Version 1.8

Appendix AP

S1SPKI Certificate Policy

FOC S1SPKI Certificate Policy

FOC S1SPKI Certificate Policy

1 INTRODUCTION

The document comprising of this Final Operating Capacity SMETS1 Service Provider Certificate Policy together with its Annexes, shall be known as the “FOC S1SPKI Certificate Policy” (and this document is referred to simply as the “Policy”).

1.1 Overview

(A) This Policy sets out the arrangements of the FOC S1SPKI related to the issuance of the following Certificates:

(i) FOC SISPKI End Entity Certificates; and

(B) FOC S1SPKI CA Certificates. This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New font`;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

Where in this Policy, a system or device is expressed to be a Registration Authority, a FOC S1SPKI CA, an Authorised Subscriber, Subscriber or a Relying Party, this shall be interpreted as meaning that the DCC Service Provider operating the relevant system or device is the Registration Authority, the Certification Authority, Authorised Subscriber, Subscriber or Relying Party (as the case may be). In the case of any SMETS1 Device, the FOC S1SP shall be the Authorised Subscriber and/or Relying Party (as the case may be).

1.2 Document name and identification

(A) This Policy has not been assigned an OID.

1.3 FOC S1SPKI participants

1.3.1 FOC S1SPKI CA

(A) The definition of FOC S1SPKI CA can be found in Annex A.

1.3.2 FOC S1SPKI Registration Authority

(A) The definition of FOC S1SPKI Registration Authority can be found in Annex A.

1.3.3 Subscribers

(A) In accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy, certain Parties may become Authorised Subscribers.

(B) In accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The FOC S1SPKI RAPP as set out in Annex E of this Policy sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the FOC S1SPKI RAPP as set out in Annex E of this Policy and Subscriber Obligations as set out in Annex C this Policy.

(E) The definitions of the following terms are set out in Annex A of this Policy:

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a FOC S1SPKI End Entity Certificate is represented by an appropriate identifier in the subject field of the FOC S1SPKI End Entity Certificate Profile (as the case may be) in accordance with Annex B.

(B) The Subject of a FOC S1SPKI CA Certificate must be the entity identified by the subject field of the FOC S1SP Operator Root CA Certificate Profile, the Intermediate Enterprise CA Certificate Profile; the Intermediate Operator CA Certificate Profile; the Application Service Root CA Certificate Profile or the Intermediate Application Service PKI CA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with this Policy, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of the Relying Party Obligations as set out in Annex D of this Policy.

(C) The definition of Relying Party is set out in Annex A.

1.3.6 Policy Management Authority

(A) The FOC S1SP's IT Steering Committee (FOC S1SP ITSC) is responsible for fulfilling the duties of the Policy Management Authority in relation to the FOC S1SPKI.

(B) This Policy is subject to periodic review by the SMKI PMA in accordance with the provisions of the SEC.

1.3.7 FOC S1SPKI Repository

(A) The FOC S1SPKI CA will be responsible for providing the FOC S1SPKI Repository in accordance with this Policy.

1.3.8 Certificate usage

(A) The FOC S1SP Intermediate CA shall ensure that FOC S1SP End Entity Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of:

a) the creation, sending, receipt and processing of communications to and from FOC SMETS1 Devices in accordance with or pursuant to the Smart Energy Code (SEC), which will further include:

1) Symmetric key generation (Digital Signature, Key Agreement);

2) TLS Communication (Digital Signature, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication); and

3) Authentication and Non-Repudiation (Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication).

(B) The FOC S1SPCA shall ensure that FOC S1SPCA Certificates are Issued only to the FOC S1SPCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the FOC S1SP Operator Root Certification Authority (CA);

(ii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate Enterprise CA; and

(iii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate Operator CA.

(C) The Intermediate Application Service PKI CA shall ensure that Application Service End Entity Certificates are Issued only:

(ii) to Eligible Subscribers; and

(iii) for the purpose of secure communications and authenticating users to the Application Service for administration purposes.

(D) The Further provision in relation to the use of Certificates is made in the Subscriber Obligations as set out in Annex C of this Policy and the Relying Party Obligations as set out in Annex D of this Policy.

1.3.9 Prohibited Certificate uses

(A) No party shall use a Certificate other than for the purposes specified in Part 1.3.8 of this policy.

1.4 Policy administration

1.4.1 Organisation administering the document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.4.2 Contact person

(A) Questions in relation to the content of this Policy should be addressed to the Chief Information Security Officer CISO at DCC.

1.4.3 Person determining CPS suitability for the policy

(A) The SMKI PMA determines the suitability of any Certification Practice Statement operating under this Policy.

1.4.4 CPS approval procedures

(A) The FOC S1SPKI CPS is subject to a review by, the SMKI PMA in accordance with the provisions of the SEC.

(B) The DCC shall keep the FOC S1SPKI CPS under review and shall in particular carry out a review of the FOC S1SPKI CPS whenever (and to the extent to which) it may be required to do so in line with its duties as set out in the SEC.

(C) Following any review of the FOC S1SPKI CPS:

- (i) the FOC S1SP may propose amendments to it, which it shall submit to the SMKI PMA for its review; and
- (ii) those amendments may be made only to the extent to which the SMKI Policy Management Authority has approved or not rejected them.

1.4.5 Registration Authority Policies and Procedures

(A) The FOC S1SPKI Registration Authority Policies and Procedures (the FOC S1SPKI RAPP) are set out in Annex E of this Policy.

1.5 Definitions and acronyms

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A of this Policy.

(B) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A of this Policy.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 FOC S1SPKI Repositories

(A) The FOC S1SPKI Operator Root CA and the FOC S1SPKI Intermediate CAs each have their own separate FOC S1SPKI Repository.

(B) The FOC S1SPKI Repository associated with the FOC S1SPKI Operator Root CA stores the following information:
- (i) All copies of Issued FOC S1SPKI Operator Root CA Certificates
- (ii) Certificate status and validity meta-data for each FOC S1SPCA Certificate

(C) The FOC S1SPKI Repository associated with the FOC S1SPKI Intermediate CAs shall store the following information:
- (i) All copies of FOC S1SP End Entity Certificates Issued by the FOC S1SPKI Intermediate CAs.
- (ii) Certificate status and validity meta-data for each FOC S1SP End Entity Certificate Issued by the FOC S1SPKI Intermediate CAs.
- (iii) The latest version of the FOC S1SPKI CRL for the FOC S1SPKI Intermediate CAs.
- (iv) All copies of Issued FOC S1SP CA Certificates.

(D) The FOC S1SPKI Repository associated with each of the individual Application Service Root CAs shall store the following information:
- (i) All copies of the Application Service Root CA Certificate self-signed by that Application Service Root CA
- (ii) All copies of Intermediate Application Service PKI CA Certificates Issued by that Application Service Root CA
- (iii) All copies of Application Service End Entity Certificates Issued by the Intermediate Application Service PKI CA referred to in ii) above;
- (iv) Certificate status and validity meta-data for each of the Application Service End Entity Certificates stored in that repository.

2.2 Publication of certification information

(A) See part 2.1 of this Policy.

2.3 Time or frequency of publication

(A) The FOC S1SPKI CA shall ensure that:
- (i) each FOC S1SPKI End Entity Certificate is promptly accepted by a Subscriber when issued;
- (ii) each FOC S1SPKICA Certificate is lodged in the applicable FOC S1SPKI Repository promptly on being Issued;
- (iii) the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy; and
- (iv) the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy.

(B) The Applications Service CA shall ensure that:
- (i) each Application Service End Entity Certificate is promptly accepted by a Subscriber when issued;
- (ii) each Application Service CA Certificate is lodged in the applicable Application Service Repository promptly on being Issued;
- (iii) the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy; and
- (iv) the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy.

(C) No ARLs exist for the Application Service.

2.4 Access controls on FOC S1SPKI Repositories

(A) All FOC S1SPKI Repositories and Application Service Repositories are subject to access controls using username and passwords. Only authorised FOC S1SPKI Systems and FOC S1SP Personnel have access to FOC S1SPKI Repositories and Application Service Repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

(A) The FOC S1SPKI CA shall ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for names to be meaningful

(A) The FOC S1SPKI CA shall ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or pseudonymity of subscribers

(A) The anonymity or pseudonymity of Subscribers is not supported under this Policy.

3.1.4 Rules for interpreting various name forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and role of trademarks

(A) No Eligible Subscriber may make a Certificate Signing Request which contains:

(i) any information that constitutes a trademark, unless it is the holder of the Intellectual Property Rights in relation to that trademark; or

(ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

3.2 Initial identity validation

3.2.1 Method to prove possession of Private Key

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this policy in relation to:

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

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of organisation identity

(A) Only Eligible Subscribers are allowed to subscribe for Certificates under this Policy.

3.2.3 Authentication of individual identity

(A) Provision is made in the FOC S1SPKI RAPP in relation to the Authentication of

(B) persons engaged by the FOC S1SP, which provides for all such persons to have their identity and authorisation verified to ISO27001 standards or to such equivalent level within a comparable authentication framework as may be agreed by the FOC S1SP ITSC.

