This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	**SECP_69_1406_10**
Action:	**For Decision**

DP074 Problem Statement

1. Purpose

Draft Proposal DP074 'Clarity on Obtaining SMKI Device Certificates' was raised by the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA) and has undergone the Development Stage. The Change Sub-Committee believe this Draft Proposal is ready to be converted to a Modification Proposal. This paper sets out our proposed approach for progressing this modification for the Panel's approval. We are recommending that this modification be progressed directly to the Report Phase and that the Panel approve the Modification Report, the implementation approach, and that MP074 is a Self-Governance Modification.

This paper provides a high-level summary of the key points. A copy of the problem statement submitted by the Proposer can be found in Appendix A, and the draft Modification Report can be found in Appendix B.

2. Summary of the proposal

What is the issue?

DCC Users must request SMKI Device Certificates for Devices that they wish to connect to the Smart Metering System. The SMKI PMA and the Security Sub-Committee (SSC) established a secure process for DCC Users who have completed the User Entry Process Tests (UEPT) to obtain SMKI Device Certificates from the DCC via a DCC Gateway connection. An Agreed Interpretation of this process has been published on the SEC website.

The Proposer believes this is not clearly reflected in the SEC and could cause ambiguity for DCC Users when requesting SMKI Device Certificates.

What is the proposed solution?

The Proposer proposes to ensure the SEC reflects the Agreed Interpretation agreed by the SMKI PMA and the SSC and published on the SEC website.

3. Proposed progression

The Change Sub-Committee have agreed that this Draft Proposal is ready to be converted to a Modification Proposal. We and the Change Sub-Committee believe that this modification should be

progressed directly to the Report Phase as no significant issues were raised during the Development Stage, and the proposed solution would not benefit from further refinement.

Determination approach

We recommend that this is progressed as a Self-Governance Modification as there are no material impacts on SEC Parties or Energy Consumers.

Implementation approach

We recommend an implementation approach of:

- **7 November 2019** (November 2019 SEC Release) if a decision to approve is received by 24 October 2019.

4. Recommendations

The Panel are requested to:

- **AGREE** that DP074 is ready to be converted to a Modification Proposal;
- **AGREE** that MP074 should be progressed to the Report Phase;
- **APPROVE** the Modification Report;
- **APPROVE** the implementation approach; and
- **AGREE** that MP074 should be progressed as a Self-Governance Modification.

Ali Beard

SECAS Team

7 June 2019

Attachments:

- **Appendix A:** DP074 problem statement
- **Appendix B:** MP074 Modification Report
    - **Annex A:** MP074 legal text

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

DP074 'Clarity on Obtaining SMKI Device Certificates'

Problem statement – version 0.2

About this document

This document provides a summary of this Draft Proposal, including the issue or problem identified, the impacts this is having, and the context of this issue within the Smart Energy Code (SEC).

Proposer

This Draft Proposal has been raised by Gordon Hextall on behalf of the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA).

What is the issue or problem identified?

Obtaining SMKI Device Certificates

Data Communication Company (DCC) Users must request SMKI Device Certificates for Devices that they wish to connect to the Smart Metering System, to ensure the secure and efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain. The SMKI PMA and the SSC established a secure process for DCC Users who have completed the User Entry Process Tests (UEPT) to obtain SMKI Device Certificates from the DCC via a DCC Gateway connection. The following Agreed Interpretation of this process has been published on the SEC website:

"*Where the DCC receives an application on the Authorised Subscriber application form wishing to be an Authorised Subscriber for SMKI Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. In determining the evidence, the Registration Authority shall ensure that the applicant organisation has completed User Entry Process Tests and that Certificate Signing Requests (CSRs) will be submitted via a DCC Gateway Connection.*"

The Proposer believes this is not clearly reflected in the SEC and could cause ambiguity for DCC Users when requesting SMKI Device Certificates.

How does this issue relate to the SEC?

