SEC
Smart Energy Code

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.

Smart Energy Code

MP168
‘CPL Security Improvements’

Modification Report

Version 1.0

21 June 2023

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

1. Summary 3
2. Issue 3
3. Solution 5
4. Impacts 5
5. Costs 7
6. Implementation approach 8
7. Assessment of the proposal 8
8. Case for change 10

Appendix 1: Progression timetable 11

Appendix 2: Glossary 12

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the full Data Communications Company (DCC) Impact Assessment response (**RED**).
- **Annex D** contains the full responses received to the Refinement Consultation.

Contact

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

Kev Duddy

020 3574 8863

kev.duddy@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

SEC Appendix Z 'CPL Requirements Document' requires the Panel to check that a communication requesting a firmware Image to be associated with a Device Model on the Central Products List (CPL) originates from the person who created the Image and is endorsed by a Supplier. At present, the nature of the signatures used by Manufacturers does not enable cryptographic authentication that the communication originates from a specific Manufacturer beyond reasonable doubt. Neither a Supplier nor the SEC Panel can therefore suitably verify the authenticity of the communication and therefore fully meet the SEC obligation. As a result, the SSC, with support from the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA), wishes to address the current SEC compliance issue and improve the security controls.

The SSC considers that the DCC, as an extension to the Infrastructure Key Infrastructure (IKI) service, could act as the Certificate Authority. Manufacturers and Suppliers would therefore need to obtain and use the IKI Certificates to sign and countersign the CPL submission.

The Certificate Revocation List (CRL) would need to be publicly available to enable Manufacturers, Suppliers, and the Smart Energy Code Administrator and Secretariat (SECAS) on behalf of the Panel, to check the validity of Certificates being used.

The solution will be available, and applicable, to Manufacturers who are not SEC Parties.

Suppliers and Manufacturers will be impacted by this modification as they will be required to obtain and use the IKI Certificates for all CPL submissions. The DCC cost to deliver the solution is £9,081. This modification is targeted for an ad-hoc SEC Release and be progressed as a Self-Governance Modification.

2. Issue

What are the current arrangements?

What is the Central Products List?

The DCC uses the CPL to manage the Devices it can communicate with. If a Device is not listed on the CPL, a User cannot communicate with it other than to update the firmware to a version that is on the CPL. Only once a Device has met the requirements set out in the CPL Requirements Document can it be added to the CPL. The CPL is a list of Device Models that are either:

- Smart Metering Equipment Technical Specifications (SMETS) 2 Devices which have received all relevant Assurance Certificates; or
- SMETS1 Devices which have been notified by the DCC and have been included as entries on the SMETS1 Eligible Products Combination list.

SEC Section F 'Smart Metering System Requirements' (Section 2) defines the CPL and is supplemented by SEC Appendix Z.

Validating CPL entries

SEC Appendix Z Sections 4.1 and 4.3 require the Panel to check that a communication requesting a firmware Image to be associated with a Device Model on the CPL originates from the person who created the Image and is endorsed by a Supplier. In practice this is carried out by SECAS on behalf of the Panel.

Relevant extract from Appendix Z

The following is an extract from version 2.0 of SEC Appendix Z setting out the obligations for associating a Hash (in relation to a firmware Image) with a Device Model on the CPL:

4. <u>Association of Hashes with Device Models on the CPL</u>

4.1 Where the DCC or a Supplier Party wishes the Panel to associate the Hash of a Manufacturer Image with a Device Model on the Central Products List, that Party shall provide the Hash and the identity of the person who created the Manufacturer Image in a communication to the Panel which has been Digitally Signed by the person who created the Manufacturer Image in a manner that reasonably enables the Panel to check that the communication originates from the person who created the Manufacturer Image.

4.2 The Panel may specify the format which the communication referred to in Clause 4.1 must take (in which case Parties sending such communications must use such format). The Panel shall notify the relevant Parties of any such required format and of any changes to such required format that the Panel may make from time to time.

4.3 The Panel shall only associate a Hash provided under Clause 4.1 with a Device Model on the Central Products List where:

(a) the Panel has successfully confirmed that the Digital Signature referred to in Clause 4.1 is that of the person who created the Manufacturer Image (validated as necessary by reference to a trusted party);

(b) there is no Hash currently associated with the Device Model; provided that, if there is a Hash currently associated with the Device Model, the Panel shall investigate the matter with the relevant Parties to identify whether it is appropriate to replace the associated Hash (and shall, where it is appropriate to do so, update the Central Products List accordingly); and

(c) if the Device Model is a SMETS1 Device Model, the communication to the Panel referred to in Clause 4.1 is from the DCC.

What is the issue?

At present, the nature of the signatures used by Manufacturers does not enable cryptographic authentication that the communication originates from a specific Manufacturer beyond reasonable doubt. Therefore, neither a Supplier nor the Panel can suitably verify the authenticity of the communication and is unable to fully meet the SEC obligation.

SEC Appendix Z Section 4.2 allows the Panel to specify the format which the communication referred to in Section 4.1 must take. The SSC has considered the security implications and considers that there are commercial solutions that are readily available that can be adopted by the DCC as an extension to the IKI service. Therefore, the SSC, with support from the SMKI PMA, wishes to address the current SEC compliance issue and improve the security controls.

What is the impact this is having?

If this issue is not resolved, the Panel will not be able to fully authenticate communications requesting a firmware Image to be associated with a Device Model on the CPL originates from the person who created the Image and is endorsed by a Supplier.

Impact on consumers

Although there are controls in place to prevent this, if this issue is not resolved, it may increase an easily avoidable risk of consumer smart metering Devices receiving improperly authorised or, in the worst case, malicious firmware.

3. Solution

The DCC will expand the existing processes detailed in the SMKI Registration Authority Policies and Procedures (SMKI RAPP) to allow Device Manufacturers to apply and obtain the IKI Certificates. This will apply regardless of whether a Device Manufacturer is a SEC Party or not. These Certificates should be used by the Device Manufacturers and Suppliers[1] to sign, and countersign, the CPL submission.

To allow the Panel to ratify the Certificates, the DCC will also make the CRL publicly available on its website. If Certificate details appear on this list, then the Certificate has been revoked and is no longer valid. Parties will be able to access these lists to check the validity of Certificates prior to signing and approving CPL submissions.

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

[1] MP222 'CPL submission efficiency improvements' is due to be implemented in the June 23 SEC Release which will remove the obligation on Suppliers to endorse applicable submissions.

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
✓	Device Manufacturers		Flexibility Providers

Suppliers will need to obtain IKI Certificates and countersign the CPL submissions from Device Manufacturers. This is a change from current process whereby Suppliers confirm the submission via email. Although IKI Certificates are already available to Suppliers, new personnel may be required to obtain them if involved specifically in the CPL submission process.

Device Manufacturers will need to obtain their IKI Certificates from the DCC, as opposed to another Certificate Authority, and use those IKI Certificates to sign the CPL submission. The remaining element of the submissions from their side should be unchanged.

DCC System

The DCC Total System is not impacted by this modification. The CRL is currently behind a firewall and will need to be hosted publicly on the DCC website and the web address will be shared with those who need to access the link. A new web server/proxy will be deployed to facilitate this whilst limiting access to the SMKI Workflow.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Impact Assessment response in Annex C. This document is classified as **RED** and can be obtained by emailing sec.change@gemserv.com.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and Interpretations
- Section L 'SMKI and DCC Key Infrastructure'
- Appendix D 'SMKI Registration Authority Policies and Procedures'
- Appendix Q 'IKI Certificate Policy'

The changes to the SEC required to deliver the Proposed Solution can be found in Annex B.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
✓	Communications Hubs		Gas Proxy Functions
	In-Home Displays		Prepayment Meter Interface Devices
✓	Standalone Auxiliary Proportional Controllers	✓	Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

Device behaviour is not impacted but this modification will impact CPL submissions where Suppliers are currently required to support the submission. Namely when a new firmware or hardware version is added to an existing Commercial Product Assurance (CPA) Certificate.