3.2.4 Non-verified subscriber information

(A) The FOC S1SPKICA shall verify all information in relation to Certificates Issued.

(B) Further provision on the content of a Certificate is made in Subscriber Obligations as set out in Annex C of this Policy.

3.2.5 Validation of authority

(A) See part 3.2.2 of this Policy.

3.2.6 Criteria for interoperation

[*Not applicable in this Policy*]

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 FOC S1SPKI CA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for re-key after revocation

[Not applicable in this policy]

3.4 Identification and Authentication for revocation request

(A) Provision is made in the Annex E of this Policy in relation to procedures designed to ensure the Authentication of FOC S1SPKI RA Personnel who submit a Certificate Revocation Request and verify that they are authorised to submit that request.
(B) Only FOC S1SPKI RA Personnel can revoke a Certificate in accordance with Annex E of this Policy.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Submission of Certificate Applications

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to:

(i) in respect of a FOC S1SPKI End Entity Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(ii) in respect of a FOC S1SPKI CA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a FOC S1SPCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and SMETS1 Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber or Authorised Subscriber in its capacity as such; and

(ii) maintenance by the FOC S1SPKI CA of a list of organisations, individuals, Systems and SMETS1 Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authorities and its Representatives

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to the establishment of an enrolment process in respect of FOC S1SP Personnel, FOC S1SPKI Systems and FOC S1SPKI RA Personnel:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the FOC S1SP in its capacity as the FOC S1SPKI Registration Authority; and

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

(a) for Authentication of all FOC S1SPKI RA Personnel by a FOC S1SPKI Registration Authority Manager; and

(b) for all FOC S1SPKI Registration Authority Personnel to have their identify and authorisation verified against a robust assured authentication framework as agreed by the FOC S1SP ITSC. See section 6.3.2 of this Certificate Policy for further information.

4.2 Certificate application processing

4.2.1 Performing identification and Authentication functions

(A) Provision is made in the FOC S1SPKI RAPP in relation to the Authentication by the FOC S1SPKI CA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or rejection of Certificate applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the FOC S1SPKI RAPP as set out in Annex E of this Policy or this Policy, the FOC S1SPKI CA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) may give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the FOC S1SPKI RAPP as set out in Annex E of this Policy or any other provision of this Policy, the FOC S1SPKI CA shall Issue the Certificate which was the subject of the Certificate Signing Request.

(C) This does not apply in circumstances where a Certificate is issued by a System to another System or device.

4.2.3 Time to process Certificate applications

(A) All Certificate Signing Requests will be processed promptly upon receipt.
(B) Upon receipt and successful validation of a Certificate Signing Request by the FOC S1SPKI CA, the FOC S1SPKI CA will promptly Issue a Certificate in response.

4.3 Certificate issuance

4.3.1 FOC S1SPCA Actions during Certificate Issuance

(A) The FOC S1SPKI CA may Issue a Certificate only:
  (i) in accordance with the provisions of this Policy and the FOC S1SPKI RAPP as set out in Annex E of this Policy; and
  (ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy.

(B) The FOC S1SPKI CA shall ensure that:
  (i) each FOC S1SPKI CA Certificate Issued by it contains information that it has verified to be correct and complete; and
  (ii) each FOC S1SPKI End Entity Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A FOC S1SPCA Certificate may only be:
  (i) Issued by the FOC S1SPCA; and
  (ii) for that purpose, self-signed using the Operator Root CA Private Key for the Operator Root CA Certificate and signed using the Operator Root CA Private Key for a FOC S1SP Intermediate CA Certificate.

(D) A FOC S1SP End Entity Certificate may only be:
  (i) Issued by an FOC S1SP Intermediate CA; and
  (ii) for that purpose, signed using a FOC S1SP Intermediate CA Private Key.

(E) The FOC S1SPCA shall not Issue:
  (i) an FOC S1SP Intermediate CA Certificate using an Operator Root CA Private Key after the expiry of the Validity Period of an Operator Root CA Certificate containing the Public Key associated with that Private Key;
  (ii) an FOC S1SP End Entity Certificate using an FOC S1SP Intermediate CA Private Key after the expiry of the Validity Period of an FOC S1SP Intermediate CA Certificate containing the Public Key associated with that Private Key; or
  (iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it.

(F) An Application Service CA Certificate may only be:
  (i) Issued by the Application Service CA; and
  (ii) for that purpose, self-signed using the Application Service Root CA Private Key for an Application Service Root CA Certificate and signed using the Application Service Root CA Private Key for an Intermediate Application Service PKI Certificate.

(G) An Application Service End Entity Certificate may only be:
  (i) Issued by an Intermediate Application Service CA; and
  (ii) for that purpose, signed using an Application Service Intermediate PKI CA Private Key.

(H) The Application Service CA shall not Issue:
  (i) an Intermediate Application Service PKI CA Certificate using an Application Service Root CA Private Key after the expiry of the Validity Period of an Applications Service Root CA Certificate containing the Public Key associated with that Private Key;

(ii) an Application Service End Entity Certificate using an Intermediate Application Service PKI CA Private Key after the expiry of the Validity Period of an Application Service Intermediate PKI CA Certificate containing the Public Key associated with that Private Key; or

(iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy for the FOC S1SP CA to notify an Eligible Subscriber where that Eligible Subscriber is issued with a Certificate which was the subject of a Certificate Signing Request made by it.

(B) This does not apply in circumstances where a Certificate is issued by a System to another System or device.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate acceptance

(A) A Certificate which has been Issued by the FOC S1SPKI CA shall be treated as valid for any purposes of this Policy or the Code until it is revoked.

(B) The FOC S1SPKI CA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

4.4.2 Publication of the Certificate by the CA

(A) Provision in relation to publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate issuance by the CA to other entities

(A) Not applicable in this Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in this Policy.

4.5.2 Relying Party Public Key and Certificate usage

(A) Relying Party obligations are set out in Annex D of this Policy.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

(A) This policy does not support the renewal of Certificates.

(B) The FOC S1SPKI CA may only replace and shall not renew any Certificate.

4.6.2 Who may request replacement

(A) Certificate replacement is an automated process and does not require manual intervention. The business process defines the rotation schedule of the certificate Processing Certificate replacement requests.

(B) Certificate Replacement operates under the governance of the Head End System. In its capacity as the Registration Authority it determines whether a Certificate needs to be issued and manages the creation of the CSR.

4.6.3 Notification of new Certificate issuance to subscriber

Not applicable to this Policy.

4.6.4 Conduct constituting acceptance of a replacement Certificate

Not applicable to this Policy.

4.6.5 Publication of the replacement Certificate by the CA

Not applicable to this Policy.

4.6.6 Notification of Certificate issuance by the CA to other entities

Not applicable to this Policy.

4.7 Certificate re-key

4.7.1 Circumstance for Certificate re-key

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

4.7.2 Who may request certification of a new public key

Not applicable to this policy.

4.7.3 Processing Certificate re-keying requests

Not applicable to this policy.

4.7.4 Notification of new Certificate issuance to subscriber

Not applicable to this policy.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Not applicable to this policy.

4.7.6 Publication of the re-keyed Certificate by the CA

Not applicable to this policy.

4.7.7 Notification of Certificate issuance by the CA to other entities

Not applicable to this policy.

4.8 Certificate modification

4.8.1 Circumstance for Certificate modification

(A) This policy does not support Certificate modification.

4.8.2 Who may request Certificate modification

Not applicable to this policy.

4.8.3 Processing Certificate modification requests

Not applicable to this policy.

4.8.4 Notification of new Certificate issuance to subscriber

Not applicable to this policy.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable to this policy.

4.8.6 Publication of the modified Certificate by the CA

Not applicable to this policy.

4.8.7 Notification of Certificate issuance by the CA to other entities

Not applicable to this policy.

4.9 Certificate Revocation and Suspension

(A) This Policy does not support Certificate suspension.

(B) Certificate status information services shall identify all revoked Certificates; at least until their assigned validity period expires. A reporting API describes the status of a Certificate at a CRL Distribution Point (CDP) and can be queried by a Privileged User.

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate in accordance with Annex E of this policy where:

- (i) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised; or
- (ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate

(B) A Certificate must be Revoked:

(i) When any of the information in the Certificate is known or suspected to be inaccurate.
(ii) Upon suspected or known compromise of the Private Key associated with the Certificate.
(iii) Upon suspected or known compromise of the media holding the Private Key associated with the Certificate.

(C) The FOC S1SPKI CA, or FOC S1SPKI RA acting on their behalf may Revoke a Certificate when an entity fails to comply with any obligations set out in this Policy.

(D) Handshake information describing the exchange of information for revocation purposes can be obtained in section 2.3 'Operator Device Certificate Update' of the DCCA-0045-VN.N-SDD Trilliant S1SP WAN communication Security' documentation.

4.9.2 Who can request revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Authorised Subscriber and shall on doing so by specifying its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1 of this Policy).

4.9.3 Procedure for revocation request

(A) Provision is made in the FOC S1SPKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the FOC S1SPKI CA shall take reasonable steps to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(C) The FOC S1SPKI CA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation request grace period

(A) None. If the Revocation request is actioned, it must reflect in the next scheduled publication of the CRL.