The Proposer expects this issue to impact SEC Appendix D with some corresponding minor changes to Appendices K, M and N:

- SEC Appendix D 'SMKI Registration Authority Policies and Procedures' provides detailed procedures for Authorised Subscribers to obtain SMKI Organisation and Device Certificates. At present, Section 5 implies that Parties can use the SMKI Portal Interface Over the Internet (SPOTI) to submit Device CSRs without having completed UEPT and without using a DCC Gateway connection.
- SEC Appendix K 'SMKI and Repository Test Scenarios Document' explains the SMKI and Repository Test Scenarios and currently describes tests to submit Device CSRs via SPOTI.
- SEC Appendix M 'SMKI Interface Design Specification' explains the SMKI Interface Design Specification and currently describes an ability to submit batched or ad hoc Device CSRs "(via a DCC Gateway connection or via the Internet)".
- SEC Appendix N 'SMKI Code of Connection' explains the SMKI Code of Connection and currently describes an ability to submit batched and ad hoc Device CSRs via SPOTI.

What is the impact this is having?

What are the impacts of doing nothing?

SEC Parties may not have enough clarity regarding the process in order to obtain SMKI Device Certificates via the SPOTI. Parties could also be unclear as to what level of security or which stage in the User Entry Process they must be at in order to access the Device Certificates.

What are the views of the industry?

Views of the DCC

The DCC were supportive of this Draft Proposal.

Views of SEC Parties

No comments were received from SEC Parties.

Views of Panel Sub-Committees

The SSC and the SMKI-PMA fully support changes to make this process less ambiguous for Users. The other Panel Sub-Committees were neutral to this Draft Proposal. No specific comments were received.

Views of the Change Sub-Committee

The Change Sub-Committee were supportive of the Draft Proposal. No specific comments were received.

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP074

‘Clarity on Obtaining SMKI Device Certificates’

Modification Report

Version 0.1

About this document

This document is the Modification Report for MP074 'Clarity on Obtaining SMKI Device Certificates'. It provides detailed information on the background, issue, solution, costs, impacts and implementation approach. It also summarises the discussions that have been held and the conclusions reached with respect to this Modification Proposal.

Contents

This document also has one annex:

- **Annex A** contains the redlined changes to the SEC required to deliver the proposed solution.

1. Summary

DCC Users must request Smart Metering Key Infrastructure (SMKI) Device Certificates for Devices that they wish to connect to the Smart Metering System. SEC Appendix D 'SMKI Registration Authority Policies and Procedures' provides detailed procedures for Authorised Subscribers to obtain SMKI Organisation and Device Certificates. The SMKI Policy Management Authority (PMA) and the Security Sub-Committee (SSC) established a secure process for DCC Users who have completed the User Entry Process Tests (UEPT) to obtain SMKI Device Certificates from the DCC via a DCC Gateway connection and an Agreed Interpretation of this process has been published on the SEC website.

The Proposer believes this is not clearly reflected in the SEC and could cause ambiguity for DCC Users when requesting SMKI Device Certificates.

MP074 proposes to make changes to the SEC to ensure the process as agreed by the SMKI-PMA and the SSC is accurately reflected in the SEC. This change will impact all Parties, ensuring a secure and clear procedure is laid out for all Parties requesting Organisation and Device Certificates.

The central implementation costs will be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort in implementing the changes to the SEC. If approved, this change is targeted for the November 2019 SEC Release.

2. Background

Obtaining Device Certificates

DCC Users must request SMKI Device Certificates for Devices that they wish to connect to the Smart Metering System. The SMKI PMA and the SSC established a secure process for DCC Users who have completed the User Entry Process Tests (UEPT) to obtain SMKI Device Certificates from the DCC via a DCC Gateway connection and an Agreed Interpretation of this process has been published on the SEC website.

The SMKI PMA and the SSC's Agreed Interpretation is as follows:

"*Where the DCC receives an application on the Authorised Subscriber application form wishing to be an Authorised Subscriber for SMKI Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. In determining the evidence, the Registration Authority shall ensure that the applicant organisation has completed User Entry Process Tests and that Certificate Signing Requests (CSRs) will be submitted via a DCC Gateway Connection.*"

What is the issue?

The Agreed Interpretation is not accurately reflected in the SEC. SEC Parties may not have enough clarity regarding the process in order to obtain SMKI Device Certificates via the SMKI Portal Interface Over the Internet (SPOTI). Parties could also be unclear as to what level of security or which stage in the User Entry Process they must be at in order to access the Device Certificates.

