Version: M4.0

Appendix M

SMKI Interface Design Specification

Contents

1 Introduction

1.1 Purpose

Section L4 of the Code sets out the obligation on the DCC to maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification. Section L4.4 sets out the content of the SMKI Interface Design Specification including the protocols and technical standards which are all based on open standards and defines the technical details of the interfaces to SMKI Services insofar as they relate to Authorised Subscribers.

1.2 Target Response Times

i. For the purposes of supporting the measurement of Target Response Times in accordance with Sections L8.3 of the Code, the terms "send" and "receipt" should interpreted as follows:

a) for the Ad Hoc Device CSR Web Service interface:
   i. "receipt" means the receipt of a Device CSR in the DCC Systems that is submitted by an Authorised Subscriber via the Ad Hoc Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specifications in relation to Ad Hoc Device CSRs submitted through the Ad Hoc Web Service interface; and
   ii. "send" means the submission of a Device Certificate or CSR processing error messages from the DCC Systems to Authorised Subscriber within the synchronous response to the corresponding request; or

b) for the Batched Device CSR Web Service interface:
   i. "receipt" means the receipt of a Batched CSR in the DCC Systems that is submitted by an Authorised Subscriber via the Batched Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specifications in relation to Batched Device CSRs submitted through the Batched Web Service interface; and
   ii. "send" means making available the files containing Device Certificates and/or CSR processing error messages via the Batched Device CSR Web Service interface, for download by the Authorised Subscriber ; or

c) for a Batched CSR via the SMKI Portal interface (via DCC Gateway or via the SMKI Portal via the Gateway):
   i. "receipt" means the receipt of a Batched CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design

Specifications in relation to Batched Device CSRs submitted through the SMKI Portal interface; and

ii. "send" means making available the files containing Device Certificates and/or CSR processing error messages on the SMKI Portal interface, for download by the an Authorised Subscriber; or

d) for an Ad Hoc Device CSR via the SMKI Portal interface (via DCC Gateway or via the SMKI Portal via the Gateway):

i. "receipt' means the receipt of an Ad Hoc Device CSR or Organisation in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to Ad Hoc Device CSRs submitted through the SMKI Portal interface; and

ii. "send" means making the Device Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.

e) for an Organisation CSR via the SMKI Portal interface (via DCC Gateway Connection or via the Internet):

i. "receipt' means the receipt of an Organisation CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to Organisation CSRs; and

ii. "send" means making the Organisation Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.

a)

2 SMKI interfaces

2.1 Interface Definition

The DCC shall make the following interfaces available, in order that Authorised Subscribers may access the SMKI Services.

In accordance with the SMKI Code of Connection, the DCC shall make four interfaces available to Parties and RDPs:

a) a SMKI Portal interface, accessed via an Authorised Subscriber's web browser and only accessible via a DCC Gateway Connection (as set out in Section 2.3 of this document);

b) an Ad Hoc Device CSR Web Service interface, for the purposes of submitting single Device CSRs, that may be accessed by an Authorised Subscriber's automated systems, and only accessible via the DCC Gateway Connection (as set out in Section 2.4 of this document);

c) a Batched Device CSR Web Service interface, for the purposes of submitting Batched CSRs for Device Certificates, that may be accessed by an Authorised Subscriber's automated systems, and only accessible via the DCC Gateway Connection (as set out in Section 2.5 of this document); and

d) a SMKI Portal interface made available over a secured Internet connection and accessed through an Authorised Subscriber's web browser that does not use a DCC Gateway Connection (as set out in Section 2.6 of this document).

2.2 General obligations

The DCC shall ensure that PKCS#10 certification request standard is used for the submission of Certificate Signing Requests (CSR). Authorised Subscribers shall submit Certificate Signing Requests according to the CSR structures as defined in Appendix F of this document.

In accordance with Section L11 of the SEC, unless an Authorised Subscriber immediately notifies the DCC of Certificate rejection, the Certificate shall be deemed to be accepted.

ii. The DCC shall ensure that the URLs of the SMKI Service Interfaces shall remain unchanged in the event of the failure of a component of interfaces to the SMKI Services, or invocation of business continuity or disaster recovery measures. The DCC shall ensure that Disaster Recovery systems are functionally identical to the main Interface.

Error codes and examples of error messages in relation to:

a) the SMKI Portal interface via DCC Gateway Connection and SMKI Portal interface via the Internet are set out in the SMKI User Guide;
b) the Ad Hoc Device CSR Web Service interface are set out in Appendix A of this document; and

c) the Batched Device CSR Web Service interface are set out in Appendix C and Appendix D of this document.

2.3 SMKI Portal interface via DCC Gateway Connection

General obligations

iii. The SMKI Portal interface via DCC Gateway Connection provides an asynchronous mechanism for SMKI Authorised Responsible Officers (AROs) to submit Organisation CSRs, and Device CSRs in batch or ad-hoc form on behalf of their Authorised Subscriber.

iv. The DCC shall ensure that the SMKI Portal interface via DCC Gateway Connection:

a) uses the HTTPS protocol, secured by mutually authenticated TLS 1.2 in line with the cryptographic standards set out in Appendix G of this document;

b) uses Javascript, Cascading Style Sheets (CSS) and images;

c) is compliant with the W3C Web Content Accessibility Guidelines (v2) at "AA" level; and

d) is only accessible using a DCC Gateway Connection.

v. The process for obtaining a DCC Gateway Connection is detailed in Section H3 of the Code.

Establishing a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection

vi. In order to establish a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection, an Authorised Subscriber shall:

a) access the SMKI Portal landing page via a defined URL (as set out in the SMKI User Guide), which shall be secured using HTTPS;

b) then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates or Device CSRs/Certificates; and

c) having selected the relevant link in b),ensure the web browser connection is secured by establishing a mutually authenticated TLS 1.2 session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting the IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via DCC Gateway Connection) to the DCC for either:

i. Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates; or

ii. Authorised Subscribers for Device Certificates, for the purposes of submitting Device CSRs and retrieval of resulting Device Certificates.

vii. In order for a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection to be established, the DCC shall ensure that the SMKI Portal via DCC Gateway Connection presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the Authorised Subscriber's web browser to validate and authenticate the DCC's server as part of establishing the mutually authenticated TLS 1.2 session.

viii. The DCC shall ensure that the SMKI Portal via DCC Gateway Connection denies access where the user does not present a valid IKI Certificate for authentication.

Submission of Organisation CSRs and retrieval of resulting Organisation Certificates

2.3.1.1 Submission of Organisation CSRs by Authorised Subscriber

ix. Subject to the provisions of 2.3.1.1 A, Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:

a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and

b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.

A. Network Parties who are Authorised Subscribers accessing the SMKI Portal via the Internet may optionally elect not to populate the value field of the "Subject Unique Identifier" with a 64 bit EUI-64 Compliant identifier, in which case:

a) they shall leave the value field of the "Subject Unique Identifier" blank, and otherwise proceed in accordance with the requirements of 2.3.1.1 (b);

b) a submission made in accordance with 2.3.1.1 A(a) shall be treated for the purposes of the Code (including this Appendix M) as a CSR and be processed accordingly by the DCC, provided that:

c) the Authorised Subscriber must subsequently provide a human readable hexadecimal representation of the EUI-64 value to be included within the Certificate (so using 0..9, a..f, A..F) to the DCC through the SMKI Portal interface via the Internet and re-submit the fully completed CSR via that interface;

d) the DCC shall ensure that a suitably authorised member of Registration Authority personnel confirms that:

i. the representation of the EUI-64 Compliant identifier that has been provided is a representation of an EUI-64 Compliant identifier that has been allocated by the SEC Panel to the Authorised Subscriber, and

ii. the Authorised Subscriber is a Network Party, and

in either case, if not, the DCC shall not Issue an Organisation Certificate to the Authorised Subscriber.

