DCCKI Certificate Policy

1 INTRODUCTION

(a) The document (together with its Annexes):

(i) shall be known as the "DCCKI Certificate Policy" (and in this document is referred to simply as the "Policy"); and

(ii) is a SEC Subsidiary Document related to Section L13.35 (The DCCKI SEC Documents) of the Code.

1.1 Overview

(a) This Policy sets out the arrangements relating to:

(i) The Root DCCKICA Certificate;

(ii) EII DCCKICA Certificates; and

(iii) UI DCCKICA Certificates;

together referred to as the "**DCCKICA Certificates"** and

(iv) DCCKI Infrastructure Certificates; and

(v) Personnel Authentication Certificates,

together with the DCCKICA Certificates referred to as the "**DCCKI Certificates**".

(b) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 Document Name and Identification

(a) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1.8641679.1.2.1.11.

1.3 DCCKI Participants

1.3.1 The DCCKI Certification Authority

(a) The definition of the DCCKI Certification Authority is set out in Annex A.

1.3.2 DCCKI Registration Authority

(a) The definition of the DCCKI Registration Authority is set out in Annex A.

1.3.3 DCCKI Subscribers

(a) In accordance with Section L13.2 of the Code (DCCKI Authorised Subscribers) certain Parties and Registration Data Providers (RDPs) may become DCCKI Authorised Subscribers.

(b) The DCCKI RAPP sets out the procedure to be followed by Parties and RDPs in order to become a DCCKI Authorised Subscriber for one or more DCCKI Certificates.

(c) The DCC (acting in its capacity as the Root DCCKICA, EII DCCKICA or UI DCCKICA) shall be a DCCKI Authorised Subscriber and:

(i) it (and only it) shall be a DCCKI Eligible Subscriber in respect of DCCKICA Certificates; and

(ii) (save for the purpose of replacement of the Root DCCKICA), it shall be a DCCKI Eligible Subscriber only in respect of a single Root DCCKICA Certificate.

(d) Where a person is a DCCKI Authorised Subscriber in accordance with this Policy, that person shall be a DCCKI Eligible Subscriber in respect of DCCKI Infrastructure Certificates where the purpose of that DCCKI Certificate is:

(i) establishing TLS communications with the DCC over a DCC Gateway Connection, and that person is a Party or RDP; or

(ii) the signing of SAML assertions in order to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not the DCC Identity Provider Service, and that person is a User.

(e) A Party that is a DCCKI Authorised Subscriber shall be a DCCKI Eligible Subscriber in respect of Personnel Authentication Certificates only in the circumstance where that DCCKI Authorised Subscriber is a User, intending to use the Identity Provider Service provided by the DCC for the purpose of Authenticating its User Personnel to the Self Service Interface as set out in section 1.4.1 of this Policy.

(f) DCCKI Eligible Subscribers are subject to the applicable requirements of this Policy, the DCCKI RAPP and Sections L13.44 to L13.48 (The DCCKI Subscriber Obligations) of the Code.

(g) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretations):

(i) DCCKI Subscriber; and

(ii) DCCKI Eligible Subscriber.

(h) The definition of a DCCKI Authorised Subscriber is set out in Annex A to this Policy.

1.3.4 DCCKI Relying Parties

(a) The definition of a DCCKI Relying Party is set out in Section A of the Code (Definitions and Interpretations).

(b) DCCKI Relying Parties shall be subject to the applicable requirements of Sections L13.50 to L13.53 (Duties in relation to DCCKI Certificates and DCCKICA Certificates) of the Code.

1.3.5 DCCKI Policy Management Authority

(a) The DCC shall fulfil the functions of the DCCKI PMA in accordance with the provisions set out in Section L13.54 of the Code.

1.3.6 DCCKI Repository Provider

(a) Provision in relation to the DCCKI Repository Service is made in Section L13.18 (The DCCKI Repository Service). of the Code

1.4 USAGE OF DCCKI CERTIFICATES

1.4.1 Appropriate Certificate Uses

(a) The DCCKICA shall ensure that DCCKICA Certificates are Issued only to:

(i) the Root DCCKICA for use in its capacity as, and for the purposes of, exercising its functions as the Root DCCKICA; and

(ii) the EII DCCKICA and the UI DCCKICA, in their capacity as, and for the purposes of exercising the functions of, issuing authorities.

(b) Subject to 1.4.1 (e), the DCCKICA shall ensure that DCCKI Infrastructure Certificates are Issued only:

(i) by the EII DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purposes of:

(1) establishing TLS communications with the DCC over a DCC Gateway Connection; or

(2) the signing of SAML assertions of a User that chooses to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not that provided by the DCC.

(c) Subject to 1.4.1 (e), the DCCKICA shall ensure that Personnel Authentication Certificates are Issued only:

(i) by the UI DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purpose of Authenticating User Personnel of Users intending to use the Identity Provider Service provided by the DCC to the Self Service Interface.

(d) Further provision in relation to Parties and RDPs obligations in respect of the use of DCCKI Certificates is made in Section L13.44 The DCCKI Subscriber Obligations of the Code () and Section L13.49 (The DCCKI Relying Party Obligations)of the Code.

(e) Nothing in this DCCKI Certificate Policy shall prevent DCC from:

(i) using the Root DCCKICA Certificate for the purposes of issuing additional issuing authority certificates;

(ii) using those issuing authorities to issue additional end entity certificates; or

(iii) issuing DCCKI Infrastructure Certificates or Personnel Authentication Certificates to DCC or DCC Service Providers other than in accordance with this Policy;

provided that in any of the above cases DCC may only do so:

(i) for the purposes of issuing DCCKI Certificates or other certificates as may be required to establish secure communications between DCC and DCC Service Providers, or to secure communications and data within DCC Service

Providers, but not between either DCC or a DCC Service Provider and any other Party or RDP; and

(ii) to the extent set out in the DCCKI Certification Practice Statement.

1.4.2 Prohibited Certificate Uses

(a) No Party or Registration Data Provider shall use a DCCKI Certificate other than for the purposes permitted in section 1.4.1 of this Policy.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

(a) This Policy is a SEC Subsidiary Document and shall be maintained in accordance with the provisions of the Code.

1.5.2 Contact Person

(a) Questions in relation to the content of this Policy should be addressed to the DCCKI PMA or the Service Desk.

1.5.3 Person determining Certification Practice Statement suitability for the Policy

(a) Provision is made in Section L13.39 (the DCCKI Certification Practice Statement) of the Code in relation to the suitability of the DCCKI CPS for the Policy.

1.5.4 CPS Approval Procedures

(a) Provision is made in Section L13.55 (the DCCKI PMA functions) of the Code for the procedure by which the DCCKI PMA may approve the DCCKI CPS.

1.5.5 Registration Authority Policies and Procedures

(a) The DCCKI Registration Authority Policies and Procedures are set out at Appendix [TBC] of the Code.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

(a) Provision is made in Section L13.18 (the DCCKI Repository Service) of the Code for the establishment, operation and maintenance of the DCCKI Repository.

2.2 Publication of Certification Information

(a) Section L13.19 (the DCCKI Repository Service) of the Code makes provision for the lodging of documents and information in the DCCKI Repository.

2.3 Time or Frequency of Publication

(a) The DCCKICA shall ensure that:

(i) Root DCCKICA Certificate and EII DCCKICA Certificate are lodged promptly in the DCCKI Repository on Issuance;

(ii) each new version of the EII DCCKICA Certificate Revocation List is lodged in the DCCKI Repository following its production as is specified in section 4.9.7 of this Policy;

(iii) each new version of the DCCKI Authority Revocation List is lodged in the DCCKI Repository following its production as is specified in section 4.9.7 of this Policy;

(iv) DCCKI Infrastructure Certificates are lodged promptly in the DCCKI Repository on Issuance; and

(v) a revised version of the DCCKI RAPP is lodged promptly in the DCCKI Repository following each modification.

2.4 Access Control on Repositories

(a) Provision in relation to access controls for the DCCKI Repository is made in Section L13.21 (the DCCKI Repository Service) of the Code and the DCCKI Interface Design Specification and the DCCKI Certification Practice Statement.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

(a) Provision is made in the DCCKI RAPP to ensure that the name of the Subject of each DCCKI Certificate is in accordance with the relevant DCCKI Certificate Profile in Annex B to this document.

3.1.2 Need for Names to be Meaningful

(a) Provision is made in the DCCKI RAPP to ensure that the name of the Subject of each DCCKI Infrastructure Certificate is meaningful and consistent with the relevant DCCKI Certificate Profile in Annex B to this document.

3.1.3 Anonymity or Pseudonymity of Subscribers

(a) Provision is made in the DCCKI RAPP to prohibit DCCKI Eligible Subscribers from requesting the Issue of a DCCKI Certificate anonymously or by means of a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

(a) Provision in relation to name forms is made in Annex B to this document.

3.1.5 Uniqueness of Names

(a) Provision in relation to the uniqueness of names is made in Annex B to this document.

3.1.6 Recognition, Authentication, and Role of Trademarks

(a) Provision in relation to the use of trademarks, trade names and other restricted information in DCCKI Certificates is made in Section L13.45 (DCCKI Certificate Signing Requests) of the Code.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

(a) Provision is made in the DCCKI RAPP in relation to:

(i) the procedure to be followed by a DCCKI Eligible Subscriber in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any DCCKI Infrastructure Certificate that is the subject of a DCCKI Certificate Signing Request which has been submitted by that Eligible Subscriber; and

(ii) that the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism as agreed by the DCCKI PMA function.

(b) Provision is made in the DCCKI CPS in relation to:

(i) the procedure to be followed by the DCCKICA in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any DCCKICA Certificate that is the subject of a DCCKI Certificate Signing Request; and

(ii) the procedure to be followed by the DCCKICA in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any Personnel Authentication Certificate that is the subject of a DCCKI Certificate Signing Request pursuant to a Personnel Authentication Certificate Application from an Eligible Subscriber.

3.2.2 Authentication of Organisation Identity

(a) Provision is made in the DCCKI RAPP in relation to:

(i) The procedure to be followed by a Party or RDP in order to become a DCCKI Authorised Subscriber;

(ii) The criteria in accordance with which the DCCKI Registration Authority shall determine whether a Party or RDP is entitled to become a DCCKI Authorised Subscriber;

(iii) The requirement that the Party or RDP shall be Authenticated by the DCCKICA for that purpose; and

(iv) The criteria in accordance with which the DCCKICA shall determine whether a Party or RDP is Authenticated.

3.2.3 Authentication of Individual Identity

(a) Provision is made in the DCCKI RAPP in relation to the Authentication of individuals engaged by DCCKI Authorised Subscribers to fulfil roles defined in this Policy.