4.9.5 Time within which CA must process the revocation request

(A) The FOC S1SPKI CA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the FOC S1SPKI RAPP.

(B) The mechanisms, if any, that a Relying Party may use in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via Certificate Revocation Lists or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified

4.9.6 CRL issuance frequency (if applicable)

(A) The FOC S1SPKI CA shall ensure that an up to date version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository:
(i) at least once in every period of twelve months; and
(ii) promptly on the revocation of an FOC S1SPCA Certificate.

(B) Each version of the FOC S1SPKI ARL shall be valid until the date which is up to 13 months after the date on which that version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository.

(C) Further provision in relation to the reliance that may be placed on the FOC S1SPKI ARL (and on versions of it) is set out in Annex D (Relying Party Agreement) of this Policy.

(D) The FOC S1SPCA shall ensure that an up to date version of the FOC S1SPKI CRL is lodged in the relevant FOC S1SPKI Repository at least once in every period of 48 hours.

(E) Each version of the FOC S1SPKI CRL shall be valid until 48 hours from the time at which it is lodged in the FOC S1SPKI Repository.

(F) Further provision in relation to the reliance that may be placed on the FOC S1SPKI CRL (and on versions of it) is set out in Annex D (Relying Party Agreement) of this Policy.

(G) The FOC S1SPCA shall ensure that each up to date version of the FOC S1SPKI ARL and FOC S1SPKI CRL:
  (i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and
  (ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The FOC S1SPCA shall ensure that the FOC S1SPKI CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The FOC S1SPCA shall retain a copy of the information contained in all versions of the FOC S1SPKI CRL and FOC S1SPKI ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the DCC, the FOC ,FOC S1SP ITSC any Subscriber or any Relying Party.

(J) No ARL or CRL is issued in relation to the Internal Application Service CA.

4.9.7 Maximum latency for CRLs (if applicable)

(A) See part 4.9.6 of this Policy

4.9.8 On-line revocation/status checking availability

(A) The availability of Certificate Status checking shall be published though a CRL Distribution Points (CDP).

4.9.9 On-line revocation checking requirements

(A) See section 4.9.8 above

4.9.10 Other forms of revocation advertisements available

[*Not applicable in this Policy*]

4.9.11 Special requirements in the event of key compromise

(A) Where any Private Key is Compromised, then the FOC S1SP shall:
  (i) immediately notify the SMKI PMA;
  (ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances in the event of Compromise or suspected Compromise; and
    (a) where the Compromise or suspected Compromise relates to any Private Key;
  (iii) ensure that the Private Key is no longer used;
  (iv) promptly notify each of the Authorised Subscribers for any Certificates Issued using that Private Key.

4.9.12 Circumstances for suspension

4.9.13 *[Not applicable in this Policy]* Who can request suspension

[*Not applicable in this Policy*]

4.9.14 Procedure for suspension request

[Not applicable in this Policy]

4.9.15 Limits on suspension period

[Not applicable in this Policy]

4.10 Certificate status services

4.10.1 Operational characteristics

(A) The types of Certificate status checking services made available to the Authorised Subscriber is by a service endpoint. This service endpoint is available to the Authorised Subscriber as an application interface which is presented by the PKI software.

4.10.2 Service availability

(A) See part 4.9.6 of this Policy.

4.11 End of subscription

[Not applicable in this Policy].

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

(A) This Policy does not cover Key Escrow services.
(B) The FOC S1SPKI CA shall not provide any Key Escrow services.
(C) The FOC S1SPKI recovery policies and practices are documented in the FOC S1SPKI CPS

4.12.2 Session key encapsulation and recovery policy and practices

[Not applicable in this Policy]

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the facility, management, and operational controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA.

5.1 Physical controls

5.1.1 Site location and construction

(A) The FOC S1SP shall ensure that all Data Centres must be located in List X Site accredited sites and must be ISO27001 certified.

(B) The FOC S1SP shall ensure that the FOC S1SPKI Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(C) The FOC S1SP shall ensure that:

(i) all of the physical locations in which the FOC S1SPKI 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; and

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

(D) The FOC S1SP shall ensure that the FOC S1SPKI Systems cannot be indirectly accessed from any location outside the United Kingdom.

(E) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

(i) SMKI PMA Guidance 003; or

(ii) any equivalent to the SMKI PMA Guidance 003 which updates or replaces it from time to time.

(F) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that all PINs, passphrases and passwords used for the purposes of carrying out the functions of the FOC S1SPCA are stored in secure containers accessible only to appropriately authorised individuals.

(G) The FOC S1SP shall ensure that the FOC S1SPKI Systems are Separated from any other DCC Systems provided that the FOC S1SPCA systems does not need to be Separated from the Application Service CA Systems

5.1.2 Physical access

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to FOC S1SPKI Systems, or any System used for the purposes of Timestamping, Certificate generation, or Certificate life-cycle management;

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

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and air conditioning

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.4 Water exposures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to water exposure at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.5 Fire prevention and protection

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.6 Media storage

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the FOC S1SPKI CA.

5.1.7 Waste disposal

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designing to ensure all media used to store Data held by it for the purposes of carrying out its functions as the FOC S1SPKI CA are disposed of only using secure methods. Where such methods such be based on:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation);
(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time; or
(iii) any equivalent standard or secure method approved by the FOC S1SP ITSC.

5.1.8 Off-Site Back-Up

(A) The FOC S1SP shall ensure that Capgemini and DXC shall regularly carry out a Back-Up of:

(i) all Data held on the S1SPKI Systems which are critical to the operation of those Systems or continuity in the provision of the S1SPKI Services; and
(ii) all other sensitive Data.

(B) The FOC S1SP shall ensure that Capgemini and DXC ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;
(ii) are protected in accordance with the outcome of a risk assessment, including when being transmitted for the purposes of Back-Up; and
(iii) to the extent to which they comprise S1SPKI Private Key Material, are
(iv) Backed Up to appropriate Security Containers which are stored off-line in encrypted format.

(C) The FOC S1SP shall ensure that Capgemini and DXC ensure that, where any elements of the S1SPKI Systems, any Data held for the purposes of providing the SS1SP PKI Services, or any items of Capgemini and DXC equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

(D) DCC will ensure that the S1SPKI CPS incorporates provisions in relation to paragraphs (A), (B) and (C) above.

5.2 Procedural Controls

5.2.1 Trusted Roles

(A) The FOC S1SP shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the FOC S1SPKI Systems unless that individual has been expressly authorised to have such access;
(ii) each member of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel has a clearly defined level of access to the FOC S1SPKI Systems and the premises in which they are located;
(iii) no individual member of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel is capable, by acting alone, of engaging in any action by means of

which the FOC S1SPKI Systems may be Compromised to a material extent; and

(iv) the FOC S1SPKI CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the FOC S1SPKI CA with the requirements of this Part 5.2.1 of this Policy.

5.2.2 Number of persons required per task

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of FOC S1SPKI Personnel, FOC S1SPKI RA Personnel; and

(ii) the application of controls to the actions of all members of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who are Privileged Users, in particular:

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

(b) providing that the revocation of any Certificate is one such function.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following areas:

(i) S1SPKI Systems administration;

(ii) S1SPKI Systems operations;

(iii) S1SPKI Systems security; and

(iv) S1SPKI Systems auditing.

5.2.3 Identification and Authentication for each role

(A) See Part 5.2.2 of this Policy.

5.2.4 Roles requiring separation of duties

(A) See Part 5.2.2 of this Policy.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

(A) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA Personnel must:

(i) be appointed to their roles in writing;

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

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

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the FOC S1SP, not have been previously relieved of any past assignment (whether for the FOC S1SP or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA Personnel have, as a minimum, passed an industry recognised and assured security check before commencing their roles.

(C) For Privileged Users, these assured security checks may include additional checks.

(D) The FOC S1SP shall ensure that the FOC S1SPKI CPS, as a minimum, makes provision for the purposes of paragraph (B) and (C) above.

5.3.2 Background check procedures

(A) See Part 5.3.1 of this Policy.

5.3.3 Training requirements

(A) See Part 5.3.1 of this Policy.

5.3.4 Retraining frequency and requirements

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.5 Job rotation frequency and sequence

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.6 Sanctions for unauthorized actions

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.7 Independent contractor requirements

(A) In accordance with the provisions of the Code and this Policy, references to the FOC S1SP in this Policy include references to persons with whom the FOC S1SP contracts in order to secure performance of its obligations as the FOC S1SP.

5.3.8 Documentation supplied to personnel

(A) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA 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 FOC S1SPKI CPS; and
- (iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of events recorded

(A) The FOC S1SP shall ensure that:

- (i) the FOC S1SPKI Systems record all activity in an audit log;
- (ii) the FOC S1SPKI CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:
  - (a) the activities of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel;
  - (b) the use of FOC S1SPKI equipment;
  - (c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the FOC S1SPCA are carried out;
  - (d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the FOC S1SPKI Systems audit log); and
- (iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of processing log

(A) The FOC S1SP shall ensure that:

- (i) the audit logging functionality in the FOC S1SPKI Systems is fully enabled at all times;
- (ii) all FOC S1SPKI Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:
  - (a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information);
- (iii) any equivalent to that British Standard which updates or replaces it from time to time; or
- (iv) an equivalent standard format that is commensurate with the standard in (i) and has been approved by the FOC S1SP ITSC.

