Version 1.0

Appendix AP

S1SPKI Certificate Policy

Secure S1SP Certificate Policy for the Secure Cohort

Table of Contents

1 Introduction

The document comprising this Secure S1SP Certificate Policy (together with its Annexes A and B) shall be known as the "**Secure S1SP Certificate Policy**" (and in this document is referred to simply as the "**Policy**"). It is one of the S1SPKI Certificate Policies in the Smart Energy Code.

1.1 Overview

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

(i) SS1SP End Entity Certificates; and
(ii) SS1SPCA Certificates.

(B) 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'.

1.2 Document name and identification

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

1.3 Secure S1SP PKI (SS1SP PKI) participants

1.3.1 The Secure S1SP Certification Authority (SS1SPCA)

(A) The definition of Secure S1SP Certification Authority is set out in Annex A.

1.3.2 SS1SP PKI Registration Authorities

(A) The definition of SS1SP PKI Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy, certain Parties may become Authorised Subscribers.

(B) In accordance with the SS1SP PKI 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 SS1SP PKI 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 SS1SP PKI RAPP as set out in Annex E of this Policy and Subscriber Obligations as set out in Annex C this Policy.

(E) Obligations on the Secure S1SP acting in the capacity of an Eligible Subscriber can be found in the SS1SP PKI RAPP as set out in Annex E of this Policy.

(F) 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 SS1SP End Entity Certificate is represented by an appropriate identifier in the subject field of the SS1SP End Entity Certificate Profile (as the case may be) in accordance with Annex B.

(B) The Subject of a SS1SPCA Certificate must be the entity identified by the subject field of the Root SS1SPCA Certificate Profile, the Intermediate SS1SPCA Certificate Profile or the Subordinate SS1SPCA 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) Obligations on the Secure S1SP acting in the capacity of a Relying Party are set out in Annex D: Relying Party Obligations of this Policy.

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

1.3.6 SS1SP PKI Policy Management Authority

(A) The duties of the SS1SP PKI Policy Management Authority fall under the Security Sub-Committee for PKI (SSC for PKI). This executive group is responsible for fulfilling the duties of the PMA in relation to the SS1SP PKI. The terms of reference for operation of SSC for PKI is outlined in SSC for PKI Terms of Reference _1.0

1.3.7 SS1SP PKI Repository Provider

(A) SS1SPCA will be the SS1SP PKI Repository Provider.

1.4 Usage of SS1SP end entity certificates and SS1SPCA certificates

1.4.1 Appropriate Certificate Uses

(A) The Subordinate SS1SPCA shall ensure that SS1SP 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 Secure 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) Code signing (Digital Signature, Non-Repudiation, Code Signing);

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

4) Authentication and Non-Repudiation of Secure SMETS1 Devices (Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, TLS

Web Client Authentication, TLS Web Server Authentication).

(B) The SS1SPCA shall ensure that SS1SPCA Certificates are Issued only to the SS1SPCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root SS1SPCA;

(ii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate SS1SPCA; and

(iii) in its capacity as, and for the purposes of exercising the functions of, the Subordinate SS1SPCA.

(C) 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.

1.4.2 Prohibited Certificate Uses

(A) No Party shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 Policy administration

1.5.1 Organisation administering the Document

(A) This Policy is a Secure S1SP document and is administered as such in accordance with the provisions of this Policy and any supporting Policy documents.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the Secure S1SP's CISO (Chief Information Security Officer).

1.5.3 Person determining SS1SP CPS suitability for the Policy

(A) Security subcommittee for PKI (SSCPKI) will be responsible for determining the suitability of the SS1SP CPS.

1.5.4 SS1SP CPS approval procedures

(A) The SSCPKI shall approve the SS1SP CPS.

(B) The SS1SP shall keep the SS1SP CPS under review and shall in particular carry out a review of the SS1SP CPS whenever (and to the extent to which) it may be required to do so by the Security Sub committee for PKI

(C) Following any review of the SS1SP CPS:

(i) the SS1SP may propose amendments to it, which it shall submit to the SSCPKI for its approval; and

(ii) those amendments may be made only to the extent to which the SSCPKI has approved them.

1.5.5 Registration Authority Policies and Procedures

(A) The SS1SP PKI Registration Authority Policies and Procedures (the SS1SP PKI RAPP are set out in in Annex E of this Policy.

1.6 Definitions and acronyms

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Annex A and shall otherwise be interpreted in accordance with the Smart Energy Code.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Annex A.

2 Publication and repository responsibilities

2.1 Repositories

2.2 SS1SP PKI Repositories

(A) Each SS1SPCA has its own secure, encrypted repository that contains:

(i) Its private key (held in encrypted state at rest and subject to Secret Shares - see Parts 6.2.2 and 6.2.4 of the SS1SP CPS);

(ii) Copies of all Certificates generated and issued; and

(iii) Audit Log information with regards to the SS1SPCA functions which includes:

a) Certificate issued

b) Certificate date and time of issuance

c) Other data and data sets related to Certificates e.g. CSR.

2.3 Publication of certification information

(A) See Part 2.2 of the Policy.

2.4 Time or frequency of publication

(A) Immediately upon a Certificate being generated and issued by the SS1SPCA.

2.5 ACCESS CONTROLS ON SS1SP PKI REPOSITORIES

(A) All SS1SP PKI Repositories are subject to stringent access controls. Only authorised SS1SPCA Systems and Privileged Users have access to SS1SP PKI Repositories.

(B) All SS1SP PKI Repositories are:

(i) Encrypted using AES-128 (Galois Counter Mode);

(ii) Held off-line and not network connected until required; and

(iii) Reside in data centres in accordance with Part 5 of this Policy.

(C) SS1SPCA Private Keys held within the SS1SP PKI Repository are encrypted and further secured using M of N Secret Shares as described in Part 6.2.2 of this Policy.

3 Identification and authentication

3.1 Naming

3.1.1 Types of Names

(A) The SS1SPCA will ensure that the name of 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 SS1SPCA will 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) Under this Policy, the SS1SPCA will:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

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

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 trade mark; or

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

3.2 Initial identity verification

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SS1SP PKI 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 the Secure S1SP organisation is allowed to subscribe for Certificates under this Policy.

3.2.3 Authentication of SS1SP Parties

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the Authentication of SS1SP Parties engaged as Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified against a robust and assured authentication framework as agreed by the SSC for PKI.

3.2.4 Non-verified Subscriber Information

(A) The SS1SPCA shall:

(i) verify all information in relation to SS1SPCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a SS1SP End Entity Certificate.

(B) Further provision on the content of SS1SPCA Certificates 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

(A) [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 only supports a limited Certificate Re-Key service.

(B) The SS1SPCA shall provide a Certificate Re-Key service for SS1SPCA End Entity Certificates with the SMSO TLS Certificate profile and the SMSO KMS Certificate Profile as defined in Annex B.

(C) SS1SPCA End Entity Certificates with the Certificate Profiles in (B) above will be re-keyed every 5 years.