Consumers

There will be no impact on consumers from this modification.

Other industry Codes

There will be no impact on other industry codes from this modification.

Greenhouse gas emissions

There will be no impact on greenhouse gas emissions from this modification.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is **£9,081.** There are no Application Support costs associated with this modification.

As this modification does not impact the DCC Total System there is no associated breakdown.

More information can be found in the DCC Impact Assessment response in Annex C. This document is classified as **RED** and can only be shared with certain Parties by emailing sec.change@gemserv.com.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is three days of effort, amounting to approximately £2,574. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry
- CPL Tool updates to validation
- CPL guidance notes to be updated
- Testing of the use of new IKI Certificates

SEC Party costs

Device Manufacturers will need to obtain IKI Certificates for their submissions from the DCC. This will be a change from their current Certificate Authority and this could be a cost saving, dependent on their organisation's current agreements.

6. Implementation approach

Approved implementation approach

The Change Sub-Committee (CSC) has agreed an implementation date of:

- **One month after decision** (ad-hoc SEC Release).

The changes required do not impact the DCC Total System and therefore the modification does not need to be implemented via a scheduled SEC Release. The DCC believes the changes can be delivered in nine Working Days and so the additional time is required for User Acceptance Testing. Device Manufacturers have requested involvement in testing the process, and SECAS will also need to carry out testing.

MP222 'CPL Submission Efficiency Improvements' has been approved for the June 23 SEC Release and the SSC has asked this modification be implemented as soon as possible following MP222's implementation.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the SSC and the SMKI PMA to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	None
SMKI PMA	Input on Proposed Solution and legal text
SSC	Input on Proposed Solution and legal text
TABASC	None

Observations on the issue

Change Sub-Committee views

A CSC member questioned whether the DCC will be impacted by this modification. SECAS explained that the Proposer is keen to see this progressed as soon as possible, but that the Proposed Solution may impact DCC processes hence why a Preliminary Assessment would be required. SECAS advised a possible solution has been discussed that would see the CRL being published on the DCC's website. However, there is a SEC obligation which denies the DCC permission to publish the CRL online and so this obligation would need to be changed. The impacts have since been confirmed via the DCC Impact Assessment.

Requirements workshop comments

An attendee questioned the intent of the proposal and if any Manufacturer impacts were foreseen for the way in which they make CPL submissions. The Proposer and other attendees clarified that the proposal is looking to improve the authentication of a communication made by a Supplier requesting to add a Manufacturer Image to the CPL. However, it does not seek to make any changes to the way in which a Manufacturer signs the Manufacturer Image.

Solution development

This solution aims to improve the authentication of communications submitting new entries to the CPL that include a Manufacturer Image Hash and/or if a CPA Certificate has been previously used. This will ultimately improve the CPL security controls.

The solution does not intend to alter current elements of the process that Device Manufacturers must follow when signing their Manufacturer Images, other than being required to do this via IKI Certificates, rather than using another reputable Certificate Authority. Suppliers or the DCC will be required to countersign CPL submissions with an IKI Certificate using the X.509 format. These IKI Certificates must be compatible with standard software packages such as Microsoft.

Certificate Revocation List

The CRL holds the list of certificates that are no longer valid, either through the expiration or because an individual has left the organisation to which it is assigned. The CRL will need to be published in the public domain and accessible by a standard web browser to allow Suppliers and SECAS to validate the IKI Certificates on the submissions.

Guidance Notes

A Device Manufacturer commented that the existing Guidance Notes for updating the CPL submissions would need to be updated to include clear instructions to enable Suppliers to easily countersign. They noted that the existing notes refer to the Microsoft website and the guidance on those CPL Guidance Notes is not clear enough.

SECAS will ensure that this is delivered prior to the implementation of the modification.

Device Manufacturers that are not SEC Parties

Device Manufacturers are not required to become SEC Parties but will be required to use IKI Certificates for CPL Submission signing. Currently only the Smart Energy Code Company (SECCo), SEC Parties or Registration Data Providers (RDPs) can obtain IKI Certificates. This is detailed in the SMKI RAPP and will be updated to include 'Manufacturer' which is already a defined term in the SEC.

How to obtain IKI Certificates

The processes for becoming a Senior Responsible Officer (SRO) and Authorised Responsible Officer (ARO) are detailed within the SMKI RAPP. The process involves using the appropriate form within the SMKI RAPP to apply to the DCC. It will verify the request and the identification of the applicant remotely before providing the relevant approvals. Once approved, the SRO or ARO will be able to apply for the IKI Certificates.

8. Case for change

Business case

If this issue is not resolved, the Panel will not be able to fully authenticate communications requesting a firmware Image to be associated with a Device Model on the CPL originates from the person who created the Image and is endorsed by a Supplier. Although there are controls in place to prevent this, it may increase an easily avoidable risk of consumers' smart metering Devices receiving improperly authorised or, in the worst case, malicious firmware. The SSC and the TABASC were presented with details of the solution and were supportive of implementation.

Views against the General SEC Objectives

Proposer's views

The Proposer believes the modification better facilitates SEC objective (f)[2] as it would close a potential security risk whereby Devices receiving improperly authorised or, in the worst case, malicious firmware could be added to the CPL.

Industry views

One Refinement Consultation respondent also indicated that this modification better supported SEC Objective (f).

Views against the consumer areas

Improved safety and reliability

This change could improve this area by mitigating a security risk of malicious Device Models being placed on the CPL.

[2] to ensure the protection of Data and the security of Data and Systems in the operation of this Code

Lower bills than would otherwise be the case

This change is neutral in this area.

Reduced environmental damage

This change is neutral in this area.

Improved quality of service

This change is neutral in this area.

Benefits for society as a whole

This change is neutral in this area.

Final conclusions

The SSC and the TABASC were presented with details of the solution, costs and impacts and were supportive of implementation. The Working Group was also presented with this information and raised no concerns.

There were two respondents to the Refinement Consultation who both agreed that the modification should be approved.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	11 Jun 2021
Presented to CSC for initial comment	29 Jun 2021
Business requirements developed with Proposer	Aug 2021 – Sep 2021
Business requirements workshop	20 Sep 2021
CSC converts Draft Proposal to Modification Proposal	28 Sep 2021
Second business requirements workshop	4 April 2022
Modification discussed with Working Group	4 May 2022
Preliminary Assessment requested	11 May 2022
Impact Assessment returned	17 Mar 2023
Modification discussed with Working Group	5 Apr 2023
Modification discussed with SSC	12 Apr 2023
Refinement Consultation	3 – 25 May 2023

Timetable	
Event/Action	**Date**
Modification Report approved by CSC	20 Jun 2023
Modification Report Consultation	21 Jun - 12 Jul 2023
Change Board Vote	26 Jul 2023

Italics denote planned events that could be subject to change

Appendix 2: Glossary

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

Glossary	
Acronym	**Full term**
ARO	Authorised Responsible Officer
CPA	Commercial Product Assurance
CPL	Central Products List
CRL	Certificate Revocation List
CSC	Change Sub-Committee
DCC	Data Communications Company
IKI	Infrastructure Key Infrastructure
OPSG	Operations Group
RDP	Registration Data Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SECCO	Smart Energy Code Company
SMETS	Smart Metering Equipment Technical Specifications
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SMKI RAPP	SMKI Registration Authority Policies and Procedures
SRO	Senior Responsible Officer
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee

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.