(B) It monitors the FOC S1SPKI Systems in compliance with:

(i) SMKI PMA Guidance 003;
(ii) any equivalent to that SMKI PMA Guidance 003 which updates or replaces it from time to time; or
(iii) equivalent guidance that is commensurate with the guidance in (i) and which has been approved by the FOC S1SP ITSC.

(C) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates 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 it in response to types of events recorded in the Audit Log.

(D) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:
(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and
(ii) access to those Data must be limited to those members of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who are performing a dedicated system audit role.

5.4.3 Retention period for audit log

(A) The FOC S1SP shall:
(i) Ensure that the FOC S1SPKI Systems retain their Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and
(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of audit log

(A) The SS1SPCA shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to:
(i) the extent to which the Audit Log is retained electronically, the 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:
(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information);
(b) any equivalent to that British Standard which updates or replaces it from time to time; or
(c) an equivalent standard format that is commensurate with the standard in (i) and has been approved by the FOC S1SP ITSC; and
(ii) the extent to 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 FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for Audit Log backup procedures. This should include, as a minimum, provisions for:
(i) Data contained in the Audit Log to be backed up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):
(a) on a daily basis; or
(b) if activity has taken place on the FOC S1SPKI Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) All Data contained in the Audit Log which are Backed-Up are, during Back-Up:
(i) be held in accordance with the outcome of a risk assessment which is documented in the FOC SS1SPKI CPS; and
(ii) be protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit collection system (internal vs. external)

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log. Notification to event-causing subject

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the audit log.

5.4.7 Vulnerability assessments

(A) Provision is made in the FOC S1SPKI CPS in relation to the carrying out of vulnerability assessments in respect of the FOC S1SPKI Systems.

5.5 Records archival

5.5.1 Types of records archived

(A) The SS1SPCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4 of this Policy;

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

(iii) any other Data specified in this Policy as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention period for archive

(A) Where there is a need to Archive Data, the FOC S1SP CA shall ensure that any Data which is to be Archived is retained in accordance with their Data Retention and Destruction Policy.

(B) Archived information is to be retained for a period of no less than 12 months

5.5.3 Protection of archive

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates the following provisions as to how Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive backup procedures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for time-stamping of records

(A) Provision in relation to Timestamping is made in Part 6.8 of this Policy.

5.5.6 Archive collection system (internal or external)

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to obtain and verify archive information

(A) The FOC S1SP shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the SS1SPCA's operations.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to the periodic verification by the FOC S1SPKI CA of the Data held in the Archive.

5.6 Key changeover

(A) The FOC S1SP shall only ever Issue a new Certificate in relation to a new Certificate Signing Request, where it is submitted by an Eligible Subscriber in accordance with the requirements of the FOC S1SPKI RAPP and the relevant provisions of this Policy.

(B) A Key Pair will require changeover in accordance with their corresponding Certificate validity period set out in Part 6.3.2 of this Policy.

(C) The FOC S1SP shall ensure that any FOC S1SPKI CA Key Pair changeovers are managed so as to prevent any disruption to the provision of the FOC S1SPKI Services.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the FOC S1SPKI Services in the event of any Compromise of the FOC S1SPKI Systems or major failure in the FOC S1SP processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date FOC S1SPKI ARL and FOC S1SPKI CRL.

(B) The FOC S1SP shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The FOC S1SP shall ensure that the FOC S1SPKI 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 FOC S1SPKI Private Key or any part of the FOC S1SPKI Systems is Compromised.

5.7.2 Computing resources, software, and/or data are corrupted

(A) The FOC S1SP shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key compromise procedures

(A) See Part 5.7.1 of this Policy.

5.7.4 Business continuity capabilities after a disaster

(A) The FOC S1SP shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the FOC S1SPKI Services within not more than 48 hours of the occurrence of any event causing discontinuity.

5.8 CA or RA termination

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA.

6.1 Key pair generation and installation

6.1.1 Key pair generation

(A) The FOC S1SP shall ensure that all FOC S1SPKI CPS incorporates detailed provision in relation to the FOC S1SPKI CA Key Pair generation, where all Key Pairs which it uses for the purposes of this Policy are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

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

(iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The FOC S1SPKI CA shall not generate any Key Pair other than a FOC S1SPKI CA Key Pair.

(C) The FOC S1SP shall ensure that all FOC S1SPKI CA Private Keys that are not required for continuous operational purposes will be encrypted and stored securely in an off-line security container which requires M of N to activate the FOC SS1SPKI CA Private Key when required.

6.1.2 Private Key delivery to Subscriber

(A) In accordance with Part 6.1.1(B) of this Policy, the FOC S1SPKI CA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key delivery to Certificate issuer

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS or the FOC S1SPKI RAPP as the case may be, incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the FOC S1SPKI CA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 FOC S1SPCA Public Key delivery to Relying Parties

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions:

(i) in relation to the manner by which each FOC S1SPKI CA Public Key is to be lodged in the relevant FOC S1SPKI Repository;

(ii) designed to ensure that the FOC S1SPKI CA Public Keys are securely lodged in the FOC S1SPKI Repository in such a manner as to guarantee that their integrity is maintained; and

(iii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10 where FOC SS1SPKI CA Public Keys are delivered direct to the Relying Party.

6.1.5 Key sizes

(A) The FOC S1SPKI CA and every Subscriber shall ensure that all Key Pairs which each of them may use for the purposes of this Policy are of the size and characteristics set out in Annex B of this Policy.

6.1.6 Public Key parameters generation and quality checking

(A) The FOC S1SPKI CA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage purposes (as per X.509 v3 keyUsage field)

(A) The FOC S1SPKI CA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The FOC S1SPKI CA shall ensure that each FOC S1SPKI End Entity Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The FOC S1SPKI CA shall ensure that each FOC S1SPKI CA Certificate that is Issued by it has a `keyUsage` of either:

(i) `keyCertSign`; or

(ii) `CRLSign`.

(D) The FOC S1SPKI CA shall ensure that no `keyUsage` values may be set in an FOC S1SPKI End Entity Certificate or FOC S1SPKI CA Certificate other than in accordance with this Part 6.1.7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the cryptographic module, standards, and controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA. Which should include, but not be limited to:

(i) ensuring that all FOC S1SPKI CA Private Keys shall be:

(a) protected to a high standard of assurance by physical and logical security controls; and

(b) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(ii) ensuring that all FOC S1SPKI CA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(iii) ensuring that no FOC S1SPKI CA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(iv) ensuring that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(a) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Organisation CPS; and

(b) require to be unblocked by an authorised Privileged User who has been Authenticated as such following a process which shall be set out in the Organisation CPS.

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

(A) See Part 6.1.1 of this Policy and the FOC S1SPKI CPS for further details.

6.2.3 Private Key escrow

(A) This Policy does not support Key Escrow.

(B) The FOC S1SPKI CA shall not provide any Key Escrow service.

6.2.4 Private Key backup

(A) The FOC S1SPKI CA may Back-Up FOC S1SPKI CA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an FOC S1SPKI CA Private Key in accordance with this Policy.

(B) Participants providing trust services may backup and archive Private Keys, including CA-keys.

6.2.5 Private Key archival

No stipulation.

6.2.6 Private Key transfer into or from a cryptographic module

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the FOC S1SPCA Private Key transfer into or from a cryptographic module for the following purposes only:

(i) Back-Up; or

(ii) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services; and

(iii) where such transfers are in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key storage on cryptographic module

(A) See Part 6.2.1 of this Policy.

6.2.8 Method of activating Private Key

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the method of activating a Private Key, whereby:

(i) The FOC S1SPKI CA shall ensure that the Cryptographic Module in which any FOC S1SPKI CA Private Key is stored may be accessed only by a Privileged User who has been Authenticated following an Authentication process which:

(a) has an appropriate level of strength to ensure the protection of the Private Key; and

(b) involves the use of Activation Data.

6.2.9 Method of deactivating Private Key

(A) The FOC S1SP shall ensure that any FOC S1SPKI CA Private Key shall be capable of being de-activated by means of the FOC S1SPKI CA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; or

(d) a period of inactivity of a length which shall be set out in the FOC S1SPKI CPS.

6.2.10 Method of destroying Private Key

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions for the exercise of strict controls in relation to the destruction of FOC S1SPKI CA Keys.

(B) The FOC S1SP shall ensure that no FOC SS1SPKI CA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the DCC or the FOC S1SP ITSC instructing the FOC S1SPKI CA to destroy it.

6.2.11 Cryptographic Module Rating

(A) See Part 6.2.1 of this Policy.