(D) Identification and authentication for routine re-key will be as per Part 3.2 of this Policy

3.3.2 Identification and Authentication for Re-Key after Revocation

(A) [Not applicable in this Policy]

3.4 Identification and authentication for revocation request

(A) [Not applicable in 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 SS1SP PKI RAPP as set out in Annex E of this Policy in relation to:

(i) in respect of a SS1SP 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 SS1SPCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a SS1SPCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the SS1SP PKI 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 Secure 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 SS1SPCA of a list of organisations, individuals, Systems and Secure SMETS1 Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the establishment of an enrolment process in respect of SS1SPCA Personnel and SS1SPCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the SS1SPCA in its capacity as the Registration Authority; and
(ii) including in particular, for that purpose, provision:

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

(b) for all Registration Authority Personnel to have their identify and authorisation verified against a robust assured authentication framework as agreed by the SSC for PKI.

4.2 Certificate application processing

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the Authentication by the SS1SPCA 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 SS1SP PKI RAPP as set out in Annex E of this Policy or this Policy, the SS1SPCA:

(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 SS1SP PKI RAPP as set out in Annex E of this Policy or any other provision of this Policy, the SS1SPCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) All Certificate applications to the SS1SPCA will be processed within 7 days.

4.3 Certificate issuance

4.3.1 SS1SPCA Actions during Certificate Issuance

(A) The SS1SPCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy and the SS1SP PKI 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 SS1SP PKI RAPP as set out in Annex E of this Policy.

(B) The SS1SPCA shall ensure that:

(i) each SS1SPCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each SS1SP End Entity Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A S1SPCA Certificate may only be:

(i) Issued by the SS1SPCA; and

(ii) for that purpose, signed using the SS1SPCA Root Private Key for the SS1SPCA Intermediate SS1SPCA or the Intermediate SS1SPCA Private Key for the Subordinate SS1SPCA.

(D) A SS1SP End Entity Certificate may only be:

(i) Issued by the Subordinate SS1SPCA; and

(ii) for that purpose, signed using a Subordinate SS1SPCA Private Key.

4.3.2 Notification to Eligible Subscriber by the SS1SPCA of Issuance of Certificate

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy for the SS1SPCA 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.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

(A) A Certificate which has been Issued by the SS1SPCA shall be treated as valid for any purposes of this Policy until it is treated as having been rejected by the Eligible Subscriber to which it was Issued.

(B) The SS1SPCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(C) Further provision in relation to the rejection and acceptance of Certificates is set out in Annex C of this Policy.

4.4.2 Publication of Certificates by the SS1SPCA

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

4.4.3 Notification of Certificate Issuance by the SS1SPCA to Other Entities

(A) The SS1SPCA shall not give notice of the Issue of a Certificate to any Other Entities.

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 Annex C: Subscriber Obligations of this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in the Relying Party Obligations as set out in Annex D of this Policy.

4.6 Certificate renewal

(A) This Policy does not support Certificate Renewal.

(B) The SS1SPCA shall not provide a Certificate Renewal service.

(C) Where a new Key Pair has been generated the Eligible Subscriber shall apply for the Issue of a new Certificate in accordance with this Part 4.7 of this Policy.

4.6.1 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.6.2 Processing Certificate Renewal Requests

[*Not applicable in this Policy*]

4.6.3 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.6.4 Conduct Constituting Acceptance of a Renewal Certificate

[*Not applicable in this Policy*]

4.6.5 Publication of the Renewal Certificate by the SS1SPCA

[*Not applicable in this Policy*]

4.6.6 Notification of Certificate Issuance by the SS1SPCA to Other Entities

[*Not applicable in this Policy*]

4.7 Certificate Re-key

4.7.1 Circumstances of Certificate re-key

(A) This Policy provides support for Certificate re-key.

(B) The SS1SPCA may only re-key Certificates in accordance with Part 3.3.1 (B) of this Policy.

(C) The SS1SPCA shall not provide support for re-key of Certificates other than those outlined in Part 3.3.1 (B), or where any Certificate is compromised (or is suspected of being) in accordance with Secure S1SP's BC/DR plans as per Part 5.7 of this Policy.

4.7.2 Circumstances of Certificate Re-key

(A) An Eligible Subscriber may apply for a Certificate to be re-keyed where either:

(i) the SS1SP End Entity Private Key associated with the Certificate has expired; or

(ii) the SS1SPCA Private Key associated with the SS1SPCA Certificate has been Compromised (or is suspecting of being) in accordance with Part 5.7 of this Policy.

(B) In relation to Part 4.7.2 (A)(i) above, the SS1SP End Entity Certificates that can be re-keyed under normal operating conditions are set out in Part 3.3.1 (B) of this policy.

4.7.3 Who May Request a Re-keyed Certificate

(A) In accordance with Part 4.7.2 (B), an Eligible Subscriber may request a Certificate re-key at any time by applying for the Issue of a new SS1SP End Entity Certificate in accordance with this Policy.

4.7.4 Processing Re-keyed Certificate Requests

(A) See Part 4.2 of this Policy

4.7.5 Notification of Re-keyed Certificate Issuance to a Subscriber

(A) See Part 4.3.2 of this Policy.

4.7.6 Conduct Constituting Acceptance of a Re-keyed Certificate

(A) See Part 4.4.1 of this Policy.

4.7.7 Publication of a Re-keyed Certificate by the SS1SPCA

(A) See Part 4.4.2 of this Policy.

4.7.8 Notification of Re-keyed Certificate Issuance by the SS1SPCA to Other Entities

(A) See Part 4.4.3 of this Policy

4.8 Certificate modification

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the SS1SPCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the SS1SPCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the SS1SPCA to Other Entities

[*Not applicable in this Policy*]

4.9 Certificate revocation and suspension

4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The SS1SPCA shall not provide any service of revoking or suspending a Certificate.

4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which SS1SPCA must process the Revocation Request

[*Not applicable in this Policy*]

4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.7.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 Certificate status services

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

[*Not applicable in this Policy*]

4.10.3 Optional Features

[*Not applicable in 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 Policies and Practices

(A) The SS1SPCA PKI does not provide Key Escrow services.

(B) SS1SPCA recovery policies and practices are documented in the SS1SP CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

(A) The SS1SPCA PKI does not provide Session Key encapsulation services.

(B) SS1SPCA recovery policies and practices are documented in the SS1SP CPS.

5 Facility management and operational controls

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The Secure S1SP shall ensure that the SS1SPCA Systems are operated in a sufficiently secure environment, where the Secure S1SP will comply with or achieve certification with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes, where the scope will be sufficient enough to include the SS1SPCA PKI:

(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.

(B) The SS1SPCA shall ensure that:

(i) all of the physical locations in which the SS1SPCA Systems are situated, operated, routed or directly accessed are in the United Kingdom or India;

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

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

(C) The SS1SPCA shall ensure that the SS1SPCA Systems cannot be indirectly accessed from any location outside the United Kingdom or India.