3.2.4 Non-verified Subscriber Information

(a) The DCCKICA shall verify all information in relation to DCCKI Certificates, save that the Subject name for Personnel Authentication Certificates is derived from the information input by DCCKI Eligible Subscriber for the purposes of populating fields in those Personnel Authentication Certificates and need not be verified by the DCCKICA.

3.2.5 Validation of Authority

See section 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[Not applicable]

3.3 Identification and Authentication for re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

(a) This Policy does not support Certificate Re-Key.

(b) The DCCKICA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[Not applicable]

3.4 Identification and Authentication for Revocation Requests

3.4.1 Authentication for Certificate Revocation Requests

(a) Provision is made in the DCCKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a DCCKI Certificate Revocation Request and to verify that they are authorised to submit that request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Applications

4.1.1 Submission of Certificate Applications

(a) Provision is made in the DCCKI RAPP with respect to the circumstances in which an DCCKI Eligible Subscriber may:

(i) submit a DCCKI Certificate Signing Request in relation to a DCCKI Infrastructure Certificate;

(ii) submit a Personnel Authentication Certificate Application in relation to a Personnel Authentication Certificate; and

(iii) submit a DCCKI Certificate Signing Request in relation to a DCCKICA Certificate,

and, in each case, the means by which that DCCKI Eligible Subscriber may do so.

4.1.2 Enrolment Process for the Subscriber and its Representatives

(a) Provision is made in the DCCKI RAPP in relation to the:

(i) establishment of an enrolment process in relation to Parties and RDPs in order to Authenticate them and verify that they are authorised to act as DCCKI Authorised Subscribers;

(ii) establishment of an enrolment process in relation to individuals nominated to act on behalf of DCCKI Authorised Subscribers as DCCKI Senior Responsible Officers or DCCKI Authorised Responsible Officers, in order to Authenticate them and verify that they are authorised to act on behalf of (and, in the case of Personnel Authentication Certificate Applications, go on to authorise others to act on behalf of) those DCCKI Authorised Subscribers; and

(iii) maintenance by the DCCKICA of a list of Parties, RDPs, and individuals enrolled in accordance with those enrolment processes.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(a) Provision is made in the DCCKI RAPP in relation to the establishment of an enrolment process in respect of DCCKICA Personnel and DCCKICA Systems for:

(i) the purpose of Authentication and to verify that they are authorised to act on behalf of the DCCKICA in its capacity as the DCCKI Registration Authority; and

(ii) including in particular, for that purpose, provision for:

(1) the Authentication of all DCCKI Registration Authority Personnel by a DCCKI Registration Authority Manager; and

(2) all DCCKI Registration Authority Personnel to have their identity and authorisation verified prior to being provided these roles.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

(a) Provision is made in the DCCKI RAPP in relation to the Authentication by the DCCKICA of a DCCKI Eligible Subscriber which submits:

(i) a DCCKI Certificate Signing Request in relation to a DCCKI Infrastructure Certificate; or

(ii) a Personnel Authentication Certificate Application in relation to a Personnel Authentication Certificate.

4.2.2 Approval or Rejection of Certificate Applications

(a) Where any DCCKI Certificate Signing Request made in relation to a DCCKI Infrastructure Certificate fails to satisfy the requirements set out in the DCCKI RAPP, this Policy or any other provisions of the Code, the DCCKICA:

(i) shall reject it and refuse to Issue the DCCKI Infrastructure Certificate which was the subject of that DCCKI Certificate Signing Request, and

(ii) shall give notice to the person that made the DCCKI Certificate Signing Request of the reasons for its rejection.

(b) Where the failure results from a failure of Authentication of the DCCKI Eligible Subscriber, then an Incident shall be raised by DCCKICA Personnel.

(c) Where any DCCKI Certificate Signing Request satisfies the requirements set out in the DCCKI RAPP, this Policy, and any other provision of the Code, the DCCKICA shall Issue the DCCKI Certificate that was the subject of that DCCKI Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(a) Provision is made in the DCCKI RAPP in relation to the agreed elapsed time for the processing of DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications made in accordance with this Policy.

4.3 DCCKI Certificate Issuance

4.3.1 DCCKICA actions during certificate Issuance

(a) The Root DCCKICA shall Issue a DCCKICA Certificate only in accordance with the provisions of this Policy and the DCCKI CPS.

(b) The DCCKICA shall Issue a DCCKI Infrastructure Certificate or a Personnel Authentication Certificate only in accordance with the provisions of this Policy and the DCCKI RAPP and:

(i) in the case of DCCKI Infrastructure Certificates, only in response to a DCCKI Certificate Signing Request made by a DCCKI Eligible Subscriber; and

(ii) in the case of Personnel Authentication Certificates, only following the creation of a DCCKI Certificate Signing Request by the DCCKICA in response to a Personnel Authentication Certificate Application made by a User Personnel of a DCCKI Eligible Subscriber via the Personnel Credentials Interface.

(c) The DCCKICA shall ensure that each DCCKI Certificate that is Issued by it contains information that:

(i) it has verified to be correct and complete; and

(ii) is consistent with the information in the DCCKI Certificate Signing Request.

4.3.2 Notification to DCCKI Eligible Subscriber by the DCCKICA of Issuance of Certificate

(a) Provision is made in the DCCKI RAPP for the DCCKICA to notify a DCCKI Eligible Subscriber of the Issuance of a DCCKI Certificate which was the subject of a DCCKI Certificate Signing Request or Personnel Authentication Certificate Application made by it.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

(a) Provision is made in the DCCKI RAPP to:

(i) specify the means by which an DCCKI Eligible Subscriber may clearly indicate to the DCCKICA its rejection of a DCCKI Certificate which has been Issued to it; and

(ii) specify the circumstances in which a DCCKI Eligible Subscriber is treated as a DCCKI Subscriber in relation to a DCCKI Certificate

(b) Further provision in relation to subscribing for or rejecting DCCKI Certificates is made in Section L13.46 (Subscribing for or rejecting DCCKI Certificates) of the Code.

4.4.2 Publication of Certificates by the DCCKICA

(a) Following Issuance, the DCCKICA shall lodge a copy of each Root DCCKICA Certificate, each EII DCCKICA Certificate and each DCCKI Infrastructure Certificate in the DCCKI Repository.

(b) Further provision in relation to the publication of DCCKI Certificates is made in section 2of this Policy and in Section L13.17 (the DCCKI Repository Service) of the Code.

4.4.3 Notification of Certificate Issuance by the DCCKICA to Other Entities

(a) The DCCKICA shall give explicit notice of the Issue of a DCCKI Certificate only to the DCCKI Eligible Subscriber who submitted the DCCKI Certificate Signing Request or Personnel Authentication Certificate Application.

4.5 Key Pair and Certificate Usage

4.5.1 DCCKI Authorised Subscriber Private Key and Certificate Usage

(a) Provision for restrictions on the use by DCCKI Authorised Subscribers of Private Keys in respect of DCCKI Certificates is made in:

(i) Section G5.24 (the User Information Security Management System) of the Code;

(ii) Section L13 (DCC Key Infrastructure) of the Code;

(iii) this Policy; and

(iv) the DCCKI Certification Practice Statement.

4.5.2 DCCKI Relying Party Public Key and Certificate Usage

(a) Provision in relation to reliance that may be placed on a DCCKI Certificate is made in Section L13.49 (the DCCKI Relying Party Obligations) of the Code.

4.6 Certificate Renewal

4.6.1 Circumstances of Certificate Renewal

(a) This Policy does not support the renewal of DCCKI Certificates.

(b) The DCCKICA may only replace, and shall not renew, any DCCKI Certificate.

4.6.2 Circumstances of Certificate Replacement

(a) A DCCKI Certificate replacement may occur:

(i) where the request for DCCKI Certificate replacement relates to normal business activity, in which case the process set out in the DCCKI RAPP shall apply;

(ii) where suspicion of Compromise is reported for a DCCKI Certificate that has been Issued, in which case the matter shall be managed through the Incident Management Policy and in accordance with the DCCKI RAPP; or

(iii) where Compromise of the EII DCCKICA Private Key, UI DCCKICA Private Key, or Root DCCKICA Key is suspected, DCCKICA Personnel shall immediately raise a Major Security Incident, and follow the associated procedures outlined within the DCCKI CPS and the Incident Management Policy.

4.6.3 Who May Request a Replacement Certificate

See section 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See section 4.2 of this Policy.

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See section 4.3 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See section 4.4 of this Policy.

4.6.7 Publication of a Replacement Certificate by the DCCKICA

See section 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the DCCKICA to Other Entities

See section 4.4.3 of this Policy.

4.7 Certificate Re-Key

(a) This Policy does not support Certificate Re-Key.

4.7.1 Circumstances for Certificate Re-Key

[Not applicable]

4.7.2 Who may request Certificate re-key

[Not applicable]

4.7.3 Processing Certificate Re-Keying Requests

[Not applicable]

4.7.4 Notification of New Certificate Issuance to Subscriber

[Not applicable]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[Not applicable]

4.7.6 Publication of the Re-Keyed Certificate by the DCCKICA

[Not applicable]

4.7.7 Notification of Certificate Issuance by the DCCKICA to Other Entities

[Not applicable]

4.8 Certificate Modification

(a) This Policy does not support DCCKI Certificate modification.

4.8.1 Circumstances for Certificate Modification

[Not applicable]

4.8.2 Who may request Certificate Modification

[Not applicable]

4.8.3 Processing Certificate Modification Requests

[Not applicable]

4.8.4 Notification of New Certificate Issuance to Subscriber

[Not applicable]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[Not applicable]

4.8.6 Publication of the Modified Certificate by the DCCKICA

[Not applicable]

4.8.7 Notification of Certificate Issuance by the DCCKICA to Other Entities

[Not applicable]

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

(a) In accordance with the DCCKI RAPP, the DCCKICA may revoke DCCKI Certificates that have been Issued to a DCCKI Subscriber:

(i) at that DCCKI Subscriber's request, as described in the DCCKI RAPP;

(ii) in accordance with Incident Management processes or, in the event of a Major Security Incident, where DCC reasonably believes that Compromise of that DCCKI Subscriber's Private Key has occurred;

(iii) where an organisation ceases to be a DCCKI Eligible Subscriber in relation to that DCCKI Certificate;

(iv) in the circumstances described in Section H10.1 (Emergency Suspension of Services) of the Code; and

(v) where a request is received by DCC from the Panel in the circumstances set out in Section M8 (Suspension, Expulsion, and Withdrawal) of the Code that would result in a requirement to revoke one or more DCCKI Certificates that have been Issued to that DCCKI Subscriber.

