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 1.1

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 typographical error in Section 4.1.1 as follows:

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, SECCo and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or SMKI Repository Services shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

To facilitate this, the SMKI Registration Authority shall:

a) make the forms as set out in SMKI RAPP Annex A, available via the internet facing DCC Website;

b) provide reasonable support and advice to each Party, RDP, SECCo and DCC Service Providers in relation to the procedures as set out in SMKI RAPP sections 5.1 to 5.5;

c) place no restriction on the number of individuals that can be nominated as SROs or AROs in respect of any Party, RDP, SECCo or the DCC (in its role as DCC Service Provider);

d) permit an individual to become an ARO to represent multiple parties, by successfully completing the procedures in SMKI RAPP section 4 as are necessary;

e) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations (but not the personal details of individuals) as set out Sections 5.1 to 5.5, and in accordance with the Code and the DCC's data retention policy and data protection policy;

f) not permit any nominated individual to access the SMKI Services or relevant SMKI Repository Services on behalf of a Party, RDP, SECCo or the DCC (in its role as DCC Service Provider) until they have become an ARO;

g) ensure that credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years following and that such credentials and shall cease to be valid after ten years following issuance;

h) for authentication and file signing credentials issued under the IKI Certificate Policy and where the Key Pair and Certificate Signing Request are both generated by the ARO on a Cryptographic Credential Token during the ARO verification meeting, that the ARO has an opportunity to validate and agree information (e.g. Role and other organisation and individual identity) against which the Certificate is Issued is accurate and that it reflects the identity of the ARO or system that is the subject of the Certificate;

i) for authentication and file signing credentials issued under the IKI Certificate Policy and which are delivered to the SMKI Registration Authority in the form of a Certificate Signing Request generated by the ARO's organisation and provided by the ARO during the ARO verification meeting–, that the ARO has an opportunity to validate the information in the resulting Certificate reflects that provided in the Certificate Signing Request and that it is accurate and reflects the identity of the ARO or system that is the subject of the Certificate;

j) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and

k) produce, each month, and make available to each Party, RDP, and SECCo, a report for that organisation which details the list of SROs, AROs, the credentials that have been issued to each ARO and those AROs for which credentials will expire in the following month.

Amend Section 4.1.2 as follows:

4.1.2 High level overview of SMKI Registration Authority procedures

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.