(D) The SS1SPCA shall ensure that the SS1SP 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 ISO/IEC 27001:2013 (Information Technology - Security Techniques - Information Security Management Systems) and industry good practice.

(E) The SS1SPCA shall ensure that, where applicable, the SS1SP CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the cryptographic and sensitive functions of the SS1SPCA are stored securely, are encrypted and are accessible only to SS1SPCA Personnel in Privileged Roles.

5.1.2 Physical Access

(A) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA Systems, or any System used for the purposes of Time-Stamping;

(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 SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the SS1SPCA Systems are situated.

5.1.4 Water Exposure

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to water exposure at all physical locations in which the SS1SPCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the SS1SPCA Systems are situated.

5.1.6 Media Storage

(A) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA.

5.1.7 Waste Disposal

(A) The SS1SPCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the SS1SPCA are disposed of only using secure methods of disposal in accordance with good industry practice.

5.1.8 Off-Site Back-Up

(A) The SS1SPCA shall regularly carry out a Back-Up of:

(i) all Data held on the SS1SPCA Systems which are critical to the operation of those Systems or continuity in the provision of the SS1SP PKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the SS1SPCA shall ensure that the SS1SP CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The SS1SPCA shall 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 SS1SPCA Private Key Material, are Backed-Up:

(a) to appropriate Security Containers which are stored off-line in encrypted format.

(D) The SS1SPCA shall ensure that, where any elements of the SS1SPCA Systems, any Data held for the purposes of providing the SS1SP PKI Services, or any items of SS1SPCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

(E) The SS1SPCA will ensure that the SS1SP CPS incorporates provisions in relation to paragraphs (A), (B), (C) and (D) above.

5.2 Procedural controls

5.2.1 Trusted Roles

(A) The SS1SPCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on the SS1SPCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of SS1SPCA Personnel has a clearly defined level of access to the SS1SPCA Systems and the premises in which they are located;

(iii) no individual member of SS1SPCA Personnel is capable, by acting alone, of engaging in any action by means of which the SS1SPCA Systems may be Compromised to a material extent; and

(iv) the SS1SP CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the SS1SPCA with the requirements of this Part 5.2.1 of this Policy.

5.2.2 Number of Persons Required per Task

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of SS1SPCA Personnel; and

(ii) the application of controls to the actions of all members of SS1SPCA Personnel who are Privileged Users, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions where reasonably practicable.

(B) The SS1SPCA shall ensure that the SS1SP CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following areas:

(i) SS1SPCA Systems administration;

(ii) SS1SPCA Systems operations;
(iii) SS1SPCA Systems security; and
(iv) SS1SPCA 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 Qualification, Experience and Clearance Requirements

(A) The SS1SPCA shall ensure that all SS1SPCA 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 SS1SPCA, not have been previously relieved of any past assignment (whether for the SS1SPCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The SS1SPCA shall ensure that all SS1SPCA Personnel have, as a minimum, passed an industry recognised and assured security check before commencing their roles.

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 SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of SS1SPCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of SS1SPCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of SS1SPCA Personnel.

5.3.7 Independent Contractor Requirements

(A) References to the SS1SPCA in this Policy include references to persons with whom the SS1SPCA contracts in order to secure performance of its obligations as the SS1SPCA.

5.3.8 Documentation Supplied to Personnel

(A) The SS1SPCA shall ensure that all SS1SPCA 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 SS1SP CPS; and

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

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

(A) The SS1SPCA shall ensure that:

(i) the SS1SPCA Systems record all systems activity in an audit log;

(ii) the SS1SP CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of SS1SPCA Personnel;

(b) the use of SS1SPCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the SS1SPCA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the SS1SPCA Systems audit log); and

(e) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The SS1SPCA shall ensure that:

(i) the audit logging functionality in the SS1SPCA Systems is fully enabled at all times;

(ii) all SS1SPCA Systems activity recorded in the Audit Log is recorded in a standard format that is aligned with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time.

(B) The SS1SPCA shall ensure that the SS1SP 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.

(C) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The SS1SPCA shall:

(i) retain the 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:

(i) to 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); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(c) to 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 Back-Up Procedures

(A) The SS1SPCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the SS1SPCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The SS1SPCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the SS1SP CPS; and

(ii) 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 or External)

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The SS1SPCA shall ensure that the SS1SP 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.

5.4.8 Vulnerability Assessments

(A) Provision is made in the SS1SP CPS in relation to the carrying out of vulnerability assessments in respect of the SS1SPCA 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 5.4.3 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 SS1SPCA shall ensure that any Data which is to be Archived is retained in accordance with their Data Retention and Destruction Policy.

5.5.3 Protection of Archive

(A) The SS1SPCA shall ensure that the SS1SP CPS details 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 Back-Up Procedures

(A) The SS1SPCA shall ensure that the SS1SP 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 Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA 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 SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to the periodic verification by the SS1SPCA of the Data held in the Archive.

5.6 Key changeover

5.6.1 SS1SP End Entity Certificate Key Changeover

(A) The SS1SPCA shall only ever Issue a new SS1SP End Entity Certificate for those SS1SP End Entity Certificates as described in Part 3.3.1 (B) of this Policy, and where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SS1SP PKI RAPP as set out in Annex E of this Policy and Part 4.7 of this Policy.

5.7 Compromise and disaster recovery

5.7.1 Incident and Compromise Handling Procedures

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates a business continuity plan which shall be designed to ensure continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SS1SP PKI Services in the event of any security compromise of the SS1SPCA Systems or major failure in the SS1SPCA processes.

(B) The SS1SPCA shall ensure that the procedures set out in the business continuity plan are:

(i) aligned 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 SS1SPCA shall ensure that the SS1SP 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 SS1SPCA Private Key or any part of the SS1SPCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The SS1SPCA 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 SS1SPCA 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 SS1SP PKI Services within not more than 48 hours of the occurrence of any event causing discontinuity.

5.8 Certification authority and registration authority termination

[*Not applicable in this Policy*]

6 Technical security controls

(A) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA.

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

(A) The SS1SPCA shall ensure that all SS1SPCA Key which it uses for the purposes of this Policy are generated in accordance with Part 6.1.1 of the SS1SP CPS.

(B) The SS1SPCA shall not generate any Private Key or Public Key other than a SS1SPCA Key.

(C) The SS1SPCA shall ensure that all SS1SPCA 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 SS1SPCA Private Key when required.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the SS1SPCA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The SS1SPCA shall ensure that the SS1SP CPS 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 Root SS1SPCA, Intermediate SS1SPCA and Subordinate SS1SPCA; and

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

6.1.4 SS1SPCA Public Key Delivery to Relying Parties

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions:

(i) in relation to the manner by which each SS1SPCA Public Key is to be lodged in the SS1SP PKI Repository; and

(ii) designed to ensure that the SS1SPCA Public Keys are securely lodged in the SS1SP PKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The SS1SPCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in Annex B to this Policy.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The SS1SPCA 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 SS1SPCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The SS1SPCA shall ensure that each SS1SPCA Certificate andSS1SP End Entity Certificate that is Issued by it, is in accordance with the SS1SPCA Certificate Profiles and the SS1SP End Entity Certificate Profiles in Annex B.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

(A) The SS1SPCA shall ensure that all SS1SPCA Private Keys shall be:

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

(ii) stored in Security Containers and operated in accordance with Part 6.2.1 of the SS1SP CPS; and

(iii) enforce M of N controls to activate the SS1SPCA Private Key.