6.3 Other aspects of key pair management

6.3.1 Public key archival

(A) The FOC S1SPKI CA shall ensure that it archives Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate operational periods and key pair usage periods

(A) The FOC S1SPKI CA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

Certificate	Validity (Years)
Operator Root CA Certificate	25 years
Intermediate Operator CA Certificate	20 years
Intermediate Enterprise CA Certificate	20 years
End Entity Operator Device Certificate	5 years
End Entity Push Certificate	5 years
End Entity Server Certificate	5 years
Application Service Root CA Certificate	25 years
Intermediate Application Service PKI CA Certificate	20 years
End Entity PKI Role CA Certificate	5 years
End Entity PKI Role RA Certificate	5 years

6.4 Activation Data

6.4.1 Activation Data generation and installation

(A) The FOC S1SPKI CA shall ensure that any secure container within which a FOC S1SPKI CA Private Key is held has Activation Data that are unique and unpredictable.

(B) The FOC S1SPKI CA shall ensure that:

(C) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the FOC S1SPKI CA Private Keys; and

(D) where the Activation Data comprise any PINs, passwords or passphrases, the FOC S1SPKI CA shall have the ability to change these at any time.

6.4.2 Activation data protection

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data/

[Not applicable in this Policy]

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the FOC S1SPKI CA;
(ii) the appropriate allocation of responsibilities to Privileged Users;
(iii) the identification and Authentication of organisations, individuals and Systems involved in FOC S1SPKI CA activities;
(iv) the use of cryptography for communication and the protection of Data stored on the FOC S1SPKI CA Systems;
(v) the audit of security related events; and
(vi) the use of recovery mechanisms for FOC S1SPKI CA Keys.

6.5.2 Computer security rating

(A) The FOC S1SP shall ensure that the Organisation CPS incorporates provisions relating to the appropriate security rating of the FOC S1SPKI CA Systems.

(B) The FOC S1SP may, where not specifically required to under this Policy, use certain system components that do not possess a formal computer security rating provided that all requirements of this Policy are satisfied.

6.6 Life cycle technical controls

6.6.1 System development controls

(A) The FOC S1SPshall ensure that any software which is developed for the purpose of establishing a functionality of the FOC S1SPKI CA Systems shall:
(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;
(ii) be undertaken by a developer which has a quality system that is:
(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); and

(B) where so required, be available for inspection and approval by the DCC or the FOC S1SP ITSC and has been so inspected and approved where the case may be.

6.6.2 Security management controls

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions which are designed to ensure that the FOC S1SPKI CA 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.

(B) As a minimum the scope of the FOC S1SPKI must achieve certification with following information security standard:
(i) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or
(ii) any equivalent to that standard which updates or replaces it from time to time.

(C) The FOC S1SP shall also ensure that the FOC S1SPKI shall be independently assessed against an assurance scheme:
(i) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;
(ii) which is based on ISO 27001; and
(iii) the provider of which:
(a) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and
(b) requires all its scheme assessors to be UKAS certified.

6.6.3 Life cycle security controls

(A) See Part 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Use of Offline Operator Root CA

(A) The FOC S1SP shall ensure that its functions as the FOC S1SPKI CA are carried out on a part of the FOC S1SPKI CA Systems that is neither directly nor indirectly connected to any System which is not a part of the FOC S1SPKI CA Systems.

(B) The Operator Root CA, when not operational, should be kept offline with no direct or indirect network access.

(C) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions which are designed to ensure the requirements of paragraphs (A) and (B) above.

6.7.2 Protection Against Attack

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to:

(i) using its best endeavours to ensure that the FOC S1SPKI Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(ii) any Denial of Service Event; and

(iii) any unauthorised attempt to connect to them.

(B) using all reasonable to steps to ensure that the FOC S1SPKI CA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of FOC S1SP Intermediate CAs

(A) The FOC S1SP shall ensure that, where its functions as the FOC S1SP Intermediate CA are carried out on a part of the FOC S1SPKI CA Systems that is connected to an external network, they are carried out on a System that is Separated from all other FOC S1SPKI CA Systems.

6.7.4 Health Check of FOC SS1SPCA Systems

(A) The FOC S1SP shall ensure that, in relation to the FOC S1SPKI CA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent S1SPKM Assurance Service Provider.

6.8 Time-Stamping

6.8.1 Use of Time-Stamping

(A) The FOC S1SP shall ensure that Timestamping takes place in relation to all Certificates and all other FOC S1SPKI CA activities which require an accurate record of time.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the FOC S1SPKI CA.

7 CERTIFICATE, CRL PROFILES

7.1 Certificate profile

(A) The FOC S1SPCA shall only Issue Certificates in accordance with the Certificate Profiles in Annex B of this Policy.

7.1.1 Version number(s)

(A) See Annex B of this Policy.

7.1.2 Certificate extensions

(A) See Annex B of this Policy.

(B) The FOC S1SPKI CA shall process the extensions identified in sections 4.2.1 and 4.2.2 of the IETF RFC 5280 Certificate Profile Specification. The following are common Certificate extensions:

I. The Basic Constraints extension is set to TRUE for CA-Certificates only; its use is critical specifying that it is a CA-Certificate. Subscriber End Entity Certificates have the value set to FALSE.

7.1.3 Algorithm object identifiers

(A) See Annex B of this Policy.

7.1.4 Name forms

(A) See Annex B of this Policy.

7.1.5 Name constraints

(A) See Annex B of this Policy.

7.1.6 Certificate policy object identifier

(A) See Part 1.2 of this Policy.

7.1.7 Usage of Policy Constraints extension

(A) See Annex B of this Policy.

7.1.8 Policy qualifiers syntax and semantics

(A) See Annex B of this Policy.

7.1.9 Processing semantics for the critical Certificate Policies extension

(A) See Annex B of this Policy.

7.2 CRL profile

7.2.1 Version number(s)

(A) The FOC S1SPKI CA shall ensure that the FOC S1SP ARL and FOC S1SP CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL entry extensions

(A) [Not applicable in this Policy].

7.3 OCSP profile

7.3.1 Version number(s)

(A) An OCSP service is not applicable in this Policy.

7.3.2 OCSP extensions

(A) [Not applicable in this Policy].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.2 Identity/qualifications of assessor

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.3 Assessor's relationship to assessed entity

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.4 Topics covered by assessment

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.5 Actions taken as a result of deficiency

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.6 Communication of results

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

(A) This document forms part of the Smart Energy Code and the DCC is required to ensure that the FOCS1SPKI is implemented and operated in accordance with this Policy and the associated FOC S1SPKI CPS.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

See the statement at the beginning of this Part.

9.1.2 Certificate access fees

See the statement at the beginning of this Part.

9.1.3 Revocation or status information access fees

See the statement at the beginning of this Part.

9.1.4 Fees for other services

See the statement at the beginning of this Part.

9.1.5 Refund policy

See the statement at the beginning of this Part.

9.2 Financial responsibility

9.2.1 Insurance coverage

See the statement at the beginning of this Part.

9.2.2 Other assets

See the statement at the beginning of this Part.

9.2.3 Insurance or warranty coverage for end-entities

See the statement at the beginning of this Part.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

See the statement at the beginning of this Part.

9.3.2 Information not within the scope of confidential information

See the statement at the beginning of this Part.

9.3.3 Responsibility to protect confidential information

See the statement at the beginning of this Part.

9.4 Privacy of personal information

See the statement at the beginning of this Part.

9.4.1 Privacy plan

See the statement at the beginning of this Part.

9.4.2 Information treated as private

See the statement at the beginning of this Part.

9.4.3 Information not deemed private

See the statement at the beginning of this Part.

9.4.4 Responsibility to protect private information

See the statement at the beginning of this Part.

9.4.5 Notice and consent to use private information

See the statement at the beginning of this Part.

9.4.6 Disclosure pursuant to judicial or administrative process

See the statement at the beginning of this Part.

9.4.7 Other information disclosure circumstances
See the statement at the beginning of this Part.

9.5 Intellectual property rights
See the statement at the beginning of this Part.

9.6 Representations and warranties
See the statement at the beginning of this Part.

9.7 Disclaimers of warranties
See the statement at the beginning of this Part.

9.8 Limitations of liability
See the statement at the beginning of this Part.

9.9 Indemnities
See the statement at the beginning of this Part.

9.10 Term and termination

9.10.1 Term
See the statement at the beginning of this Part.

9.10.2 Termination
See the statement at the beginning of this Part.

9.10.3 Effect of termination and survival
See the statement at the beginning of this Part.

9.11 Individual notices and communications with participants

9.11.1 Subscribers
See the statement at the beginning of this Part.

9.11.2 Issuing Authority
See the statement at the beginning of this Part.

9.11.3 Notification
See the statement at the beginning of this Part.

9.12 Amendments

9.12.1 Procedure for amendment
See the statement at the beginning of this Part.

9.12.2 Notification mechanism and period
See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID must be changed
See the statement at the beginning of this Part.