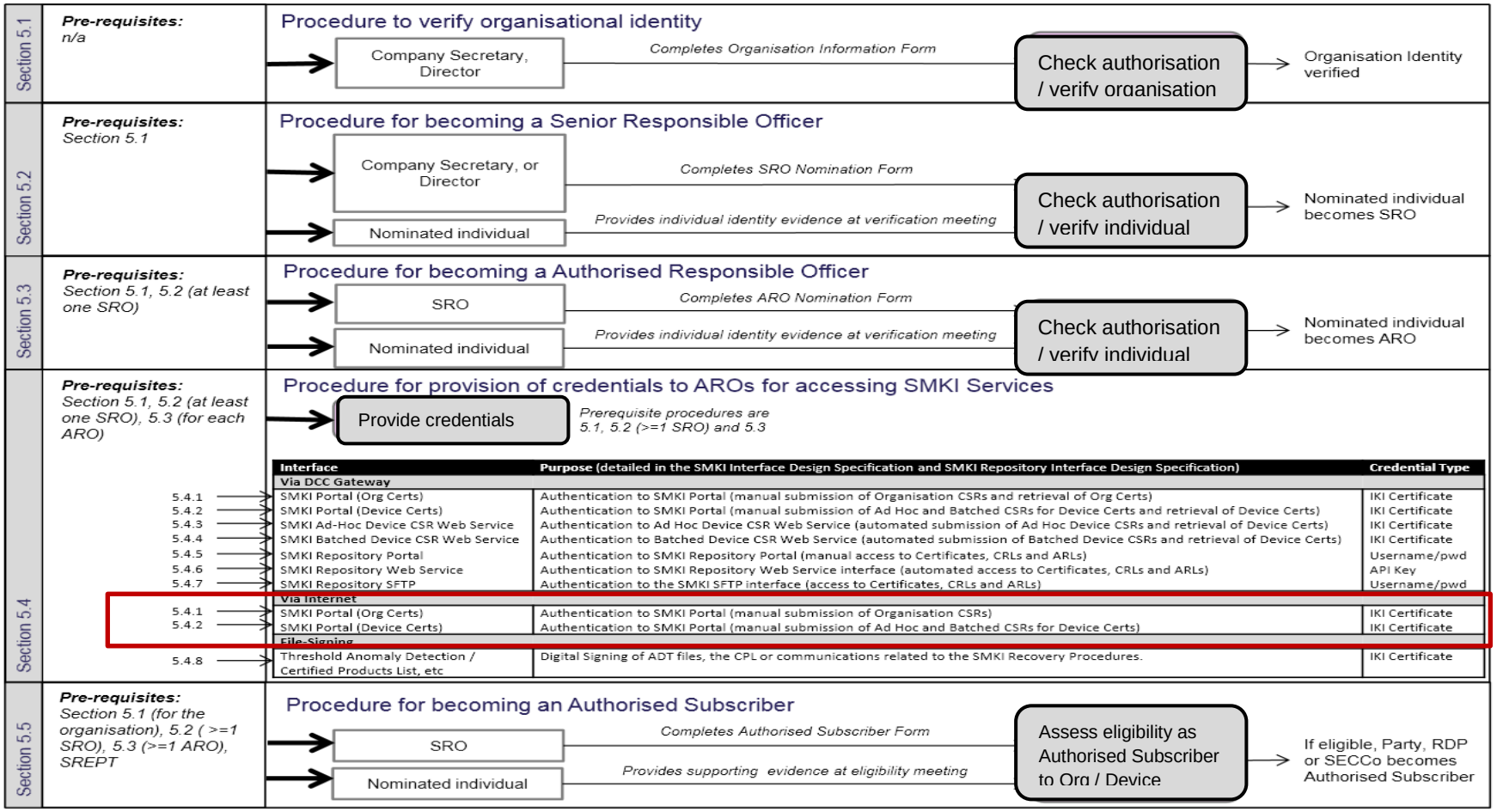

Figure 1: Overview of SMKI access registration processes

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	SMKI Registration Authority	5.4.2

Step	When	Obligation	Responsibility	Next Step
		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 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 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. Where there is such reasonable evidence, and where the	SMKI Registration Authority	5.4.3

Step	When	Obligation	Responsibility	Next Step
		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: 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. ~~a) 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.~~		

Step	When	Obligation	Responsibility	Next Step
		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 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. 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.	SMKI Registration Authority	5.4.5

Step	When	Obligation	Responsibility	Next Step
		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 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

Step	When	Obligation	Responsibility	Next Step
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
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

Amend Section 5.5 as follows:

Procedure for becoming an Authorised Subscriber

An organisation is an Authorised Subscriber for IKI File Signing Certificates where it has successfully appointed and maintains in place at least one SRO and at least one ARO.

The procedure detailed immediately below shall be conducted by the DCC, in order to determine whether a Party or RDP has become an Authorised Subscriber for Organisation Certificates, an Authorised Subscriber for Device Certificates, or both.