4.9.2 Who can Request Revocation

(a) In accordance with the DCCKI RAPP and section 4.9.1 of this Policy, the following may request the revocation of DCCKI Certificates:

(i) a DCCKI Authorised Subscriber in relation to DCCKI Infrastructure Certificates for which it is a DCCKI Subscriber; and

(ii) the DCC.

4.9.3 Procedure for Revocation Request

(a) Provision is made in the DCCKI RAPP in relation to the procedure for submitting and processing a DCCKI Certificate Revocation Request.

4.9.4 Revocation Request Grace Period

(a) Provision is made in the DCCKI RAPP in relation to the grace period for requesting a DCCKI Certificate revocation.

4.9.5 Time within which the DCCKICA must process the Revocation Request

(a) The DCCKICA shall ensure that it processes all DCCKI Certificate Revocation Requests as soon as reasonably practicable following receipt and in accordance with the procedures set out in the DCCKI RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(a) Provision in relation to the revocation checking requirements for DCCKI Relying Parties is made in Section L13 (DCC Key Infrastructure) of the Code.

4.9.7 CRL Issuance Frequency

(a) The DCCKICA shall ensure that an up to date version of any DCCKI ARL is lodged in the DCCKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of a EII DCCKICA Certificate or UI DCCKICA Certificate.

(b) Each version of the DCCKI ARL shall be valid until the date which is 13 months after the date on which that version is lodged in the DCCKI Repository or until it is subsequently replaced with an updated version.

(c) The DCCKICA shall ensure that each up to date version of the DCCKI ARL:

(i) continues to include each relevant revoked EII DCCKICA Certificate and relevant revoked UI DCCKICA Certificate until such time as the Validity

Period of that EII DCCKICA Certificate or UI DCCKICA Certificate has expired; and

(ii) does not include any revoked EII DCCKICA Certificate or revoked UI DCCKICA Certificate after the Validity Period of that EII DCCKICA Certificate or UI DCCKICA Certificate has expired.

(d) The EII DCCKICA shall ensure that an up to date version of the EII DCCKICA CRL is lodged in the DCCKI Repository:

(i) at least once in every period of twelve months; and

(ii) within one hour on the revocation of a DCCKI Infrastructure Certificate.

(e) The EII DCCKICA shall ensure that each up to date version of the EII DCCKICA CRL:

(i) continues to include each relevant revoked DCCKI Infrastructure Certificate until such time as the Validity Period of that DCCKI Infrastructure Certificate has expired; and

(ii) does not include any revoked DCCKI Infrastructure Certificate after the Validity Period of that DCCKI Infrastructure Certificate has expired.

(f) The EII DCCKICA shall ensure that the EII DCCKICA CRL contains a non-critical entry extension which identifies the reason for the revocation of each DCCKI Infrastructure Certificate listed on it in accordance with RFC 5280 or an equivalent cryptographic standard.

(g) The UI DCCKICA shall not lodge a version of the UI DCCKICA CRL in the repository.

4.9.8 Maximum Latency for DCCKI CRLs (if applicable)

(a) In accordance with section 4.9.7.

4.9.9 On-line Revocation/Status Checking Availability

[Not applicable]

4.9.10 On-line Revocation Checking Requirements

[Not applicable]

4.9.11 Other Forms of Revocation Advertisements Available

[Not applicable]

4.9.12 Special Requirements in the Event of Key Compromise

(a) See section 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

(a) This Policy does not support suspension of DCCKI Certificates.

4.9.14 Who can Request Suspension

[Not Applicable]

4.9.15 Procedure for Suspension Request

[Not Applicable]

4.9.16 Limits on Suspension Period

[Not Applicable]

4.10 Certificate Status Services

4.10.1 Operational Characteristics

[Not applicable]

4.10.2 Service Availability

[Not applicable]

4.10.3 Optional Features

[Not applicable]

4.11 End of Subscription

(a) Provision is made in the DCCKI RAPP in relation to end of subscription.

4.12 KEY ESCROW AND RECOVERY

(a) This Policy does not support Key Escrow.

(b) The DCCKICA shall not provide a Key Escrow service.

4.12.1 Key Escrow and Recovery Policies and Practices

[Not applicable]

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[Not applicable]

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

(a) The DCCKICA shall ensure that the DCCKICA Systems are operated in a sufficiently secure environment which shall at least satisfy the requirements set out in Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to physical controls including in particular provisions designed to ensure that :

(i) all of the physical locations in which the DCCKICA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom;

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom;

(iv) the DCCKICA systems cannot be indirectly accessed from any location outside the United Kingdom;

(v) the Root DCCKICA shall operate as a secure offline entity that is Separate from the rest of the DCC Systems; and

(vi) all Private Keys used to support the DCCKICA are generated, stored and processed within the cryptographic envelope of a Cryptographic Module which meets the FIPS 140-2 Level 3or equivalent cryptographic standard.

(c) The functions of the DCCKI Registration Authority shall securely interoperate with the other operational elements of the DCCKICA, as detailed in the DCCKI CPS.

5.1.2 Physical access

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to access control including in particular provisions designed to:

(i) establish and maintain controls such that only appropriately authorised personnel may have unescorted physical access to DCCKICA Systems;

(ii) ensure that any unauthorised personnel may have physical access to DCCKICA Systems only if appropriately authorised and supervised;

(iii) ensure that site access procedures are audited as part of both internal audits and third party audits carried out in accordance with ISO/IEC 27001;

(iv) ensure that all material in relation to cryptographic operation is securely managed; and

(v) ensure that removable media which contain sensitive data are kept in secure locations, managed through life and disposal and, accessible only to appropriately authorised individuals.

5.1.3 Power and air conditioning

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the DCCKICA Systems are situated.

5.1.4 Water exposure

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to water exposure at all physical locations in which the DCCKICA Systems are situated.

5.1.5 Fire prevention and protection

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DCCKICA Systems are situated.

5.1.6 Media storage

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to media storage at all physical locations in which the DCCKICA Systems are situated.

5.1.7 Waste disposal

(a) The DCCKICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions is securely disposed of in accordance with HMG Information Assurance Standard No 5 or an equivalent standard.

5.1.8 Off-site backup

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to off-site back up and data management of data held in the DCCKICA Systems.

(b) The DCCKICA shall ensure that backups shall be made to support disaster recovery models as defined within the DCCKI CPS.

(c) The DCCKICA shall ensure that:

(i) regular backups of critical DCCKICA and DCCKI Registration Authority operational data relating to the Issuing of DCCKI Certificates are made;

(ii) appropriate backups of the Root DCCKICA are made on a periodic basis;

(iii) backup of cryptographic material used in support of the Root DCCKICA, EII DCCKICA and the UI DCCKICA shall be in line with manufacturer procedures and FIPS 140-2 Level 3 or an equivalent cryptographic standard; and

(iv) security of off-site storage shall be managed and implemented in alignment with security in place at the main locations.

5.2 Procedural controls

5.2.1 Trusted roles

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions designed to ensure that:

(i) trusted roles are managed in accordance with principle of least privilege, clearly defined role and access level;

(ii) allocated roles are pertinent to the required task;

(iii) roles and responsibilities are documented;

(iv) no individual member of DCCKICA Personnel is capable, by acting alone, of engaging in any action by means of which the DCCKICA Systems may be Compromised to a material extent;

(v) roles are implemented in line with best practice for a certification authority; and

(vi) multi-person controls are applied with respect to Root DCCKICA Private Key management.

5.2.2 Number of persons required per task

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of DCCKICA Personnel;

(ii) the application of controls to the actions of all members of DCCKICA Personnel who are Privileged Persons, in particular:

(1) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions;

(2) identifying the number of roles that an individual may hold; and

(3) providing that the revocation of any DCCKICA Certificate is one such function; and

(iii) the DCCKICA shall apply such multi-person controls:

(1) in accordance with the operation and risk as identified with within the DCC Information Security Management System ;

(2) in accordance with best practice in the case of management of cryptographic material; and

(3) with respect to Root DCCKICA Private Key management.

5.2.3 Identification and authentication for each role

(a) All DCCKICA Personnel shall be required to authenticate via a strong two factor Authentication in accordance with Level 2 of the HMG Authentication Framework before they can access any facilities.

5.2.4 Roles requiring separation of duties

(a) The DCCKICA shall identify roles that require separation of duties for DCCKICA functions in line with industry best practice.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions that ensure separation of duties in roles requiring separation of duties.

5.3 Personnel controls

5.3.1 Qualification, experience and clearance requirements

(a) The DCCKICA shall ensure that all DCCKICA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions and non-disclosure agreements relevant to their roles;

(iii) have received appropriate training with respect to their duties; and

(iv) have, as a minimum, passed an HMG Security Check (SC) level of vetting, before commencing their roles.

5.3.2 Background check procedures

(a) The DCCKICA shall ensure that all DCCKICA Personnel with access to DCCKICA operations shall undergo formal security checks, as set out within the DCCKI CPS.

5.3.3 Training requirements

(a) See section 5.3.1 of this Policy.

5.3.4 Retraining frequency and requirements

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by DCCKICA Personnel.

5.3.5 Job rotation frequency and sequence

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by DCCKICA Personnel.

5.3.6 Sanctions for unauthorised actions

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by DCCKICA Personnel.

5.3.7 Independent contractor requirements

(a) The DCCKICA shall ensure that all contractors engaged by it adhere to requirements laid out in this section 5.3.

5.3.8 Documentation supplied to personnel

(a) The DCCKICA shall ensure that all DCCKICA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the DCCKI CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of events recorded

(a) The DCCKICA shall ensure that:

(i) the DCCKICA Systems record all relevant systems activity in Audit Logs;

(ii) the DCCKI CPS incorporates a comprehensive list of all events that are to be recorded in an Audit Log in relation to the activities of DCCKICA Personnel and the use of DCCKICA equipment which shall include access, both authorised and violations; and

(iii) activities in relation to the DCCKI Registration Authority, are logged in an appropriate manner by the DCCKICA.

5.4.2 Frequency of processing log

(a) DCCKICA audit logging shall:

(i) operate at all times within the DCCKICA Systems; and

(ii) ensure that audit monitoring of the DCCKICA Systems is in compliance with the protective monitoring requirements of DCC Systems.

(b) The DCCKI CPS shall incorporate provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by the DCCKICA in response to types of events recorded in the Audit Log.

5.4.3 Retention period for Audit Log

(a) The DCCKICA shall retain an Audit Log that incorporates, on any given date, a record of all DCCKICA System events occurring during a period of at least twelve months prior to that date.

(b) A copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period shall be archived in accordance with the requirements of section 5.5 of this Policy.

(c) The DCCKICA shall ensure that the DCCKI CPS makes provision for the specification of the Audit Log record.