9.13 Dispute resolution provisions
See the statement at the beginning of this Part.

9.14 Governing law
See the statement at the beginning of this Part.

9.15 Compliance with applicable law
See the statement at the beginning of this Part.

9.16 Miscellaneous provisions

9.16.1 Entire agreement
See the statement at the beginning of this Part.

9.16.2 Assignment
See the statement at the beginning of this Part.

9.16.3 Severability
See the statement at the beginning of this Part.

9.16.4 Enforcement (attorneys' fees and waiver of rights)
See the statement at the beginning of this Part.

9.16.5 Force Majeure
See the statement at the beginning of this Part.

9.17 Other provisions

9.17.1 Certificate Policy Content
See the statement at the beginning of this Part.

9.17.2 Third party rights
See the statement at the beginning of this Part.

Glossary

10 Annex A: Definitions and Interpretation

Definitions	Interpretations
Activation	means the process of making the FOC S1SP HES and Operator Private Keys stored available for use.
Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Security Container.
Application Service End Entity Certificate	means either an End Entity PKI Role CA Certificate or an End Entity PKI Role RA Certificate issued by an Intermediate Application Service PKI CA as set out in Annex B of this Policy.
Application Service CA	means the FOC S1SP exercising the function of the Application Service Root CA to Issue Certificates to the Intermediate Application Service PKI CA and the Intermediate Application Service PKI CA and storing and managing Private Keys associated with those functions.
Application Service CA Certificate	means either an Application Service Root CA Certificate or an Intermediate Application Service CA Certificate.
Application Service PKI	means one of the three public key infrastructures that support the operation of each of the FOC S1SP Operator Root CA, the Intermediate Operator CA and the Intermediate Enterprise CA.
Application Service Registration Authority (Application Service RA)	Means the Application Service CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
Application Service Root Certification Authority (Application Service Root CA)	means the FOC S1SP exercising the functions of each or all of three Application Service Root CAs to Issue Intermediate Application Service PKI CA Certificates to each or all of the three Intermediate Application Service PKI CAs and storing and managing Private Keys associated with that function.
Application Service Root CA Certificate	means one of the self-signed Certificate issued by the Application Service Root CA that meets the requirements of the Application Service Root CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
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 and the FOC S1SPKI CPS.
Authentication	means the process of establishing that an individual, Certificate, System, SMETS1 Device or Organisation is what he or it claims to be (and “Authenticate” shall be interpreted accordingly).
Authorised Subscriber	means one of the entities described as such in Annex E of this Policy.
Back-Up	means, in relation to Data which is held on any FOC S1SP HES System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and “Backed-Up” is to be interpreted accordingly.
Certificate	means any public key certificate Issued under this Certificate Policy by the FOC S1SPCA or the Application Service CA, the certificate being an electronic document issued by a FOC S1SPCA that is used to prove the

	ownership of a Public Key. Valid Certificates under this Policy are: • FOC S1SPCA Certificates; • FOC S1SP End Entity Certificates; • Application Service CA Certificates; • Application Service End Entity Certificates.
Certification Authority	means the FOC S1SPCA and/or the Application Service CA as the context requires.
Certificate Policy (known as the 'Policy' in this document)	is a document which aims to state what are the different entities of a Public Key Infrastructure (PKI), their roles and their duties.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Revocation List Distribution Point (CDP)	means a shared location on the network that is used to store the CRLs
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number which results in a new Certificate being issued.
Certificate Revocation Request (CRR)	means a request for the revocation of a Certificate made to the FOC S1SPCA, submitted in accordance with the FOC S1SPKI RAPP and this Policy.
Certificate Signing Request (CSR)	means a request for a Certificate submitted by an Authorised Subscriber in accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy.
Certificate Status	Provides details of the validity of Certificates and includes Revocation information.
Cryptographic Module	Means a Security Container.
Cryptographic Processing	means the generation, storage or use of any Secret Key Material
Data	means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Eligible Subscriber	means one of the entities described as such (and in relation to the relevant Certificate types) in Annex E of this Policy:
End Entity Operator Device Certificate	A Certificate issued by the Operator CA that meets the requirements of the End Entity Operator Device Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role CA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role RA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role RA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Push Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Push Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Server Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Server Certificate profile set out in Annex B and which is issued in accordance with this Policy.

FOC S1SP	Means any one of the following DCC Service Providers responsible for the delivery and operation of the FOC S1SPKI service: • TRILLIANT NETWORKS OPERATIONS (UK) LTD] (registered in England and Wales under number 011321639 whose registered office is at Morgan House, Madeira Walk, Windsor, Berkshire SL4 1EP acting in its capacity as a DCC Service Provider. • CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21 6DB acting in its capacity as a DCC Service Provider. • (DXC) ENTSERV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider. Where they are acting in the capacity of, and exercising the functions of one or more of: (a) FOC S1SPCA; (b) the FOC S1SPKI Registration Authority; (c) and any other aspects of the wider FOC S1SPKI Systems.
FOC S1SP Authority Revocation List (FOC S1SP ARL)	means a list, produced by the FOC S1SPCA, of all FOC S1SPCA Certificates that have been revoked in accordance with this Policy.
FOC S1SP CA Certificates	Means either an Operator Root CA Certificate, an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy.
FOC S1SP Certification Authority (or FOC S1SPCA)	means the Secure S1SP, acting in the capacity and exercising the functions of one or more of the: (a) FOC S1SP Operator Root CA; (b) Intermediate Operator CA; (c) Intermediate Enterprise CA; (d) FOC S1SPCA Systems; and (e) FOC S1SP PKI Registration Authority.
FOC S1SP Certificate Revocation List (FOC S1SPKI CRL)	means a list, produced by the FOC S1SPKI Intermediate CA, of all FOC S1SP End Entity Certificates that have been revoked in accordance with this Certification Policy.
FOC S1SP End Entity Certificates	means either an End Entity Server Certificate, an End Entity Push Certificate, or an End Entity Operator Device Certificate issued by a FOC S1SP CA as set out in Annex B of this Policy.
FOC S1SP Head End System	means the head end system which is used by the FOC S1SP to communicate with SMETS1 CHs.
FOC S1SP Intermediate Certification Authority (FOC S1SP Intermediate CA)	means the FOC S1SP exercising the function of the FOC S1SP Intermediate Enterprise CA and the Intermediate Operator CA to Issue FOC S1SP End Entity Certificates in accordance with Annex B of this Policy.
FOC S1SP Intermediate Certification Authority Certificate (FOC S1SP Intermediate CA Certificate)	Means either an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy and Issued by the FOC S1SP Root CA in accordance with this Policy.
FOC S1SP Intermediate Certification Authority Private Key (FOC S1SP Intermediate CA Private Key)	Means either: • The Intermediate Operator CA Private Key; or • The Intermediate Enterprise CA Private Key.

FOC S1SP Intermediate Certification Authority Service Provider (FOC S1SP Intermediate CA SP)	Means (DXC) ENTSERV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider.
FOC S1SP Operator Root Certification Authority (CA)	means the FOC S1SP exercising the function of the FOC S1SP Operator Root CA to Issue Certificates to the FOC S1SP Operator Root CA and the FOC S1SP Intermediate CA and storing and managing Private Keys associated with those functions.
FOC S1SP Operator Root Certification Authority Service Provider (FOC S1SP Operator Root CA SP)	means CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21 6DB acting in its capacity as a DCC Service Provider.
FOC S1SPKI	means the S1SPKIs operated by the FOC S1SP including the FOC S1SP Head End Systems, FOC S1SPCA Systems, personnel, policy and procedures and any public key infrastructure established (or to be established) by FOC S1SP for the purpose, among other things, of providing secure communications between FOC S1SP, the DCC and SMETS1 Devices. It also includes the Application Service PKIs.
FOC S1SPKI CA	Means the FOC S1SPCA and the Application Service CA.
FOC S1SPKI CA Certificate	Means any FOC S1SPCA Certificate and any Application Service CA Certificate.
FOC S1SPKI CA Private Key	Any Private Key associated with a Public Key contained with any FOC S1SPCA Certificate or any Application Service CA Certificate.
FOC S1SPKI CA Key Pair	A Public Key that is (or is to be) contained within any FOC S1SPCA Certificate or any Application Service CA Certificate and the associated Private Key.
FOC S1SPKI CPS	means the Certification Practice Statement describing how this PKI is operated and maintained and corresponds to this Policy
FOC S1SPKI End Entity Certificate	Means any FOC S1SPKI End Entity Certificate or any Application Service End Entity Certificate.
FOC S1SPKI Personnel	means those persons who are engaged by the FOC S1SP under this Policy, in so far as such persons carry out, or are authorised to carry out, any function of such FOC S1SPKI System or FOC S1SPCA or Application service CA but not Registration Authority functions (see FOC S1SPKI RA Personnel).
FOC S1SPKI RAPP	is set out in the SEC document set and is the Registration Authority Policy and Procedures (RAPP) for this policy document
FOC S1SPKI Registration Authority (RA)	Means the FOC S1SPKI CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Manager	means either a director of the FOC S1SP or any other person who may be identified as such in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Personnel (FOC S1SPKI RA Personnel)	means those persons who are engaged by the FOC S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the FOC S1SPKI Registration Authority
FOC S1SPKI Repository	For the purposes of the FOC S1SPKI, the “FOC S1SPKI Repository” means a number of Systems for storing and (subject to