3. Solution

Proposed Solution

After consideration of industry comments and discussions with the DCC, the Proposer (the SMKI PMA) believes that the most effective solution is to change the legal text in the SEC to reflect the Agreed Interpretation thereby ensuring there is clarity and consistency in the process of obtaining Device Certificates.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties		DCC

There is no impact on Parties to implement this modification. All Parties will benefit from this as it will ensure clarity for all Parties. There may be some consequential impacts to Parties who currently use SPOTI.

DCC System

There is no impact on DCC Central Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix D 'SMKI Registration Authority Policies and Procedures'
- Appendix K 'SMKI and Repository Test Scenarios Document'
- Appendix M 'SMKI Interface Design Specification'
- Appendix N 'SMKI Code of Connection'

Other industry Codes

There are no impacts identified on other industry codes.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with implementing this modification.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

There will be no costs on Parties to implement this modification.

6. Implementation approach

Recommended implementation approach

SECAS are recommending an implementation date of:

- **7 November 2019** (November 2019 SEC Release) if a decision to approve is received on or before 24 October 2019.

This is the next available SEC Release that this change can be included in.

7. Discussions and development

Discussions by the Sub-Committees

The Sub-Committees were all supportive of this modification. No comments were received.

Comments from the DCC

Comments were received from the DCC indicating that any Registered User on the DCC Gateway can have access to device certificates (whether or not they are installing devices) and it should be made clear that Parties using SPOTI can only access Organisation Certificates not Device Certificates.

Comments from Parties

No comments were received from any Parties.

8. Conclusions

Benefits and drawbacks

The Proposer identified the following benefits and drawbacks in implementing this modification:

Benefits

- The SEC will accurately reflect the process for obtaining Device Certificates, in line with the Agreed Interpretation published by the SMKI-PMA and SSC.

Drawbacks

- No drawbacks have been identified.

Proposer's rationale against the General SEC Objectives

Objective (a)[1]

The Proposer believes that MP074 will better facilitate SEC Objective (a) by ensuring the SEC provides accurate information for Parties on the process of obtaining Device Certificates.

Objective (e)[2]

The Proposer believes that MP074 will better facilitate SEC Objective (e) by ensuring the SEC accurately reflects the security procedures in the process of obtaining Device Certificates.

Sub-Committee views

The Sub-Committees were supportive of this modification and had no specific comments.

[1] Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain

[2] Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy

Appendix 1: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CSR	Certificate Signing Request
DCC	Data Communications Company
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMKI	Smart Metering Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SMKI RAPP	Smart Metering Key Infrastructure Registration Authority Policies and Procedures
SPOTI	SMKI Portal Interface Over the Internet
SSC	Security Sub-Committee
UEPT	User Entry Process Testing

If you have any questions on this modification, please contact:

Ali Beard

020 3970 1105

Alison.beard@gemserv.com

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

sec.change@gemserv.com

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP074 'Clarity on Obtaining SMKI Device Certificates'

Annex A

Legal text – version 0.1

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

These changes have been drafted against SEC Version 6.12.

Appendix D 'SMKI Registration Authority Policies and Procedures (SMKI RAPP)'

Amend Section 1.1 as follows:

1.1 Purpose

Section L9.6 of the Code sets out the process for the DCC to develop the SMKI Registration Authority Policies and Procedures (SMKI RAPP) as a SMKI SEC Document as defined in Section L 9.4 (a) (v).

The SMKI RAPP sets out the principle obligations and activities undertaken by the DCC in its capacity as the SMKI Registration Authority in accordance with Section L of the Code, and Appendices A, B ~~[and the IKI Certificate Policy]~~and Appendix Q to the Code. The SMKI RAPP also sets out the activities undertaken by the SMKI Registration Authority in support of the procedures set out in the DCCKI RAPP, as set out in Section 2 of this document.