MP168 'CPL Security Improvements'

Annex A

Business requirements – version 1.0

About this document

This document contains the business requirements that support the solution(s) for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The DCC will use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	**Requirement**
1	The DCC shall publish the Infrastructure Key Infrastructure (IKI) Certificate Revocation List (CRL) on-line for a range of uses that require authentication via IKI (e.g. Central Products List (CPL) submissions)
2	Any organisation that needs to authenticate IKI Certificates is given access to and is required to check the CRL when receiving requests authenticated with an IKI Certificate
3	It shall be possible for non-Smart Energy Code (SEC) Parties (e.g. Device Manufacturers) to apply for Certificates

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

This solution aims to improve the authentication of communications submitting new entries to the Central Products List (CPL) that include a Manufacturer Image Hash and/or if a Commercial Product Assurance (CPA) Certificate has been previously used. This will ultimately improve the CPL security controls.

This modification does not intend to alter current elements of the process that Device Manufacturers must follow when signing their Manufacturer Images, other than that they will be required to do this via IKI Certificates, rather than using another reputable Certificate Authority. Suppliers or the DCC will be required to countersign CPL submissions with an IKI Certificate using the X.509 format. These IKI Certificates must be compatible with standard software packages such as Microsoft.

2.2 Requirement 1: The DCC shall publish the IKI CRL on-line for a range of uses that require authentication of IKI

Use cases have arisen that would benefit from the IKI CRL being published on-line to allow non-DCC Users to use IKI as means of authentication. These would improve security controls and help parties maintain compliance with the SEC security arrangements. These use cases include using the IKI CRL to authenticate CPL submissions beyond all reasonable doubt.

The Security Sub-Committee (SSC), with support from the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), wishes to address these use cases by publishing the IKI CRL on-line to enable non-DCC Users to use IKI as a secure means of authentication.

However, currently SEC Appendix Q 'IKI Certificate Policy' section 4.9.9 explicitly states that the IKI CRL shall not be supported on-line. Therefore, this area of the SEC must be updated if this solution is approved.

2.3 Requirement 2: Any organisation that needs to authenticate IKI Certificates is given access to and is required to check the CRL when receiving requests authenticated with an IKI Certificate

Parties will require access to an on-line version of the IKI CRL. However, organisations such as the SEC Panel and SECAS who going forward will rely on the IKI Certificates to verify CPL Submissions are not SEC Parties or Registration Data Providers (RDPs). Therefore, the SEC needs an amendment to support the IKI CRL being made available to any organisation that needs to authenticate IKI Certificates.

Appendix Q sets out the arrangements for **Relying Parties** to check the CRL, mainly in sections 4.9.6 and 4.9.7. However, the main reference is to Section L12 to define a Relying Party. Based on these SEC references, the DCC will need to make the CRL available to:

- Suppliers, in the case of a Device which relies on a Certificate;
- The DCC, in the case of a Communications Hub Function or Gas Proxy Function which relies on a Certificate;
- Device Manufacturers, who are Parties who must use IKI to sign CPL submissions;
- The SEC Panel, who are required to authorise CPL submissions; and
- The Smart Energy Code Administrator and Secretariat (SECAS) who carry out this activity on behalf of the Panel.

2.4 Requirement 3: It shall be possible for non-SEC Parties to apply for Certificates

Device Manufacturers do not currently need to become SEC Parties. Therefore, a process needs to be developed that allows non-SEC Parties to obtain Certificates. Whilst it is acknowledged that a new process will be required to deliver this requirement, it should not impact the requirements that Device Manufacturers must follow when signing their Manufacturer Images.

3. Glossary

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

Glossary	
Acronym	**Full term**
CPA	Commercial Product Assurance
CPL	Central Products List
CRL	Certificate Revocation List
DCC	Data Communications Company

Glossary	
Acronym	**Full term**
IKI	Infrastructure Key Infrastructure
RDP	Registration Data Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee

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.

MP168 'CPL Security Improvements'

Annex B

Legal text – version 1.0

About this document

This document contains the redlined changes to the Smart Energy Code (SEC) that would be required to deliver this Modification Proposal.

Section A 'Definitions and Interpretations'

These changes have been redlined against Section A version 31.0.

Amend the following definitions to Section A1.1 as follows:

Authorised Subscriber	means SECCo, a Party, a Manufacturer or an RDP which is an Authorised Subscriber for the purposes of (and in accordance with the meaning given to that expression in) any of the Certificate Policies.

Amend Section A1.1 as follows (housekeeping change):

S1SPKI Certificate Policy (or S1SPKI CP)	means any SEC Subsidiary Document of that name set out in Appendix AP Appendices AP1 or AP2, which is originally to be developed pursuant to Section L14.5 (The S1SPKI Certificate Policies: Document Development) and Section L14.8 (Document Development: Process).

Schedule L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'

These changes have been redlined against Section L version 18.0.

Amend 'Authorised Subscribers' as follows:

Authorised Subscribers

General Provisions

L3.1 For the purposes of this Section L3:

(a) any Party which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of any of the Certificate Policies;

(b) any RDP which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of the Organisation Certificate Policy; and

(c) SECCo or a Manufacturer in respect of the IKI Certificate Policy,

may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, that Certificate Policy and the SMKI RAPP.

L3.2 The DCC shall authorise SECCo, any Party, a Manufacturer or any RDP to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where SECCo, that Party, that Manufacturer or that RDP has successfully completed the relevant procedures and satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP.

L3.3 The DCC shall provide any SMKI Services that may be requested by an Authorised Subscriber where the request is made by that Authorised Subscriber in accordance with the applicable requirements of the SMKI SEC Documents.

L3.4 The DCC shall ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L3.5 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become an Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L.

L3.6 Where a Registration Data Provider has been nominated as such by more than one Network Party:

(a) that RDP shall not, by virtue of acting in the capacity of an RDP for different Network Parties, be required to become a Subscriber for different Organisation Certificates;

(b) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP;

(c) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP.

Determinations by the Panel

L3.7 Where the DCC has notified SECCo, a Party, a Manufacturer or an RDP that has applied to become an Authorised Subscriber that the DCC does not consider that it has satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, SECCo, that Party, that Manufacturer or that RDP (as the case may be) may refer the matter to the Panel for determination.

L3.8 Following any reference made to it under Section L3.8, the Panel:

(a) shall determine whether the relevant applicant satisfies the criteria set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where the Panel determines that the relevant applicant meets those criteria, it shall notify the DCC, and the applicant shall (subject to any other requirements of the relevant Certificate Policy or the SMKI RAPP) become an Authorised Subscriber.

L3.9 Subject to the provisions of Section L3.11, any such determination of the Panel shall be final and binding.

L3.10 Nothing in Sections L3.8 to L3.10 shall be taken to prevent SECCo, any Party, any Manufacturer or any RDP from making a new application to DCC to become an Authorised Subscriber, in accordance with Section L3.2, at any time.

Changes in Circumstance

L3.11 Where SECCo, a Party, a Manufacturer or an RDP which is an Authorised Subscriber becomes aware of a change in circumstance which would be likely, if it were to make a new application to the DCC to become an Authorised Subscriber, to affect whether it would satisfy the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, it shall as soon as is reasonably practicable notify the DCC of that change in circumstance.