B. The provisions of 2.3.1.1 A shall not apply until such time as the DCC notifies the Security Sub-Committee that the DCC Systems capability to support the provisions of 2.3.1.1 A has been adequately tested and is ready to be used.

C. Following a notification from the DCC to the Security Sub-Committee in accordance with the provisions of 2.3.1.1 B, sub-Clause 2.3.1.1 B and this sub-Clause 2.3.1.1 C shall automatically be deleted from this Appendix M.

2.3.1.2 Receipt and validation of Organisation CSRs by the DCC

x. Following receipt by the DCC of an Organisation CSR, the DCC shall:

a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; and

b) either accept, or reject the CSR;

i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, log an error and return an error message via the SMKI Portal interface to the Authorised Subscriber.

2.3.1.3 Actions following acceptance of Organisation CSRs by the DCC

xi. Where an Organisation CSR is accepted, the DCC shall:

a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and

b) either approve the CSR for further processing or reject the CSR;

i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors and reasons for the

rejection of that CSR, where such errors shall be in accordance with "Response Status" table in Appendix A of this document.

xii. If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR.

2.3.1.4 Actions following approval of Organisation CSRs by the DCC

xiii. Where an Organisation CSR is approved by the DCC, the DCC shall:

a) Issue a corresponding Organisation Certificate;

b) lodge the resulting Organisation Certificate in the SMKI Repository; and

c) make the Organisation Certificate available for download via the SMKI Portal interface via DCC Gateway Connection and the SMKI Repository.

2.3.1.5 Actions following download of an Organisation Certificate by an Authorised Subscriber

xiv. Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.5 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR.

xv. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.5 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

xvi. Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated CRL in the SMKI Repository in accordance with Appendix B of the Code.

Submission of Device CSRs (Ad Hoc or Batched) and retrieval of resulting Device Certificates

A Device Certificate can be submitted through the SMKI Portal interface via DCC Gateway Connection in Ad Hoc CSR form or as a number in Batched CSR form.

2.3.1.6 Submission of Ad Hoc Device CSR or Batched CSR by Authorised Subscriber

xvii. Authorised Subscribers wishing to be issued with a Device Certificate or Device Certificates shall ensure that they generate the relevant Device

CSRs in line with Appendix F of this document, and Appendix A of the Code.

b) **Ad Hoc Device CSR submission** - where the Authorised Subscriber wishes to submit an Ad Hoc Device CSR, the Authorised Subscriber shall paste the CSR into the Ad Hoc Device CSR form (as set out in the SMKI User Guide) and then submit it to the SMKI Portal interface; or

c) **Batched CSR submission** - where the Authorised Subscriber wishes to submit a Batched CSR, the Authorised Subscriber shall:

i. generate the relevant Device CSRs; and

ii. create a .zip file containing the individual Device CSRs, formatted in line with Appendix F of this document, then upload and submit the .zip file using the Batched CSR web form (as set out in the SMKI User Guide) to the SMKI Portal interface.

2.3.1.7 Receipt and validation of Device CSR (Ad Hoc or Batched) by the DCC

iii. Following receipt by the DCC of an Ad Hoc Device CSR or Batched CSR to the SMKI Portal via DCC Gateway Connection, the DCC shall:

a) for an Ad Hoc Device CSR submission:

i. validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;

ii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code; and

iii. either accept, or reject the CSR; and

A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

B. where the CSR is rejected, log an error and return an error message that is in accordance with "Response Status" table in Appendix A of this document, via the SMKI Portal interface to the Authorised Subscriber; or

b) for a Batched CSR submission:

i. validate that the structure of the submitted .zip file is in accordance with the format set out in Appendix F to this document;

ii. validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;

A. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR) ; or

B. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;

iii. either accept, or reject the Batched CSR and/or each constituent Device CSR, log relevant errors and return a synchronous response via the SMKI Portal interface to notify the Authorised Subscriber as to:

A. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; or

B. where the Batched CSR is rejected, relevant error messages that are in accordance with "Response Status" table in Appendix C of this document.

2.3.1.8 Actions following acceptance of Device CSRs by the DCC

iv. If a Device CSR is accepted, the DCC shall:

a) for an Ad Hoc Device CSR submission:

i. perform such additional checks as DCC determines is necessary on the Device CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

ii. check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates;

iii. either approve, or reject the Device CSR; and

A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber; or

b) for a Batched CSR submission:

i. validate the format, and verify the signature of each Device CSR contained within the Batched CSR in line with Appendix F of this document and PKCS#10;

ii. perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

iii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;

iv. check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;

v. either approve, or reject each Device CSR in the Batched CSR; and

A. where the CSR is approved, include a notification in the Batched CSR response file, as set out in section 2.3.4.4d) of this document, to the Authorised Subscriber; or

B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix C of this document, and include an error notification in the Batched CSR response file, as set out in section 2.3.4.4d) of this document.

v. Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the DCC's Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

vi.

vii. If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

2.3.1.9 Actions following approval of Device CSRs by the DCC

viii. Where a Device CSR is approved by the DCC, the DCC shall:

a) Issue a corresponding Device Certificate;

b) lodge the resulting Device Certificate in the SMKI Repository; and

c) for Ad Hoc Device CSRs:

i. make the corresponding Device Certificate, for up to 30 days following provision by the DCC, available for download via the 'certificate pickup' page on the SMKI Portal interface via DCC Gateway Connection (as set out in the SMKI User Guide) and the SMKI Repository;

ix. In order to retrieve the Device Certificate, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates; or

d) for Batched CSRs:

i. make available, for up to 30 days following provision by the DCC, two files for download via the 'certificate pickup' page on the SMKI Portal interface, comprising:

A. a .zip file containing the Certificates in Base64 encoded DER format resulting from successfully processed CSRs; and

B. a .txt file containing a report showing the processed status of each CSR in the Batched CSR, including errors.

x. In order to retrieve the response files (as set out above) which correspond with a Batched CSR submission, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway

Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates.

2.3.1.10 Actions following download of an Device Certificate by an Authorised Subscriber

xi. Upon downloading the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

xii. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

xiii.

2.4 Ad Hoc Device CSR Web Service interface

General obligations

xiv. The Ad Hoc Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber's systems to submit individual Device CSRs.

xv. The DCC shall ensure that the Ad Hoc Device CSR Web Service interface:

a) is only accessible to Authorised Subscribers for Device Certificates acting on behalf of Parties in the User Role of Import Supplier, Gas Supplier, or the DCC;

b) uses the HTTPS protocol, secured by mutually authenticated TLS 1.2, in line with the cryptographic properties set out in Appendix G of this document;

c) uses Extensible Markup Language (XML) over REST for Device CSR message requests and responses;

d) provides message responses which are consistent with Appendix A of this document;

e) uses the XML Schema for CSR message requests and responses defined in Appendix B of this document; and

f) is only accessible using a DCC Gateway Connection.

xvi. Prior to gaining access to the Ad Hoc Device CSR Web Service interface, Authorised Subscribers shall prepare and provide to the DCC

a CSR, as set out in Appendix G, in electronic form in respect of an IKI Certificate in accordance with the procedures set out in the SMKI RAPP and as set out immediately below.

xvii. The DCC shall validate the format, and verify the signature of the CSR in line with Appendix G of this document and the IKI Certificate Policy. If accepted, the DCC shall process the CSR and shall, if accepted, provide the Authorised Subscriber with the following, in accordance with the SMKI RAPP:

a) an IKI Certificate issued under the appropriate Infrastructure Certificate Authority for the purpose of enabling client authentication to the Ad Hoc Device CSR Web Service interface; and

b) a CA/Browser Forum recognised certificate authority root certificate and all corresponding issuing authority certificates, for the purposes of enabling server authentication of the Ad Hoc Device CSR Web Service interface.