(B) The SS1SPCA shall ensure that all SS1SPCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated in accordance with Part 6.2.1 of the SS1SP CPS.

(C) The SS1SPCA shall ensure that no SS1SPCA Private Key shall be made available in either complete or unencrypted form in accordance with Part 6.2.1 of the SS1SP CPS.

(D) The SS1SPCA shall ensure that any secure mechanism 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 SS1SP CPS; and

(b) require to be unblocked by an authorised member of SS1SPCA Personnel who has been Authenticated as such following a process which shall be set out in the SS1SP CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions for the exercise of strict controls in relation to Private Key (m out of n) Multi-Person Control.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The SS1SPCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The SS1SPCA may Back-Up SS1SPCA 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 SS1SPCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The SS1SPCA shall ensure that no SS1SPCA Key, which is a Private Key, is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The SS1SPCA shall ensure that no SS1SPCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SS1SP PKI Services; and

(ii) kept secure and encrypted within a Security Container, with appropriate access controls enforced at all times.

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 SS1SPCA shall ensure that the Security Container in which any SS1SPCA Private Key is stored may be accessed only by an authorised member of SS1SPCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the commensurate protection of the Private Key;

(ii) involves the use of Activation Data; and

(iii) requires M of N access to activate the SS1SPCA Private Key within the Security Container.

6.2.9 Method of Deactivating Private Key

(A) The SS1SPCA shall ensure that any SS1SPCA Private Key shall be capable of being de-activated by means of the SS1SPCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the SS1SP CPS.

6.2.10 Method of Destroying Private Key

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions for the exercise of strict controls in relation to the destruction of SS1SPCA Keys.

(B) The SS1SPCA shall ensure that no SS1SPCA 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 SSC for PKI instructing the SS1SPCA 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 SS1SPCA shall ensure that, where necessary, it archives SS1SPCA 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 SS1SPCA shall ensure that:

(i) the Validity Period of each Certificate, unless explicitly documented otherwise in Annex B, shall be an indefinite period; and

(ii) for this purpose, it uses the notAfter value specified in Annex B.

6.4 Activation data

6.4.1 Activation Data Generation and Installation

(A) The SS1SPCA shall ensure that any secure container within which a SS1SPCA Key is held has Activation Data that are unique and unpredictable.

(B) The SS1SPCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the SS1SPCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or passphrases, the SS1SPCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The SS1SPCA shall ensure that the SS1SP 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 SS1SPCA shall ensure that the SS1SP 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 SS1SPCA;

(ii) the appropriate allocation of responsibilities to Privileged Users;

(iii) the identification and Authentication of organisations, individuals and Systems involved in SS1SPCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the SS1SPCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for SS1SPCA Keys.

6.6 Life cycle technical controls

6.6.1 System Development Controls

(A) The SS1SPCA shall ensure that any software which is developed for the purpose of establishing a functionality of the SS1SPCA 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); or

(b) available for inspection and approval by the SSC for PKI and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions which are designed to ensure that the SS1SPCA Systems shall comply with or achieve certification with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its SS1SPCA Systems:

(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.

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 Root SS1SPCA and Intermediate SS1SPCA

(A) The SS1SPCA shall ensure that its functions as the Root SS1SPCA and Intermediate SS1SPCA are carried out on a part of the SS1SPCA Systems that is neither directly nor indirectly connected to any System which is not a part of the SS1SPCA Systems.

(B) The SS1SPCA CPS will provide further detail with respect to SS1SPCA network security controls.

6.7.2 Protection Against Attack

(A) The SS1SPCA shall use its best endeavours to ensure that the SS1SPCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event;

(ii) any unauthorised attempt to connect to them.

(B) The SS1SPCA shall take reasonable steps to ensure that the SS1SPCA 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 Subordinate SS1SPCA

(A) The DCC shall ensure that, where any Subordinate SS1SPCA functions are carried out on a System that is connected to an external network, they are carried out on a System that is Separated from all other SS1SPCA Systems.

6.7.4 Health Check of SS1SPCA Systems

(A) The SS1SPCA shall ensure that, in relation to the SS1SPCA Systems, a vulnerability assessment in accordance with the SS1SP CPS and 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 SS1SPCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other SS1SPCA activities which require an accurate record of time.

(B) The SS1SPCA shall ensure that the SS1SPCA 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 SS1SPCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The SS1SPCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[Not applicable in this Policy]

7.1.3 Algorithm Object Identifiers

[Not applicable in this Policy]

7.1.4 Name Forms

[Not applicable in this Policy]

7.1.5 Name Constraints

[Not applicable in this Policy]

7.1.6 Certificate Policy Object Identifier

[Not applicable in this Policy]

7.1.7 Usage of Policy Constraints Extension

[Not applicable in this Policy]

7.1.8 Policy Qualifiers Syntax and Semantics

[Not applicable in this Policy]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[Not applicable in this Policy]

7.2 CRL PROFILE

7.2.1 Version Number(s)

[Not applicable in this Policy]

7.2.2 CRL and CRL Entry Extensions

[Not applicable in this Policy]

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[Not applicable in this Policy]

7.3.2 OCSP Extensions

[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 the SS1SP CPS.

8.2 Identity/qualifications of assessor

(A) Provision in relation to this is made in the SS1SP CPS.

8.3 Assessor's relationship to assessed entity

(A) Provision in relation to this is made in the SS1SP CPS.

8.4 Topics covered by assessment

(A) Provision in relation to this is made in the SS1SP CPS.

8.5 Actions taken as a result of deficiency

(A) Provision in relation to this is made in the SS1SP CPS.

8.6 Communication results

(A) Provision in relation to this is made in the SS1SP CPS.

9 Other business and legal matters

(A) In so far as provision is made in relation to any or all the matters referred to in this Part, these can be found in the S1SP commercial contracts, this Policy and the provisions of Annex C: Subscriber Obligations of this Policy and Annex D: Relying Party Obligations of this Policy.