L3.12 Where the DCC receives a notification from an Authorised Subscriber in accordance with Section L3.12, or otherwise becomes aware of a change in circumstance of the nature referred to in that Section, it shall:

(a) assess whether that Authorised Subscriber continues to satisfy the relevant criteria to be an Authorised Subscriber as set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where it determines that the Authorised Subscriber does not continue to satisfy the relevant criteria, notify the Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised Subscriber in accordance with the Certificate Policy.

L3.13 Where the DCC has notified an Authorised Subscriber in accordance with Section L3.13(b):

(a) the provisions of Section L3.8 to L3.11 shall apply as if the person notified had made an unsuccessful application to become an Authorised Subscriber in respect of the relevant Certificate Policy; and

(b) where the relevant Certificate Policy is the Organisation Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, revoke any Organisation Certificates for which that person is the Subscriber;

(c) where the relevant Certificate Policy is the IKI Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, take such steps in relation to any IKI Certificates for which that person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

Amend 'Eligible Subscribers' as follows:

Eligible Subscribers

L3.14 An Authorised Subscriber:

(a) shall be known as an "**Eligible Subscriber**" in respect of a Certificate if it is entitled to become a Subscriber for that Certificate; and

(b) will be entitled to become a Subscriber for a Certificate only if it is identified as an Eligible Subscriber in respect of that Certificate in accordance with the following provisions of this Section L3.

Device Certificates

L3.15 A Party which is an Authorised Subscriber in accordance with the Device Certificate Policy will be an Eligible Subscriber in respect of a Device Certificate only where that Subject of that Device Certificate is one that is identified with that Party in the table immediately below.

Party	Subject
The DCC	Either: (a) a Communications Hub Function; or (b) a Gas Proxy Function.
An Import Supplier	Either: (a) an Electricity Smart Meter; or (b) a Type 1 Device.

A Gas Supplier	Either: (a) a Gas Smart Meter; (b) a Gas Proxy Function; or (c) a Type 1 Device.
Any other Party	Either: (a) an Electricity Smart Meter (b) a Gas Smart Meter; or (c) a Type 1 Device, but only in so far as the SMI Status of that Device is not set to 'commissioned' or 'installed not commissioned'.
The DCC acting as the Production Proving Function	Any Production Proving Device.

DCA Certificates

L3.16 Where the DCC (acting in its capacity as Root DCA or Issuing DCA) is an Authorised Subscriber in accordance with the Device Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of DCA Certificates;

(b) (save for the purposes of the replacement of the Root DCA Certificate) it will be an Eligible Subscriber only in respect of a single Root DCA Certificate.

Organisation Certificates and OCA Certificates

L3.17 Where the DCC, a Network Party or another Party which is (or is to become) a User, or any RDP, is an Authorised Subscriber in accordance with the Organisation Certificate Policy, that person will be an Eligible Subscriber in respect of an Organisation Certificate or OCA Certificate only where:

(a) if the Subject of that Certificate is:

(i) either the DCC (acting pursuant to its powers or duties under the Code) or a DCC Service Provider, that person is the DCC; or

(ii) not the DCC, that person is the Subject of the Certificate; and

(b) if the value of the X520OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

(i) that person is the DCC, it is the Party identified with that Remote Party Role in the second column of that table, the Certificate Signing Request originates from the individual System referred in the paragraph of the definition of DCC Live Systems identified in the fourth column of that table, and the Certificate is to be issued to the same individual System from which the Certificate Signing Request originates; or

(ii) that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or

RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table.

Remote Party Role	Party	User Role or RDP	DCC Live Systems definition paragraph
root	The DCC	[Not applicable]	(d)
recovery	The DCC	[Not applicable]	(f)
transitionalCoS	The DCC	[Not applicable]	(c)
wanProvider	The DCC	[Not applicable]	(a)
accessControlBroker	The DCC	[Not applicable]	(a) or (b) (as provided for in Section L3.18A)
issuingAuthority	The DCC	[Not applicable]	(d)
networkOperator	A Network Party	Either: (a) Electricity Distributor; or (b) Gas Transporter.	[Not applicable]
supplier	A Supplier Party	Either: (a) Import Supplier; or (b) Gas Supplier.	[Not applicable]
other	An RDP or any Party other than the DCC	Either: Other User; Registered Supplier Agent; Registration Data Provider; or Export Supplier.	[Not applicable]
pPPXmlSign	The DCC	[Not Applicable]	(g)
pPRDPFileSign	The DCC	[Not Applicable]	(g)
s1SPxmlSigning	The DCC	[Not Applicable]	(h)
xmlSign	An RDP or any Party other than the DCC	Either: Import Supplier; Gas Supplier; Electricity Distributor; Gas Transporter; Other User; Registered Supplier Agent; Registration Data Provider; or Export Supplier.	[Not applicable]
commissioningPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
requestingPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]

s1SPMigrationSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
commissioningPartyXmlSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
loadController	None	None	[Not applicable]
cSSProvider	The DCC	[Not Applicable]	(j)
coSPartyXmlSign	The DCC	[Not Applicable]	(c)
dSPXmlSign	The DCC	[Not Applicable]	(a)
aCBXmlSign	The DCC	[Not Applicable]	(b)
wANProviderXmlSign	The DCC	[Not Applicable]	(a)

L3.18A For the purposes of the fourth column of row 5 of the above table, where:

(a) the Certificate to be issued is to have a keyUsage value of digitalSignature, the Certificate Signing Request must only have originated from the individual System referred to at paragraph (a) of the definition of DCC Live Systems; and

(b) the Certificate to be issued is to have a keyUsage value of keyAgreement, the Certificate Signing Request must only have originated from the individual System referred to at paragraph (b) of the definition of DCC Live Systems.

L3.18B For the purposes of Section L3.18A, the term 'keyUsage', 'digitalSignature', and 'keyAgreement' shall have the meaning given to that term in the Organisation Certificate Policy.

OCA Certificates (further provisions)

L3.19 Where the DCC (acting in its capacity as Root OCA or Issuing OCA) is an Authorised Subscriber in accordance with the Organisation Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of OCA Certificates;

(b) (save for the purposes of the replacement of the Root OCA Certificate) it will be an Eligible Subscriber only in respect of a single Root OCA Certificate.

IKI Certificates

L3.20 Where SECCo or any Party or Manufacturer or RDP is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate in the circumstances set out in the IKI Certificate Policy.

ICA Certificates

L3.21 Where the DCC (acting in its capacity as Root ICA or Issuing ICA) is an Authorised Subscriber in accordance with the IKI Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of ICA Certificates;

(b) (save for the purposes of the replacement of the Root ICA Certificate) it will be an Eligible Subscriber only in respect of a single Root ICA Certificate.

Appendix D 'SMKI Registration Authority Policies and Procedures'

These changes have been redlined against Appendix D version 5.0.

Amend Section 3 as follows:

3. SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, Manufacturers, SECCo and the DCC in the context of access to SMKI Services and/or the SMKI Repository Service as set out in the Code, this SMKI RAPP and the SMKI interface documents. The SMKI RAPP sets out the procedures by which nominated individuals may become Senior Responsible Officers and/or Authorised Responsible Officers in order to act on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and the SMKI Repository Service.

This SMKI RAPP also details the obligations in respect of the SMKI Registration Authority and the individuals acting on its behalf as SMKI Registration Authority Managers or SMKI Registration Authority Personnel.

From time to time, the SMKI PMA may require documents or information to be lodged in the SMKI Repository. In such instances, it shall submit a request via the Service Desk and provide such documents and/or information to be lodged in the SMKI Repository. The DCC shall lodge documents and/or information provided to the SMKI Repository, as soon as reasonably practicable following receipt.