5.4.4 Protection of audit log

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to access to the Audit Log, providing, in particular, that:

(i) access to those DCCKICA Audit Log Data (other than those relating to protective monitoring) must be limited to those members of DCCKICA Personnel who are specifically responsible for performing a system audit role in accordance with the DCCKI CPS;

(ii) to the extent to which the Audit Log is retained electronically, the DCCKICA event log Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with British Standard BS 10008:2008 (Evidential weight and legal admissibility of electronic information) or an equivalent standard; and

(iii) to the extent which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log backup procedures

(a) The DCCKICA shall ensure that the Data contained in the Audit Log are backed up on a daily basis or, if activity has taken place on the DCCKICA Systems only infrequently, such as in relation to the Root DCCKICA, in accordance with the schedule for the regular backup of the Data held on those DCCKICA Systems.

(b) The DCCKICA shall ensure that all DCCKI Data contained in the Audit Logs that are backed up are, during backup, held in accordance with the DCC Information Security Management System and protected to the same standard of protection as the primary copy of the Audit Log in accordance with section 5.4.4 of this Policy.

5.4.6 Audit collection system (internal or external)

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to event-causing subject

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any DCCKICA System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability assessments

(a) The DCCKICA shall carry out periodic vulnerability assessments covering the DCCKICA Systems with recorded corrective action.

5.5 Records archival

5.5.1 Types of records archived

(a) The DCCKICA shall ensure that it archives:

(i) relevant Audit Data in accordance with section 5.4 of this Policy;

(ii) records of all Data submitted to it by DCCKI Eligible Subscribers for the purposes of DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications;

(iii) records of all Data submitted to it by DCCKI Subscribers for the purposes of revocation or suspension of DCCKI Certificates; and

(iv) any other data specified in this Policy as requiring to be archived in accordance with this section 5.5 of this Policy.

(b) The DCCKICA shall ensure that all DCCKICA audit data are recorded in a standard format that is compliant with British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information) or an equivalent standard.

(c) The DCCKICA shall ensure that provision is made in the DCCKI CPS in relation to the specification of data to be archived.

5.5.2 Retention period for archive

(a) The DCCKICA shall ensure that all Data, excluding audit data, which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of archive

(a) The DCCKICA shall ensure that Data held in its Archive are protected against any unauthorised access, adequately protected against environmental threats such as temperature, humidity and magnetism and incapable of being modified or deleted.

5.5.4 Archive backup procedures

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its procedures for the backup of its Archive.

5.5.5 Requirements for Time-Stamping of records

(a) Provision in relation to Time-Stamping is made in section 6.8 of this Policy.

5.5.6 Archive collection system (internal or external)

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to maintaining internal and external archives.

5.5.7 Procedures to obtain and verify archive information

(a) The DCCKICA shall ensure that Data held in the Archive are stored in a readable format during their retention period and that the Data remain accessible at all times during the retention period.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the periodic verification by the DCCKICA of the Data held in the Archive.

5.6 Key changeover

5.6.1 EII DCCKICA key changeover

(a) Where the DCCKICA ceases to use a EII DCCKICA Private Key after the expiry of the Validity Period of a EII DCCKICA Certificate, it shall:

(i) not revoke the related EII DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the EII DCCKICA Private Key);

(ii) generate a new Key Pair following key generation procedures, generate a DCCKI Certificate Signing Request in relation to the EII DCCKICA Certificate and submit to the Root DCCKICA for signing and Issuance;

(iii) in its role as the DCCKICA:

(1) Issue a new relevant EII DCCKICA Certificate;

(2) confirm acceptance of the EII DCCKICA Certificate once Issued; and

(3) promptly lodge that EII DCCKICA Certificate in the DCCKI Repository;

(iv) ensure that any relevant DCCKI Infrastructure Certificate subsequently Issued by the EII DCCKICA is Issued using the EII DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued EII DCCKICA Certificate ; and

(v) verifiably destroy the Private Key Material relating to the previous EII DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.2 UI DCCKICA key changeover

(a) Where the DCCKICA ceases to use a UI DCCKICA Private Key after the expiry of the Validity Period of a UI DCCKICA Certificate, it shall:

(i) not revoke the related UI DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the UI DCCKICA Private Key);

(ii) generate a new Key Pair following key generation procedures, generate a DCCKI Certificate Signing Request in relation to the UI DCCKICA Certificate, and submit to the Root DCCKICA for signing and Issuance;

(iii) Issue a new relevant UI DCCKICA Certificate in its role as the Root DCCKICA;

(iv) confirm acceptance of the UI DCCKICA Certificate once Issued;

(v) ensure that any relevant Personnel Authentication Certificate subsequently Issued by the UI DCCKICA is Issued using the UI DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued UI DCCKICA Certificate; and

(vi) verifiably destroy the Private Key Material relating to the previous UI DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.3 DCCKI Root Key changeover

(a) Where the Root DCCKICA ceases to use a Root DCCKICA Private Key after the expiry of the Validity Period of a Root DCCKICA Certificate, it shall:

(i) not revoke the related Root DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the Root DCCKICA Private Key);

(ii) generate a DCCKI Certificate Signing Request covering its own signing key and submit to itself for signing and Issuance.;

(iii) issue to itself a new relevant Root DCCKICA Certificate;

(iv) ensure that any relevant EII DCCKICA Certificate or UI DCCKICA Certificate subsequently Issued by the Root DCCKICA is Issued using the Root DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued Root DCCKICA Certificate; and

(v) verifiably destroy the Private Key Material relating to the previous Root DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates Business Continuity and Disaster Recovery Procedures which shall be designed to ensure the continuity or (where there has been unavoidable discontinuity) the recovery of the provision of

the DCCKI Services in the event of any Compromise of the DCCKICA Systems or major failure in the DCCKI processes.

(b) In the event of an Incident involving Compromise of the DCCKICA Systems, the DCCKICA shall:

(i) ensure that the Incident Management Policy is invoked;

(ii) not request revocation of any DCCKICA Certificate in the first instance but follow procedures defined in the DCCKI CPS;

(iii) not revoke Issued DCCKI Certificates in the first instance but follow procedures defined in the DCCKI CPS; and

(iv) treat the event as a Major Security Incident.

(c) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any EII DCCKICA Private Key or any UI DCCKICA Private Key or any part of the DCCKICA Systems is Compromised.

5.7.2 Computing resources, software and/or data are corrupted

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the steps to take to manage computing resources and software, and to deal with corrupted data.

5.7.3 Entity private key compromise procedures

(a) See section 5.7.1 of this Policy.

5.7.4 Business continuity capabilities after a disaster

(a) The DCCKICA shall ensure that Business Continuity and Disaster Recovery Procedures are invoked in accordance with section 5.7 of this Policy and the DCCKI CPS.

5.7.5 DCCKICA and DCCKI Registration Authority termination

(a) DCC shall at all times fulfil the functions of the DCCKICA and DCCKI Registration Authority.

6 TECHNICAL SECURITY CONTROLS

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates detailed provision in relation to technical security controls so that such technical security controls are defined, documented and managed for the purpose of exercising its functions as Root DCCKICA, EII DCCKICA, UI DCCKICA and DCCKI Registration Authority.

6.1 Key pair generation and installation

6.1.1 Key pair generation

(a) The DCCKICA shall ensure that all DCCKICA Key Pairs are generated:

(i) in a protected environment to be compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard;

(ii) using multi-person control, such that no single person is capable of generating any DCCKICA Private Key; and

(iii) in accordance with the DCCKI CPS, with records from the event to be held as archive.

(b) The DCCKICA shall ensure that Key Pairs associated with Personnel Authentication Certificates are generated in accordance with the DCCKI CPS.

(c) The DCCKICA shall not generate any Key Pairs other than a Key Pair associated with a DCCKICA Certificate or a Key Pair associated with a Personnel Authentication Certificate.

6.1.2 Private Key delivery to DCCKI Subscriber

(a) The DCCKICA shall ensure that the DCCKI RAPP makes provision for the generation of a Key Pair associated with a Personnel Authentication Certificate for delivery to a DCCKI Eligible Subscriber by the UI DCCKICA.

6.1.3 Public Key delivery to certificate issuer

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the mechanism by which Public Keys of DCCKI Eligible Subscribers are delivered to or generated by, the DCCKICA for the purpose of the exercise of its functions as the Root DCCKICA, EII DCCKICA and UI DCCKICA.

6.1.4 DCCKICA Public Key delivery to Relying Parties

(a) The DCCKICA shall ensure that the DCCKI RAPP incorporates provisions in relation to how Root DCCKICA Public Keys and EII DCCKICA Public Keys shall be delivered to Relying Parties, and in particular that these are placed in the DCCKI Repository following Issuance.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to how UI DCCKICA Public Keys shall be delivered to Relying Parties, and in particular that UI DCCKICA Public Keys:

(i) are delivered in a secure fashion and in a manner that precludes substitution attacks;

(ii) may be delivered as specified in a certificate validation or path discovery policy file; and

(iii) that are part of an updated Key Pair may be distributed as a self-signed certificate, and as a new DCCKICA Certificate.

6.1.5 Key sizes

(a) The Root DCCKICA shall employ RSA 4096 bit Private Keys, with a SHA256 hashing algorithm.

(b) The EII DCCKICA shall employ RSA 2048 bit Private Keys, with a SHA256 hashing algorithm.

(c) The UI DCCKICA shall employ RSA 2048 bit Private Keys, with a SHA256 hashing algorithm.

6.1.6 Public Key parameters generation and quality checking

(a) The DCCKICA shall ensure that any Public Key used for the purposes of this Policy shall:

(i) be generated using the required key parameters, as defined in the DCCKI Certificate Profiles in Annex B to this policy, which are in accordance with FIPS 186-4 or an equivalent cryptographic standard; and

(ii) ensure that the quality of the generated key parameters is verified in accordance with FIPS 186-4 or an equivalent cryptographic standard.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

(a) The DCCKICA shall ensure that each DCCKI Certificate that is Issued by it shall include key usage extension fields that specify the intended use of that DCCKI Certificate and technically limit the certificate's functionality in X.509v3 compliant software.

(b) The DCCKICA shall set key usage bits or assert extended key usage OIDs for each DCCKI Certificate type in accordance with the relevant DCCKI Certificate Profile defined in Annex B to this Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

(a) The DCCKICA shall ensure that all DCCKICA Private Keys are protected within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard at all times.

(b) The DCCKICA shall ensure that the key encryption key used to protect the DCCKICA Private Keys is only stored within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

(c) DCCKI Authorised Subscribers shall ensure that all Private Keys provided to them by the DCCKICA or generated by them are protected in accordance with and subject to any conditions specified within Sections G (Security) and L (Smart Metering Key Infrastructure and DCC Key Infrastructure) of the Code, the DCCKI Interface Design Specification and the DCCKI Code of Connection.