9.1 Fees

[Not applicable in this Policy]

9.1.1 Certificate Issuance or Renewal Fees

[Not applicable in this Policy]

9.1.2 SS1SP End Entity Certificate Access Fees

[Not applicable in this Policy]

9.1.3 Revocation or Status Information Access Fees

[Not applicable in this Policy]

9.1.4 Fees for Other Services

[Not applicable in this Policy]

9.1.5 Refund Policy

[Not applicable in this Policy]

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

[Not applicable in this Policy]

9.2.2 Other Assets

[Not applicable in this Policy]

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

[Not applicable in this Policy]

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

[Not applicable in this Policy]

9.3.2 Information not within the Scope of Confidential Information

[Not applicable in this Policy]

9.3.3 Responsibility to Protect Confidential Information

[Not applicable in this Policy]

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

[Not applicable in this Policy]

9.4.2 Information Treated as Private

[Not applicable in this Policy]

9.4.3 Information not Deemed Private

[Not applicable in this Policy]

9.4.4 Responsibility to Protect Private Information

[Not applicable in this Policy]

9.4.5 Notice and Consent to Use Private Information

[Not applicable in this Policy]

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

[Not applicable in this Policy]

9.4.7 Other Information Disclosure Circumstances

[Not applicable in this Policy]

9.5 INTELLECTUAL PROPERTY RIGHTS

[Not applicable in this Policy]

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

[Not applicable in this Policy]

9.6.2 Registration Authority Representations and Warranties

[Not applicable in this Policy]

9.6.3 Subscriber Representations and Warranties

[Not applicable in this Policy]

9.6.4 Relying Party Representations and Warranties

[Not applicable in this Policy]

9.6.5 Representations and Warranties of Other Participants

[Not applicable in this Policy]

9.7 DISCLAIMERS OF WARRANTIES

[Not applicable in this Policy]

9.8 LIMITATIONS OF LIABILITY

[Not applicable in this Policy]

9.9 INDEMNITIES

[Not applicable in this Policy]

9.10 TERM AND TERMINATION

9.10.1 Term

[Not applicable in this Policy]

9.10.2 Termination of SS1SP End Entity Certificate Policy

[Not applicable in this Policy]

9.10.3 Effect of Termination and Survival

[Not applicable in this Policy]

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

[Not applicable in this Policy]

9.11.2 SS1SPCA Certification Authority

[Not applicable in this Policy]

9.11.3 9.11.3 Notification

[Not applicable in this Policy]

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

[Not applicable in this Policy]

9.12.2 Notification Mechanism and Period

[Not applicable in this Policy]

9.12.3 Circumstances under which OID Must be Changed

[Not applicable in this Policy]

9.13 DISPUTE RESOLUTION PROVISIONS

[Not applicable in this Policy]

9.14 GOVERNING LAW

[Not applicable in this Policy]

9.15 COMPLIANCE WITH APPLICABLE LAW

[Not applicable in this Policy]

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

[Not applicable in this Policy]

9.16.2 Assignment

[Not applicable in this Policy]

9.16.3 Severability

[Not applicable in this Policy]

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

[Not applicable in this Policy]

9.16.5 Force Majeure

[Not applicable in this Policy]

9.17 OTHER PROVISIONS

9.17.1 SS1SP End Entity Certificate Policy Content

[Not applicable in this Policy]

9.17.2 Third Party Rights

[Not applicable in this Policy]

10 Annex A: Definitions and interpretation

In this Policy, except where the context otherwise requires -

- the expressions in the left-hand column below shall have the meanings given to them in the right hand column below,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Definition	Interpretation
Activation	means the process of making a SS1SPCA Private Key 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.
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 SS1SP CPS.
Authentication	means the process of establishing that an individual, organisation, System or Secure SMETS1 Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).
Authorised Subscriber	means an individual or organization which complies with the procedures of the SS1SP PKI RAPP as set out in Annex E of this Policy and is duly authorised by the SS1SPCA to submit a Certificate Signing Request.
Back-Up	means, in relation to Data which is held on any SS1SPCA 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 either a SS1SP End Entity Certificate or a SS1SPCA Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
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 Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy.
Cryptographic Module	See 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: a) in relation to a SS1SP End Entity Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy; and b) in relation to a SS1SPCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy.

Intermediate Secure S1SP Certification Authority (or Intermediate SS1SPCA)	means the Secure S1SP exercising the function of the Intermediate SS1SPCA to Issue Certificates to Subordinate SS1SPCAs and of storing and managing the Private Keys associated with that function. Intermediate SS1SPCAs comprise the following: a) Operations CA; and b) Manufacturing CA.
Intermediate SS1SPCA Certificate	means a certificate in the form set out in the Intermediate SS1SPCACertificate Profile in accordance with Annex B and Issued by the Root SS1SPCA to the Intermediate SS1SPCA in accordance with this Policy.
Intermediate SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Intermediate SS1SPCA.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or **OID**)	means an Object Identifier assigned by the Internet Address Naming Authority.
Policy	means this Secure S1SP Certificate Policy.
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key cryptography
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 member of SS1SPCA Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the SS1SPCA System and which are capable of being a means by which the SS1SPCA System, any other Systems, or Secure SMETS1 Device are (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.
Registration Authority	means the Secure S1SP exercising the function of receiving and processing Certificate Signing Requests made in accordance with Annex E: SS1SP PKI RAPP of this Policy.
Registration Authority Manager	means either a director of the Secure S1SP or any other person who may be identified as such in accordance with Annex E: SSS1SP PKI RAPP of this Policy.
Registration Authority Personnel	means those persons who are engaged by the Secure S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the SS1SPCA Registration Authority.
Relying Party	means a SS1SP Party who, pursuant to this Policy, receives and relies upon a Certificate.
Root SS1SP Certification Authority (or **Root SS1SPCA**)	means the Secure S1SP exercising the function of Root SS1SPCA to Issue Certificates to the Intermediate SS1SPCA and storing and managing Private Keys associated with that function.
Root SS1SPCA Certificate	means a certificate in the form set out in the Root SS1SPCA Certificate Profile in accordance with Annex B and self-signed by the Root SS1SPCA in accordance with this Policy.
Root SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Root SS1SPCA.
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 SS1SPCA.

Secure SMETS1 Service Provider (or SS1SP)	means Secure Meters (UK) Limited (Company number: 02199653).
Secure S1SP Certification Authority (or SS1SPCA)	means the Secure S1SP, acting in the capacity and exercising the functions of one or more of the: (a) Root SS1SPCA; (b) Intermediate SS1SPCA; (c) Subordinate SS1SPCA; (d) SS1SPCA Systems; and (e) the SS1SP PKI Registration Authority.
Secure SMETS1 Device	means one of the following devices manufactured and provided by Secure: a SMETS1 ESME; a SMETS1 GSME; a SMETS1 CHF; a SMETS1 GPF; a SMETS1 PPMID; a SMETS1 IHD; and any other device operating on a home area network created by a SMETS1 CHF.
Secure SMETS1 Service Provider End Entity Certificate (or SS1SP End Entity Certificate)	means a Certificate only issued by one of the Subordinate SS1SPCAs. SS1SP End Entity Certificates comprise the following: a) SMSO TLS Certificate b) SMSO KMS Certificate c) Code Signing Certificate d) Device Certificate
Secure SMETS1 Service Provider PKI (or SS1SP PKI)	means the SS1SPCA System and any public key infrastructure established (or to be established) by Secure for the purpose, among other things, of providing secure communications between Secure S1SP, the DCC and Secure SMETS1 Devices.
Security Container	means a set of hardware, software and/or firmware.