3.1 Party, RDP, Manufacturer, SECCo and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) are as set out immediately below:

- **Senior Responsible Officer (SRO)**. The process by which an individual is nominated and their authorisation is checked and their identity verified, so as to be an SRO and act on behalf of an organisation is set out in SMKI RAPP Section 5.2. An individual is nominated to become an SRO by a Director or Company Secretary for a Party, RDP, Manufacturer, SECCo or the DCC (for DCC Service Provider personnel). Once an individual has become an SRO, the SRO may at any time nominate individuals to undertake to become Authorised Responsible Officers (AROs) and to access SMKI Services and/or the SMKI Repository Service. An SRO may also nominate themselves to become an ARO as described below.
- **Authorised Responsible Officer (ARO)**. The process by which an individual is nominated, verified and authorised to be an ARO is set out in SMKI RAPP Section 5.3. The means by which AROs are provided with credentials to authenticate access to SMKI Services and/or the SMKI Repository Service is set out in Section 5.4. The DCC shall permit only AROs to act on behalf of a Party, RDP, Manufacturer, SECCo

or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or the SMKI Repository Service. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party, RDP or the DCC (in its role as DCC Service Provider) to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following successful completion of SMKI and Repository Entry Process Tests. All AROs are also permitted to access the SMKI Repository Service on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) that wishes to

a) become an Authorised Subscriber for Organisation Certificates and/or Device Certificates;

b) become an Authorised Subscriber for an IKI Certificate for the purposes of Digitally Signing of files; or

c) have access only to the SMKI Repository,

shall have at least one ARO successfully appointed (and therefore one SRO).

The DCC shall not be required to repeat processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming an SRO and/or ARO in respect of SMKI Services or the SMKI Repository Service, where the required verification processes have already been carried out for the purposes of identifying them as being a DCCKI SRO and/or DCCKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing an ARO or SRO or the Party or RDP becoming an Authorised Subscriber, be treated as if it had taken place after that date.

3.2 SMKI Registration Authority representatives

Individuals acting as representatives of the DCC in its role as SMKI Registration Authority are:

- **SMKI Registration Authority Manager**. The process by which a SMKI Registration Authority Manager is nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or the SMKI Repository Service is set out in SMKI RAPP Sections 6.2 and 6.4.

- **SMKI Registration Authority Personnel.** The process by which SMKI Registration Authority Personnel are nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository is set out in SMKI RAPP Sections 6.3 and 6.4.

The DCC shall ensure that only a SMKI Registration Authority Manager or SMKI Registration Authority Personnel may act on behalf of the DCC in respect of matters relating to the SMKI

Registration Authority. Each Party, RDP, Manufacturer, SECCo and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC Personnel (including SMKI Registration Authority Managers and SMKI Registration Authority Personnel) other than as directed by the Service Desk for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs).

The DCC, in order to perform its role as SMKI Registration Authority, shall nominate at least two individuals to become a SMKI Registration Authority Manager, each of which will have responsibility for:

a) management of the SMKI Registration Authority function and SMKI Registration Authority Personnel;

b) nomination of individuals to become SMKI Registration Authority Personnel;

c) authentication and verification of SMKI Registration Authority Personnel, as set out in Section 6.3 of this document;

d) provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, Manufacturer or SECCo representatives and DCC Personnel (including SMKI Registration Authority Personnel);

e) managing the process by which documents and information are lodged in the SMKI Repository; and

f) approval of CRRs.

A SMKI Registration Authority Manager may nominate individuals to become SMKI Registration Authority Personnel and to act on behalf of the SMKI Registration Authority as set out in this SMKI RAPP and the Code. The primary responsibilities of SMKI Registration Authority Personnel are:

a) to conduct registration processes as set out in SMKI RAPP Sections 5.1 to 5.5, incorporating:

    i. verification of organisational identity;

    ii. verification and authorisation of individuals nominated to become SROs or AROs, as set out in Section 5.2 and 5.3 of this document;

    iii. provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, Manufacturer, SECCo representatives and DCC personnel; and

    iv. assessment of whether an organisation qualifies to become an Authorised Subscriber for Organisation Certificates and/or Device Certificates.

b) processing and approval (where required) of Certification Signing Requests and processing of Certificate Revocation Requests; and

c) processing of requests for revocation of credentials used to access SMKI Services and/or the SMKI Repository Service.

The DCC shall ensure that SMKI Registration Authority Managers and SMKI Registration Authority Personnel, where required, are available to undertake the obligations in respect of procedures set out in this SMKI RAPP:

a) in respect of the verification, processing and approval of CRRs, on a 24*7 basis; and

b) in respect of all other procedures as set out in this SMKI RAPP, on a Working Day basis and during standard working hours in England.

The DCC and any Party, RDP, Manufacturer or SECCo may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, be treated as if it had taken place after that date.

Amend Section 4 as follows:

4. Party, RDP, Manufacturer, SECCo and DCC (as DCC Service Provider) registration procedures

4.1 General registration obligations

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, Manufacturer, SECCo and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service 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 from the DCC Website or via the DCC SharePoint site as advised by the DCC;
b) provide reasonable support and advice to each Party, RDP, Manufacturer, 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, Manufacturer, 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 5.3 and 5.4 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 the SMKI Repository Service on behalf of a Party, RDP, Manufacturer, 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 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 prospective ARO on a Cryptographic Credential Token during the ARO verification meeting, that the prospective 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 prospective ARO's organisation and provided by the prospective ARO during the ARO verification meeting, that the prospective 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 prospective 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, Manufacturer 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.

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, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become an SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or the SMKI Repository Service;
- 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 verifying Digital Signatures 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 File Signing Certificates, and their corresponding Private Keys to be used for the purposes of Digitally Signing files.

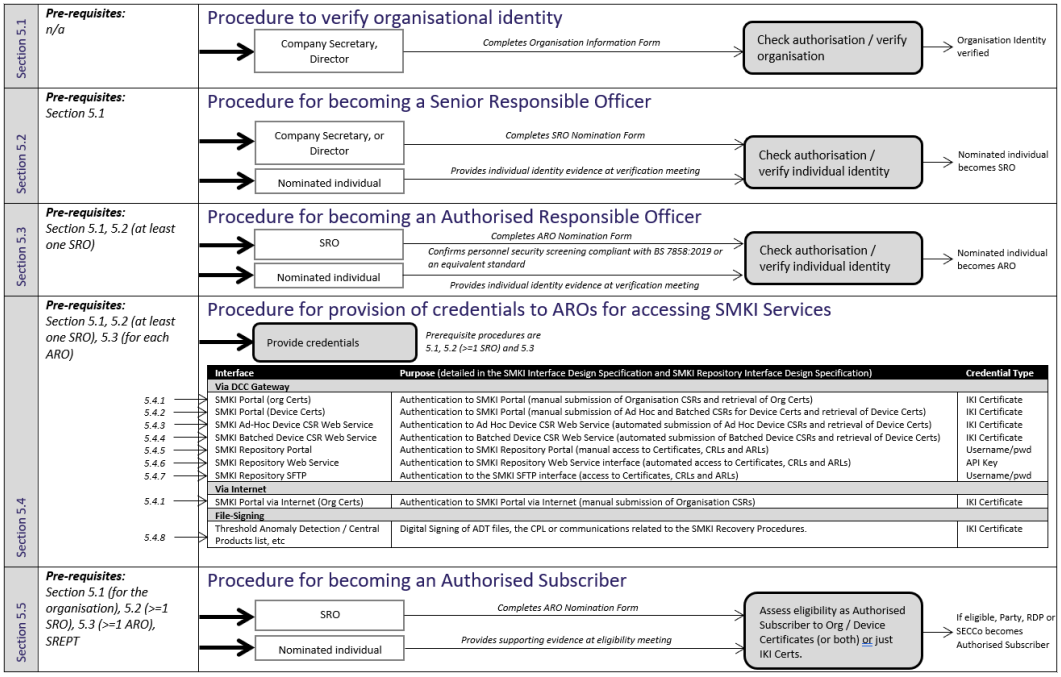

Figure 1: Overview of SMKI access registration processes

- SMKI RAPP Section 5.1 sets out the procedure and detailed processes for confirming the role of the nominating individual and verifying the organisational identity of the Party, RDP, Manufacturer, SECCo or DCC Service Provider, which shall be conducted where its identity has not previously been established.

