RETAIL
ENERGY
CODE

Central Switching Service Certificate Authority Service Definition

Contents

RETAIL ENERGY CODE

Technical Specification Document

Central Switching Service Certificate Authority Service Definition

Version: 0.2 Effective Date: CSS Go Live

Change History

Version Number	Implementation Date	Reason for Change
0.1	TBD	Initial Draft for Spring 2021 Switching Consultation
0.2	CSS Go live	Final update for SCR Modification

1 Description of Service

1.1. The CSS Certificate Authority is responsible for delivering the 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 Market Messages across the communication channel is via a secure encrypted channel; and

(b) Message Signing Certificates - for each Market Participant Identifier, to authenticate individual Market Messages sent across the communication channel through the application of a digital signature.

1.3. The CSS Certificate Authority shall establish, keep under review and from time to time update certificate policy document for the certificates to be used to exchange Market Messages with 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 Internet Engineering Task Force (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 shall prevail.

1.4. 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.

1.5. 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.

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, where a CSS User trusts the CSS Certificate

Authority (and knows its public key), it can trust that the specific party's public key included in the certificate is genuine.

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

3.4. CSS Users 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 Officer, 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, seven 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 month, 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 Switching Service Management Schedule .

4.4. In the event of an unplanned outage, then the CSS Certificate Authority shall notify the Switching Operator in accordance with the Switching 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 with the Switching Service Management Schedule .

6 Service Levels

6.1. The following Service Levels shall be applied to the management of security certificates:

6.2.

Activity	Service Level
Nomination of security officers	5 Working Days (09:00 - 17:00)
Request for security certificate	2 Working Days (09:00 - 17:00)
Revocation of security certificate (standard)	4 Working Hours
Revocation of security certificate (security breach)	4 hours (24 / 7)
Revocation of security certificate (as a result of a Last Resort Supply Direction)	Where the Switching Operator is notified, during Working Hours, the failed Energy Supplier's security certificate(s) will be revoked within 4 hours (this shall extend beyond Working Hours as required).

Management of BCDR events

6.3. Where a BCDR event is invoked, the Recovery Time Objective for the CSS Certificate Authority will be:

(a) four hours target time; and

(b) eight hours target time.

6.4. Where a BCDR event is invoked, the Recovery Point Objective for the CSS Certificate Authority will be 15 minutes.

7 Maximum Demand Volumes

7.1. There are no maximum volumes specified.

8 Reporting

8.1. The CSS Certificate Authority shall provide a monthly performance report to the Code Manager for consideration by the REC Performance Assurance Board, providing details of overall service performance against requirements set out within this service definition.

8.2. Where a security certificate is revoked by the CSS Certificate Authority without a Certificate Signing Request being submitted by the CSS User or the Code Manager, the CSS Certificate Authority shall provide a post event report to the Code Manager in accordance with the CSS Schedule.

9 System Audit

9.1. The CSS Certificate Authority Service shall be audited by a third party against an approved compliance standard or methodology on an annual basis.

9.2. 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 during a period of at least 12 months.

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

9.4. The CSS Certificate Authority shall 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 for a period of no less than 7 years.

10 Data Handling

10.1. The CSS Certificate Authority shall receive all Certificate Signing Requests and Certificate Revocation Requests via the Switching Portal and shall respond to requests within timescales defined in Paragraph 6.

10.2. Data received to support validation of the Nominating Officer is deleted immediately following validation. Only details of Nominating Officer, Senior Responsible Officer and Appointed Responsible Officer names are recorded within the Switching Service Management System.

11 Security

11.1. The CSS Certificate Authority Service shall include:

(a) cryptographic modules to generate, store and operate the CSS Certificate Authority private keys;

(b) capability to generate TLS Certificates that meet the RSA (Rivest-Shamir-Adleman) 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 with IETF RFC 3647; and

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