Establishing a secured connection to the Ad Hoc Device CSR Web Service interface

In order to establish a secured TLS1.2 connection to the Ad Hoc Device CSR Web Service interface, an Authorised Subscriber for Device Certificates acting as an Import Supplier or Gas Supplier, or the DCC, shall:

a) configure its system(s) to connect to the Ad Hoc Device CSR Web Service interface URL, as set out in the SMKI User Guide;

b) establish a TLS 1.2 session by presenting the IKI Certificate which has been Issued in accordance with the SMKI RAPP for the purposes of TLS 1.2 mutual authentication to secure access to the Ad Hoc Device CSR Web Service interface.

c) configure its systems such that the TLS 1.2 session renegotiation timeout is set to 5 minutes for each connection to the Ad Hoc Device CSR Web Service interface.

xviii. In order for a secured connection to the Ad Hoc Device CSR Web Service interface to be established, the DCC shall ensure that the Ad Hoc Device CSR Web Service presents the CA/Browser Forum certificate referenced in section 2.4.1 of this document, for the purposes of allowing the Authorised Subscriber's systems to authenticate the server as part of establishing the mutually authenticated TLS1.2 session.

xix. The DCC shall ensure that access to the Ad Hoc Device CSR Web Service interface is denied where the user does not present a valid IKI Certificate for authentication.

Submission of Device CSRs and retrieval of resulting Device Certificates

2.4.1.1 Submission of Device CSRs by Authorised Subscriber

Authorised Subscribers wishing to be Issued with a Device Certificate via the Ad Hoc Device CSR Web Service interface shall ensure that they:

a) generate a Device CSR in line with Appendix F of this document and Appendix A of the Code; and
b) include the Device CSR in the XML format defined in the XML Schema set out in Appendix B of this document and submit the CSR via HTTP POST to the Ad Hoc Web Service interface.

2.4.1.2 Receipt and validation of Device CSRs by the DCC

Following receipt of a Device CSR to the Ad Hoc Device CSR Web Service interface, the DCC shall:

a) validate that the format of the XML document complies with the XML schema as set out in Appendix B of this document;
b) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;
c) either accept, or reject the CSR;
    i. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems.

2.4.1.3 Actions following acceptance of Device CSRs by the DCC

xx. If a Device CSR is accepted, the DCC shall:

a) check that at least one Key Agreement Certificate or Digital Signing Certificate has previously been Issued for the Device ID to which the Device CSR relates;
b) check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates;
c) either approve, or reject the Device CSR; and
    i. where the CSR is approved, return a notification of acceptance in the synchronous XML response, to the Authorised Subscriber's systems; or
    ii. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems.

2.4.1.4 Actions following approval of Device CSRs by the DCC

xxi. Where a Device CSR submitted via the Ad Hoc Device CSR Web Service interface is approved, the DCC shall:

a) Issue a corresponding Device Certificate;
b) lodge the resulting Device Certificate in the SMKI Repository; and

c) return the Device Certificate to the Authorised Subscriber, as set out in Appendix A to this document, in the synchronous XML response to the submission of the Device CSR via the Ad Hoc Device CSR Web Service interface.

2.4.1.5 Actions following download of an Device Certificate by an Authorised Subscriber

xxii. Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

xxiii. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

2.5 Batched Device CSR Web Service interface

General obligations

xxiv. The Batched Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber's systems to submit Batched CSRs containing Device CSRs and subsequently a synchronous mechanism to retrieve the resulting Device Certificates.

xxv. The DCC shall ensure that the Batched Device CSR Web Service interface:

a) uses the HTTPS protocol, secured by mutually authenticated TLS 1.2, in line with the cryptographic properties set out in Appendix G of this document;

b) uses Extensible Markup Language (XML) over REST for Batched CSR message requests, Batched CSR responses and provision of Device Certificates;

c) provides message responses corresponding with submission of Batched CSRs which are consistent with Appendix C of this document;

d) provides message responses in relation to the processing of individual Device CSRs that are contained within a Batched CSR which are consistent with Appendix D of this document;

e) uses the XML Schema for Batched CSR message requests and responses defined in Appendix E; and

f) is only accessible using a DCC Gateway Connection.

xxvi. Prior to gaining access to the Batched Device CSR Web Service interface, an Authorised Subscriber for Device Certificates shall prepare and provide to the DCC a CSR, as set out in Appendix G, in electronic form in respect of an IKI Certificate in accordance with the procedures set out in the SMKI RAPP.

xxvii. The DCC shall validate the format, and verify the signature of the CSR in line with Appendix G of this document and the IKI Certificate Policy. If accepted, the DCC shall process the CSR and shall, if accepted, provide the following in accordance with the SMKI RAPP:

a) an IKI Certificate issued under the appropriate Infrastructure Certificate Authority enabling authentication to the Batched Device CSR Web Service interface; and

b) a CA/Browser Forum recognised certificate authority root certificate and all corresponding issuing authority certificates for the purposes of enabling server authentication of the Batched Device CSR Web Service interface.

Establishing a secured connection to the Batched Device CSR Web Service interface

In order to establish a connection to the Batched Device CSR Web Service interface, an Authorised Subscriber for Device Certificates shall:

a) configure its system(s) to connect to the Batched Device CSR Web Service interface URL, as set out in the SMKI User Guide;

b) establish a TLS session by presenting an IKI Certificate Issued in accordance with the SMKI RAPP for the purposes of TLS mutual authentication in order to secure access to the Batched Device CSR Web Service interface; and

c) configure its system(s) such that the TLS session renegotiation timeout is set to 5 minutes.

xxviii. The DCC shall ensure that the Batched Device CSR Web Service presents the CA/Browser Forum certificate referenced in section 2.5.1 of this document, for the purposes of allowing the Authorised Subscriber's client to authenticate the DCC's server as part of establishing the mutually authenticated TLS session.

xxix. The DCC shall ensure that access to the Batched Device CSR Web Service interface is denied where the user does not present a valid IKI Certificate for authentication.

Submission of Batched CSRs and retrieval of resulting Device Certificates

2.5.1.1 Submission of Batched CSRs by Authorised Subscriber

An Authorised Subscriber wishing to be Issued with Device Certificates in response to a Batched CSR submission via the Batched Device CSR Web Service interface shall ensure that it:

a) generates each CSR to be contained within the Batched CSR in line with Appendix F of this document and Appendix A of the Code;
b) include each Device CSR in the Batched CSR in the XML format defined in the XML Schema set out in Appendix E of this document; and
c) submit the XML document containing the Batched CSR via HTTP POST to the Batched Web Service interface.

2.5.1.2 Receipt and validation of Batched CSR by the DCC

On receipt of an XML document containing a Batched Device CSR to the Batched Device CSR Web Service interface from an Authorised Subscriber's system, the DCC shall:

a) validate that the format of the XML document complies with the XML schema as set out in Appendix E of this document;
b) validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;
    i. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR) ; or
    ii. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;
c) either accept, or reject the Batched CSR, log relevant errors and return in the synchronous XML response to the Authorised Subscriber's systems, to notify the Authorised Subscriber as to:
    i. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR;
    ii. where the Batched CSR is rejected, relevant error messages; and
    iii. a Batched CSR identifier that can be used to retrieve the Batched CSR XML response file as set out in section 2.5.3.4 of this document.

2.5.1.3 Actions following acceptance of Device CSRs in a Batched CSR by the DCC

Upon acceptance of a Batched CSR as set out immediately above, the DCC shall:

a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;

e)

b) perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

c) apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;

d) check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;

e) either approve, or reject each Device CSR in the Batched CSR and include (where applicable) resulting Device Certificates, notifications and error messages in a Batched CSR XML response file that is separate from the synchronous response file described in section 2.5.3.2 of this document; and

i. where the CSR is approved, include a notification in the Batched CSR XML response file, to the Authorised Subscriber; or

ii. where the CSR is rejected, log an error and include an error notification in the Batched CSR XML response file.

xxx. Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the DCC's Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

xxxi. If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

2.5.1.4 Actions following approval of Device CSRs in a Batched CSR by the DCC

xxxii. Where a Device CSR submitted via the Batched CSR Web Service interface is approved, the DCC shall:

a) Issue a corresponding Device Certificate;

b) lodge the resulting Device Certificate in the SMKI Repository;

c) make the Device Certificate available to the Authorised Subscriber for download in the Batched CSR XML response file, as described in section 2.5.3.3, Appendix D and Appendix E to this document; and

d) generate files for download via the 'certificate pickup' page on the SMKI Portal interface, as set out in section 2.3.4.4 of this document.

xxxiii. An Authorised Subscriber may, at any point up to 30 days following provision by the DCC, download the XML response file containing success and error information and Device Certificates Issued in response to Device CSRs in a Batched CSR, by:

a) establishing a TLS mutual authentication session to the Batched Device CSR Web Service interface; and

b) appending the Batched CSR identifier supplied in response to the Batched CSR submission to the URL as defined in the SMKI User Guide for the purposes of retrieving response XML files for Batched CSR submissions.

2.5.1.5 Actions following download of a Device Certificate by an Authorised Subscriber

xxxiv. Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

xxxv. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

2.6 SMKI Portal interface via the Internet

General obligations

xxxvi. The SMKI Portal interface via the Internet provides an asynchronous mechanism for SMKI Authorised Responsible Officers (AROs) not accessing the SMKI Service through a DCC Gateway Connection to submit Organisation CSRs and to retrieve resulting Certificates, on behalf of their Authorised Subscriber.

xxxvii. The SMKI Portal via the Internet also provides a mechanism by which Authorised Subscribers may access certain SMKI Repository content.

xxxviii. The DCC shall ensure that the SMKI Portal interface via the Internet:

a) uses the HTTPS protocol, secured by mutually authenticated TLS 1.2 in line with the cryptographic standards set out in Appendix G of this document;

b) uses Javascript, Cascading Style Sheets (CSS) and images;

c) is compliant with the W3C Web Content Accessibility Guidelines (v2) at "AA" level;

d) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the North Region;

e) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the Central Region and South Region;

f) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI CRL;

g) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation CRL;

h) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI ARL;

i) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation ARL;

j) provides a web form, as set out in the SMKI User Guide, where persons with access to the SMKI Portal via the Internet can request information

held within the SMKI Repository. The DCC shall process such requests and provide information via electronic means; and

k) is only accessible via the Internet.

xxxix. Provision of a connection to the Internet is the responsibility of the Authorised Subscriber.

xl. The DCC shall ensure that the Organisation Certificates and OCA Certificates contained within the two Device anchor slot Certificate files shall be the same, other than the Organisation Certificates required to populate the WAN provider Device anchor slot.

xli. The DCC shall lodge a document in the SMKI Repository, which sets out details of which of the base set of Organisation Certificates and OCA Certificates may be placed in specific Device anchor slots.

Establishing a secured web browser connection to the SMKI Portal interface via the Internet

xlii. In order to establish a connection to the SMKI Portal interface via the Internet, an Authorised Subscriber shall:

a) access a SMKI Portal landing page via defined URL (as defined in the SMKI User Guide) which shall be secured using HTTPS;

b) then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates; and

c) having selected the relevant link in b), ensure the web browser connection is secured by establishing a mutually authenticated TLS 1.2 session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting an IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via the Internet) to the DCC for either:

i. Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates.

xliii. In order for a secured web browser connection to the SMKI Portal interface via the Internet to be established, the DCC shall ensure that the SMKI Portal via the Internet presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the Authorised Subscriber's systems to authenticate the server as part of establishing the mutually authenticated TLS 1.2 session.

xliv. The DCC shall ensure that the SMKI Portal via the Internet denies access where the user does not present a valid IKI Certificate for authentication.

Submission of Organisation CSRs and retrieval of resulting Organisation Certificates

2.6.1.1 Submission of Organisation CSRs by Authorised Subscriber

xlv. Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:

a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and

b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.

2.6.1.2 Receipt and validation of Organisation CSRs by the DCC

xlvi. Following receipt of an Organisation CSR, the DCC shall:

a) validate the format, and verify the signature of the CSR in line with Appendix F of this document and PKCS#10;

b) either accept, or reject the CSR:

i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber.

2.6.1.3 Actions following acceptance of Organisation CSRs by the DCC

xlvii. Where an Organisation CSR is accepted, the DCC shall:

a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and

b) either approve the CSR for further processing or reject the CSR;

i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors, which shall be in accordance with "Response Status" table in Appendix A of this document, and reasons for the rejection of that CSR.

xlviii. If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant

Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR.

2.6.1.4 Actions following approval of Organisation CSRs by the DCC

xlix. Where an Organisation CSR is approved by the DCC, the DCC shall:

a) process the CSR;

b) Issue a corresponding Organisation Certificate;

c) lodge the resulting Organisation Certificate in the SMKI Repository; and

d) make the Organisation Certificate available for download via the SMKI Portal interface via the Internet and the SMKI Repository.

2.6.1.5 Actions following download of an Organisation Certificate by an Authorised Subscriber

l. Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.4 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR.

li. Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.4 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

lii. Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated CRL in the SMKI Repository in accordance with Appendix B of the Code.

Appendix A Ad-Hoc Device CSR Web Service Messages

Example: Device Certificate Signing Request Message

The following message format is used to request a Device Certificate from SMKI via the Ad Hoc Device CSR Web Service interface.

```
Host: localhost:443
Content-Length: 439
User-Agent: Jakarta Commons-HttpClient/3.0.1
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="utf-8"?>
 <DeviceCertificateSigningRequest ID="clientId1">
 <Version>1.0</Version>
<CertificateSigningRequest>MIIBDTC……HULdtQN</CertificateSigningRequest>
</DeviceCertificateSigningRequest>
```

Device Certificate Signing Request: Element Table

Element Name	*Description*
DeviceCertificateSigningRequest	*The root element*
Version	*This element contains the version of the Ad Hoc Device CSR Web Service interface. In the schema specified in Appendix B of this document, this value is set to "1.0"*
CertificateSigningRequest	*This element contains the Base64 encoded PKCS#10 Certificate Signing Request (CSR) without whitespace. Base64 is defined by "Standard 'base64' in RFC4648 section 4". The CSR shall NOT use Privacy Enhanced Mail (PEM) headers. E.g. -----BEGIN CERTIFICATE REQUEST---- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----*

Device Certificate Signing Request: Attribute Table

Attribute Name	*Description*
ID	*The client reference to the request. This value will be returned in the response unless the original request is incorrectly formed.*

Example: Response to Ad Hoc Device Certificate Signing Request – Success

The following message is returned in response to Device Certificate Signing Request when the DCC has successfully Issued a Device Certificate. The message includes the Device Certificate that was Issued.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="utf-8"?>
<DeviceCertificateSigningResponse ID="clientid1">
      <Version>1.0</Version>
      <Build>1.1.4</Build>
      <TransactionId>12345</TransactionId>
      <Status>SUCCESS</Status>
<Certificate>MIAGCSqGSIb3DQEHA……AAAAAA</Certificate>
</DeviceCertificateSigningResponse>
```

Example: Response to Ad Hoc Device Certificate Signing Request – Incorrect XML

The following message is returned in response to invalidly formed Device CSR. Where there is an invalidly formed Device CSR, the DCC may be unable to return the client supplied ID value.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="utf-8"?>
 <DeviceCertificateSigningResponse>
      <Version>1.0</Version>
      <Build>1.1.4</Build>
      <TransactionId>12344</TransactionId>
      <Status>FORMAT_ERROR</Status>
      <Error>
        <ErrorCode>FM:123</ErrorCode>
       <ErrorText>An XML format error</ErrorText>
      </Error>
```

Example: Response to Ad Hoc Device Certificate Signing Request – other error

The following message is returned in response to Device CSR when the DCC failed to issue a Device Certificate.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="utf-8"?>
<DeviceCertificateSigningResponse ID="clientid1">
      <Version>1.0</Version>
      <Build>1.1.4</Build>
      <TransactionId>12345</TransactionId>
      <Status>CSR_ERROR</Status>
      <Error>
        <ErrorCode>CR:9999</ErrorCode>
        <ErrorText>Request for duplicate certificate not permitted</ErrorText>
      </Error>
</DeviceCertificateSigningResponse>
```

Response to Ad Hoc Device Certificate Signing Request: Element Table

Element Name	***Description***
DeviceCertificateSigningResponse	*The root element*
Version	*This element contains the version of the web service interface. In the schema specified in Appendix B of this document, this value is set to "1.0"*
Build	*This element specifies the software build of the web service.*
TransactionId	*This is the SMKI internal reference to the request.*
Status	*This element reports on the condition of the response. See the section "*Response Status*"*
Certificate	*This element contains a Base64 encoded DER X509v3 certificate without whitespace and shall not include PEM headers. Base64 is defined by "Standard 'base64' in RFC4648 section 4".*
Error	*Container for ErrorCode and ErrorText*
ErrorCode	*This element holds an internal reference code to a specific error occurrence. See the section "*Response Status*"*
ErrorText	*This element holds a human readable error string corresponding to the ErrorCode. See the section "*Response Status*"*

Response to Ad Hoc Device Certificate Signing Request: Attribute Table

Attribute Name	***Description***
ID	*This holds the client reference to the original request.*

Response Status

Value	*Error Code*	*Description*
SUCCESS	*n/a*	*This value indicates a certificate has been generated and is returned in the response.*
UNKNOWN_DEVICE	*UD:<Value>*	*The request has been rejected. The device has not had a device certificate previously and hence the request to replace an existing certificate is not valid.*
ISSUANCE_ANOMALY	*CA:<Value>*	*The request has been rejected. A certificate issued from the submitted CSR would result in unexpected issuance behaviour. Manual action by the DCC RA team would need to be taken to allow a future submission of this CSR to result in a certificate.*
CSR_ERROR	*CR:<Value>*	*The request has failed. This is due to a corrupt CSR or incorrect CSR format. The client should correct the mistake and re-submit the error.*
CA_ERROR	*CA:<Value>*	*The request has failed. An internal error has prevented the CA from issuing the certificate. Re-submission may fix this issue.*
FORMAT_ERROR	*FM:<Value>*	*The request has failed. This is due to the request XML format error. The client should correct the mistake and re-submit the error.*
WORKFLOW_ERROR	*WF:<Value>*	*The request has failed. A workflow error has prevented to issuance of the certificate. Re-submission is unlikely to remedy this issue and should report the error code to the DCC helpdesk.*

Appendix B Schema for Ad Hoc Device CSR Web Service interface

This section specifies the XML schema that will be used to verify the contents for the web service request and response messages relevant to the Ad Hoc Device CSR Web Service interface, as per the figure below.

The Ad Hoc Device CSR Web Service Interface version will be specified in the URL, the schema filename and data contained in the XML requests and responses. The web service interface version allowed value will be hardcoded in the schema.

There will be different URL used when the XML Schema for the Ad Hoc Device CSR Web Service interface changes.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xsd:element name="DeviceCertificateSigningResponse">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="Version">
            <xsd:simpleType>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="1.0"/>
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:element>
        <xsd:element name="Build" type="xsd:string" nillable="false" />
        <xsd:element name="TransactionId" type="xsd:positiveInteger" nillable="false"/>
        <xsd:element name="Status" nillable="false">
          <xsd:simpleType>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="SUCCESS"/>
              <xsd:enumeration value="ISSUANCE_ANOMALY"/>
              <xsd:enumeration value="UNKNOWN_DEVICE"/>
              <xsd:enumeration value="CA_ERROR"/>
              <xsd:enumeration value="CSR_ERROR"/>
              <xsd:enumeration value="FORMAT_ERROR"/>
              <xsd:enumeration value="WORKFLOW_ERROR"/>
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:element>
        <xsd:choice>
          <xsd:element name="Certificate" type="xsd:base64Binary" nillable="true"/>
          <xsd:element name="Error">
            <xsd:complexType>
              <xsd:sequence>
                <xsd:element name="ErrorCode" nillable="false">
                  <xsd:simpleType>
                    <xsd:restriction base="xsd:string">
                      <xsd:minLength value="1"/>
                      <xsd:maxLength value="10"/>
                      <xsd:pattern value="[A-Z]{2}:[A-Za-z0-9]+"/>
                    </xsd:restriction>
                  </xsd:simpleType>
                </xsd:element>
                <xsd:element name="ErrorText" type="xsd:string" nillable="false"/>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
```

```
        </xsd:choice>
      </xsd:sequence>
      <xsd:attribute name="ID" use="optional">
        <xsd:simpleType>
          <xsd:restriction base="xsd:string">
            <xsd:minLength value="1"/>
            <xsd:maxLength value="32"/>
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:attribute>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="DeviceCertificateSigningRequest">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="Version">
          <xsd:simpleType>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="1.0"/>
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:element>
        <xsd:element name="CertificateSigningRequest" nillable="false">
            <xsd:simpleType>
            <xsd:restriction base="xsd:base64Binary"/>
          </xsd:simpleType>
        </xsd:element>
      </xsd:sequence>
      <xsd:attribute name="ID" use="required">
        <xsd:simpleType>
          <xsd:restriction base="xsd:string">
            <xsd:minLength value="1"/>
            <xsd:maxLength value="32"/>
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:attribute>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

Appendix C Submission of Batched CSRs via the Batched Device CSR Web Service Interface

In order to submit the Device Certificates that are the subject of a Batched CSR via the Batched Device CSR Web Service interface, a request shall be sent by the requestor to SMKI using HTTP POST.

The batch submission response shall be returned by the DCC, providing the field "BatchId" upon successful submission. The value of "BatchId" shall be used in the retrieval of Device Certificates, as specified in Appendix D of this document.

The destination URL for the post will include the web service interface version and must match the version specified in the section of this Appendix C titled "**Batched CSR Response message: Element Table**" and will take the form as set out below:

a) https://example.com:443/1.0/PortalCSRBatch/SubmitCSRBatch

f) where "1.0" in the above URL is the web service interface version

Example: Submit Batched CSR Message

The following message is used to request Device Certificates from SMKI via the Batched Device CSR Web Service.

```
Host: localhost:443
Content-Length: 439
User-Agent: Jakarta Commons-HttpClient/3.0.1
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0" encoding="utf-8"?>
<SubmitCSRBatch ID="b1999">
        <Version>1.0</Version>
        <DeviceCSR ID="ID0">UjBsR09EbGhj……1tQ1p0dU1GUXhEUzhi</DeviceCSR>
        <DeviceCSR ID="ID1">UjBsR09EbGh……U1GUXhEUzhi</DeviceCSR>
        <DeviceCSR ID="ID2">UjBsR09…..0dU1GUXhEUzhi</DeviceCSR>
</SubmitCSRBatch>
```

Submit Batched CSR Message: Element Table

Element Name	*Description*
SubmitCSRBatch	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E of this document, this value is set to "1.0"
DeviceCSR	This element contains the Base64 encoded PKCS#10 certificate signing request (CSR) without whitespace. Base64 is defined by "Standard 'base64' in RFC4648 section 4". The CSR shall NOT use PEM headers. e.g. -----BEGIN CERTIFICATE REQUEST---- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----

Submit Batched CSR Message: Attribute Table

Attribute Name	*Parent Element*	*Description*
ID	SubmitCSR Batch	The client reference to the batch request. This value will be returned in the completed batch result.
ID	DeviceCSR	The client reference to an individual CSR request within the batch request. This value will be returned in the completed batch result to help correlate the resulting certificate with the CSR request. This value MUST be unique within the batch. The format of the ID will be enforced by the associated field type defined in the schema.

Example: Response to Batched CSR – success

The following message is returned in response to the "SubmitCSRBatch" request when the submitted Batched CSR has been accepted.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="utf-8"?>
<SubmitCSRBatchStatus ID="b1999">
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>PENDING</BatchStatus>
        <BatchId>1234</BatchId>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR – Incorrect XML

The following message is returned in response to an invalidly formed "SubmitCSRBatch" request. In this scenario, DCC is unable to return the client supplied ID field.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="utf-8"?>
 <SubmitCSRBatchStatus>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>FORMAT_ERROR</BatchStatus>
        <Error>
                <ErrorCode>FM:AA1</ErrorCode>
                <ErrorText>Invalid XML in request</ErrorText>
        </Error>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR– maximum batch size exceeded

The following message is returned in response to the "SubmitCSRBatch" request when the maximum number of certificate signing requests in the request is exceeded. The maximum batch size is 50,000 CSRs, this figure is detailed in the SMKI Code of Connection. The maximum batch size stated in the SMKI Code of Connection would take precedence should the size differ from that stated in this document.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<SubmitCSRBatchStatus ID=”b1999”>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>FORMAT_ERROR</BatchStatus>
        <Error>
                <ErrorCode>FM:AA2</ErrorCode>
                <ErrorText>Number of submitted CSRs exceeds maximum volume</ErrorText>
        </Error>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR response– other error

The following message is returned in response to the "SubmitCSRBatch" request when SMKI failed to accept the Batched CSR.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
<SubmitCSRBatchStatus ID=”b1999”>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>WORKFLOW_ERROR</BatchStatus>
        <Error>
                <ErrorCode>WF:BB2</ErrorCode>
                <ErrorText>An internal error.</ErrorText>
        </Error>
</SubmitCSRBatchStatus>
```

Batched CSR response message: element table

Element Name	***Description***
SubmitCSRBatchStatus	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E, this value is set to "1.0"
Build	This element specifies the software build of the web service.
BatchId	This is the SMKI internal reference to the batch request. This value should be used to query the CSRBatchResult.

Element Name	*Description*
BatchStatus	This element reports on the condition of the response, as set out below.
Error	Container for ErrorCode and ErrorText
ErrorCode	This element holds an internal reference code to a specific error occurrence, as set out below.
ErrorText	This element holds a human readable error string corresponding to the ErrorCode, as set out below

Batched CSR response message: attribute table

Attribute Name	Parent Element	Description
ID	SubmitCSRBatch Status	The client reference to the batch. This value corresponds to the SubmitCSRBatch ID attribute in the SubmitCSRBatch message.

Batched CSR response message: response status values

Value	*Error Code*	*Description*
PENDING	n/a	The Batched CSR has been uploaded, accepted and is awaiting approval.
FORMAT_ERROR	FM:<Value>	The request has failed. This is due to the request XML format error. The client should correct the mistake and re-submit the request.
WORKFLOW_ERROR	WF:<Value>	The request has failed. A workflow error has prevented acceptance of the batch request. Re-submission is unlikely to remedy this issue and should report the error code to the DCC Service Desk.

Appendix D Retrieval of Device Certificates as a result of Batched CSR submission

In order to retrieve the Device Certificates that are the subject of a Batched CSR submitted via the Batched Device CSR Web Service interface, a batch result poll request shall be sent by the requestor to SMKI using HTTP GET.

The batch result shall be returned by the DCC using the form field "BatchId", which will be encoded within the GET URL. The value of the "BatchId" field is returned to the requesting system in response to the initial successful "SubmitCSRBatch" web service message. Parties may query for batches they have submitted, however any other values of the "BatchId" field will be rejected.

The destination URL for the get will include the web service interface version and must match the version specified in the section of this Appendix D titled "**Batched CSR Result: Element Table**" and will take the form as set out below:

b) https://example.com:443/1.0/PortalCSRBatch/CSRBatchResult?BatchId=99, where "1.0" in the above URL is the web service interface version

Example: Batched CSR Result Message – Incomplete batch processing

The following message is returned in response to "CSRBatchResult" query and the corresponding batch processing has not been completed. The following batch status values may be returned in this message and where such values are defined in the section titled "Batched CSR Result: BatchStatus values" within this Appendix:

PENDING, REJECTED, PARSING, QUEUED, PROCESSING, PAUSED, TAMPERED

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult ID="b1999">
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>PENDING</BatchStatus>
        <BatchId>1234</BatchId>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Batch Completed

The following message is returned in response to a "CSRBatchResult" query when each Device CSR has been processed. This file shall contain, for all Device CSRs that were included in the corresponding Batched CSR, either a successfully generated Device Certificate or details of rejected Device CSR.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 662
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult ID="b1999">
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>COMPLETED</BatchStatus>
        <BatchId>1234</BatchId>
        <DeviceCertificate ID="ID000000">
                <Status>SUCCESS</Status>
                <Certificate>UjBsR09EbGhjZ0dTQUxNQUF……..Q1p0dU1GUXhEUzhi</Certificate>
        </DeviceCertificate>
        <DeviceCertificate ID="ID000001">
                <Status>CSR_ERROR</Status>
               <Error>
                        <ErrorCode>CR:CC1</ErrorCode>
                        <ErrorText>Wrong CSR OID</ErrorText>
                </Error>
        </DeviceCertificate>
        <DeviceCertificate ID="ID000002">
                <Status>SUCCESS</Status>
                <Certificate>UjBsR09EbGhjZ0d……Q1p0dU1GUXhEUzhi</Certificate>
        </DeviceCertificate>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Unknown BatchId