- SMKI RAPP Section 5.2 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an SRO. The DCC shall ensure that an individual cannot become an SRO until the organisational identity of the applicant has been verified

- SMKI RAPP Section 5.3 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an ARO. The DCC shall ensure that an individual cannot become an ARO until the organisation has at least one SRO and the organisational identity of the applicant has been verified.

- Once an individual has become an ARO, SMKI RAPP Section 5.4 sets out the procedure and detailed processes by which the appropriate credentials used to access SMKI Services and/or the SMKI Repository Service are provided to AROs.

- Where an applicant wishes to be an Authorised Subscriber for Organisation Certificates or Device Certificates or both, Section 5.5 of the SMKI RAPP sets out the procedure and detailed processes by which the DCC determines if the applicant is eligible to become an Authorised Subscriber for such Organisation Certificates or Device Certificates or both.

This document has a Classification of White

In respect of the procedures and detailed processes set out in SMKI RAPP Sections 5.1 to 5.5, the DCC shall place no restriction on the number of forms that can be submitted by an individual Party, RDP, Manufacturer, SECCo or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.5 such that where multiple forms are submitted at the same time, multiple procedures can be conducted within a single visit to the DCC's offices by the applicant's nominated individuals.

4.1.3 Change of details

If there is a change to any of the information used to verify the organisational identity of any Party, RDP, Manufacturer, SECCo or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 5.1 is undertaken in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs.

If there is a material change to any of the information used to verify the identity of any SRO or ARO, an SRO shall:

a) advise the Service Desk of the change;

b) where required to do so by the SMKI Registration Authority, check the name and address of an ARO before issuing a replacement token, ensure that its SRO or ARO undertakes the procedures as set out in SMKI RAPP Sections 5.2 or 5.3 in respect of the revised evidence of identity, as soon as is reasonably practicable after a material change occurs; and

c) where necessary, for an ARO ensure that credentials used to access SMKI Services and/or the SMKI Repository Service are revoked as set out in SMKI RAPP Section 8.3.

No Party, RDP, Manufacturer, SECCo or the DCC (acting as DCC Service Provider) shall unreasonably withhold information that is required by the SMKI Registration Authority in order to perform the procedures as set out in SMKI RAPP Sections 5.1 to 5.5.

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo

Where Director or Company Secretary ceases to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the Director or Company Secretary themselves, or a Senior Responsible Officer (SRO) whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from a Director, Company Secretary or SRO; and

c) if b) is successful, the DCC shall update the DCC's records of authorised individuals for the Party, RDP, Manufacturer or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, Manufacturer or SECCo.

4.1.5 SROs ceasing to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo

Where an SRO ceases to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the SRO themselves, or a Director, Company Secretary or SRO whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from an SRO, Director or Company Secretary; and

c) if b) is successful, update the DCC's records of authorised individuals for the Party, RDP, Manufacturer or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, Manufacturer or SECCo.

Amend Section 5 as follows:

5. Detailed Party, RDP, Manufacturer, SECCo and DCC (as DCC Service Provider) registration procedures and processes

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

5.1 Procedure and processes to verify organisational identity

The processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to verify the organisational identity of a Party, RDP, Manufacturer, SECCo or DCC Service Provider (acting on behalf of the DCC).

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Annex A (A1). In doing so, the applicant organisation shall ensure that: a. the information entered on the form is complete and accurate; b. the EUI-64 Compliant identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with the EUI-64 Compliant identifier range for any other User Role, other than where a particular EUI-64 Compliant identifier is allowed to be used for more than one User Role in accordance with H1.5; and c. the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation. The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	5.1.2

		Annex A (A5), for the Director or Company Secretary that has authorised the Organisation Information Form. In doing so, the applicant organisation shall ensure that the information entered on the form is complete and accurate.		
5.1.2	As required, following 5.1.1	Submit the completed Organisation Information Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	5.1.3
5.1.3	As soon as reasonably practicable following receipt of completed Organisation Information Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the Organisation Information Form.	Service Desk	5.1.4
5.1.4	As soon as reasonably practicable following 5.1.3	Confirm that the nominating Director or Company Secretary holds such a position within the application organisation, via a public information source. Analyse the information entered on the Organisation Information Form and Nominee Details Form, to determine completeness, discrepancies and whether the submitted EUI-64 Compliant identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted identifier ranges are not consistent with the restriction set out in step 5.1.1, the SMKI Registration Authority shall agree actions and/or amendments, via email, with the Director or Company Secretary that has authorised the Organisation Information Form.	SMKI Registration Authority Personnel	If complete, accurate and no discrepancies, 5.1.6; if not complete and accurate or any discrepancies, 5.1.5
5.1.5	Once omissions / discrepancies addressed	Submit a revised Organisation Information Form and/or Nominee Details Form to the SMKI Registration Authority, or in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant	5.1.3

This document has a Classification of White

			organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	

5.1.6	As soon as reasonably practicable, following 5.1.4	Agree with the applicant organisation and confirm, by email, the date and time of a meeting to verify the organisation identity to the Director, or Company Secretary that has signed the Organisation Information Form. The meeting shall be held via a video link or face to face if preferred.	SMKI Registration Authority	5.1.7

5.1.7	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the applicant Director or Company Secretary by email, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the individual(s) shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.1.8

5.1.8	In meeting to verify organisational identity	Verify: a. the organisational identity of the applicant organisation to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website; b. via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c. proof of individual identity provided for the nominating individual against the information listed on the Organisation Information Form and the Nominee Details Form; and d. the individual identity of the nominating individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority Personnel	If not successful, 5.1.9; if successful, 5.1.10

5.1.9	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is unsuccessful, notify the nominating Director, Company Secretary or SRO that verification of the organisational identity has been unsuccessful, by email.	SMKI Registration Authority Personnel	5.1.5 once issues addressed

5.1.10	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is successful, inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, by email.	SMKI Registration Authority	5.1.11

5.1.11	As soon as reasonably practicable, following 5.1.10	Add the verified organisation to the DCC's list of such organisations, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of procedure

5.2 Procedure for becoming a Senior Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become a Senior Responsible Officer in respect of that Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SMKI SRO Nomination Form and Nominee Details Form, as set out in SMKI RAPP Annex A (A3) and Annex A (A5). In doing so, the individual completing the SMKI SRO Nomination Form and Nominee Details Form shall ensure that the information entered on the forms is complete and accurate, and that: a. the nominating individual is for a Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider), a Director of, or Company Secretary of and an employee of, the applicant organisation or its parent organisation; and b. the SMKI SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary on behalf of the applicant organisation.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	5.2.2
5.2.2	As required, following 5.2.1	Submit the completed SMKI SRO Nomination Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which	5.2.3

			shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	
5.2.3	As soon as reasonably practicable following receipt of completed SRO Nomination Form	Acknowledge receipt to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	Service Desk	5.2.4
5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SMKI SRO Nomination Form and Nominee Details Form, to: a. determine completeness and any discrepancies; and b. confirm, using the DCC's records or using publicly available information, that the Director or Company Secretary that has authorised the SMKI SRO Nomination Form has the role indicated on the SMKI SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email.	SMKI Registration Authority Personnel	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised SMKI SRO Nomination Form and/or Nominee Details Form to the SMKI Registration Authority, in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	If the SMKI Registration Authority has any questions about the information submitted, contact the Director or Company Secretary that nominated the individual, via telephone, using the telephone number provided previously in the SMKI SRO Nomination Form, to confirm whether each nominated individual on the SMKI SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SMKI SRO Nomination Form in order to provide confidence that the correct person has been contacted.	SMKI Registration Authority Personnel	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7