	the provisions of this Policy) making available copies of Certificates Issued pursuant to the Policy.
Hardware Security Module (HSM)	means a security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
Intermediate Application Service PKI CA Certificate	means one of the Certificates issued by the Application Service Root CA that meets the requirements of the Intermediate Application Service PKI CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
Intermediate Enterprise Certification Authority (Intermediate Enterprise CA)	means the FOC S1SP exercising the function of the Intermediate Enterprise CA to Issue End Entity Push Certificates, End Entity Server Certificates, and of storing and managing the Private Keys associated with that function.
Intermediate Enterprise Certification Authority Certificate (Intermediate Enterprise CA Certificate)	means a Certificate in the form set out in the Intermediate Enterprise CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Enterprise CA in accordance with this Policy.
Intermediate Enterprise Certification Authority Private Key (Intermediate Enterprise CA Private Key)	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Enterprise CA Certificate.
Intermediate Operator CA Certificate (Intermediate Operator CA Certificate)	means a Certificate in the form set out in the Intermediate Operator CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Operator CA in accordance with this Policy.
Intermediate Operator Certification Authority (Intermediate Operator CA)	means the FOC S1SP exercising the function of the Intermediate Operator CA to Issue End Entity Operator Device Certificates and of storing and managing the Private Keys associated with that function.
Intermediate Operator Certification Authority Private Key (Intermediate Operator CA Private Key)	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Operator CA Certificate.
Intermediate Application Service PKI Certification Authority (Intermediate Application Service PKI CA)	means the FOC S1SP exercising the functions of each or all of the three Intermediate Application Service PKI CAs to Issue End Entity PKI Role CA Certificates and End Entity PKI Role RA Certificates and storing and managing Private Keys associated with that Function.
Policy	means this FOC S1SP Certificate Policy.
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key cryptography and which is associated with a Public Key that is contained within any Certificate that is Issued (or to be Issued) in accordance with this Policy.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Privileged User	means a FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the FOC S1SPCA System and which are capable of being a means by which the FOC S1SPCA System (or are capable of being) being compromised to a material extent
Public Key	means the public part of an asymmetric Key Pair used for the purposes of public key cryptography.
Public Key Infrastructure	is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store

	and revoke digital Certificates and manage public-key encryption
Relying Party	means any System, Device, organisation or individual that relies on a Certificate that has been Issued under this Policy.
S1SP	means SMETS1 Service Provider
S1SPKI	means any public key infrastructure established (or to be established) for the purpose, among other things, of providing secure communications between the DCC and SMETS1 Devices.
S1SPKI CA Systems	means the FOC S1SPCA Systems and the Application Service CA Systems.
Secret Key Material	means any Private Key, Shared Secret, Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by the FOC S1SP CA
Security Container	means a set of hardware, software and/or firmware that is designed for : a) the secure storage of Secret Key Material; and b) the implementation of Cryptographic Processing without revealing Secret Key Material.
Security Related Functionality	means the functionality of the FOC S1SP HES Systems which is designed to detect, prevent or mitigate the adverse effect of any security compromise of that System.
Security Sub-Committee or SSC	means the Security Sub-Committee under the Smart Energy Code
Smart Energy Code	means the code of that name maintained pursuant to the smart meter communication licences granted under the UK Gas Act 1986 and the UK Electricity Act 1989
SMETS1	means the Smart Metering Equipment Technical Specifications 1
Subject	the Subject of any Certificate is the entity identified in the subject field of that Certificate
Subscriber	the FOC S1SPKI Systems or a person engaged by the S1SPKI CA (acting on behalf of the S1SPKI CA) to which a Certificate has been Issued in accordance with the requirements of this Policy.
System	means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware, databases and Data associated with issuing Certificates in accordance with this Policy.
Task Manager	is a function in the Trilliant software which instructs an API to perform specific tasks such as certificate administration services.
Timestamping	means the act that takes place when a Time-Stamping Authority, in relation to a 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.
Timestamping Authority	A trusted timestamp is a timestamp issued by a Trusted Third Party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point without the possibility that the owner can backdate the timestamps.
Trust Store	or Repository holding the Certificates for each trusted CA

Validity Period	means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

11 Annex B: FOC S1SP CA and End Entity Certificate Profiles

11.1 Certificate Structure and Contents

(A) This Annex lays out requirements as to structure and content with which FOC S1SPCA Certificates and FOC S1SP End Entity Certificates shall comply. All terms in this Annex shall, where not defined in this Policy, or the GB Companion Specification (GBCS), have the meanings in IETF RFC 5759 or IETF RFC5280.

11.2 Common requirements applicable to FOC S1SPCA Certificates and FOC S1SP End Entity Certificates

(A) All Certificates shall be compliant with IETF RFC 5759 and so with IETF RFC5280. The FOC S1SPCA shall only issue X.509 v3 certificates as defined in IETF RFC 5280 and IETF RFC 6818.

Public Key and algorithm	Issued Certificates	Internal TLS Certificates
Signature Algorithm	OID 1.2.840.10045.4.3.2 [ecdsa-with-SHA256]	OID 1.2.840.10045.4.3.2 [ecdsa-with-SHA256]
Subject Public Key	OID 1.2.840.10045.3.1.7 [ECDSA secp256r1]	OID 1.3.132.0.34 [ECDSA secp384r1]

Operator Root Certificate

Number of Keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
basicConstraints	yes	cA: TRUE	
keyUsage	yes	keyCertSign, cRLSign	

Intermediate Operator CA Certificate

Number of keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Operator	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: TRUE	
`keyUsage`	yes	`keyCertSign, cRLSign`	

Intermediate Enterprise CA Certificate

Number of keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: TRUE	
`keyUsage`	yes	`keyCertSign, cRLSign`	

End Entity Operator Device Certificate

Number of keys: One per device

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Dynamic Per Device]	Printable String
	OU	[Environment Specific]	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	**Critical**	**Value**	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	
`extKeyUsage`	no	TLS Web Server Authentication	

End Entity Push Certificate

Number of keys: One per environment (HES instance)

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Environment Specific]	Printable String
	OU	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	

End Entity Server Certificate

Number of keys: One per environment (HES instance)

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Environment Specific]	Printable String
	OU	[Environment Specific]	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	
`extKeyUsage`	no	TLS Web Server Authentication	

Application Service Root CA Certificate – Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
basicConstraints	Yes	cA:TRUE	
keyUsage	Yes	keyCertSign, CRLSign	

Intermediate Application Service PKI CA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
basicConstraints	Yes	cA:TRUE	
keyUsage	Yes	keyAgreement, digitalSignature, keyCertSign	

End Entity PKI Role CA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	PKI Role CA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
basicConstraints	yes	cA:FALSE	
keyUsage	yes	keyAgreement, digitalSignature	

End Entity PKI Role RA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	PKI Role RA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
basicConstraints	yes	cA:FALSE	
keyUsage	yes	keyAgreement, digitalSignature	

12 Annex C: Subscriber Obligations

12.1 Certificate Signing Requests

(A) Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate.

(B) No Eligible Subscriber may make a Certificate Signing Request which contains:

- (i) any information that constitutes a trademark, unless it is the holder of the Intellectual Property Rights in relation to that trademark; or
- (ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

(C) Each Eligible Subscriber shall ensure that the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

(D) No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

- (i) a FOC S1SPKI CA Certificate or FOC S1SP End Entity Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other FOC S1SPKI CA Certificate or FOC S1SPKI End Entity Certificate.

12.2 Use of Certificates and Key Pairs

(A) Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or a Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from SMETS1 Devices, the DCC and the FOC S1SP pursuant to the Code.

12.3 FOC S1SPKI CA and End Entity Certificates: Protection of Private Keys

(A) Each Subscriber shall take reasonable steps to ensure that no Compromise occurs to any:

- (i) Private Key which is associated with a Public Key contained in a Certificate for which it is the Subscriber; or
- (ii) Secret Key Material associated with that Private Key.

12.4 Certificates: Expiry of Validity Period

(A) Each Subscriber shall, prior to the expiry of the Validity Period of a Certificate for which it is the Subscriber:

- (i) request a replacement for that Certificate by applying for the Issue of a new Certificate in accordance with the provisions of this Policy.

13 Annex D: Relying Party Obligations

13.1 Relying Parties

(A) For the purposes of this Policy, a Relying Party in relation to a FOC S1SPKI CA Certificate or a FOC S1SPKI End Entity Certificate means any FOC S1SPKI System, SMETS1 Device or person which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from the FOC S1SPKI System, the DCC, any person or SMETS1 Device pursuant to this Policy.

(B) For the purposes of Section L13.1, a Relying Party shall be deemed to include:

- (i) in the case of a FOC S1SPKI System which relies on a Certificate, the FOC S1SP; and
- (ii) in the case of a SMETS1 Device which relies on a Certificate, the FOC S1SP.

13.2 Duties in relation to Certificates

(A) Each Relying Party shall:

- (i) before relying on any FOC S1SPKI End Entity Certificate:
  - (a) Check Cryptographic Protection in respect of the FOC S1SP CRL on the relevant FOC S1SPKI Repository; and
  - (b) where that Certificate is shown on the FOC S1SPKI CRL as having been revoked, not rely on the Certificate;
- (ii) before relying on any FOC S1SPCA Certificate:
  - (a) Check Cryptographic Protection in respect of the FOC S1SPKI ARL on the FOC S1SPKI Repository; and
- (iii) where that Certificate is shown on the FOC S1SPKI ARL as having been revoked, not rely on the Certificate;

(B) No Relying Party may rely on a Certificate where the Validity Period of that Certificate has expired.