The following message is returned in response to a “CSRBatchResult” query where the supplied “BatchId” does not exist.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>FORMAT_ERROR</BatchStatus>
        <Error>
                <ErrorCode>FM:AA3</ErrorCode>
                <ErrorText>Unknown BatchId</ErrorText>
        </Error>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Other Error

The following message is returned in response to a "CSRBatchResult" query when SMKI failed to interrogate the batch state.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>WORKFLOW_ERROR</BatchStatus>
        <Error>
                <ErrorCode>WF:BB1</ErrorCode>
                <ErrorText>An Internal Error</ErrorText>
        </Error>
</CSRBatchResult>
```

Batched CSR Result: Element Table

Element Name	Description
CSRBatchResult	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E, this value is set to "1.0"
Build	This element specifies the software build of the web service.
BatchId	This is the SMKI internal reference to the batch request.
BatchStatus	This element reports on the condition of the response. See the section "Batched CSR Result: BatchStatus values"
Error	Container for ErrorCode and ErrorText
ErrorCode	This element holds an internal reference code to a specific error occurrence. See the section "Response Status" and "Batched CSR Result: Status values".
ErrorText	This element holds a human readable error string corresponding to the ErrorCode.
DeviceCertificate	This element holds a response to a certificate signing request.
Certificate	This element contains a Base64 encoded DER X509v3 certificate without whitespace and shall not include PEM headers. Base64 is defined by "Standard 'base64' in RFC4648 section 4".
Status	This element holds the outcome of processing the certificate signing request. See the section "Batched CSR Result: Status values"

Batched CSR Result: Attribute Table

Attribute Name	Parent Element	Description
ID	CSRBatchResult	The client reference to the batch. This value corresponds to the SubmitCSRBatch ID attribute in the SubmitCSRBatch message.
ID	DeviceCertificate	The client reference to an individual certificate within the batch response. This value corresponds to the DeviceCSR ID attribute in the SubmitCSRBatch message

Batched CSR Result: BatchStatus values

Value	Error Code	Description
PENDING	n/a	The batch has been uploaded, accepted and is awaiting approval.
REJECTED	n/a	The batch has been rejected by a DCC RA agent. The batch will not be processed further.
PARSING	n/a	The batch has been approved by DCC RA Agent and the batch request and associated certificate signing requests are being parsed
QUEUED	n/a	The batch request and associated certificate signing requests have been parsed and are queued ready for processing.
PROCESSING	n/a	The batch certificate signing requests are being processed.
PAUSED	n/a	The daily time window for processing batches is closed. The processing of the batch is suspended until the next processing time window.
COMPLETED	n/a	The processing of the batch is completed. The results of the batch processing are contained with the returned XML.
TAMPERED	n/a	The submitted batch contents has changed between upload and parsing. The batch will not be processed further.
FORMAT_ERROR	FM:<Value>	The query for the batch result has failed. This is due to the request format error. The client should correct the mistake and re-submit the request.
WORKFLOW_ERROR	WF:<Value>	The query for the batch result has failed. A workflow error has prevented construction of the batch result message. Re-submission is unlikely to remedy this issue. This issue should be reported, stating the error code, to the DCC helpdesk.

Batched CSR Result: Status values

Value	Error Code	Description
SUCCESS	n/a	This value indicates a certificate has been generated and is returned in the response.
ISSUANCE_ANOMALY	CA:<Value>	The request has been rejected. A certificate issued from the submitted CSR would result in unexpected issuance behaviour. Manual action by the DCC RA team would need to be taken to allow a future submission of this CSR to result in a certificate.
INELIGIBLE	IN:<Value>	This value indicates that the CSR has failed the eligibility check as set out in Section L3.16 of the Code. The Remote Party Role of the Requester is limited to requesting certificates for meters in certain provisioning states. The Error Code will detail the reason that the eligibility check failed.
CSR_ERROR	CR:<Value>	The request has failed. This is due to a corrupt CSR or incorrect CSR format. The client should correct the mistake and re-submit the CSR.
CA_ERROR	CA:<Value>	The request has failed. An internal error has prevented the CA from issuing the certificate. Re-submission of the CSR may fix this issue.
WORKFLOW_ERROR	WF:<Value>	The request has failed. A workflow error has prevented issuance of the certificate. Re-submission is unlikely to remedy this issue. This issue should be reported, stating the error code, to the DCC helpdesk.

Appendix E Schema for Batched Device CSR Web Service interface

liii.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="SubmitCSRBatch" nillable="false">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:sequence maxOccurs="unbounded">
          <xs:element name="DeviceCSR" nillable="false">
            <xs:complexType>
              <xs:simpleContent>
                <xs:extension base="xs:base64Binary">
                  <xs:attribute name="ID" use="required">
                    <xs:simpleType>
                      <xs:restriction base="xs:ID">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="100"/>
                      </xs:restriction>
                    </xs:simpleType>
                  </xs:attribute>
                </xs:extension>
              </xs:simpleContent>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:sequence>
      <xs:attribute name="ID" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>
  <xs:element name="SubmitCSRBatchStatus" nillable="false">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:element ref="Build"/>
        <xs:element name="BatchStatus" nillable="false">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="PENDING"/>
              <xs:enumeration value="FORMAT_ERROR"/>
              <xs:enumeration value="WORKFLOW_ERROR"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:choice>
          <xs:element ref="BatchId"/>
          <xs:element ref="Error"/>
        </xs:choice>
      </xs:sequence>
      <xs:attribute name="ID" use="optional">
```

```
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>
  <xs:element name="CSRBatchResult">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:element ref="Build"/>
        <xs:element name="BatchStatus" nillable="false">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="PENDING"/>
              <xs:enumeration value="REJECTED"/>
              <xs:enumeration value="PARSING"/>
              <xs:enumeration value="QUEUED"/>
              <xs:enumeration value="PROCESSING"/>
              <xs:enumeration value="PAUSED"/>
              <xs:enumeration value="COMPLETED"/>
              <xs:enumeration value="TAMPERED"/>
              <xs:enumeration value="FORMAT_ERROR"/>
              <xs:enumeration value="WORKFLOW_ERROR"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:choice minOccurs="0">
          <xs:element ref="Error"/>
          <xs:sequence>
            <xs:element ref="BatchId"/>
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
              <xs:element name="DeviceCertificate">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Status" nillable="false">
                      <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="SUCCESS"/>
                          <xs:enumeration value="ISSUANCE_ANOMALY"/>
                          <xs:enumeration value="INELIGIBLE"/>
                          <xs:enumeration value="CSR_ERROR"/>
                          <xs:enumeration value="CA_ERROR"/>
                          <xs:enumeration value="WORKFLOW_ERROR"/>
                        </xs:restriction>
                      </xs:simpleType>
                    </xs:element>
                    <xs:choice>
                      <xs:element name="Certificate" type="xs:base64Binary" nillable="false"/>
                      <xs:element ref="Error"/>
                    </xs:choice>
                  </xs:sequence>
                  <xs:attribute name="ID" use="required">
                    <xs:simpleType>
                      <xs:restriction base="xs:ID">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="100"/>
                      </xs:restriction>
                    </xs:simpleType>
                  </xs:attribute>
```

```
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:sequence>
            </xs:choice>
          </xs:sequence>
          <xs:attribute name="ID">
            <xs:simpleType>
              <xs:restriction base="xs:string">
                <xs:minLength value="1"/>
                <xs:maxLength value="256"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:complexType>
      </xs:element>
      <xs:element name="Version" nillable="false">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="1.0"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="Build" type="xs:string" nillable="false"/>
      <xs:element name="BatchId" type="xs:positiveInteger" nillable="false"/>
      <xs:element name="Error" nillable="false">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="ErrorCode" nillable="false">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:minLength value="1"/>
                  <xs:maxLength value="10"/>
                  <xs:pattern value="[A-Z]{2}:[A-Za-z0-9]+"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:element>
            <xs:element name="ErrorText" type="xs:string" nillable="false"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:schema>
```