5.2.7	As soon as reasonably practicable following rejection	Inform the applicant organisation that the application to become a Senior Responsible Officer has not been successful, by email to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	SMKI Registration Authority Personnel	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the individual nominated to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a face to face verification meeting in person or by video link.	SMKI Registration Authority Personnel	5.2.9
5.2.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) nominated to act on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the nominated individual shall inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting in person or by video link, the SMKI Registration Authority shall, in person: a. check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the Nominee Details Form; and b. verify the individual identity for each nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12
5.2.11	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has not been verified successfully and has not become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.5 once issues addressed

5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.13

5.2.13	As soon as reasonably practicable, 5.2.12	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of Procedure

5.3 Procedure for becoming an Authorised Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become an Authorised Responsible Officer in respect of that Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the SMKI ARO Nomination Form and Nominee Details Form as set out in SMKI RAPP Annex A (A4) and Annex A (A5), ensuring that; a. the information entered on the forms is complete and accurate; b. the SMKI ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation; and c. the SRO has confirmed that the SMKI ARO Nominee has been subject to a standard that is compliant with BS 7858:2019 or an equivalent standard.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	5.3.2
5.3.2	As required, following 5.3.1	Submit the completed SMKI ARO Nomination Form and Nominee Details 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, RDP, Manufacturer, ~~the~~ SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.3	As soon as reasonably practicable following receipt of completed ARO Nomination	Acknowledge receipt by email to the SRO as identified on the SMKI ARO Nomination Form.	Service Desk	5.3.4

	Form and Nominee Details Form			
5.3.4	As soon as reasonably practicable following 5.3.3	Analyse the information entered on the SMKI ARO Nomination Form and Nominee Details Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email.	SMKI Registration Authority	If complete, 5.3.6; if not complete, 5.3.5
5.3.5	Once omissions / discrepancies are addressed	Submit a revised SMKI ARO Nomination Form and/or Nominee Details Form to the Registration Authority in writing as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.6	As soon as reasonably practicable, following 5.3.4	If the SMKI Registration Authority has any questions about the information submitted, contact an SRO of the applicant organisation via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm whether the nominated individual is authorised to become an ARO.	SMKI Registration Authority	If confirmed as authorised, 5.3.8; if not authorised, 5.3.7
5.3.7	As soon as reasonably practicable following rejection	Notify the individual and an SRO that the procedure for becoming an ARO has not been successful for relevant nominated individual, by email.	SMKI Registration Authority	5.3.5 once issues addressed
5.3.8	As soon as reasonably practicable, following 5.3.6	Agree with the applicant organisation and confirm the date and time for the ARO verification meeting, via email to the nominated individual and an SRO of the applicant organisation.	SMKI Registration Authority	5.3.9
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform an SRO and the nominated individual, by email, and shall agree and confirm an alternative date and time. If it is identified that the nominated individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10

		the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.		

5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a. check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11

5.3.11	As soon as reasonably practicable, following ARO verification meeting	Notify: a. the nominated individual that they have become an ARO, verbally; or b. in writing to the SRO, that the verification has not been successful for the nominated individual, that the nominated individual has not become an ARO, and provide reasons for the rejection and request that the nominated individual is required to attend a further ARO verification meeting once the issues have been remedied.	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed

5.3.12	As soon as reasonably practicable, following ARO verification meeting	Ensure that the applicant organisation is notified of the individuals whose identity has been verified and have become AROs by email or via the Service Desk updating the relevant ticket, ensuring that there is a record for audit purposes.	SMKI Registration Authority or Service Desk	5.3.13

5.3.13	As soon as reasonably practicable, following 5.3.12	Add the relevant individual to the DCC's list of AROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	Procedure as set out in SMKI RAPP section 5.5

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and the SMKI Repository Service 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 the SMKI Repository Service or for file signing to Authorised Responsible Officers in respect of a Party, RDP, Manufacturer, 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, Manufacturer, 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 CSRs in respect of Organistion Certificates 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, Manufacturer, 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 CSRs in respect of Organisation Certificates 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	SMKI Registration Authority	5.4.2

		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 CSRs in respect of Organisation Certificates 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, Manufacturer, 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, Manufacturer, 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 CSRs in respect of Device Certificates using SMKI Portal via DCC Gateway Connection** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the	SMKI Registration Authority	5.4.3

		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 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: 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 CSRs in respect of Device Certificates 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. 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	SMKI Registration Authority	5.4.4

		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 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, sections 2.4 xv, xvi & xvii. 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.		

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 organistaion has access to a DCC Gateway Connection and 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 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	SMKI Registration Authority	5.4.5

		accordance with the SMKI Interface Design Specification, sections 2.5 xxvi & xxvii. 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, section 2.1.2. 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, section 2.1.2.	SMKI Registration Authority	5.4.6

5.4.6	During ARO verification meeting and	**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	SMKI Registration Authority	5.4.7

	after becoming an ARO	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 section 2.2.1, 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 the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Design Specification section 2.2.1.		

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, as set out in the SMKI Repository Interface Design Specification section 2.3.1. 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, as set out in the SMKI Repository Interface Design Specification section 2.3.1.	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.	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 to confirm credential issuance either manually or digitally and give the form to the ARO, retaining a copy of the original. 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) either manually or digitally. The SMKI Registration Authority shall retain a copy of the receipt. 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 Clause 8.3.1 as follows:

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and / or the SMKI Repository Service and / or File Signing Certificates

A Senior Responsible Officer on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, Manufacturer, SECCo or the DCC

(as DCC Service Provider) or revocation of an IKI File Signing Certificate for which that Party, RDP, Manufacturer, SECCo is an Authorised Subscriber, using the form as set out in Annex A (A7) and clearly identifying the credentials to be revoked.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) An applicant wishes an IKI File Signing Certificate or the credentials of an ARO to be revoked.
b) A Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or the SMKI Repository Service or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate.
c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change).
d) A Party, RDP, Manufacturer, DCC (as DCC Service Provider), or SECCo notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or the SMKI Repository Service.
e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate.
f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Where access credentials have been revoked and the Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

Amend Clause 8.3.2 as follows:

8.3.2 Procedure for revocation of SMKI Services and / or the SMKI Repository Service access credentials for AROs and / or IKI File Signing Certificates

The procedure for verification and, where verified, revocation of authentication credentials or IKI File Signing Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.2.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised by an SRO on behalf of the applicant organisation.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.2

