprint biometrics obtained from MRDs. These biometrics must be deleted immediately after finishing the comparison process between the fingerprint biometric collected by the IS from the bearer and the fingerprint biometric read from the MRD.
Logging or transmitting of fingerprint data obtained from the bearer by Inspection Systems at border control is permitted but data must be deleted as soon as practicable after facilitating the transaction.

9.5 INTELLECTUAL PROPERTY RIGHTS

Not applicable.

9.6 REPRESENTATIONS AND WARRANTIES

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

9.7 DISCLAIMERS OF WARRANTIES

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

9.8 LIMITATIONS OF LIABILITY

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

9.9 INDEMNITIES

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

9.10 TERM AND TERMINATION

Not applicable.

9.11 INDIVIDUAL NOTICES AND COMMUNICATING WITH PARTICIPANTS

For communications between states all UK CVCAs and DVs carry out such communications using the UK Single Point of Contact (SPOC). Other additional online or offline communication channels are mutually agreed especially to cover situation when the UK or a foreign SPOC communication channel is not available.

In the event of disruption to the UK CVCA's normal communication channels it will notify subscribing DVs of an alternate channel by which Certificate Requests can be submitted. This is done in a timeframe that minimises the risk of current certificates expiring.

The UK complies with the additional requirements specified in Appendix C of the UK's Certificate Policy and the Common EU Certificate Policy (as amended).

9.12 AMENDMENTS

This Certificate Practice Statement is accepted by the UK Border Agency (UKBA). Amendments to this document may be made following a mutual decision by the UKBA and the Home Office.

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

Notification of the UK CVCA's intention to modify the CPS will be no less than 3 months before entering in a modification process on the CPS and include the scope of modification.

CPS OIDs will be changed if the UK determines that a change in the CPS modifies the level of trust provided by the CPS.

9.13 DISPUTE RESOLUTION PROCEDURES

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

9.14 GOVERNING LAW

This is defined in the Agreement between participants.

9.15 COMPLIANCE WITH APPLICABLE LAW

Not applicable.

9.16 MISCELLANEOUS PROVISIONS

Not applicable

9.17 OTHER PROVISIONS

Not applicable

10. GLOSSARY

Abbreviation / Term	Description / Definition
Certification Authority (CA)	An entity that issue certificates
Certificate Revocation List (CRL)	A list of revoked certificates
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirement;
Certificate Practice Statement (CPS)	A statement of the practice that a certification authority employs in issuing, managing, revoking and renewing or re-keying certificates;
Certificate Thumbnail	Hash Value of the Certificate Public Key;
CESG	CESG is the Information Assurance (IA) arm of GCHQ based in Cheltenham, Gloucestershire, UK. They are the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help our customers achieve their business aims.
EU Common Certificate Policy	The outline Certificate Policy published by the Commission which sets the minimum requirements that a Member State's National Certificate Policies must meet, in order to operate as an EAC-PKI within the EU.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.
Country Signing Certification Authority (CSCA)	The Certificate Authority responsible for issuing Country Signing Certificates. These are used to validate the Document Signing Certificates which are signed by the CSCA.
Extended Avccess Control Public Key Infrastructure (EAC-PKI)	The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control
Document Signing Certificate	A digital certificate held on the chip, and also distributed by the Document Signer. It is used in to validate signed data held on the chip. In turn it is validated using a CSCA certificate during Passive Authentication to confirm the chip data is authentic to the issuing state.
Document Signer	The entity signing the original document, in this case the organisation that issues the MRD
Document Verifier (DV)	An entity within the EAC-PKI that requests certificates from CVCAs and, on the basis of those certificates, issues certificates to Inspection Systems;
Evaluation Assurance Level	A numeric grade assigned to an IT system or product following the completion of a Common Criteria security evaluation
Extended Access Control (EAC)	A reading mechanism that combines assessing if a document chip is genuine, Chip Authentication (prevents cloning) and ensuring that an Inspection System has the right to read the sensitive biometric data held on a document chip, Terminal Authentication.
Inspection System (IS)	The operational system that can be issued the right to read sensitive biometrics data e.g. fingerprints from MRDs
International Civil Aviation Organisation (ICAO)	A UN organisation tasked with fostering the planning and development of international air transport. In this role it sets international standards for MRTDs
Key ceremony	A procedure whereby a key pair is generated using a cryptographic module and where the public key is certified.
Link Certificate	Link certificates ensure a trusted link between two Root certificates. This allows automated systems to verify a new root certificate as succeeding its predecessor cryptographically.
Machine Readable Travel Document (MRTD)	An international travel document containing printed and machine-readable data
MRD	Machine Readable Document. Used as not all documents issued under this policy will be travel documents although they will conform to the Machine Readable Travel Document (MRTD) standards for EAC.

Abbreviation / Term	Description / Definition
Memorandum of Understanding (MoU)	A legal document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action and may not imply a legal commitment. In the case of this CPS they will be used where a commercial contract would be inappropriate, for example between UK government departments or between the UK and other States.
National Certificate Policy	A Members State's Certificate Policy for management of the process of issuing and receiving certificates to and from other Member States
Object Identifier (OID)	A unique numerical sequence allowing a document to be identified
Public Part of the Certification Practice Statement	A subset of the provisions of a complete CPS that is made public by a CA
Registration Authority(RA)	An entity that establishes enrolment procedures for certificate applicants; performs identification and authentication of certificate applicants; initiates or passes on revocation requests for certificates, and approves applications for renewal or re-keying of certificates on behalf of a CA
Trusted certification path	A chain of multiple certificates needed to validate a certificate containing the required public key. An EAC certificate chain consists of one or more CVCA-certificates, CVCA link certificates as appropriate, a DV-certificate and an IS certificate