6.2.2 Private Key (key (m out of n) multi-person control

(a) The DCCKICA shall ensure that multi-person controls are applied for the generation and management of DCCKICA Private Keys.

(b) DCCKI Authorised Subscribers shall implement multi-person control, where applicable, in accordance with their Information Security Management System.

(c) Private Keys associated with Personnel Authentication Certificates shall not be subject to multi-person control.

6.2.3 Private Key escrow

(a) Key Escrow shall not be used for the DCCKICA.

6.2.4 Private Key backup

(a) The DCCKICA shall back up the DCCKICA Private Keys using multi-person control and shall protect all copies in the same manner as the originals, and in accordance with provisions set out within the DCCKI CPS.

(b) The backup shall be available for use during disaster recovery as described within the DCCKI CPS.

6.2.5 Private Key archival

(a) Private Key archival shall not be implemented for the DCCKICA.

6.2.6 Private Key transfer into or from a Cryptographic Module

(a) The DCCKICA shall ensure that no DCCKICA Private Key is transferred or copied other than:

(i) for the purposes of:

(1) backup;

(2) restoration; or

(3) addition of new hardware, software, or firmware to a Cryptographic Module; and

(ii) in any event, in accordance a level of protection that is compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

(b) The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates:

i. are transferred from the DCCKICA Systems to the systems of DCCKI Eligible Subscribers in a PKCS#12 format and protected with a password; and

ii. following such transfer, that any copies held are verifiably destroyed by the DCCKICA.

(c) The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates for use by Administration Users are generated on a Personal Identity Verification (PIV) compliant Smart Card Token.

6.2.7 Private Key Storage on Cryptographic Module

(a) The DCCKICA shall ensure that DCCKICA Private Keys are stored within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

6.2.8 Method of Activating Private Key

(a) The DCCKICA shall ensure that:

(i) the Cryptographic Module in which any DCCKICA Private Key is stored may be accessed only by an authorised member of DCCKICA Personnel; and

(ii) the requirements of the Cryptographic Module, including switching on and authenticating themselves to the Cryptographic Module shall be undertaken by the DCCKICA Personnel.

6.2.9 Method of deactivating Private Key

(a) The DCCKICA shall ensure that any DCCKICA Private Keys shall be capable of being deactivated by means of the DCCKICA Systems, at least by:

(i) the actions of:

(1) turning off the power;

(2) logging off; or

(3) carrying out a system reset;

or;

(ii) following key changeover in accordance with procedures defined in section 5.6 of this Policy.

6.2.10 Method of destroying Private Key

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions for a set of procedures covering the destruction of DCCKICA Private Keys and Private Keys associated with Personnel Authentication Certificates delivered to User Personnel of DCCKI Eligible Subscribers. These shall be in accordance with the guidelines provided by the cryptographic manufacturer and compliant with UK Government publication 'IS4 - Management of Cryptographic Systems' or an equivalent cryptographic standard.

(b) The DCCKI CPS shall incorporate provisions for procedures for secure back up of cryptographic material.

(c) Positive decisions on significant key management life cycle events shall be managed directly by the DCCKI PMA.

(d) DCCKI Subscribers shall ensure that their User Information Security Management System includes procedures in relation to the secure management of all Secret Key Material provided to them by the DCCKICA in relation to this Policy. Such procedures shall in particular make provision for:

(i) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to the revocation of the DCCKI Certificate associated with the Secret Key Material; and

(ii) the destruction of any Smart Card Token beyond reasonable use once it is no longer to be used, in accordance with this Policy or as otherwise set out in the Code.

6.2.11 Cryptographic module rating

(a) Any Cryptographic Module used in support of the DCCKICA Systems shall meet the module rating specified within sections 6.2.1 and 6.2.7 of this Policy.

6.3 Other aspects of Key Pair management

6.3.1 Public Key archival

(a) Public Key archival shall be managed in accordance with section 5.5 of this Policy and in line with DCCKI Repository management requirements as detailed within the DCCKI CPS.

6.3.2 Certificate operational periods and Key Pair usage periods

(a) Annex B to this Policy specifies the detail for Key Pair usage, Validity Period and categories.

(b) The DCCKICA shall ensure that the Validity Period of each DCCKI Certificate Issued by it shall be as follows:

(i) in the case of a Root DCCKICA Certificate, 20 years;

(ii) in the case of a EII DCCKICA Certificate, or UI DCCKICA Certificate, 10 years; and

(iii) in the case of a DCCKI Infrastructure Certificate or Personnel Authentication Certificate, 3 years.

(c) The DCCKICA shall ensure that no DCCKICA Private Key can be used after the end of the Validity Period of the DCCKICA Certificate containing the Public Key which is associated with that Private Key.

6.4 Activation Data

6.4.1 Activation data generation and installation

(a) The DCCKICA shall ensure that any Cryptographic Module within which a DCCKICA Private Key is held has Activation Data that apply sufficient security protection to protect that DCCKICA Private Key.

(b) Activation Data pertaining to the DCCKICA Private Key Material shall:

(i) have access controls applied as defined within the DCCKI CPS;

(ii) have key management lifecycle procedures applied as defined within the DCCKI CPS; and

(iii) have records generated, logged and archived on generation and each invocation.

6.4.2 Activation data protection

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the physical and logical controls to be employed to protect activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

(a) The DCC Information Security Management System shall define security technical requirements according to a risk assessment and risk treatment plan, or following corrective action that may result from an audit or IT health check service, which shall be undertaken by a CESG CHECK service provider.

6.5.2 Computer security rating

(a) This Policy makes no stipulation in relation to computer security rating.

6.6 Life cycle technical controls

6.6.1 System development controls

(a) The DCCKICA shall ensure that the DCCKI CPS makes provision regarding controls in relation to development of the DCCKICA Systems; and

(b) any such development of the DCCKICA Systems shall be made in accordance with DCC secure development policy as defined within the DCC Information Security Management System.

6.6.2 Security management controls

(a) The DCCKICA shall ensure that the DCCKI CPS, incorporates provisions which are designed to ensure that the DCCKICA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life cycle security controls

(a) See section 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Protection against attack

(a) The DCCKICA shall ensure that the DCCKICA systems are protected against attack in accordance with provisions made in the DCCKI CPS and by at least the following means:

(i) continual protective monitoring shall be enforced; and

(ii) access to the systems shall be on a least privilege principle for access.

(b) The DCCKICA Systems shall be designed and operated so as to detect and prevent:

(i) Denial of Service Events; and

(ii) unauthorised attempts to connect to them.

6.7.2 Health Check of DCCKICA Systems

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions for periodically scheduled assessments of the DCCKICA Systems by a CESG CHECK service provider to form part of the input to the risk management process.

6.8 Time-stamping

6.8.1 Use of time-stamping

(a) The DCCKICA shall ensure Time-Stamping takes place in relation to all DCCKI Certificates and other DCCKI activities that require an accurate record of time.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority in relation to any Time-Stamping on behalf of the DCCKICA.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

(a) The DCCKICA shall use only the DCCKI Certificate Profiles in Annex B to this Policy, and in accordance with the DCCKI CPS.

7.1.1 Version number(s)

(a) The version field in the DCCKI Certificates shall have a value of 2, indicating X.509v3 certificates.

7.1.2 Certificate extensions

(a) In compliance with RFC 5280, the inclusion of the following certificate extensions shall be utilised:

(i) authorityKeyIdentifier NOT CRITICAL;

(ii) authorityInfoAccess NOT CRITICAL, for EII DCCKICA Certificates and DCCKI Infrastructure Certificates only;

(iii) basicConstraints CRITICAL;

(iv) extKeyUsage CRITICAL;

(v) keyUsage CRITICAL;

(vi) certificatePolicies NOT CRITICAL;

(vii) cRLDistributionPoints NOT CRITICAL;

(viii) subjectAltName NOT CRITICAL;

(ix) subjectKeyIdentifier NOT CRITICAL.

7.1.3 Algorithm object identifiers

(a) No stipulation.

7.1.4 Name forms

(a) The DCCKI CPS sets out the name forms utilised.

7.1.5 Name constraints

(a) The DCCKI CPS sets out the applicable Name Constraints.

7.1.6 Certificate policy object identifier

(a) No stipulation.

7.1.7 Usage of Policy Constraints extension

[Not applicable].

7.1.8 Policy qualifiers syntax and semantics

[Not applicable].

7.1.9 Processing semantics for the critical Certificate Policies extension

[Not applicable].

7.2 CRL profile

7.2.1 Version number(s)

(a) The version field in the certificate shall state 1, indicating X.509v2 CRL.

7.2.2 CRL and CRL entry extensions

(a) No stipulation.

7.3 OCSP profile

(a) The DCCKICA shall not employ an OCSP.

7.3.1 Version number(s)

[Not applicable].

7.3.2 OCSP extensions

[Not applicable].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

(a) The DCC Information Security Management System shall include provisions relating to the compliance and audit of the DCCKICA, and DCCKICA Systems that shall be in accordance with relevant provisions made in Section G (Security) of the Code.

8.1 Frequency or circumstances of assessment

(a) The DCCKICA shall be subject to assessment schedules set out in the DCC Information Security Management System, with such assessments taking place at least annually.

8.2 Identify/qualifications of assessor

(a) In accordance with the DCC Information Security Management System, the DCCKICA shall be subject to independent assessment by a UKAS approved certification body whose qualifications shall include ISO/IEC 27001 Lead Audit and IRCA Registration.

8.3 Assessor's relationship to assessed entity

(a) Any UKAS approved certification body carrying out independent assessments shall be subject to UKAS scrutiny with regards to independence of the chosen assessor.

8.4 Topics covered by assessment

(a) The DCC Information Security Management System shall cover all aspects of the DCCKI Service and the DCCKI Repository Service, including but not limited to:

(i) the DCCKI Repository;

(ii) the Root DCCKICA;

(iii) the UI DCCKICA;

(iv) the EII DCCKICA;

(v) The DCCCKI Registration Authority;

(vi) Cryptographic Modules relied upon in support of the service; and

(vii) this Policy and its supporting DCCKI RAPP and DCCKI CPS.

8.5 Actions taken as a result of deficiency

(a) Any deficiencies identified through third party assessment, internal audit or IT health check shall be raised as non-conformances and be processed through risk assessment and processes defined within the DCC Information Security Management System.

8.6 Communication of results

(a) The DCCKICA shall make the results of corrective action available to the DCCKI PMA.