Step	When	Obligation	Responsibility	Next Step
5.5.1	As required	Complete the Authorised Subscriber Application Form as set out in SMKI RAPP Annex A (A2), ensuring that the information entered on the form is complete and accurate, and the Authorised Subscriber Application Form is authorised by an SRO on behalf of the applicant organisation	Nominating officer or SRO on behalf of the applicant organisation, which shall be a Party or RDP	5.5.2
5.5.2	As required, following 5.5.1	Submit the completed Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website	Applicant organisation, which shall be a Party or RDP	5.5.3
5.5.3	As soon as reasonably practicable following 5.5.2	Acknowledge receipt by email to the SRO or nominating officer as identified on the Authorised Subscriber Application Form	SMKI Registration Authority	5.5.4
5.5.4	As soon as reasonably practicable following 5.5.3	Analyse the information entered on the Authorised Subscriber Application Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 5.5.6; if not complete, 5.5.5
5.5.5	Once omissions / discrepancies are addressed	Submit a revised Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party or RDP	5.5.3

Step	When	Obligation	Responsibility	Next Step
5.5.6	As soon as reasonably practicable, following 5.5.4	Contact the SRO as identified on the Authorised Subscriber Application Form via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority. The SMKI Registration Authority shall verbally confirm details for the SRO as held by the DCC to verify that the correct individual has been contacted. The SMKI Registration Authority shall confirm the applications indicated on the Authorised Subscriber Application Form are authorised	SMKI Registration Authority	If confirmed as authorised, 5.5.8; if not authorised, 5.5.7
5.5.7	As soon as reasonably practicable following rejection	Notify the SRO as identified on the Authorised Subscriber Application Form that the procedure in respect of the application has not been successful, in writing	SMKI Registration Authority	5.5.5 once issues addressed
5.5.8	As requested	Where the application organisation is not a DCC Service Provider, conduct the SMKI and Repository Entry Process Tests if SMKI and Repository Entry Process Tests have not been completed previously, in accordance with Sections H14.22 to H14.31 of the Code	Applicant organisation, in respect of the corresponding Authorised Subscriber Application Form	If successful or the applicant organisation is a DCC Service Provider (acting on behalf of the DCC), 5.5.10; if not successful, 5.5.9
5.5.9	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing, to SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the SMKI and Repository Entry Process Tests were not completed successfully	DCC	5.5.8 once issues addressed
5.5.10	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing to the relevant Party that the SMKI and Repository Entry Process Tests have been completed successfully	DCC	5.5.11

Step	When	Obligation	Responsibility	Next Step
5.5.11	As soon as reasonably practicable, following 5.5.10	If the applicant organisation has indicated on its Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Organisation Certificate Policy, the SMKI Registration Authority shall confirm in writing to the SRO as identified on the Authorised Subscriber Application Form that it the applicant organisation has become an Authorised Subscriber for Organisation Certificates Where appropriate, the DCC shall issue credentials enabling the applicant to act as an Authorised Subscriber for Organisation Certificates, in accordance with the procedural steps as set out in section 0 of this document.	SMKI Registration Authority	If the applicant organisation has indicated that it wishes to become an Authorised Subscriber for Organisation Certificates, 5.5.12; otherwise, 5.5.13
5.5.12	As soon as possible, following 5.5.11	~~Other than in the case of a Party who is a Supplier Party or a DCC Service Provider, i~~If the applicant organisation has indicated on the Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy, the SMKI Registration Authority shall assess whether there is ~~reasonable~~ evidence to ~~suggest that it is necessary for the applicant organisation to become such an Authorised Subscriber in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises.~~confirm that the Party has completed the User Entry Process (defined in Section H1.10) and will use a DCC Gateway Connection to obtain Device Certificates.	SMKI Registration Authority	If determined to be an Authorised Subscriber for Device Certificates, 5.5.~~16~~15; otherwise 5.5.~~14~~13
5.5.13	As soon as possible, following 5.5.12	Confirm in writing, to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the DCC has determined that applicant organisation is not eligible to become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	~~If the applicant organisation wishes to refer the matter to the SMKI PMA or Panel, 5.5.14, otherwise End of procedure~~5.5.14