Appendix F Certificate Signing Request Structure

Information to be contained within an Organisation CSR

Section	Attributes	Value
Version		Version 0
Subject	Common Name (id-at-commonName)	This field shall only be populated where, should it be placed in an Organisation Certificate produced using this CSR's details, it would comply with the requirements for the Subject X520 Common Name field in such Organisation Certificates, where those terms have their Appendix B Organisation Certificate Policy meaning.
	Organisational Unit (id-at-organizationalUnitName)	Remote Party Role Code of the Subject of the Certificate (2 character hexadecimal representation of the Remote Party Role Code). E.g. for supplier, value = '02')
	Subject Unique Identifier (id-at-uniqueIdentifier)	The 64 bit EUI-64 Compliant identifier of the subject of the Certificate
Subject Public Key Information	Public Key Algorithm	id-ecPublicvKey
	Prime256r1 (256 bit)	Public Key Value
Key Usage	Criticality	True
	Key Usage	digitalSignature or keyAgreement
Signature Algorithm		ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection and the SMKI Portal via the Internet will be accepted in PKCS#10 format Base64 encoded. The standard format for CSR forms submitted to the SMKI Portal via DCC Gateway Connection and the SMKI Portal via the Internet will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for CSR forms submitted to the SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet will also be accepted:

a) No PEM headers

b) Base64 all in one line

c) Base64 with line breaks at 64 or 76 characters

d) If line breaks are used the \n and \r\n are both acceptable

Information to be contained within a Device CSR

Section	Attributes				Value
Version					Version 0
Subject					Empty
Subject Public Key Information	Public Key Algorithm				id-ecPublicvKey
	Prime256r1 (256 bit)				Public Key Data
Key Usage	Criticality				True
	Key Usage				digitalSignature or keyAgreement
Subject Alternative Name	General Name	Other Name	id-on-hardwareModuleName	hwType	Object Identifier, OID
				hwSerialNum	Device ID (EUI-64)
Signature Algorithm					ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be accepted in PKCS#10 format Base64 encoded. The standard format for CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for Device CSRs submitted to the SMKI Portal via DCC Gateway Connection will also be accepted:

a) No PEM headers

b) Base64 all in one line

c) Base64 with line breaks at 64 or 76 characters

d) If line breaks are used the \n and \r\n are both acceptable

CSRs submitted via the Ad Hoc Device CSR Web Service interface or the Batched Device CSR Web Service interface shall not use PEM headers, as set out in Appendix A and Appendix C respectively.

Format of Batched Certificate Signing Requests via SMKI Portal interface

The format that shall be used for .zip files is defined in *info-zip.org/doc/appnote-19970311-iz.zip*.

Request File

g) The format of the batch request is a ZIP archive containing up to 50,000 individual files with a "csr" extension, which must be in the following format:

a) Each of these files must be uniquely named in the root level of the archive;

b) The individual files must contain a Base64 (as defined by RFC 4868 Section 4) encoded PKCS#10 CSR; and

c) The name of the each file with a 'csr' extension within the ZIP archive is preserved within the SMKI workflow, excluding the "csr" extension, so that the name of the corresponding Device Certificate file in the response ZIP archive will include the name supplied in the 'csr' file.

Response File

h) The "Response File" is a ZIP archive containing:

a) a text file record for each CSR contained within the Batched CSR, which shall contain the fields as set out immediately below:

i. identifier for the CSR contained within the Batched CSR;

ii. the file name for the CSR;

iii. the status of the processing of the CSR, which shall have a value of one of 'success', 'error', 'anomaly' or 'ineligible'; and

iv. where relevant, an error code associated with the processing of the CSR; and

b) a ZIP archive which contains all Certificates from the request which have been issued, in the following format:

c) Certificates will be in Base64 encoded X.509 format;

d) The filename is that of the request ZIP file with "-response" appended, and issued certificates are stored in the root level of the archive; and

e) The Certificate names are the same as their corresponding request files, but with the "crt" rather than "csr" extension.

Appendix G Authentication Credentials

liv. The SMKI Portal for Users, Ad-Hoc Device CSR Web Service Interface and Batched Device CSR Web Service Interface shall use server and client certificates with the following cryptographic properties:

Criteria	***Version***
Protocol	*TLS1.2**
Protocol Cyphers	*ECDHE-RSA-AES256-GCM-SHA384*
	ECDHE-RSA-AES256-SHA384
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-SHA256
Client Certificate Key	*RSA 2048 bit*
Client Certificate Hash Algorithm	*SHA256*
Server Certificate Key	*RSA 2048 bit*
Server Certificate Hash Algorithm	*SHA256*

lv. * TLS 1.2 should be implemented in accordance with Java and Apache standards. Java 7 and above supports TLS1.2. The TLS version is specified in the HTTP client protocol initialisation. To enable AES256, the Java runtime should be patched with "JCE Unlimited Strength Jurisdiction Policy Files" for the version of Java being used. This is obtained from the public Oracle Java download web pages.

Information to be contained within a CSR for IKI Certificates (client credentials) used to access the Ad Hoc Device CSR Web Service interface and/or the Batched Device CSR Web Service interface

lvi. Each CSR for an IKI Certificate used to access the Ad Hoc Device CSR Web Service interface and/or the Batched Device CSR Web Service interface shall comply with the format as set out immediately below. Each such CSR shall only apply to one of the interfaces listed immediately below:

a) Ad Hoc Web Service interface; or

b) Batched CSR Web Service interface.

Section	Attributes	Value
Version		Version 0
Subject	Organisation (id-at-organizationName)	Organisation Trading Name
	Organisational Unit (id-at-organizationalUnitName)	Remote Party Role Code
	Common Name (id-at-commonName)	Unique Name of the Authorised System, which the submitting Party must ensure is unique for: 1) multiple CSRs for the Ad Hoc Device CSR Web Service interface; or 2) multiple CSRs for the Batched Device CSR Web Service interface.
Subject Public Key Information	Public Key Algorithm	RSAPublicKey
	Key Size	2048
Key Usage	Criticality	True
	Key Usage	digitalSignature
Signature Algorithm		SHA256withRSAEncryption

Appendix H Definitions

Term	Meaning as defined in SEC
AES	Advanced Encryption Standard
Portal	Portal is a generic term in the SMKI SEC Documents. It refers to a web-based interface, within which there may be multiple views, depending on the permissions of the individual accessing it.
SMKI Portal	'Portal' is a generic term in the SMKI environment: the portals for the OCA and DCA exist as separate URLs within the primary SMKI Portal with security applied in line with the ARO's role.