Security Related Functionality	means the functionality of the SS1SPCA 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.
SSCPKI	means the Security Sub-Committee when performing its PKI functions.
SS1SPCA CSR Generation Tool	means the part of the SS1SPCA System responsible for creating Certificate Requests and validating Certificate Requests.
SS1SPCA Key	means any Private Key or a Public Key generated by the SS1SPCA for the purposes of complying with its obligations under this Policy.
SS1SPCA Management Tool	means the part of the SS1SPCA System responsible for creating and Issuing Certificates.
SS1SPCA Personnel	means those persons who are engaged by the Secure S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the SS1SPCA.
SS1SPCA Public Key	means the Public Key which is part of a Key Pair of a Root SS1SPCA Private Key, an Intermediate SS1SPCA Private Key or a Subordinate SS1SPCA Private Key.
SS1SPCA Private Key	means a SS1SPCA Key which is a Private Key.
SS1SPCA Systems	means the Systems used by the SS1SPCA in relation to the SS1SP PKI services.
SS1SPCA Certificate	means either a Root SS1SPCA Certificate, an Intermediate SS1SPCA Certificate or a Subordinate SS1SPCA Certificate.

SS1SP CPS	means the Certification Practice Statement describing how the PKI is operated and maintained.
SS1SP End Entity Certificate	means a certificate in the form set out in the SS1SP End Entity Certificate Profile in accordance with Annex B of this Policy and Issued by the Subordinate SS1SPCA.
SS1SP Party	means, Secure Meters UK Limited including where they act in this capacity through an individual engaged to act on their behalf or through the use of a System or Secure SMETS1 Device that is the Subject of a Certificate in accordance with this Policy.
SS1SP PKI RAPP	Means the Secure SMETS1 Service Provider Public Key Infrastructure Registration Authority Policy and Procedures as set out in Annex E of this Policy.
Subject	means: (a) in relation to a SS1SP End Entity Certificate, the subject identified by the population of the subject field of the relevant SS1SP End Entity Certificate Profile in Annex B of this Policy; and (b) in relation to a SS1SPCA Certificate, the Root SS1SPCA, Intermediate SS1SPCA or Subordinate SS1SPCA as identified by the subject field of the relevant Certificate Profile in Annex B of this Policy.
Subordinate Secure S1SP Certification Authority (or Subordinate SS1SPCA)	means the Secure S1SP exercising the function of the Subordinate SS1SPCA to Issue SS1SP End Entity Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function. Subordinate SS1SPCAs comprise the following: a) SMSO CA b) SMSO KMS CA c) Code Signing CA d) Device CA

Subordinate SS1SPCA Certificate	means a certificate in the form set out in the Subordinate SS1SPCA Certificate Profile in accordance with Annex B and Issued by the Intermediate SS1SPCA to the Subordinate SS1SPCA in accordance with this Policy.
Subordinate SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Subordinate SS1SPCA.
Subscriber	means, in relation to any Certificate, an individual, organisation, System or Secure SMETS1 Device which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
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 and Data associated therewith. This includes the SS1SP PKI System.
Time-Stamping	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.
Validity Period	means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

11 Annex B: SS1SPCA Certificate and SS1SP End entity certificate profiles

11.1 Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which SS1SPCA Certificates and SS1SP 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 SS1SPCA Certificates and SS1SP End Entity Certificates

All SS1SPCA Certificates and SS1SP End Entity Certificates that are validly authorised within the SS1SP PKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all SS1SPCA Certificates and SS1SP End Entity Certificates shall:
    - contain the `authorityKeyIdentifier` in the form `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the SS1SPCARoot, in which case `authorityKeyIdentifier` may be omitted;
    - contain the `keyUsage` extension which shall be marked as critical;
    - be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
    - only contain Public Keys of types that are explicitly allowed by the Great Britain Companion Specification (GBCS)[1]. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
    - only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
    - only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
    - contain a serialNumber which is a positive integer;
    - contain a subjectKeyIdentifier which shall be marked as non-critical;

[1] The latest version of the GBCS can be found here: https://smartenergycodecompany.co.uk/the-smart-energy-code-2/

- only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an issuer field whose contents MUST be identical to the contents of the signer's subject field in the signer's Certificate;
- have a valid notBefore field consisting of the time of issue encoded;
- other than the S1SP End Entity SMSO TLS and SMSO KMS Certificates, have a valid notAfter field for a not well-defined expiration date as per IETF RFC 5280 Section 4.1.2.5 (so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z).

11.3 Common Requirements applicable to SS1SP End Entity Certificates only

All SS1SP End Entity Certificates that are issued by the SS1SPCA shall:

- other than the S1SP End Entity SMSO TLS and SMSO KMS Certificates, not have a well-defined expiration date and so the `notAfter` shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- have a `subject` field populated in accordance with each specific SS1SP End Entity Certificate Profile;
- contain a single Public Key;
- SS1SP End Entity Certificates shall contain the extensions described below:
  - `subjectAltName`
  - `keyUsage`
  - `authorityKeyIdentifier`
  - `subjectKeyIdentifier`
- contain a keyUsage extension marked as critical, with a value of one or more of:
  - `digitalSignature`;
  - `keyAgreement`;
  - `nonRepudiation`
  - `keyEncipherment`
  - `dataEncipherment`
- SS1SP End Entity Certificates may contain the `ExtKeyUsage` extension, with a value of one or more of:
  - `id-kp-serverAuth`
  - `id-kp-clientAuth`
  - `id-kp-codeSigning`
- SS1SP End Entity Certificates may contain the `BasicConstraints` extension, with the following values only. `cA` must be FALSE:
  - End Entity

- pathLen=0

11.4 Common Requirements applicable to the Root SS1SPCA, Intermediate SS1SPCA and Subordinate SS1SPCA ONLY

All SS1SPCA Certificates issued by the SS1SPCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- must have a Valid notBefore field consisting of the time of issue encoded as per RFC5280;
- Per RFC5280, the IssuerName of any certificates MUST be identical to the signer's subject;
- have a globally unique subject;
- contain a single Public Key;
- contain a keyUsage extension marked as critical and defined as keyCertSign and cRLSign;
- For the Intermediate SS1SPCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=1. This extension shall be marked as critical.
- For the Subordinate SS1SPCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical.
- For the Root SS1SPCACertificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.
- must create SerialNumbers that are unique and non-negative.

11.5 SS1SP End Entity Certificate Profile - SMSO TLS Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer’s credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 5 years from the notBefore Time	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Common Name of SS1SP End Entity Certificate	
Key Usage	keyUsage	The permitted Key Usages.	
Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

The SMSO TLS End Entity Certificates are valid to operate for 5 years from date of creation.

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

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

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a SS1SP End Entity Certificate is expected to be used. The SMSO TLS End Entity Certificate are valid for 5 years from date of creation.