Step	When	Obligation	Responsibility	Next Step
5.5.14	As soon as possible, following 5.5.13	~~Determine~~ Where the DCC has determined ~~whether~~ that there is ~~reasonable~~ no evidence ~~to suggest that it is necessary for~~as defined in 5.5.12 to support the applicant organisation to become such an Authorised Subscriber, the DCC shall notify the SMKI PMA of the refusal. ~~in order for them to carry out business process that will, or are likely to, lead to the installation of Devices in premises. The SMKI PMA or Panel shall confirm the outcome to the DCC, in writing.~~	SMKI PMA or Panel	~~If determined to be an Authorised Subscriber for Device Certificates, 5.5.15; otherwise~~ End of procedure
5.5.15	As soon as reasonably practicable, following 5.5.14, or, where a Supplier Party or the DCC (in its role as DCC Service Provider) has indicated that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy	The SMKI Registration Authority shall confirm in writing, to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the applicant organisation has become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	5.5.16
5.5.16	As soon as reasonably practicable, following 5.5.15	The SMKI Registration Authority shall arrange and conduct a meeting, as soon as reasonably practicable, at which the credentials as set out in steps 5.4.2, 5.4.3 and 5.4.5 (as set out in Section 5.4 of this document) shall be provided, as appropriate.	SMKI Registration Authority	5.5.17
5.5.17	As soon as reasonably practicable, following 5.5.15 or 5.5.16	Update the DCC's list of Authorised Subscribers for Organisation Certificates and/or Device Certificates, for audit purposes.	SMKI Registration Authority	End of procedure

Amend Section 7.1 as follows:

7 Submission of CSRs and Issuance of Certificates

7.1 Submission of Certificate Signing Requests

The SMKI Interface Design Specification and the Code sets out the provisions in respect of:

a) the mechanism established for this purpose is in accordance with the procedure in PKCS#10;

b) naming restrictions in respect of the Subject of each Certificate in accordance with the relevant Certificate Profile;

c) the circumstances in which an Authorised Subscriber may submit a Certificate Signing Request (CSR) in respect of a Device Certificate and the means by which it may do so;

d) the circumstances in which an Authorised Subscriber may submit a CSR in respect of an Organisation Certificate and the means by which it may do so;

e) the circumstances in which an Authorised Subscriber for an IKI Certificate may submit a CSR in respect of an IKI Certificate and the means by which it may do so; and

f) requirements in respect of validation of the format of a CSR, checking that the submitting organisation is an Eligible Subscriber for the Certificate and rejection if such requirements are not met.

The SMKI Registration Authority shall validate the Subject of each Certificate to ensure that each CSR corresponds with an EUI64 Identifier range that is applicable to the relevant User Role, as provided in the Organisation Information Form.

Subject to the provisions of the Code and this SMKI RAPP, the DCC shall accept requests for copies of Organisation Certificates and/or Device Certificates from non DCC Users by phone via the DCC Service Desk or, in the case of Organisation Certificates, via the SMKI Portal via the Internet. The DCC shall, following such a request, provide the relevant information as soon as is reasonably practicable, via a secured electronic means.

Appendix K 'SMKI and Repository Test Scenarios Document'

Amend Section 5.2.2 as follows:

5.2.2 Test Scenarios for Parties without a DCC Gateway Connection

		Applicant Organisations		
SMKI SRTSD Scenario Reference	Headline Scenario Title	Supplier	Non-Supplier Party	SMKI RAPP Ref
SMKI 04	Access the test SMKI Services for (i) Organisation Certificates ~~and (ii) Device Certificates,~~ through the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1, 5.4.2
SMKI 08	Submit Requests for Repository Content using the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1, 5.4.2
SMKI 26	Submit Organisation Certificate Signing Request (CSR) and receive Organisation Certificates through the SMKI Portal interface over the internet	✓	✓	5.4.1
~~SMKI 27~~	~~Submit a Device Certificate Signing Request (CSR) through the SMKI Portal interface over the internet~~	~~✓~~	~~✓*~~	~~5.4.2~~
~~SMKI 28~~	~~Submit a Batched Certificate Signing Request (Batched CSR) through the SMKI Portal interface over the internet~~	~~✓~~	~~✓*~~	~~5.4.2~~
SMKI 38	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1, 5.4.2

Table 1 SREPT Matrix – No DCC Gateway Connection

Key

✓	Applicant organisation required to undertake this test if they wish to receive credentials for this service / access to this interface
✓*	Applicant organisation required to undertake this test if they wish to access this interface and can provide 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.