8.3.2.2	As required, following 8.3.2.1	Submit the completed Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.3	As soon as reasonably practicable following 8.3.2.2	Acknowledge receipt by email to the SRO as identified on the Credential Revocation Request Form or via the Service Desk updating the relevant ticket, ensuring a record is kept.	SMKI Registration Authority or Service Desk	8.3.2.4
8.3.2.4	As soon as reasonably practicable following 8.3.2.3	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with an SRO via email.	SMKI Registration Authority	If complete, 8.3.2.6; if not complete, 8.3.2.5
8.3.2.5	Once omissions / discrepancies are addressed	Submit a revised Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.6	As soon as reasonably practicable, following 8.3.2.4	Contact the SRO as identified on the Credential Revocation Request Form, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm the application identified by the Credential Revocation Request Form is authorised.	SMKI Registration Authority	If confirmed as authorised, 8.3.2.8; if not authorised, 8.3.2.7
8.3.2.7	As soon as reasonably practicable following rejection	Notify the SRO that was contacted in step 8.3.2.3, that the procedure in respect of the application has not been successful, by email.	SMKI Registration Authority	End of procedure
8.3.2.8	As soon as reasonably practicable following 8.3.2.6	Notify the SRO that was contacted in step 8.3.2.3, and the DCC's CISO by email that the revocation request has been accepted.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.9

8.3.2.9	As soon as reasonably practicable following 8.3.2.8	Revoke the credentials for the relevant service, for the identified ARO or relevant IKI File Signing Certificate as indicated by the SRO on the Credential Revocation Request Form. In doing so, the DCC shall, where required to revoke the credentials, revoke all associated IKI Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10
8.3.2.10	As soon as reasonably practicable following 8.3.2.9	Notify the SRO that was contacted in step 8.3.2.3 of the successful revocation of credentials for the ARO or relevant IKI File Signing Certificate. Where such revocation results in the individual that is the subject of the Credential Revocation Request Form no longer having any valid credentials issued to them in accordance with the SMKI RAPP, the SMKI Registration Authority shall notify the SRO that was contacted in step 8.3.2.3 that the individual is no longer an ARO, by email.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.11
8.3.2.11	As soon as reasonably practicable following 8.3.2.10	Where the revoked credentials were issued on a Cryptographic Credential Token or Cryptographic Credential Tokens, the Party, RDP, Manufacturer, SECCo or DCC Service Provider shall, where such Cryptographic Credential Tokens are in the possession of the applicant organisation, send the Cryptographic Credential Token or Cryptographic Credential Tokens to the DCC, via secure courier.	SRO on behalf of the applicant organisation	8.3.2.12
8.3.2.12	As soon as reasonably practicable following 8.3.2.11	The DCC shall verifiably destroy all Secret Key Material or Certificates contained on the returned Cryptographic Credential Token.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.2.13
8.3.2.13	As soon as reasonably practicable following 8.3.2.12	Record the details of the credentials that have been revoked in respect of the ARO as identified on the Credential Revocation Request Form or relevant IKI File Signing Certificate, plus, if relevant, update the DCC's list of AROs, in a manner which is auditable.	SMKI Registration Authority	End of procedure

Amend the following definitions in Annex B as follows:

Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, Manufacturer, SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).

Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, Manufacturer, SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).

Appendix Q 'IKI Certificate Policy'

These changes have been redlined against Appendix Q version 5.0.

Amend Clause 1.3.3 as follows:

1.3.3 Subscribers

(A) In accordance with Section L3.20 of the Code (IKI Certificates), certain Parties, Manufacturers, RDPs and SECCo may become Authorised Subscribers.

Amend Clause 1.4.2 as follows:

1.4.2 Prohibited Certificate Uses

(A) No Party, Manufacturer, RDP or SECCo shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

Amend Clause 3.2.2 as follows:

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

(i) procedure to be followed by a Party, Manufacturer, RDP or SECCo in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the ICA will determine whether a Party, Manufacturer, RDP or SECCo is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party, Manufacturer, RDP or SECCo shall be Authenticated by the ICA for that purpose.

(B) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the ICA shall Authenticate a Party, Manufacturer, RDP or SECCo shall be set to the level pursuant to the SMKI PMA Guidance on 'Verifying Organisation Identity' published on the Website.

Amend Clause 4.2.2 as follows:

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party, Manufacturer, RDP or SECCo which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA shall Issue the Certificate which was the subject of the Certificate Signing Request.

Amend Clause 4.9.9 as follows:

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy ~~does not~~ supports on-line revocation status checking.

(B) The ICA shall ~~not~~ provide ~~any~~ on-line revocation status checking service.

Amend the following definitions as follows:

Authorised Responsible Officer (ARO)	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, Manufacturer, an RDP, a DCC Service Provider or SECCo in accordance with the SMKI RAPP.
Authorised Subscriber	means a Party, Manufacturer, RDP or SECCo which has successfully completed the procedures set out in this Policy and has been authorised by the ICA to submit a Certificate Signing Request.
Eligible Subscriber	Means an Authorised Subscriber and: a) in respect of each IKI Certificate Issued by the IKI Administrator CA or the IKI Registration Authority CA, the DCC; b) in respect of each IKI Certificate Issued by the IKI Authorised Organisation Subscriber CA, each Eligible Subscriber in respect of Organisation Certificates; c) in respect of each IKI Certificate Issued by the IKI Authorised Device Subscriber CA, each Eligible Subscriber in respect of Device Certificates;

d) in respect of each IKI Certificate Issued by the IKI Authorised Web Service Subscriber CA, each Eligible Subscriber for Device Certificates that is the DCC or a Supplier; or

e) in respect of each ICA Certificate, the DCC;

f) in respect of each IKI Certificate Issued by the IKI File Signing Certification Authority, an Authorised Subscriber that is a Party, Manufacturer, RDP or SECCo.

Subscriber means, in relation to any Certificate, a Party, Manufacturer, RDP or SECCo which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

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.

MP168 'CPL Security Improvements'

Annex D

Refinement Consultation responses

About this document

This document contains the full collated responses received to the MP168 Refinement Consultation.

Question 1: Do you agree that the solution put forward will effectively resolve the identified issue?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	For reasons given in Modification Report
OVO Energy	Large Supplier	Yes	Although this solution offers no major benefit to SEC parties like OVO, we can see the benefits for device manufacturers.

Question 2: Do you agree that the legal text will deliver MP168?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	-
OVO Energy	Large Supplier	Yes	-

Question 3: Do you agree with the proposed implementation approach?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	-
OVO Energy	Large Supplier	Yes	-

Question 4: Will there be any impact on your organisation to implement MP168?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	No	Subject to resource within relevant team
OVO Energy	Large Supplier	No	-

Question 5: Will your organisation incur any costs in implementing MP168?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	No costs	Subject to authorised IKI roles being available within relevant team
OVO Energy	Large Supplier	No costs	

Question 6: How long from the point of approval would your organisation need to implement MP168?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Not long to implement from point of approval	Subject to authorised IKI roles being available within relevant team
OVO Energy	Large Supplier	Immediately	We do not anticipate any changes

Question 7: Do you believe that MP168 would better facilitate the General SEC Objectives?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	Modification will better facilitate General SEC Objective (f)
OVO Energy	Large Supplier	-	-

Question 8: Do you believe there will be any impacts on or benefits to consumers if MP168 is implemented?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	No	-
OVO Energy	Large Supplier	No	-

Question 9: Noting the costs and benefits of this modification, do you believe MP168 should be approved?

Question 9				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
E.ON	Large Supplier	Yes	For reasons given in Modification Report	
OVO Energy	Large Supplier	Yes	Please note that the costs are not outlined in the mod report, but in the working group notes. We would expect any costs to be covered by the mod report. We do not have any objections to this modification.	SECAS acknowledges that the Modification Report on the website was not the latest version and that has now been corrected. The correct Modification Report was circulated with the Refinement Consultation documents however so we do not believe the Consultation needs to be repeated.

Question 10: Please provide any further comments you may have.

Question 10		
Respondent	**Category**	**Comments**
E.ON	Large Supplier	None
OVO Energy	Large Supplier	-