Amend Section 4.1.2 as follows:

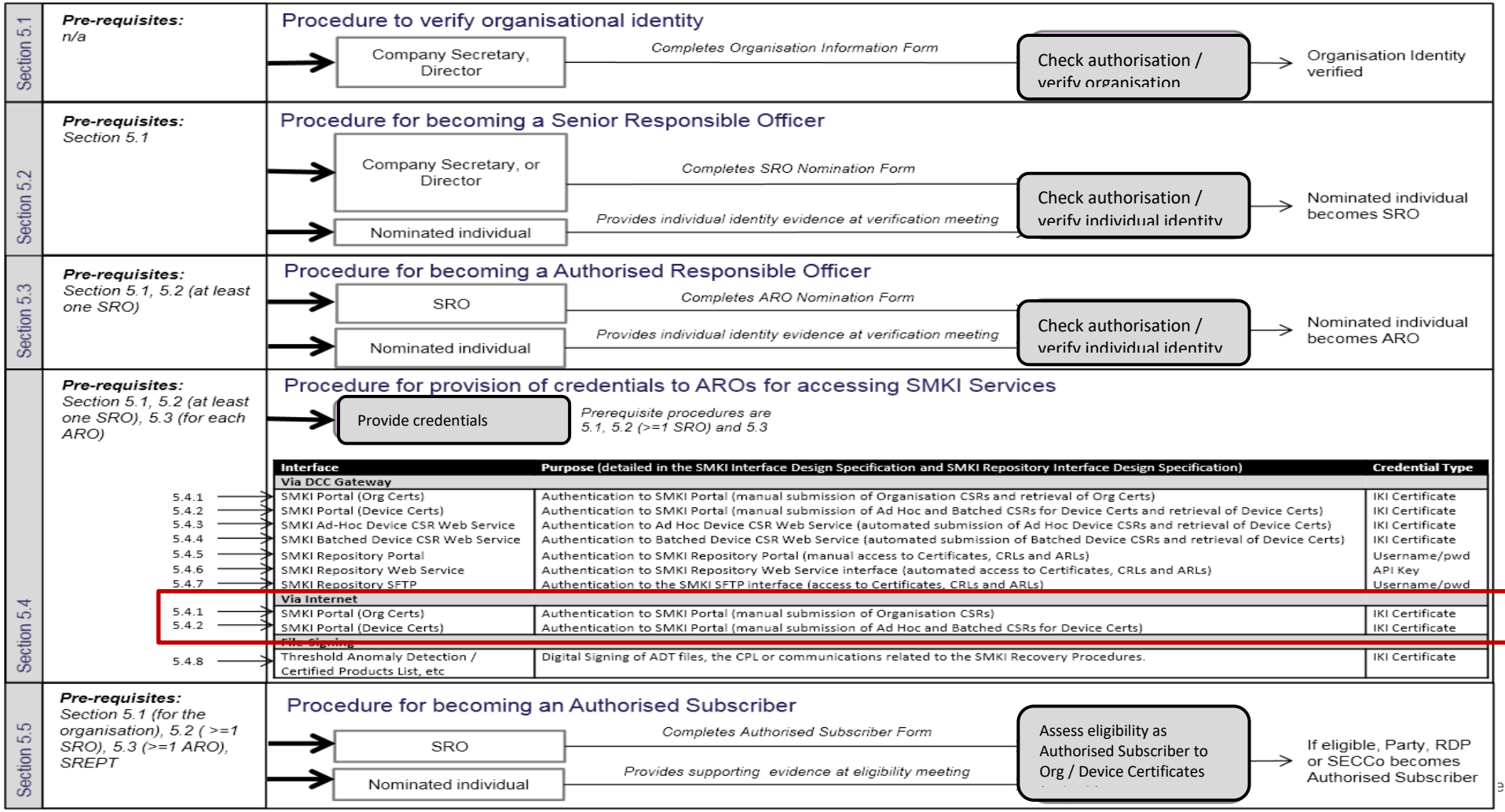
4.1.2 High level overview of SMKI Registration Authority procedures

Delete line 5.4.2 in the red box:

Figure 1 as set out immediately below provides a high level view of the procedures required in order for a Party, RDP, SECCo or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become a SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or SMKI Repository;
- become an Authorised Subscriber for:
    - Organisation Certificates or Device Certificates, or both;
    - a File Signing Certificate (issued under the IKI Certificate Policy) for the purposes of Digitally Signing of files in accordance with the Code;
- gain access to Organisation Certificates and/or Device Certificates and other material via the SMKI Repository; and
- gain access to the File Signing Certificate to be used for the purposes of Digitally Signing of files.