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~~

8.2.3 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 1.2 as follows:

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 ~~Connection or via the Internet~~):

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 ~~Connection or via the Internet~~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.

Amend Section 2.6 as follows:

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 Device CSRs in batch or ad-hoc form,~~ 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~~ 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~~

~~xliii.~~

~~i. 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.

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.

~~**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.~~

~~) **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~~

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

~~. generate the relevant Device CSRs; and~~

~~. 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:**

- validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;
- apply the Eligible Subscriber checks as set out in Section L3.16 of the Code; and
- either accept, or reject the CSR; and
  - where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or
  - 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

a) **for a Batched CSR submission:**

- validate that the structure of the submitted .zip file is in accordance with the format set out in Appendix F to this document;
- validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;
  - 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
  - should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;
- 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:
  - where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; or
  - 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;

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

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

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

. 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

a) **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

i. 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;

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

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

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

. 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

. 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:

) process the CSR;

) Issue a corresponding Device Certificate;

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

) for Ad Hoc Device CSRs:

. 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

) for Batched CSRs:

. make available two files for download via the 'certificate pickup' page on the SMKI Portal interface, comprising:

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

. 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.~~

Appendix M – Appendix F Certificate Signing Request Sturcture

Amend Appendix F as follows:

Certificate Signing Request Structure

Information to be contained within an Organisation CSR

Section	Attributes	Value
Version		Version 0
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

Section	Attributes	Value
	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
	General Name	Other Name		hwType	Object Identifier, OID

Section	Attributes				Value
Subject Alternative Name			id-on-hardwareModuleName	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.

Appendix Q 'IKI Certificate Policy'

Amend Section 6.1.8 as follows:

6.1.8 Extended Key Usage Purposes

(A) The ICA shall ensure that each Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, ~~IKI Authorised Internet Device Subscriber CA,~~ IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedkeyUsage' field in accordance with RFC5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, ~~IKI Authorised Internet Device Subscriber CA,~~ IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedKeyUsage' set to 'clientAuth'.

Appendix Q – Annex A: Definitions and Interpretation

Amend Annex A as follows:

~~**IKI Authorised Internet Device Subscriber Certification Authority (or CA)**~~	~~means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs in respect of Device Certificates over the Internet.~~
Issuing ICA Certificate	means a certificate in the form set out in the Issuing ICA Certificate Profile in accordance with Annex B, and Issued by the Root ICA to the Issuing ICAs in accordance with this Policy. The Issuing ICA may act in one of the following capacities: a) IKI Administrator CA; b) IKI Registration Authority CA; c) IKI Authorised Organisation Subscriber CA; d) IKI Authorised Device Subscriber CA; e) IKI Authorised Internet Organisation Subscriber CA; ~~f) IKI Authorised Internet Device Subscriber CA;~~ ~~g)~~f) IKI Authorised Web Service Subscriber CA; and ~~h)~~g) IKI File Signing CA

Appendix Q – Annex B: ICA Certificate and IKI Certificate Profiles

Amend Annex B as follows:

- IKI Certificates ~~issued by the IKI Authorised Internet Device Subscriber CA,~~ contain~~s~~ an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates underand a X520commonName attribute whose value will be set to the ARO's or system name.

- For Certificates Issued ~~by~~ by the IKI Administrator CA, ~~IKI Authorised Device Subscriber CA,~~ IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Device Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Wed Service Subscriber CA and IKI Registration Authority CA contain a extKeyUsage extension marked critical, with a value of: