Version: N3.0

# Appendix N

# SMKI Code of Connection

# Purpose and Scope

This document is the SMKI Code of Connection produced pursuant to Section L4.5 of the Code.

For the purpose of the SMKI Code of Connection, defined terms shall have the meaning in SEC Section A (Definitions and Interpretation), SEC Appendix M (SMKI Interface Design Specification) and Appendix A of this document.

# 1. Connection Mechanism

The DCC shall ensure that only persons who are Authorised Responsible Officers (AROs) and have been issued with the appropriate IKI credentials used to access SMKI Services, as defined in the SMKI RAPP, shall be able to access the SMKI Services on behalf of their organisation. Prior to use any of the SMKI Interfaces, any person representing a Party or RDP shall first become an Authorised Responsible Officer, via the process as set out in the SMKI RAPP.

Any Party or RDP which has use of a DCC Gateway Connection may connect to the SMKI Services via that DCC Gateway Connection, and shall use this mechanism to connect to the service unless it is not reasonably practicable to do so. Any Party or RDP may connect to the SMKI Services via an Internet connection where such Party or RDP does not have a DCC Gateway Connection or where it is not reasonably practicable to use such a connection.

## 1.1. Browser Policy

The DCC shall publish and keep up to date the web browsers and versions which the SMKI Portal interface via a DCC Gateway Connection, and SMKI Portal interface via the Internet supports.

The DCC shall not be required to continue to support any browser versions from which the browser's vendor removes support.

Browsers other than those published may also be compatible, though they will not be supported.

The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection and SMKI Portal interface via the Internet are tested with the published browsers on different operating systems. The DCC shall publish and keep up to date the list of operating systems that have been tested.

Operating systems other than those listed above may also be compatible, though they will not be supported.

The browsers (and versions) and operating systems supported by the DCC shall be reviewed from time to time. The DCC shall seek views from Parties and RDPs prior to the withdrawal of support for any version of a browser, a browser itself, or an operating system set out above.

# 2. SMKI Services interfaces

The DCC shall ensure that SMKI Services shall be made available via four interfaces, as set out in this document. The DCC shall provide relevant technical support information to persons in respect of the use of the SMKI interfaces, upon receipt of a request via the Service Desk.

## 2.1. SMKI Services interfaces via a DCC Gateway Connection

### 2.1.1 SMKI Portal interface via a DCC Gateway Connection

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an interface where a Party or RDP may connect to the SMKI Portal interface using a compatible web browser via a DCC Gateway Connection.

The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection enables Parties or RDPs with access to the interface to navigate to a landing page via a published URL and from there, further choose to:

(a) submit Organisation Certificate Signing Requests (CSR) and retrieve resulting Organisation Certificates;

(b) submit Ad Hoc Device CSRs and retrieve resulting Device Certificates; and

(c) submit Batched CSRs and retrieve resulting Device Certificates.

### 2.1.2 Ad Hoc Device CSR Web Service interface

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an Ad Hoc Device CSR Web Service interface to which an Authorised Subscriber for Device Certificates, which is one of the DCC, Import Supplier, or Gas Supplier, may connect.

The DCC shall ensure that the Ad Hoc Device CSR Web Service interface supports submission of Ad Hoc Device CSRs to the DCC and the subsequent issuance of Device Certificates by the DCC, to support the replacement of a certificate on a Device.

### 2.1.3 Batched Device CSR Web Service interface

The DCC shall at all times (subject to Planned Maintenance) provide and maintain a Batched Device CSR Web Service interface to which an Authorised Subscriber for Device Certificates may connect.

The DCC shall ensure that the Batched Device CSR Web Service interface supports submission of Batched CSRs to the DCC and the subsequent issuance of Device Certificates by the DCC.

## 2.2. SMKI Portal interface via the Internet

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an interface where a Party or RDP may connect to the SMKI Portal interface via the Internet using a compatible web browser.

The DCC shall enable Parties or RDPs with access to the SMKI Portal interface via the Internet to:

(a) submit Organisation CSRs and retrieve resulting Organisation Certificates.

## 2.3. Authentication to SMKI Services interfaces

### 2.3.1 Authentication to SMKI Portal interface via a DCC Gateway Connection or via the Internet

The DCC shall secure the SMKI Portal interface via a DCC Gateway Connection or SMKI Portal interface via the Internet through a mutually authenticated TLS session as set out in the SMKI Interface Design Specification.

The DCC shall publish to Parties and RDPs a 'SMKI User Guide' meeting the requirements of this document.

In order to authenticate to the SMKI Portal, Cryptographic Credential Tokens shall be issued in accordance with the procedures set out in the SMKI RAPP.

Each Party or RDP wishing to access the SMKI Portal interface shall install the Authentication Client software on each ARO's computer used to access the SMKI Portal interface.

The DCC shall make the Authentication Client software available to Parties and RDPs and ensure that the software:

(a) is accessible via a URL that shall be specified and updated from time to time in the SMKI User Guide, using One Way Authentication which can be validated using a 'CA Browser Forum 'server certificate that is signed by a 'Root CA' that is present in in the Windows 'Trusted Root Certification Authorities' certificate store';

(b) is compatible with published operating systems;

(c) is digitally signed using the private key associated with a code signing certificate that is signed by a root CA that is present in in the Windows 'Trusted Root Certification Authorities' certificate store'; and

(d) is supported by instructions as to how to install the Authentication Client software, as set out in the SMKI User Guide.

The Party or RDP may download, and verify the authenticity and integrity of, the Authentication Client software on first use by checking the digital signature used to sign the software and validating the 'CA Browser Forum'[1] server certificate using the certification authority certificates present in the Windows 'Trusted Root Certification Authorities' certificate store'. If such checks are successful, the Party or RDP may install the Authentication Client software on each computer that they wish to use to access the SMKI Portal. In Windows, "Administrator" privileges are required to install the Authentication Client software but are not required to run such software.

The DCC shall ensure that each Cryptographic Credential Token issued contains the appropriate IKI Certificate and Private Key for that Party or RDP, which is needed to authenticate the ARO to the SMKI Portal interface via the DCC Gateway Connection or the SMKI Portal via the Internet.

Furthermore, the DCC shall ensure that:

(a) access to the Cryptographic Credential Token is PIN-protected and the Private Key corresponding with the IKI Certificate used for authentication cannot be removed from the Cryptographic Credential Token;

(b) the Authentication Client software is made available for use by AROs to enable authentication to the SMKI Portal in conjunction with the Cryptographic Credential Token;

(c) it provides support for the Authentication Client software via the Service Desk;

(d) updates are made available to the Authentication Client software accessible via a URL, as set out in the SMKI User Guide; and

1 https://cabforum.org/

(e) ensure that all browsers listed in section 1.1 of this document are capable of supporting the requirements set out in this section.

The process for TLS1.2 mutual authentication to the SMKI Portal interface via the DCC Gateway Connection or the SMKI Portal via the Internet is as set out in the SMKI Interface Design Specification.

### 2.3.2 Authentication to Ad Hoc Device CSR Web Service interface

The DCC shall secure the Ad Hoc Device CSR Web Service interface through a TLS1.2 mutual authenticated session to the SMKI Portal in accordance with the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate, in order to authenticate to the Ad Hoc Device CSR Web Service interface. This IKI Certificate shall be issued by the DCC on successful completion of the process as set out in the SMKI RAPP and in accordance with the SMKI Interface Design Specification.

### 2.3.3 Authentication to Batched Device CSR Web Service interface

The DCC shall secure the Batched Device CSR Web Service interface through a TLS1.2 mutually authenticated session to the SMKI Portal as set out in the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate in order to authenticate to the Batched Device CSR Web Service interface. This shall be issued by DCC on successful completion of the process as set out in the SMKI RAPP in accordance with the SMKI Interface Design Specification.

# 3. Managing Demand

## 3.1. Capacity Management

### 3.1.1 SMKI Portal via a DCC Gateway Connection and SMKI Portal via the Internet

**Organisation CSRs**

The Registration Authority shall process Organisation Certificate Signing Requests received via the DCC Gateway Connection or via the Internet in the same manner.