Delete line 5.4.2 in the red box:



Amend Section 5.4 as follows:

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services and file signing

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or SMKI Repository Services or for file signing to Authorised Responsible Officers in respect of a Party, RDP SECCo or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, SECCo or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP, SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a) If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of Organisation CSRs and retrieval of corresponding Organisation Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet.	SMKI Registration Authority	5.4.2

Step	When	Obligation	Responsibility	Next Step
		b) If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of Organisation CSRs and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection. Where the Party, RDP, SECCo or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP, SECCo or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.2	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection ~~or SMKI Portal via the Internet~~ If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section **Error! Reference source not found.** of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with:	SMKI Registration Authority	5.4.3

Step	When	Obligation	Responsibility	Next Step
		~~a)~~ If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of Device CSRs and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. ~~b) If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of Device CSRs and retrieval of corresponding Device Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection.~~ Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		

5.4.3	During ARO verification meeting and after becoming an ARO	IKI credentials for Ad Hoc Device CSR Web Service If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Ad Hoc Device CSR Web Service, the SMKI Registration Authority shall, if the applicant organisation has access to a DCC Gateway Connection and is a Supplier Party or the DCC, and where the Supplier Party or DCC (in its role as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via USB token or optical media, with: a) Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided, via USB token or optical media, by the applicant organisation in accordance with the SMKI Interface Design Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the Ad Hoc Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Ad Hoc Device CSR Web Service interface If the Supplier Party or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the Supplier Party or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.4

Step	When	Obligation	Responsibility	Next Step
5.4.4	During ARO verification meeting and after becoming an ARO	IKI credentials for Batched Device CSR Web Service If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Batched Device CSR Web Service, the SMKI Registration Authority shall determine, if the applicant is not a Supplier Party or the DCC, in accordance with the steps set out in Section **Error! Reference source not found.** of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the appointed ARO, via USB token or optical media, with: a) Batched Device CSR Web Service access credentials for Device Certificates, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the Batched Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Batched Device CSR Web Service interface. If the applicant organisation has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic	SMKI Registration Authority	5.4.5

Step	When	Obligation	Responsibility	Next Step
		means, the appointed ARO with Batched Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		
5.4.5	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository Portal If the applicant organisation has access to a DCC Gateway Connection, and it wishes to access the SMKI Repository via the SMKI Repository Portal and has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password, to be accessed via the SMKI Repository Portal, that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification. If the applicant organisation has access to a DCC Gateway Connection, it wishes to access the SMKI Repository via the SMKI Repository Portal but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting: a) DCC shall, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password via secured electronic means that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification.	SMKI Registration Authority	5.4.6

Step	When	Obligation	Responsibility	Next Step
5.4.6	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository Web Service If the applicant organisation has access to a DCC Gateway Connection, and wishes to access the SMKI Repository Web Service interface and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification, along with a certificate which enables verification of the SMKI Repository Web Service server identity. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository Web Service interface but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on electronic media as set out in the SMKI Repository User Guide, the ARO with: a) the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the SMKI Repository Web Service interface server identity, and that will be used as part of mutual authentication to the SMKI Repository Web Service interface.	SMKI Registration Authority	5.4.7

Step	When	Obligation	Responsibility	Next Step
5.4.7	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository Portal SFTP If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via the SMKI Repository Portal profile page, with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface.	SMKI Registration Authority	5.4.8
5.4.8	During ARO verification meeting and after becoming an ARO	IKI credentials for file signing If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code, the SMKI Registration Authority shall either a) provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate; in which case, the ARO shall use the software on the Cryptographic Credential Token to generate a Private Key for a File Signing Certificate to submit a CSR for a File Signing Certificate; and if the CSR is valid, the ICA shall Issue a File Signing Certificate under the IKI Certificate Policy, to be used for the purposes as set out in the Code; or b) provide the appointed ARO, via USB token or optical media, with an IKI File Signing Certificate, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.9