9 OTHER BUSINESS AND LEGAL MATTERS

(a) In so far as provision is made in relation to all the matters referred to in this section, it is found in the DCC Licence and the provisions of the Code.

9.1 Fees

[Not applicable].

9.1.1 Certificate Issuance or renewal fees

[Not applicable].

9.1.2 Device certificate access fees

[Not applicable].

9.1.3 Revocation or status information access fees

[Not applicable].

9.1.4 Fees for other services

[Not applicable].

9.1.5 Refund policy

[Not applicable].

9.2 Financial responsibility

9.2.1 Insurance coverage

(a) See the statement at the beginning of this section.

9.2.2 Other assets

(a) See the statement at the beginning of this section.

9.2.3 Insurance or warranty coverage for subscribers and subjects

(a) See the statement at the beginning of this section.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

(a) See the statement at the beginning of this section.

9.3.2 Information not within the scope of confidential information

(a) See the statement at the beginning of this section.

9.3.3 Responsibility to protect confidential information

(a) See the statement at the beginning of this section.

9.4 Privacy of personal information

9.4.1 Privacy plan

(a) See the statement at the beginning of this section.

9.4.2 Information treated as private

(a) See the statement at the beginning of this section.

9.4.3 Information not deemed private

(a) See the statement at the beginning of this section.

9.4.4 Responsibility to protect private information

(a) See the statement at the beginning of this section.

9.4.5 Notice and consent to use private information

(a) See the statement at the beginning of this section.

9.4.6 Disclosure pursuant to judicial or administrative process

(a) See the statement at the beginning of this section.

9.4.7 Other information disclosure circumstances

(a) See the statement at the beginning of this section.

9.5 Intellectual property rights

(a) See the statement at the beginning of this section.

9.6 Representations and warranties

9.6.1 CA representations and warranties

(a) See the statement at the beginning of this section.

9.6.2 RA representation and warranties

(a) See the statement at the beginning of this section.

9.6.3 Subscriber representations and warranties

(a) See the statement at the beginning of this section.

9.6.4 Relying party representations and warranties

(a) See the statement at the beginning of this section.

9.7 Representations and warranties of other participants

(a) See the statement at the beginning of this section.

9.8 Disclaimers of warranties

(a) See the statement at the beginning of this section.

9.9 Limitations of liability

(a) See the statement at the beginning of this section.

9.10 Indemnities

(a) See the statement at the beginning of this section.

9.11 Term and termination

9.11.1 Term

(a) See the statement at the beginning of this section.

9.11.2 Termination

(a) See the statement at the beginning of this section.

9.11.3 Effect of termination and survival

(a) See the statement at the beginning of this section.

9.12 Individual notices and communications with participants

(a) See the statement at the beginning of this section.

9.13 Amendments

9.13.1 Procedure for amendment

(a) See the statement at the beginning of this section.

9.13.2 Notification mechanism and period

(a) See the statement at the beginning of this section.

9.13.3 Circumstances under which OID must be changed

(a) See the statement at the beginning of this section.

9.14 Dispute resolution provisions

(a) See the statement at the beginning of this section.

9.15 Governing law

(a) See the statement at the beginning of this section.

9.16 Compliance with applicable law

(a) See the statement at the beginning of this section.

9.17 Miscellaneous provisions

9.17.1 Entire agreement

(a) See the statement at the beginning of this section.

9.17.2 Assignment

(a) See the statement at the beginning of this section.

9.17.3 Severability

(a) See the statement at the beginning of this section.

9.17.4 Enforcement (attorneys' fees and waiver of rights)

(a) See the statement at the beginning of this section.

9.17.5 Force Majeure

[Not applicable].

9.18 Other provisions

(a) See the statement at the beginning of this section.

ANNEX A DEFINED TERMS

In this Policy, except where the context otherwise requires:

- expressions defined in Section A (Definitions and Interpretation) of the Code have the same meaning as is set out in that section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A (Definitions and Interpretation)of the Code and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Definitions for this Policy

Administration User	has the meaning given to the term Administration User in Appendix [TBC] of the Code (Self Service Interface Code of Connection)
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "Archives" and "Archived" shall be interpreted accordingly)
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy
Authentication	means the process of establishing that an individual, DCCKI Certificate, system or organisation is who or what they or it claims or is claimed to be (and "Authenticate" shall be interpreted accordingly)
Business Continuity and Disaster Recovery Procedure	means that part of the Incident Management Policy which describes the business continuity and disaster recovery procedures applicable to the DCCKI Services.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.

DCCKI Authorised Responsible Officer (or **DCCKI ARO)**	means an individual that has successfully completed the process for becoming (and remains) a DCCKI ARO on behalf of a Party or RDP in accordance with the DCCKI RAPP.
DCCKI Authorised Subscriber	means (in relation to DCCKICA Certificates), the DCC or (in relation to DCCKI Infrastructure Certificates and Personnel Authentication Certificates), a Party or Registration Data Provider that: (i) has successfully completed the enrolment procedures to become a DCCKI Authorised Subscriber as set out in the DCCKI RAPP; (ii) continues to have at least one (1) DCCKI SRO currently appointed in accordance with the procedures set out in the DCCKI RAPP; (iii) continues to have at least one (1) DCCKI ARO currently appointed in accordance with the procedures set out in the DCCKI RAPP; (iv) has not ceased to be a DCCKI Authorised Subscriber in accordance with any other provision of the Code; and (v) and in the case of the DCC only, subject to any alternative provisions in the DCCKI CPS.
DCCKI Authority Revocation List (or DCCKI ARL)	means a list, produced by the Root DCCKICA, of all EII DCCKICA Certificates that have been revoked in accordance with this Policy.
DCCKI Certificate	has the meaning given to that expression in section 1.1 of this Policy
DCCKI Certificate Profile	means a table bearing that title in Annex B to this Policy and specifying the parameters to be contained within a DCCKI Certificate

DCCKI Certificate Revocation Request	means a request for the revocation of a DCCKI Certificate by the DCCKICA, submitted by the DCCKI Subscriber for that DCCKI Certificate to the DCCKICA in accordance with the DCCKI RAPP and this Policy.
DCCKI Certification Authority (or DCCKICA)	means the Certification Authority for the DCCKI, meaning the DCC, acting in this capacity and exercising the functions of (a) the Root DCCKICA; (b) the EI DCCKICA; (c) the UI DCCKICA; and (d) the DCCKI Registration Authority.
DCCKI Infrastructure Certificate	means a certificate in the form set out in the DCCKI Infrastructure certificate profile in accordance with Annex B to this Policy, and Issued by the EII DCCKICA in accordance with this Policy or the DCCKI CPS for the purposes set out in section 1.4.1 (e) of this Policy.
DCCKI Policy Management Authority (or DCCKI PMA)	means the DCC acting in this capacity for the purposes of administering this Policy and related matters.
DCCKI Registration Authority	means the DCCKI CA exercising the function of receiving and processing DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications made in accordance with the DCCKI RAPP.
DCCKI Registration Authority Manager	means any person who may be identified as such in accordance with the DCCKI RAPP.
DCCKI Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCCKI Registration Authority.

DCCKI Senior Responsible Officer (or **DCCKI SRO)**	means an individual that has successfully completed the process for becoming (and remains) a DCCKI SRO on behalf of a Party, or RDP in accordance with the DCCKI RAPP.
DCCKICA Certificate	means, as the context requires, either: (a) the Root DCCKICA Certificate; (b) an EII DCCKICA Certificate; or (c) an UI DCCKICA Certificate.
DCCKICA Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCCKICA.
DCCKICA Private Key	means a Private Key which is stored by the DCCKICA acting in its capacity as either the Root DCCKICA, the EII DCCKICA or the UI DCCKICA.
DCCKICA Systems	means the Systems used by the DCCKICA in relation to the DCCKI Services.
EII DCCKICA	means the External Infrastructure Issuing Authority, being a subordinate Issuing Authority for the DCCKICA whose functions are carried out by the DCCKICA.
EII DCCKICA Certificate	means a certificate of the form set out in the EII DCCKICA Certificate DCCKI Certificate Profile in accordance with Annex B to this Policy, and Issued by the Root DCCKICA to the EII DCCKICA in accordance with this Policy.
EII DCCKICA Certificate Revocation List (or EII DCCKICA CRL)	means a list, produced by the EII DCCKICA, of all DCCKI Infrastructure Certificates that have been revoked in accordance with this Policy.
EII DCCKICA Private Key	means a Private Key which is stored and managed by the DCCKICA acting in its capacity as the EII DCCKICA.
EII DCCKICA Public Key	means the Public Key of a Key Pair related to a EII DCCKICA Certificate.

Identity Provider Service	has the meaning given to that term in the Self Service Interface Code of Connection.
Issue	means the act of the DCCKICA acting in accordance with this Policy, and in its capacity as the Root DCCKICA, the EII DCCKICA or the UI DCCKICA as the context requires, of creating and signing a Certificate which contains the information set out in the relevant DCCKI Certificate Profile in Annex B to this Policy (and "Issuance", "Issued" and "Issuing" shall be interpreted accordingly).
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or **OID)**	means an object identifier assigned by the Internet Address Naming Authority.
Personnel Authentication Certificate	means a certificate in the form set out in the Personnel Authentication Certificate DCCKI Certificate Profile in Annex B to this Policy, and Issued by the UI DCCKICA in accordance with this Policy.
Personnel Authentication Certificate Application	means an application for a Personnel Authentication Certificate made via the Personnel Credentials Interface.
Personnel Credentials Interface	means the interface that allows for the activation of user accounts, the submission of Personnel Authentication Certificate Applications, and the provision of Personnel Authentication Certificates to persons.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Public Key	shall have the meaning ascribed to that term in the definition of Key Pair in Section A (Definitions and Interpretation) of the Code.

Root DCCKICA	means the DCC exercising the function of Issuing the Root DCCKI Certificate and other DCCKI CA Certificates to the EI DCCKICA and UIDCCKI, and storing and managing Private Keys associated with that function.
Root DCCKICA Certificate	means a certificate of the form set out in the Root DCCKI Certificate DCCKI Certificate Profile in accordance with Annex A of this Policy and self-signed, and Issued, by the Root DCCKICA in accordance with this Policy.
Root DCCKICA Private Key	means the Private Key which is stored and managed by the DCCKICA acting in its capacity as the Root DCCKICA.
Root DCCKICA Public Key	means the Public Key of a Key Pair related to the Root DCCKICA Certificate.
SAML	means Security Assertion Markup Language, being a standard that allows secure web domains to exchange user authentication and authorisation data.
Security Related Functionality	means the functionality of the DCCKICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of those Systems.

Subject	means: (a) in relation to a DCCKI Infrastructure Certificate, the Organisation identified in the 'Subject Name' field of the DCCKI Infrastructure Certificate DCCKI Certificate Profiles in Annex B to this Policy; (b) in relation to a Personnel Authentication Certificate, the person identified in the 'Subject Name' field of the Personnel Authentication Certificate DCCKI Certificate profile in Annex B to this Policy; or (c) in relation to an DCCKICA Certificate, the globally unique name of the Root DCCKICA, EII DCCKICA, or UI DCCKICA as identified in the 'Subject' field of the relevant DCCKI Certificate Profile in Annex B to this Policy.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a DCCKI Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority	means that part of the DCCKICA that: (a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and (b) relies on a time source that is: (i) accurate; (ii) determined in a manner that is independent of any other part of the DCCKICA Systems; and (iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.
Transport Layer Security (or TLS)	means TLS 1.2 as defined in the Internet Engineering Task Force (IETF) Request For Change (RFC) 5246
UI DCCKICA	means the User Issuing Authority, being a subordinate Issuing Authority for the DCCKICA whose functions are carried out by the DCCKICA.
UI DCCKICA Certificate	means a certificate in the form set out in the EII DCCKICA Certificate DCCKI Certificate Profile in accordance with Annex B to this Policy, and Issued by the Root DCCKICA to the EII DCCKICA in accordance with this Policy.
UI DCCKICA Private Key	means a Private Key which is stored and managed by the DCCKICA acting in its capacity as the EII DCCKICA.
UI DCCKICA Public Key	means the Public Key of a Key Pair related to a UI DCCKICA Certificate.
Validity Period	means, in respect of a DCCKI Certificate, the period of time for which that DCCKI Certificate is intended to be valid.

ANNEX B DCCKI CERTIFICATE PROFILES

End Entity Certificate Structure and Contents

This Annex B sets out requirements as to structure and content with which DCCKICA Certificates, DCCKI Infrastructure Certificates, and Personnel Authentication Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in and IETF RFC5280.

Common Requirements applicable to all DCCKI Certificates

All DCCKI Certificates that are validly authorised within the DCCKI shall:

- Be an X.509 v3 certificate;
- Have a Serial number of no more than 8 octets;
- have a valid notBefore field consisting of the time of issue, encoded as in ~~–~~section 4.1.2.5 of RFC5280;
- have a fixed expiration date in the notAfter field, encoded as in section 4.1.2.5 of RFC5280; and
- Contain an authorityKeyIdentifier and subjectKeyIdentifier in the form [0] KeyIdentifier. This extension shall be marked as non-critical, and calculated using method 2 of section 4.2.1.2 of RFC5280.

Requirements applicable to DCCKI Infrastructure Certificates only

A DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA for the purposes of establishing Transport Layer Security (TLS) and File Transfer Protocol over TLS (FTPS) communications over a DCC Gateway Connection shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of digitalSignature, and keyEncipherment ~~and keyAgreement~~. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- have an extendedKeyUsage extension (as per section 4.2.1.12 of RFC5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical;
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy; and
- have a Validity Period of 3 years.

A DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA for the purposes of establishing SAML Assertions to the DCC shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of digitalSignature, This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- ~~have an extendedKeyUsage extension (as per section 4.2.1.12 of RFC5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical;~~
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy; and
- have a Validity Period of 3 years.

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 0.63 cm, Line spacing: 1.5 lines, Bulleted + Level: 1 + Aligned at: 0 cm + Indent at: 0.63 cm

Requirements Applicable to –Personnel Authentication Certificates (ordinary users) only

Personnel Authentication Certificates that are issued by the UI DCCKICA for the purposes of Authenticating User Personnel to the Self Service Interface shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of digitalSignature. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC5280. This extension shall be marked as non-critical;
- include the Subject name as a meaningful name or other means of identifying an individual as provided by the DCCKI Eligible Subscriber; and
- have a Validity Period of 3 years.

Requirements Applicable to Personnel Authentication Certificates only

Personnel Authentication Certificates that are issued by the UI DCCKICA for the purposes of Authenticating Administration Users to the Self Service Interface shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of digitalSignature. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- contain a two policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy and the OID for validation policy of the Smart Card Token PIV Authentication Key;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC5280. This extension shall be marked as non-critical;
- include the Subject name as a meaningful name or other means of identifying an individual as provided by the DCCKI Eligible Subscriber; and
- have a Validity Period of 3 years.

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 0.63 cm, Line spacing: 1.5 lines, Bulleted + Level: 1 + Aligned at: 0 cm + Indent at: 0.63 cm

Requirements Applicable to EII DCCKICA and UI DCCKICA Certificates only

An EII DCCKICA Certificate or UI DCCKICA Certificate issued by the Root DCCKICA shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of keyCertSign and cRLSign. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy;
- contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical; and
- have a Validity Period of 10 years.

Requirements Applicable to Root DCCKICA Certificates only

Root DCCKICA Certificates that are issued by the Root DCCKICA shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of keyCertSign and cRLSign. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280);
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for anyPolicy;
- contain the basicConstraints extension, with values cA=True, and pathLen absent (unlimited). This extension shall be marked as critical; and
- have a Validity Period of 20 years.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing TLS Communications

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-withSHA256	
Issuer	Name	CN= EII DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN=<FQDN>, O=~~SEC~~ Party or RDP Signifier, C=UK	
subjectPublicKeyInfo		RSA	
~~encryptionAlgorithm~~		~~AES-GCM~~	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
~~cRLDistributionPoint~~	~~http location~~	~~URL:http://<TBC>~~	
~~authorityInfoAccess~~	~~http location~~	~~URL:http://<TBC>~~	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature, keyEncipherment~~,~~ ~~keyAgreement~~	
certificatePolicies		1.2.826.0.1.8641679.1 .2.1.11	
extendedKeyUsage		id-kp-serverAuth, id-kp-clientAuth	
cRLDistributionPoint	http location	URL:http://<TBC>	
authorityInfoAccess	http location	URL:http://<TBC>	

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Bold

notAfter

The latest time ~~an~~a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier or RDP Signifier of the DCCKI Subscriber who is also a SMKI Subscriber and a Common Name (CN) which will be the Fully Qualified Domain Name of the DCCKI Subscriber.

subjectKeyPublicInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

~~**encryptionAlgorithm**~~

~~The Encryption Algorithm shall be AES-GCM as defined in IETF RFC 5288.~~

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier~~.~~
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical~~.~~
- extendedKeyUsage~~.~~

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC5280.

subjectKeyIdentifier

Calculated using method 2of section 4.2.1.2 of RFC5280.

keyUsage

As per RFC5280 section 4.2.1.3 with a value of digitalSignature, and keyEncipherment ~~and keyAgreement~~.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per section 4.2.1.12 of RFC5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical.

cRLDistributionPoint

Formatted: Font: Bold

URI string, which shall identify the URL of the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing FTPS Communications

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-withSHA256	
Issuer	Name	CN= EII DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as	

		not before + 3 years	
Subject	Name	CN= <Party or RDP Signifier >	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature, keyEncipherment	
certificatePolicies		1.2.826.0.1.8641679.1 .2.1.11	
subjectAltName		<Fully Qualified Domain Name>	
extendedKeyUsage		id-kp-serverAuth, id-kp-clientAuth	
cRLDistributionPoint	http location	[1]URL:http://<TBC>	
authorityInfoAccess	http location	URL:http://<TBC>	

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

notAfter

The latest time a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) shall be populated with the Party Signifier or RDP Signifier of the DCCKI Subscriber.

subjectKeyPublicInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical
- subjectAltName: non-critical
- extendedKeyUsage

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC5280.

subjectKeyIdentifier

Calculated using method 2of section 4.2.1.2 of RFC5280.

keyUsage

As per RFC5280 section 4.2.1.3 with a value of digitalSignature and keyEncipherment.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

subjectAltName

Subject Alternative Name (SAN) shall be populated with the Fully Qualified Domain Name (FQDN) of the DCCKI Subscriber pertaining to the service for which the DCCKI Infrastructure Certificate will be used.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per section 4.2.1.12 of RFC5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical.

cRLDistributionPoint

URI string, which shall identify the URL of the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing SAML Assertions

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN=EII DCCKICA O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	~~O=SEC~~ CN=Party Signifier~~, C=UK~~	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier ~~cRLDistributionPoint~~	~~http~~ ~~location~~KeyIdentifier	~~URL:http://<TBC>~~Calculated by CA	
subjectKeyIdentifier~~authorityKeyIdentifier~~	KeyIdentifier	Calculated by CA	
keyUsage~~subjectKeyIdentifier~~	~~KeyIdentifier~~	~~Calculated by CA~~digitalSignature	
~~keyUsage~~certificatePolicies		~~digitalSignature,~~ 1.2.826.0.1.8641679.1.2.1.11	
cRLDistributionPoint~~certificatePolicies~~	http location	~~1.2.826.0.1.8641679.1.2.1.11~~ URL:http://<TBC>	
authorityInfoAccess~~extendedKeyUsage~~	http location	~~id-kp-serverAuth, id-kp-clientAuth~~URL:http://<TBC>	

Formatted Table

Formatted: Font: Bold

Formatted Table

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

notAfter

The latest time a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of ~~the Country (C), the Organisation~~a Common Name (~~O) which will~~CN) shall be populated with the Party Signifier of the DCCKI Subscriber.

Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

subjectPublicKeyInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical~~.~~
- ~~extendedKeyUsage.~~

~~**authorityKeyIdentifier**~~

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC5280.

~~**subjectKeyIdentifier**~~

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC5280.

keyUsage

Formatted: Font: Bold

~~**keyUsage**~~

As per RFC5280 section 4.2.1.3 with a value of digitalSignature.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

~~**extendedKeyUsage**~~

~~This~~**cRLDistributionPoint**

URI string, which shall ~~be an extendedKeyUsage extension (as per RFC5280 section 4.2.1.12) with a value~~identify the URL of ~~id-kp-serverAuth and id-kp-clientAuth.~~the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

Personnel Authentication Certificate DCCKI Certificate Profile (ordinary users)

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
~~Issuer~~	~~Name~~	~~CN= UI DCCKICA, O=DCC, C=UK~~	
Issuer	Name	CN= UI DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN = <Name>	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	

Extensions	Extensions	Critical and non-critical extensions	
authority Key Identifier	KeyIdentifier	Calculated by CA	
subject Key Identifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11	
subjectAltName		Other Name =<username>	
extendedKeyUsage~~keyUsage~~		~~digitalSignature~~Client Authentication (1.3.6.1.5.5.7.3.2)	
~~certificatePolicies~~cRLDistributionPoint		~~1.2.826.0.1.8641679.1.2.1.11~~[1] CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN= UI DCCKICA O=DCC Party Signifier C=UK	

Interpretation

Version

~~**Interpretation**~~

~~**Version**~~

The version of the X.509 Personnel Authentication Certificate. Personnel Authentication Certificates shall identify themselves as version 3.

serialNumber

Personnel Authentication Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the Personnel Authentication Certificate, and shall be created by the Issuing UI DCCKICA that signs the Personnel Authentication Certificate. The

Serial Number shall be unique in the scope of Personnel Authentication Certificates signed by the Issuing UI DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Personnel Authentication Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Personnel Authentication Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be UI DCCKICA (as defined in the UI DCCKICA Certificate certificate profile).