**Batched CSRs**

The Registration Authority shall process Batched CSRs received via either SMKI Portal interface in the same manner.

Batch CSRs are processed overnight, and the system is scaled to process a total, across all Authorised Subscribers, of 375,000 CSRs contained within Batched CSRs from 20:00 to 08:00 each day.

The DCC shall ensure that Batched CSRs submitted before 8:00pm are processed by 8:00am the following day. Batched CSRs received after 8:00pm may be delayed until the following night's processing period.

In order to preserve the overall system capacity, should a Party foresee a need to submit in excess of 50,000 Device Certificate Signing Requests through the SMKI Portal interface in any 24 hour period, the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the Service Desk. The Batched CSRs exceeding this number shall be queued for processing as soon as reasonably practicable.

Batched CSRs shall be processed by the Registration Authority in turn.

**Ad Hoc Device CSRs**

The Registration Authority shall process Ad Hoc Device CSRs received via the DCC Gateway Connection.

Each Party shall take reasonable steps not to submit more than 150 Ad Hoc Device CSRs in any 24 hour period without the prior agreement of DCC. Should a Party foresee a need to exceed this number the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the DCC's Service Desk.

### 3.1.2 Ad Hoc Device CSR Web Service interface

Each Party shall take reasonable steps not to submit more than one Certificate Signing Request via the Ad Hoc Device CSR Web Service interface in any 0.8 second period during core service hours (07:00 to 20:00) and one Certificate Signing Request in any four second period outside of these hours.

Should a Party foresee a need to exceed either of these numbers, the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the Service Desk.

### 3.1.3 Batched Device CSR Web Service interface

Each Party shall ensure that a synchronous response to the submission of a Batched CSR is received before an additional Batched CSR is submitted via the Batched CSR Web Service interface. Each Party may submit multiple Batched CSRs during the period of time between submission of a Batched CSR and downloading the response file containing the Device Certificates and success/error messages.

Each Party shall comply with the following restrictions in respect of retrieving such Device Certificates:

(a) where a Batched CSR is submitted before 20:00, the Party shall comply with the following restrictions in respect of accessing the response file corresponding with a particular Batched CSR:

i. the Party shall not seek to access the response file containing the Device Certificates prior to 08:00 on the day following the date of submission of the corresponding Batched CSR;

ii. the Party shall not seek to access the response file again via the Batched CSR Web Service interface, at any point once the response file has been successfully retrieved; and

iii. if the response indicates that the Batched CSR has been accepted and that the batch processing is not complete, the Party shall not seek to access the response file more than once each hour during the period from 22:00 and 08:00 on the following day.

(b) where a Batched CSR is submitted after 20:00, the Party shall comply with the following restrictions in respect of accessing the response file corresponding with a particular Batched CSR:

i. the Party shall not seek to access the response file containing the Device Certificates prior to 22:00 on the day after the submission of the corresponding Batched CSR; and

ii. the Party shall not seek to access the response file again via the Batched CSR Web Service interface, at any point once the response file has been successfully retrieved; and

iii. if the response indicates that the Batched CSR has been accepted and that the batch processing is not complete, the Party shall not seek to access the response file again more than once each hour during the period from 22:00 on the day after the submission of the corresponding Batched CSR and 08:00, two days after the date of submission of the corresponding Batched CSR.

## Appendix A Definitions

| Term | Meaning as defined in SEC |
|---|---|
| Ad Hoc Device CSR | Means a CSR submitted via the Ad Hoc Device CSR Web Service interface |
| Authentication Client | Means client software which supports authentication of Authorised Responsible Officers |
| Batched CSR | Means a Batched Certificate Signing Request with its SEC Section A definition. |
| One Way Authentication | Means the industry standard terminology for HTTPS whereby the client is not required to authenticate with a client credential |
| SMKI User Guide | Means the document published by the DCC pursuant to the requirement in section 2.3.1 |