Technical Specification Document

Central Switching Service Certificate Authority Service Definition

Version: 0.1 Effective Date: TBC

Change History

Version Number	Implementation Date	Reason for Change
0.1	TBD	Initial Draft for Spring 2021 Switching Consultation

Contents Table

1 Description of Service

1.1 The CSS Certificate Authority is responsible for delivering the PKI Managed Service to support the provision of security certificates for organisations who are obliged (or wish) to exchange Market Messages via the Central Switching Service (CSS).

1.2 Two types of certificate are provided by the CSS Certificate Authority:

(a) Transport Layer Security (TLS) Certificates - to secure either end of the network connection, ensuring the transfer of messages across the communication channel is via a secure encrypted channel; and

(b) Message Signing Certificates - to authenticate individual messages sent across the communication channel through the application of a digital signature. This type of certificate is only required for CSS Users sending messages to the CSS.

1.3 The PKI Managed Service is based upon a two-tier hierarchy consisting of a tScheme[1] compliant root Certificate Authority and issuing subordinate Certificate Authority(ies).

1.4 The CSS Certificate Authority shall establish, keep under review and from time to time update a a certificate policy document for the certificates to be used in the CSS (referred to as the CSS Certificate Policy). The CSS Certificate Authority shall ensure that the CSS Certificate Policy is consistent with (and does not contain material obligations on CSS Users over and above those detailed in) this Code, and is otherwise reasonable and consistent with Good Industry Practice for such a certificate policy. The CSS Certificate Policy shall be structured in accordance with the guidelines in IETF RFC 3647, with appropriate modifications, deletions, and references to this Code. The CSS Certificate Policy shall be published on the Switching Portal. Where any discrepancy arises between the contents of the CSS Certificate Policy and this Code, the provisions of this Code provisions shall prevail.

1.5 The CSS Certificate Authority shall:

(a) ensure that security certificates are only issued to eligible subscribers and are only used for the purposes of creation, sending, receiving and processing communications with the CSS;

(b) maintain one or more repositories which store all copies of issued certificates, with certificate status and validity metadata associated with each certificate;

(c) maintain a Certificate Revocation List, published at the location defined in the Certificate Revocation List distribution point field within every certificate, detailing security certificates that have been revoked in accordance with the CSS Schedule.

1.6 This Service Definition should be read in conjunction with:

(a) the CSS Service Definition which sets out the security certificate requirements for CSS Users; and

(b) the CSS Schedule which defines the process for requesting security certificates and obligations on CSS Users.

[1] tScheme is the self-regulatory body for electronic trust service approval in the UK, publishing agreed best practice criteria for secure electronic transaction services.

2 Definition of Users

2.1 The CSS Users (and applicants) are the recipients of the CSS Certificate Authority's services. A full list of CSS User categories is included in the CSS Schedule.

2.2 Those wishing to become CSS Users must apply for certificates in accordance with the CSS Schedule.

2.3 Where a Market Participant/Switching Data Service Provider is using a CSS Interface Provider to communicate with the CSS, then the TLS Certificate must be requested and owned by the CSS Interface Provider; and the Message Signing Certificate must be owned by the Market Participant/Switching Data Service Provider, but may be requested and used by the CSS Interface Provider on behalf of the Market Participant/Switching Data Service Provider.

3 System Access and User Management

3.1 Once a potential CSS User has completed the required steps in the Entry Assessment process in accordance with the Qualification and Maintenance Schedule, the Code Manager will inform the CSS Certificate Authority who will facilitate the issuing of the required security certificates in accordance with the process set out in the CSS Schedule.

3.2 These certificates are digitally signed by the CSS Certificate Authority and bind CSS Users with their public keys. As a result, if you trust the CSS Certificate Authority (and know its public key), you can trust that the specific party's public key included in the certificate is genuine.

3.3 A Senior Responsible Officer shall be appointed by each CSS User (or potential CSS User) in accordance with the CSS Schedule. The Senior Responsible Officer may at any time nominate individuals to become Appointed Responsible Officers who will be authorised to request certificates on behalf of their organisation if explicitly stated by the Senior Responsible Officer.

3.4 Organisations may also nominate a Technical Contact to request certificates on their behalf and receive the certificate when issued via a secure channel.

3.5 The CSS Certificate Authority shall receive and validate Certificate Signing Requests from a Senior Responsible Office, Appointed Responsible Officer or Technical Contact and store the required certificate within the repository.

4 Service Availability

4.1 The CSS Certificate Authority shall be available for issuing certificates and updating the Certificate Revocation List 24 hours a day, 7 days a week, except during scheduled maintenance periods and unplanned outages.

4.2 The CSS Certificate Authority shall ensure that the service achieves 99% availability over each calendar year, excluding scheduled maintenance periods.

4.3 In the event of scheduled maintenance, the CSS Certificate Authority shall provide notice to the Switching Operator for inclusion in the forward schedule of change, in accordance with the Service Management Schedule.

4.4 In the event of an unplanned outage (e.g. to fix a priority incident), then the CSS Certificate Authority shall notify the Switching Operator in accordance with the Service Management Schedule.

5 User Support

5.1 The CSS Certificate Authority Service does not have an externally facing service desk. Any Switching Incidents and Switching Service Requests will be raised via the Switching Portal. The CSS Certificate Authority Service shall provide second line support in accordance withthe Service Management Schedule.

6 Service Levels

6.1 [This section needs to updated to include any user facing service levels e.g the time for responding to a certificate request including validation of CSR and making certificate available to the user]

6.2 Where a security certificate is compromised, the CSS Certiifcate Authority will revoke the relevant certificate and update the Certificate Revocation List within 1 hour.

7 Maximum Design Volumes

7.1 There are no maximum volumes specified[2].

8 Business Continuity

8.1 In the event of an unplanned outage, the system shall resume operation within 8 hours[3].

9 Reporting

9.1 [This section needs to include any standard reports provided by the service].

10 System Audit

10.1 The CSS Certificate Authority Service will be audited by tScheme.

10.2 The CSS Certificate Authority Service has auditing capabilities built into all key components and shall maintain a record of all certificates which have been issued by it and accepted by a CSS User.

10.3 The CSS Certificate Authority will record all activities in its audit and systems log, whether success of failure. Logs shall be configurable in terms of size, scope and level.

11 Data Handling

11.1 As a minimum, the CSS Certificate Authority shall retain records for seven years.

12 Security

12.1 The CSS Certificate Authority Service shall include:

(a) cryptographic modules to generate, store and operate the CSS Certificate Authority private keys shall be FIPS 140-2 Level 3 compliant;

[2] [Subject to confirmation by DCC]
[3] [Subject to confirmation by DCC]

(b) capability to generate TLS Certificates that meet the RSA standard with “2048-bit RSA with SHA256” parameters;

(c) capability to generate Message Signing Certificates for signing with “ECDSA-256 with SHA256 on the P-256 curve” parameters;

(d) compliance of all certificate policy documents (e.g. Base Certificate Policy, Certification Practice Statement (CPS) framework) with IETF RFC 3647; and

(e) compliance of certificate profiles with the defined standard for the Switching Arrangements.