(C) No Relying Party may rely on a Certificate where it suspects that the Certificate has been Compromised.

(D) Each Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Certificate.

14 Annex E: FOC S1SPKI RAPP

14.1 Purpose

(A) This Annex E: FOC S1SPKI RAPP sets out the high-level principal obligations and activities undertaken by the FOC S1SPKI CA in its capacity as the FOC S1SPKI Registration Authority in accordance with this Policy. The FOC S1SPKI RAPP also sets out the activities undertaken by the FOC S1SPKI Registration Authority in support of the procedures as set out in this section.

(B) The FOC S1SPKI CA shall ensure that no Certificate is Issued under this Policy other than to an Eligible Subscriber for a Certificate of the relevant type.

14.2 FOC S1SPKI RAPP Principles

(A) All Certificates requested and Certificates issued under the auspices of the FOC S1SPKI CA must be:

- (i) compliant with PKCS#10;
- (ii) BER encoded;
- (iii) compliant with the Certificate Profiles as set out in Appendix B of this Policy; and
- (iv) compliant with the obligations as set out in Annex C of this Policy.

14.3 FOC S1SPKI Registration Authority Roles

(A) The FOC S1SPKI RA consists of the following roles:

- (i) The Intermediate Operator CA performing the technical RA role for automatically approving End Entity Operator Device Certificates for issuance (as requested by the FOC S1SP HES on behalf of the SMETS1 Device);
- (ii) FOC S1SPKI RA Personnel submitting and approving all other Certificates for issuance.

(B) Only FOC S1SPKI RA Personnel with Privileged User rights can submit and approve Certificates on behalf of Eligible Subscribers using the FOC S1SPKI CA Systems. This is enforced through:

- (i) Pre-authorised and pre-approved access to FOC S1SPKI CA Systems;
- (ii) Access control to the FOC S1SPKI CA Systems;
- (iii) User account management (audit and logging);
- (iv) Dedicated named accounts on the FOC S1SPKI CA System;

(C) Prior to being granted access to FOC S1SPKI CA Systems, all such FOC S1SPKI RA Personnel with Privileged User rights will either have:

- (i) identities checked in line with personnel security standard BS7858; and/or
- (ii) /background clearance checks performed in accordance with this Policy and the FOC S1SPKI CPS.

14.4 Authorised Subscribers

(A) The following are Authorised Subscribers under this Policy:
(B) a SMETS1 Device with which the FOC S1SP is to communicate;
(C) the FOC S1SP HES;
(D) the FOC S1SPCA;
(E) the Application Service CA; and
(F) FOC S1SPKI Personnel (acting on behalf of the FOC S1SP).
(G) At the point of the FOC S1SPKI RA approving the above, then it (or they) become an Authorised Subscribers.

14.5 Eligible Subscribers

(A) Where it is, or they are, an Authorised Subscriber, the following is/are an Eligible Subscriber in respect to the specified Certificates:

- (i) the FOC S1SP HES which is an Eligible Subscriber for the following FOC S1SP End Entity Certificates only:

(a) End Entity Server Certificate; or
(b) End Entity Push Certificate;

(ii) the FOC S1SPCA is an Eligible Subscriber for all FOC S1SPCA Certificates.

(iii) SMETS1 Devices are Eligible Subscribers for the following FOC S1SP End Entity Certificate only:
(a) End Entity Operator Device Certificate.

(iv) The Application Service CA which is an Eligible Subscriber for the following Application CA Certificates only:
(a) Application Service Root CA Certificate;
(b) Intermediate Application Service PKI CA Certificate.

(v) FOC S1SPKI Personnel, who are Eligible Subscribers for End Entity PKI Role RA Certificates only.

(vi) S1SPKI CA Systems which is are only Eligible Subscriber for End Entity PKI Role CA Certificates.

14.6 FOC S1SPKI Technical RA Verification and Issuance of Certificates

(A) For personnel controls, resources providing trust services, have either SC or BS7858 Clearance and training for the provisioning of digital certificates.

(B) All relevant personnel are security cleared and trained to manage the provisioning of digital certificates. The overall management of the vetting process is provided by the relevant Secure Vetting Team, liaising directly with the Account Security Officer at DCC.

Comments	Manual Certificate Generation	Automated Certificate Generation
(A) Both the Intermediate Enterprise CA and the Intermediate Operator CA are subscribers of Certificates that are Issued by the Operator Root CA which is operated by Capgemini. Another subscriber includes the Comms Hub as Certificates are issued to it by the Intermediate Operator CA. (B) The Intermediate Operator CA performs the following technical RA check in response to a Certificate Signing Request. I. An Operator Device Certificate (ODC) is issued to each Comms Hub. The Certificates are signed by the Intermediate Operator CA, with the Head End acting as a registration authority and delivering these Certificates to the Comms Hub. Each Comms Hub will	Before sending the CSR the file must be encrypted with the requestors GPG public key and signed with the senders own GPG key. This will allow the sender to validate the encryption before sending. Once encrypted the file is emailed to the requesting party representative.	Certificate changes take place under the governance of the Head End System. In its capacity as the Registration Authority it determines whether a Certificate needs to be issued and manages the creation of the CSR, rather than the end-device deciding that a Certificate needs to be issued and requesting the RA to forward a CSR to the CA. The Head End System will have established that it is communicating with a trusted device before if performs any Certificate operations. This uses the chain of trust that the Head End System has been explicitly configured with.

Comments	Manual Certificate Generation	Automated Certificate Generation
have its own ODC and Private Key, and the Head End will hold a copy of all ODCs. Each Comms Hub uses its ODC to identify itself during TLS session setup. The Certificate Signing Request is sent to a production central system (which incorporates the FOC S1SP CA Operator CA) in PKCS#10 file format. II. The Operator CA verifies the Certificate Signing Request as well as performing a proof of possession check using the PKCS#10 format. III. When the Operator CA verifies the CSR, then: a. it passes the CSR to the Comms Hub to process the Certificate Signing Request; b. If all verification checks are successful, the Comms Hub stores the Certificate chain and its own internal storage.		

14.7 Revocation of a Certificate

14.7.1 General Organisation Certificate revocation obligations

(A) The FOC S1SP shall permit each of the following individuals to request the revocation of a Certificate, where the reasons for such revocation request must be one of the permitted reasons for Certificate revocation as set out in Part 4.9 of this Policy:
(B) Any FOC S1SP ITSC member, on behalf of the FOC S1SP ITSC;
(C) Any Subscriber for a Certificate; or
(D) Any FOC S1SPKI RA Personnel, on behalf of the FOC S1SP.
(E) The FOC S1SP, in its role as FOC S1SPKI Registration Authority, shall only accept CRR via a secured electronic means as set out in this Annex E;
(F) The revocation of a Certificate shall be permanent and the FOC S1SPKI Registration Authority shall ensure that no revoked Certificate may be reinstated.
(G) The FOC S1SP shall, each month, prepare and submit a report to the DCC regarding the number and nature of Certificate revocations.

14.7.2 Procedure for Certificate Revocation

(A) The procedure for authorisation, verification and, where verified, revocation of Certificates is as set out immediately below.
(B) As soon as reasonably practicable when Certificate revocation is required:
  (i) An individual as per 14.7.1 (A) of this Annex E shall submit, using the mechanisms set out in 14.7.1 (B) of this Annex E, a CRR to the FOC S1SPKI Registration Authority.
  (ii) The reason for such CRR shall be one of the permitted reasons for Certificate revocation as set out in Section 4.9 of this Policy.
  (iii) Each CRR shall contain the following information:
    (a) Identity of the Subscriber;
    (b) Unambiguously (i.e. by specifying the serial number of the Certificate) identification of the Certificate to be revoked; and
    (c) The reason for the Certificate revocation.
(C) Upon receipt of the CRR, the FOC S1SPKI RA Personnel on behalf of the FOC S1SPKI RA shall, as soon as reasonably practicable:
  (i) Verify and authenticate the CRR; and
  (ii) Where verified and authenticated successfully, approve and then process the CRR; or
  (iii) Where the CRR cannot be successfully verified and authenticated:
    (a) Reject the CRR; and
    (b) Inform the individual making the CRR of such rejection; and
    (c) Immediately notify the FOC S1SP ITSC and the DCC of failed CRR attempts.
(D) The FOC S1SPKI RA shall, as soon as reasonably practicable following a successful CRR:
  (i) Revoke the identified Certificate that is the subject of the CRR;
  (ii) Update the relevant FOC S1SPKI ARL or FOC S1SPKI CRL and publish such ARL or CRL to the FOC S1SPKI Repository, as set out in this Policy; and
  (iii) Notify the FOC S1SP and the DCC of the successfully revocation of the Certificate in the CRR.
(E) The FOC S1SPKI Registration Authority shall treat each CRR and any associated circumstances as confidential.
(F) The FOC S1SPKI RA shall ensure that no single individual can request and subsequently approve a CRR.

14.8 Certificate Rotation

(A) Prior to the expiry of the validity period of a given Certificate the Registration Authority (Head End [automated] and system operator [manual]) must request a new Certificate by applying for the Issuance of a new Certificate in accordance with the provisions of this Policy.