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’

Modification Report

Version 0.4

3 May 2023

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

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

Contents

This document also has three 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**).

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. Therefore, 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 will target 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. Association of Hashes with Device Models on the CPL

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 for 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 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 their 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

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.

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 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 other 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

Recommended implementation approach

SECAS is recommending 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 believe the changes can be delivered in nine working days so the additional time is required for User Acceptance Testing. Device Manufacturers have requested involvement in testing the process, and SECAS would also need to test on their end.

MP222 'CPL Submission Efficiency Improvements' is targeted for June 23 SEC Release and the SSC has asked this modification be implemented as soon as possible following that 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 Change Sub-Committee (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 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.

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 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 consumer 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)[1] 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

These will be sought as part of the Refinement Consultation.

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.

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.

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

Improved quality of service

This change is neutral in this area.

Benefits for society as a whole

This change is neutral in this area.

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
Modification Report approved by CSC	*20 Jun 2023*
Modification Report Consultation	*21 Jun - 12 Jul 2023*
Change Board Vote	*26 Jul 2023*
Targeted Release Date	*26 Aug 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

Glossary	
Acronym	**Full term**
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