Step	When	Obligation	Responsibility	Next Step
5.4.9	During ARO verification meeting and after issuance of credentials	Acceptance of credentials issued in steps 5.4.1 to 5.4.8 The SMKI Registration Authority shall complete the relevant sections of the Nominee Details Form in Annex A (A5) accordingly. The ARO shall confirm receipt of and acceptance of the credentials issued by completing the relevant sections of the Nominee Details Form in Annex A (A5). Should the ARO not wish to accept these credentials, the ARO shall notify the SMKI Registration Authority immediately and not sign for the Certificate and / or Cryptographic Credential.	SMKI Registration Authority ARO	End of procedure

Appendix K 'SMKI and Repository Test Scenarios Document'

Amend Section 8.2 as follows:

8.2 SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection

The following sub sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that do not have access to a DCC Gateway Connection.

8.2.1 Security Credentials Access Tests to SMKI

ID	SMKI 04
Title:	Access the Test SMKI Service, through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the Test SMKI Service, through the SMKI Portal interface using the security credentials supplied by the DCC.
Objective	• To prove that the SafeNet Client Installed on the SMKI ARO's computer validates their security credentials • To prove that a Party's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the internet

8.2.2 Submission of CSR and Receipt of Certificates

ID	SMKI 26
Title:	Submit Organisation Certificate Signing Requests and receive Organisation Certificates through the SMKI Portal interface over the internet

Description	For a Party without a DCC Gateway Connection, a SMKI ARO submits an Organisation Certificate Signing Request (CSR) and receives an Organisation Certificates for that CSR through the SMKI Portal interface over the internet
Objective	• To prove a Party can generate and submit an Organisation CSR in the format specified in the SMKI Interface Design Specification • To prove that a Party can download Organisation Certificates issued in respect of the submitted CSRs, and to confirm the information contained in the issued Organisation Certificate is consistent with the information contained within the corresponding CSR • To prove that an Organisation Certificate can be rejected by the Party (according to the mechanism set out in the RAPP and / or specified in the Portal specification)

~~ID~~	~~SMKI 27~~
~~Title:~~	~~Submit a Device Certificate Signing Request and receive a Device Certificate through the SMKI Portal interface over the internet~~
~~Description~~	~~For a Party without a DCC Gateway Connection, SMKI ARO submits a Device Certificate Signing Request (CSR) and receives a Device Certificate for that Device CSR through the SMKI Portal interface over the internet~~
~~Objective~~	~~• To prove that the Party's ARO can use the SMKI Portal Interface to submit an Ad Hoc Device Certificate Signing Request~~ ~~• To prove that the Party can use the SMKI Portal Interface to download individual Device Certificates and confirm the information contained in the issued Device Certificate is consistent with the information contained within the corresponding submitted Device CSR~~ ~~• To prove that the issued Device Certificate can be rejected by the Party (according to the mechanism set out in the RAPP and / or specified in the Portal specification)~~

~~ID~~	~~SMKI 28~~
~~Title:~~	~~Submit Batched Device Certificate Signing Requests and receive Device Certificates through the SMKI Portal interface over the internet~~
~~Description~~	~~For a Party without a DCC Gateway Connection, an SMKI ARO submits a Batched Device Certificate Signing Request (CSR) and receives Device Certificates for each valid Device CSR through the SMKI Portal interface over the internet~~
~~Objective~~	~~• To prove that the Party's ARO can use the SMKI Portal Interface to submit Batched Device CSR~~ ~~• To prove that Device CSRs are batched correctly by the Party~~ ~~• To prove that the Party's ARO can use the SMKI Portal interface to download Device Certificates issued from the Batched Device CSRs~~

Submit Requests for Repository Content and Obtain DCA, OCA and DCC Certificates

ID	SMKI 08
Title:	Submit Requests for and Receive Repository Content using the SMKI Portal interface over the Internet
Description	For a Party without a DCC Gateway Connection, an SMKI ARO accesses the SMKI Portal interface and makes a request for and receives content from the test SMKI Repository
Objective	• To prove that a Party's SMKI ARO can use the SMKI Portal interface to request and receive the latest Organisation CRL and latest Organisation ARL

ID	SMKI 38
Title:	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the SMKI Portal interface over the Internet, locates and downloads Organisation Certificates that are required to be installed on Devices ahead of installation
Objective	• To prove that the Party's ARO can locate and download the zip file of Device trust anchor Organisation Certificates through the SMKI Portal over the internet

Amend Section 10 as follows:

10 Appendix E: Test Completion Certificate

TEST COMPLETION CERTIFICATE

To: [Party / RDP] [SEC Party / RDP ID]

From: [DCC]

[Date]

Dear Sirs,

TEST COMPLETION CERTIFICATE

The relevant tests have been successfully completed to provide the following credentials:

Test Scenarios for Parties or RDPs with a DCC Gateway Connection
IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for Ad Hoc Device CSR Web Service
IKI credentials for Batched Device CSR Web Service
Credentials for SMKI Repository Portal
Credentials for SMKI Repository Web Service
Credentials for SMKI Repository Portal SFTP

Test Scenarios for Parties without a DCC Gateway Connection
IKI credentials for submission of Organisation CSRs using SMKI Portal via the Internet
~~**IKI credentials for submission**~~

~~of Device CSRs using SMKI Portal via the Internet~~

We confirm that the relevant tests have been executed in accordance with the relevant Test Documents. We confirm that the relevant Exit Criteria have been achieved.

Yours faithfully

[Name]

[Position]

Acting on behalf of the DCC

Appendix M 'SMKI Interface Design Specification'

Amend Section 2.6 as follows:

2.6 SMKI Portal interface via the Internet

General obligations

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 Device CSRs in batch or ad-hoc form,~~ and to retrieve resulting Certificates, on behalf of their Authorised Subscriber.

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

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.

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

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.

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

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~~ 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 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~~; or~~

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

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.

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

Submission of Organisation CSRs by Authorised Subscriber

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.

Receipt and validation of Organisation CSRs by the DCC

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.

Actions following acceptance of Organisation CSRs by the DCC

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.

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.

Actions following approval of Organisation CSRs by the DCC

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.

Actions following download of an Organisation Certificate by an Authorised Subscriber

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.

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.

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 the Internet in Ad Hoc CSR form or as part of a Batched CSR.~~

2.6.1.6 Submission of Device CSRs by Authorised Subscriber

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.

a) **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

b) **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.

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

Following receipt by the DCC of an Ad Hoc Device CSR or Batched CSR to the SMKI Portal via the Internet, 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 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 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 that are in accordance with "Response Status" table in Appendix C of this document, 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.

Actions following acceptance of Device CSRs by the DCC

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; and

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 the 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 2.3.4.4e) 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 2.3.4.4e) of this document.

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.

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.

Actions following approval of Device CSRs by the DCC

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

a) process the CSR;

b) Issue a corresponding Device Certificate;

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

d) for Ad Hoc Device CSRs:

i. make the corresponding Device Certificate available for download via the 'certificate pickup' page on the SMKI Portal interface via the Internet (as set out in the SMKI User Guide) and the SMKI Repository;

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

~~e) for Batched CSRs:~~

~~i. make available 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.~~

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

~~**Actions following download or viewing of a Device Certificate by an Authorised Subscriber**~~

~~Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.5, 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.~~

~~Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device 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.~~

Amend Appendix F as follows:

Certificate Signing Request Structure

Information to be contained within an Organisation CSR

Section	Attributes	Value
Version		Version 0

Section	Attributes	Value
Subject	Common Name (id-at-commonName)	Organisation Trading Name (Optional field, only present for Supplier Digital Signing Certificate CSR – maximum of 16 characters)
	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 ~~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 Device CSRs submitted to the SMKI Portal via DCC Gateway Connection ~~and the 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

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.

Appendix N 'SMKI Code of Connection'

Amend Section 2.2 as follows:

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;

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

~~c) submit Batched CSRs and retrieve resulting Device Certificates; and~~

~~d)~~b) access the documents set out in section 2.6.1 of the SMKI Interface Design Specification.

Amend Section 3 as follows:

3 Managing Demand

3.1 Capacity Management

3.1.1 SMKI Portal via 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 the applicable SMKI Portal interfaces 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 DCC Service Desk. The Batch or Batches 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 ~~or via the Internet in the same manner~~.

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 DCC Service Desk.