Validity

The time period over which the UI DCCKICA expects the Personnel Authentication Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Personnel Authentication Certificate may be used. This shall be the time the Personnel Authentication Certificate is created.

notAfter

The latest time a Personnel Authentication Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) which shall be consistent with the information held in the User Personnel's SSI account.

~~**subjectAltName**~~

~~The Personnel Authentication Certificate shall contain a single GeneralName of type OtherName. The OtherName shall be the SSI username of the User Personnel of the DCCKI Eligible Subscriber.~~

subjectKeyPublicInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

Personnel Authentication Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical~~.~~

- subjectAltName: non-critical
- extendedKeyUsage

authorityKeyIdentifier

Formatted: Left, Space After: 10 pt, Line spacing: Multiple 1.15 li

This shall be in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 ofRFC5280. This extension shall be marked as non-critical.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of of RFC5280.

keyUsage

As per RFC5280 section 4.2.1.3 with a value of digitalSignature. This extension shall be marked as critical (as per RFC5280 section 4.2.1.3).

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

subjectAltName

The Personnel Authentication Certificate shall contain a single GeneralName of type OtherName. The OtherName shall be the SSI username of the User Personnel of the DCCKI Eligible Subscriber.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per RFC5280 section 4.2.1.12) with a value id-kp-clientAuth. This extension shall be marked as non-critical.

cRLDistributionPoint

This shall identify the directory address of the UI DCCKICA CRL. This extension shall be marked as non-critical.

Personnel Authentication Certificate DCCKI Certificate Profile (Administration Users)

~~**EII DCCKICA Certificate DCCKI Certificate Profile**~~

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	

Formatted Table

serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= UI DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN = <Name>	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authority Key Identifier	KeyIdentifier	Calculated by CA	
subject Key Identifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	
certificatePolicies		[1] 1.2.826.0.1.8641679.1.2.1.11 (DCCKI CP OID) [2] 16.840.1.101.3.2.1.3.13 (PIV Authentication Key OID)	
subjectAltName		Other Name =<username>	
extendedKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	
cRLDistributionPoint		[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN= UI DCCKICA O=DCC Party Signifier C=UK	cRLDistributionPoint
2.16.840.1.101.3.2.1.3.13		(01 01 00) (PIV Authentication Key) 2.16.840.1.101.3.2.1.3.13 (PIV Authentication Key)	PIV authentication OID

Interpretation

Version

The version of the X.509 Personnel Authentication Certificate. Personnel Authentication Certificates shall identify themselves as version 3.

serialNumber

Personnel Authentication Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the Personnel Authentication Certificate, and shall be created by the Issuing UI DCCKICA that signs the Personnel Authentication Certificate. The Serial Number shall be unique in the scope of Personnel Authentication Certificates signed by the Issuing UI DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Personnel Authentication Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Personnel Authentication Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be UI DCCKICA (as defined in the UI DCCKICA Certificate certificate profile).

Validity

The time period over which the UI DCCKICA expects the Personnel Authentication Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Personnel Authentication Certificate may be used. This shall be the time the Personnel Authentication Certificate is created.

notAfter

The latest time a Personnel Authentication Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) which shall be consistent with the information held in the Administration User's SSI account.

subjectKeyPublicInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

Personnel Authentication Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical
- subjectAltName: non-critical
- extendedKeyUsage

authorityKeyIdentifier

This shall be in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 ofRFC5280. This extension shall be marked as non-critical.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of of RFC5280.

keyUsage

As per RFC5280 section 4.2.1.3 with a value of digitalSignature. This extension shall be marked as critical (as per RFC5280 section 4.2.1.3).

certificatePolicies

Contain a policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy and a policyIdentifier with PIV Authentication Key OID.

subjectAltName

The Personnel Authentication Certificate shall contain a single GeneralName of type OtherName. The OtherName shall be the SSI username of the Administration User of the DCCKI Eligible Subscriber.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per RFC5280 section 4.2.1.12) with a value id-kp-clientAuth and a value of "Smart Card Logon". This extension shall be marked as non-critical.

cRLDistributionPoint

This shall identify the directory address of the UI DCCKICA CRL. This extension shall be marked as non-critical.

EII DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= Root DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 10 years	
Subject	Name	CN= EII DCCKICA, O=DCC Party Signifier, C=UK	
subjectKeyPublicInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical	

		extensions	
~~cRLDistributionPoint~~	~~http location~~	~~URL:http://<TBC>~~	
~~authorityInfoAccess~~	~~http location~~	~~URL:http://<TBC>~~	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign, cRLSign	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11; anyPolicy	
basicConstraints		CA=True, path Length=0	

Formatted Table

~~**Interpretation**~~

~~**Version**~~

cRLDistributionPoint	http location	[1] URL:http://<TBC> [2] CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN= Root DCCKICA O=DCC Party Signifier C=UK	
authorityInfoAccess	http location	URL:http://<TBC>	

Interpretation

Version

The version of the X.509 EII DCCKICA Certificate. EII DCCKICA Certificates shall identify themselves as version 3.

serialNumber

EII DCCKICA Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the EII DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the EII DCCKICA Certificate. The Serial Number shall be unique in the scope of DCCKICA Certificates signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the EII DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the EII DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root DCCKICA (as defined in the Root DCCKICA Certificate certificate profile).

Validity

The time period over which the Root DCCKICA expects the EII DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

Formatted: Font: Bold

notBefore

The earliest time ~~a~~an EII DCCKICA Certificate may be used. This shall be the time the EII DCCKICA Certificate is created.

notAfter

The latest time an EII DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be EII DCCKICA.

subjectKeyPublicInfo.

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The keyLength shall be RSA 2048 bits.

Extensions

EII DCCKICA Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical.
- basicConstraints: critical.

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 ofRFC5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC5280.

keyUsage

Formatted: Left, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

The EII DCCKICA Certificate shall have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of keyCertSign and cRLSign. This extension shall be marked as critical (as per RFC5280 section 4.2.1.3).

certificatePolicies

The EII DCCKICA Certificate shall contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen=0. This extension shall be marked as critical.

Formatted: Font: Bold

cRLDistributionPoint

URI string, which shall identify the URL of the DCCK ARL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the Root DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

UI DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= Root DCCKICA, O=DCC Party Signifier, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 10 years	
Subject	Name	CN=UI DCCKICA, O=DCC Party Signifier, C=UK	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical	

		extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeydentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign, cRLSign	
certificatePolicies		1.2.826.0.1.8641679.1.2. 1.11; anyPolicy	
basicConstraints		CA=True, path Length=0	
cRLDistributionPoint	http location	[1] URL:http://<TBC> [2] CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN= Root DCCKICA O=DCC Party Signifier C=UK	cRLDistributionPoint

Interpretation

Version

The version of the X.509 UI DCCKICA Certificate. UI DCCKICA Certificates shall identify themselves as version 3.

serialNumber

UI DCCKICA Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the UI DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the UI DCCKICA Certificate. The Serial Number shall be unique in the scope of DCCKICA Certificates signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the UI DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the UI DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name

(CN) which will be Root DCCKICA (as defined in the Root DCCKICA Certificate certificate profile).

Validity

The time period over which the Root DCCKICA expects the UI DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a UI DCCKICA Certificate may be used. This shall be the time the UI DCCKICA Certificate is created.

notAfter

The latest time a UI DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be UI DCCKICA.

subjectPublicKeyInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

UI DCCKICA Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.

- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical.
- basicConstraints: critical.

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC5280.

keyUsage

The UI DCCKICA Certificate shall have a keyUsage extension (as per section 4.2.1.3 of RFC5280) with a value of keyCertSign and cRLSign. This extension shall be marked as critical (as per section 4.2.1.3 of RFC5280).

certificatePolicies

The UI DCCKICA Certificate shall contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen=0. This extension shall be marked as critical.

cRLDistributionPoint

URI string, which shall identify the URL of the DCCKI ARL within the DCCKI Repository. This extension shall be marked as non-critical.

Root DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	

serialNumber	Integer	calculated by CA	
signatureAlgorithm	AlgortithmIdentifier	rsa-with-SHA256	
Issuer	Name	CN= Root DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 20 years	
Subject	Name	CN=Root DCCKICA, O=DCC, C=UK	
subjectPublicKeyInfo		RSA	
keyLength		4096 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		keyCertSign, cRLSign	
certificatePolicies		1.2.826.0.1.8641679.1 .2.1.11; anyPolicy	
basicConstraints		CA=True, path Length= None	

Interpretation

These certificates are the root of trust for the DCCKI.

Version

The version of the X.509 Root DCCKICA Certificate. Valid Root DCCKICA Certificates shall identify themselves as version 3.

Serial Number

Root DCCKICA Certificate serial number, a positive integer of no more than 8 octets. The Serial Number identifies the Root DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the Root DCCKICA Certificate (self-signed by the Root DCCKICA). The Serial Number shall be unique in the scope of DCCKICA Certificate signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Root DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Root DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be Root DCCKICA which will be the same as the Subject Name as it is self-signed by the Root DCCKICA.

Validity

The time period over which the Root DCCKICA expects the Root DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ

notBefore

The earliest time a Root DCCKICA Certificate may be used. This shall be the time the Root DCCKICA Certificate is created.

notAfter

The latest time a Root DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier of the DCC and a Common Name (CN) which will be Root DCCKICA

subjectPublicKeyInfo.

The Public Key algorithm shall be RSA as defined in NIST FIPS 180-6.

keyLength

The keyLength shall be RSA 4096 bits.

Extensions

Root DCCKICA Certificate MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: critical.
- basicConstraints: critical.

authorityKeyIdentifier

A keyIdentifier calculated using method 2 of section 4.2.1.2 of RFC5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC5280.

keyUsage

The Root DCCKICA Certificate shall have a keyUsage extension (as per RFC5280 section 4.2.1.3) with a value of keyCertSign and cRLSign. This extension shall be marked as critical (as per RFC5280 section 4.2.1.3).

certificatePolicies

The RootDCCKICA Certificate shall contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen absent (unlimited). This extension shall be marked as critical.