Subject X520 Common Name

This field must be populated as follows:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
O = Secure Meters (UK) Ltd
CN = s1t.smartwse.net
```

Key Usage

The `keyUsage` extension should be populated as follows:

`digitalSignature`; and

`keyAgreement`.

Enhanced Key Usage

The `ExtKeyUsage` extension should be populated as follows:

`id-kp-serverAuth`; and
`id-kp-clientAuth`.

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

`cA=False`

`End Entity`

`pathLen=0`

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL
       -- specifiedCurve  SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used:

- `o namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the SS1SPCAIssuing SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.6 SS1SP End Entity Certificate Profile - SMSO KMS Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common Name")	`UTF8String`	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	

keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 5 years from the notBefore Time	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	

Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

The SMSO KMS End Entity Certificates is valid to operate for 5 years from date of creation.

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

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

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a SS1SP End Entity Certificate is expected to be used. The SMSO KMS End Entity Certificate is valid for 5 years from date of creation.

Subject X520 Common Name

This field must be populated as follows:

```
C = [Country]
S = [County]
L = [Location/City]
OU = [Supplier's Organisational Unit]
O = [Supplier's Organisation Name]
CN = [Supplier's Trading Name]
```

Key Usage

The `keyUsage` extension should be populated as follows:

`digitalSignature`; and

`keyAgreement`.

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

`cA=False`

`End Entity`

`pathLen=0`

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve    NULL
```

```
    -- specifiedCurve  SpecifiedECDomain

}
```

Only the following field in ECParameters shall be used:

- `o namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.7 SS1SP End Entity Certificate Profile - Code Signing Certificate

Field Name	RFC 5759/5280 Type	Value	Reference

version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	
Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

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

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

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Code Signing End Entity Certificates are expected to operate indefinitely into the future and should use the value `99991231235959Z`. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

```
C = IN

S = Rajasthan

L = Udaipur

OU = Secure Meters Ltd

O = Secure Meters Ltd

CN = Secure Meters Firmware Signer
```

Key Usage

The `keyUsage` extension should be populated as follows:

`digitalSignature`; and

`nonRepudiation`.

Enhanced Key Usage

The `ExtKeyUsage` extension should be populated as follows:

`id-kp-codeSigning`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=False

End Entity

pathLen=0
```

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL
       -- specifiedCurve  SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used:

- `o namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.8 SS1SP End Entity Certificate Profile - Device Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common Name")	`UTF8String`	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	

keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	

Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and

including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

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

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Code Signing End Entity Certificates are expected to operate indefinitely into the future and should use the value `99991231235959Z`. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

```
SERIALNUMBER = 000000000195BB18
CN = Q0007098
```

Key Usage

The `keyUsage` extension should be populated as follows:

```
digitalSignature;
```

keyAgreement;

nonrepudiation;

keyEncipherment;and

dataEncipherment.

Enhanced Key Usage

The ExtKeyUsage extension should be populated as follows:

id-kp-serverAuth; and

id-kp-clientAuth.

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=False

End Entity

pathLen=0

Subject Public Key Info

The SS1SP End Entity Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the KeyUsage SS1SP End Entity Certificate extension (explained further under the next **extensions** heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve    NULL
       -- specifiedCurve  SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The OBJECT IDENTIFIER for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.9 Root SS1SPCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Root SS1SPCA	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifider")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	

notBefore	Time	Creation time of the Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Root SS1SPCA (same as Issuer name)	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the Secure S1SP PKI.

Version

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

Serial Number

Certificate serial number, which is a positive integer. The `serialNumber` identifies the Certificate, and shall be created by the SS1SPCA that signs the Certificate (self-signed by Root SS1SPCA). The `serialNumber` shall be unique in the scope of Certificates signed by the SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm heading**.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA. This will be the same as the `subject` as it is self-signed by the Root SS1SPCA.

S**ubject Key Identifier**

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Validity

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

Root SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
```

```
O = Secure Meters (UK) Ltd
CN = Secure Meters (UK) Root CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

`cA=TRUE`

`pathLen=Absent`

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next **extensions** heading).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve    NULL         --
specifiedCurve   SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used: o

namedCurve - identifies all the required values for a particular

set of elliptic curve domain parameters to be represented by an

OBJECT IDENTIFIER.

The object identifier for the curve choice to be used in SS1SPCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading .

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.10 Intermediate SS1SPCA Certificate Profile - Operations CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Intermediate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Intermediate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (notAfter). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-DCC Operations CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
    }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.11 Intermediate SS1SPCA Certificate Profile - Operations CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Intermediate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Intermediate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (notAfter). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-MFG Operations CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
    }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.12 Subordinate SS1SPCA Certificate Profile - SMSO CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the “Subject Key Identifier”)	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the “Authority Key Identifier”)	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer’s credential	
notBefore	Time	Creation time of the certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

`C = GB`

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-HES CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve    NULL         --
specifiedCurve   SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used: o

namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an OBJECT IDENTIFIER.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.13 Subordinate SS1SPCA Certificate Profile - SMSO KMS CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the “Subject Key Identifier”)	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the “Authority Key Identifier”)	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer’s credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (notAfter). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-Key Management CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
    }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.14 Subordinate SS1SPCA Certificate Profile - SMSO Code Signing CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (notAfter). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-Code Signing CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
    }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.15 Subordinate SS1SPCA Certificate Profile - Device CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

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

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

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

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

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = IN

S = Rajasthan

L = Udaipur

OU = Secure Meters Ltd

O = Secure Meters Ltd

CN = Secure Meters Production CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
    }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

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 conform with the relevant Certificate Profiles as set out in Annex B of this Policy.

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

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

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

(A) 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.

(B) An Eligible Subscriber shall take all reasonable steps to ensure that a Certificate Signing Request for the Issue of a Certificate does not contain the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Certificate.

12.2 Subscribing for or Rejecting Certificates

(A) Where any Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(i) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(ii) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(a) reject that Certificate; and

(b) inform the SS1SPA that it rejects the Certificate; and

(iii) where it does not reject the Certificate, become a Subscriber for that Certificate.

12.3 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 Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes set out in Part 1.4.1 of this Policy.

12.4 SS1SPCA Certificates: Expiry of Validity Period

(i) Each Subscriber for a Certificate as set out in Part 3.3.1 (b) of this Policy shall, prior to the expiry of the Validity Period that Certificate for which it is the Subscriber, request a re-key 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 Section Annex D, a 'Relying Party' in relation to a Certificate means the Secure S1SP which relies on the Certificate for the purposes as set out in Part 1.4 of this Policy in order to meet its security obligations to its customers as set out in their respective contractual arrangements.

13.2 Duties in relation to Certificates

(A) The Relying Party shall not rely on a Certificate where the Validity Period of that Certificate has expired.

(B) The Relying Party shall not rely on a Certificate where it suspects that the Certificate has been Compromised.

(C) The 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: SS1SP PKI RAPP

14.1 Purpose

(A) This Annex E: SS1SP PKI RAPP sets out the high level principle obligations and activities undertaken by the SS1SPCA in its capacity as the SS1SP PKI Registration Authority in accordance with this Policy. The SS1SP RAPP also sets out the activities undertaken by the SS1SP PKI Registration Authority in support of the procedures as set out in this Section.

14.2 SS1SP PKI RAPP Principles

(A) All Certificates requested and Certificates issued under the auspices of the SS1SPCA must be:

(i) compliant with PKCS#10;

(ii) DER encoded

(iii) compliant with the Certificate Profiles as set out in Annex B of this Policy

(iv) compliant with the obligations as set out in Annex C of this Policy.

14.3 SS1SP PKI Registration Authority Roles

(A) The SS1SP PKI RA consists of the following roles:

(i) SS1SPCA Systems technical RA role; and

(ii) SS1SPCA Personnel requesting and approving Certificates for issuance.

(B) The Subordinate SS1SPCA Device CA acts as a technical RA for Certificates requested by Secure SMETS1 Devices only. The SS1SPCA Systems have been authorised to act as technical RAs through a combination of access controls and IP whitelisting. Only valid Secure SMETS1 Devices may request a Certificate. Therefore, acting as an Authorised Subscriber for such SS1SP End Entity Certificates.

(C) Authorised and approved SS1SPCA Personnel are responsible for requesting and issuing all other SS1SPCA End Entity Certificates using SS1SPA Systems. Thereby acting as an Authorised Subscriber.

(D) Only SS1SPCA Personnel with Privileged User rights can request and approve Certificate requests through the SS1SPCA Systems. This is enforced through:

(i) Pre-authorised and pre-approved access to SS1SPCA Systems for such SS1SPCA Personnel;

(ii) Access control to the SS1SPCA Systems;

(iii) User account management (audit and logging);

(iv) Dedicated named accounts on the SS1SPCA System;

(E) Prior to being granted access to SS1SPCA Systems, all such SS1SPCA Personnel with Privileged User rights will either have:

(i) identities checked in line with personnel security standard BS7858;

(ii) background clearance checks performed in accordance with security check (SC) cleared to an appropriate level (in accordance with the latest version of the HMG Cabinet Office Security Policy; and/or

(iii) Screening and background verifications equivalent to BS7858. The personnel and key personnel, based in India, engaged in providing support for Smart metering services and solutions shall comply at all times with a background verification equivalent to personnel security British Standard BS 7858:2012 (Security Screening of Individuals Employed in Security Environment - Code of Practice),

14.4 Eligible and authorised subscribers

(A) Only those systems and SS1SPCA Personnel described in Part 14.3 of this Policy are Authorised to Subscribe for Certificates under the auspices of the SS1SP PKI. At the point of the SS1SP PKI RA approving such systems or SS1SPCA Personnel they become Authorised Subscribers.

(B) An Authorised Subscriber is an Eligible Subscriber in respect to the following:

(i) SS1SPCA Personnel who are Authorised Subscribers are Eligible Subscribers for the following SS1SPCA End Entity Certificates only:

(a) SMSO TLS Certificate;

(b) SMSO KMS Certificate; and

(c) Code Signing Certificate.

(ii) SS1SPA Systems who are Authorised Subscribers are Eligible Subscribers for the following SS1SPCA End Entity Certificate only:

(a) Device Certificate,

14.5 SS1SP PKI Technical RA Verification and Issuance of Certificate

(A) The Subordinate SS1SPCA Device CA performs the following technical RA check in response to a Certificate Signing Request from a Secure SMETS1 Device:

(i) The SS1SPCA Root Certificate is loaded on the Secure SMETS1 Device at point of manufacture;

(ii) The Secure SMETS1 Device generates a Certificate Signing Request using a Private Key generated on the Secure SMETS1 Device within the manufacturing facility;

(iii) The Certificate Signing Request is sent to a production central system (which incorporates the SS1SPCA Device CA) in PKCS#10 file format.

(iv) The production central system verifies the Certificate Signing Request against the production record it holds for each Secure SMETS1 Device (Device serial number and Device model) as well as performing a proof of possession check using the PKCS#10 format.

(v) If the production central system finds a match between its records and the Secure SMETS1 Device serial number and Secure SMETS1 Device model within the CSR, and it is expecting to manufacture such Secure SMETS1 Device, then:

(a) it passes the CSR to the Device CA to process the Certificate Signing Request;

(b) The Device CA then:

(1) signs the SS1SP End Entity Certificate for the Secure SMETS1 Device; and

(2) sends the SS1SP End Entity Certificate along with the SS1SPCA Certificate chain (in PKCS#7 file format) to the Secure SMETS1 Device.

(c) The Secure SMETS1 Device then verifies the SS1SP End Entity Certificate as well as performing Certificate Path Validation check on the SS1SPCA Certificates provided.

(d) If all verification checks are successful, the Secure SMETS1 Device stores the SS1SPCA Certificate chain and its own SS1SP End Entity Certificate in its internal storage.

14.6 SS1SP PKI Personnel RA verification and issuance of certificate

(A) Only authorised SS1SPCA Personnel (in accordance with Part 3.2.3 of the Policy) are granted a Privileged Role allowing them to create Certificate Requests, approve Certificate Requests and Issuing Certificates in accordance with this procedure and in accordance with the Policy:

(i) A service request is raised by the Service Team for issuance of a SS1SP End Entity Certificate as outlined in Part 3.3.1 (B) of the Policy;

(ii) A CSR is generated by SS1SPCA Personnel using the SS1SPCA CSR Generation Tool;

(iii) The SS1SPCA Personnel who generated the CSR then submits the CSR to the SS1SPCA Management Tool;

(iv) The SS1SPCA Management Tool parses the CSR in order to display the content of the CSR (including Subject information);

(v) The SS1SPCA Personnel who submitted the CSR verifies the contents of the CSR output and:

  (a) If successful, confirms the Certificate issuance through the SS1SPCA Management Tool;

  (b) The SS1SPCA Personnel then export the Certificate in PKCS#7 format file from SS1SPCA Management Tool; or

  (c) If unsuccessful, the SS1SPCA Personnel rejects the Certificate and starts the process again from Part 14.6 (A)(i) of this Annex E of the Policy;

(vi) This PKCS#7 file containing the Certificate is loaded back into the SS1SPCA CSR Generation Tool by the SS1SPCA Personnel;

(vii) The SS1SPCA CSR Generation Tool then verifies the PKCS#7 file including the issued SS1SP End Entity Certificate and the SS1SPCA Certificate chain within the PKCS#7 file, and:

  (a) If the PKCS#7 file validates successfully, the SS1SPCA CSR Generation Tool creates a PKCS#12 file ready for download by SS1SPCA Personnel. This file contains both the SS1SP End Entity Private Key associated with Public Key in the SS1SP End Entity Certificate and the complete SS1SPCA Certificate chain;

  (b) The SS1SPCA Personnel download the PKCS#12 file and then load into the appropriate System accordingly; or

  (c) If the PKCS#7 file cannot be validated successfully, the PKCS#7 file is rejected by the SS1SPCA Personnel and the process starts again.