



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.

# SECMP0052 Initial Modification Report

## About this document

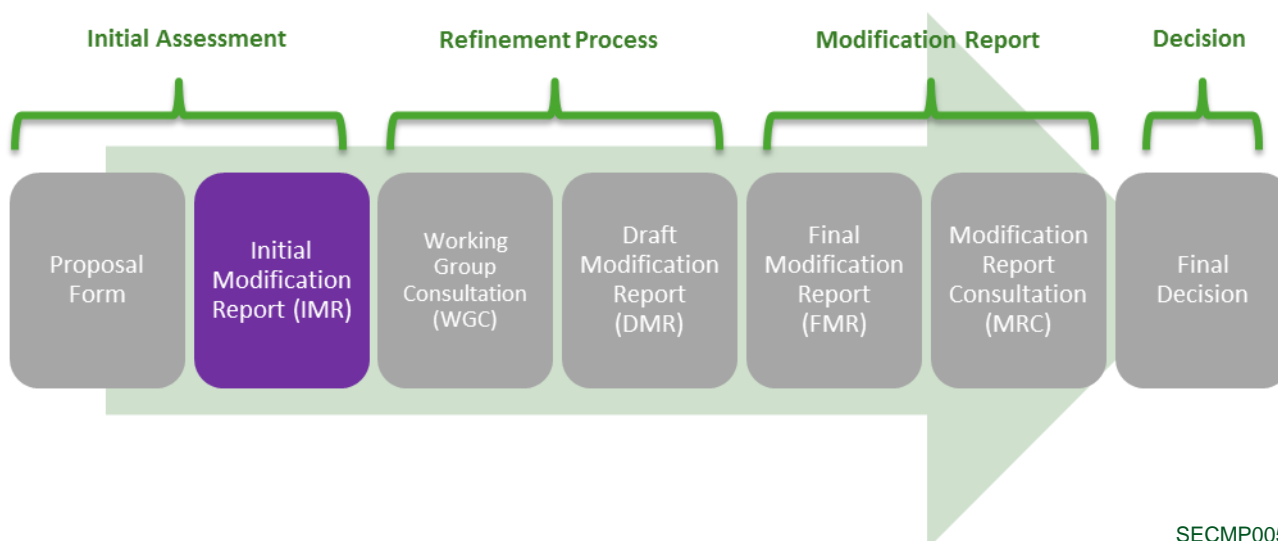
This Initial Modification Report (IMR) contains our initial assessment of SECMP0052. It also provides information on the issue, the Proposer's solution, potential impacts, costs and proposed progression.

This document was submitted to the Smart Energy Code (SEC) Panel on 11<sup>th</sup> May 2018 for consideration to determine how this Modification Proposal should be progressed through the Modification Process.

As part of this document the Panel:

- **AGREED** that this modification should be submitted to Modification Report Consultation (MRC);
- **AGREED** the progression timetable set out in Section 6; and
- **AGREED** that SECMP0052 should be progressed as a Path 3 Modification Proposal.

## Where are we in the process?



SECMP0052  
Initial Modification  
Report

11<sup>th</sup> May 2018

Version 1.0

Page 0 of 13

This document is  
classified as **White**

© SECCo 2018



## Stage 01: Initial Modification Report

# SECMP0052:

# Updates to the DCCKI CP and DCCKI RAPP

What stage is this document in the process?

|      |                     |
|------|---------------------|
| 01   | Initial Assessment  |
| 02   | Refinement Process  |
| 03   | Modification Report |
| ▶ 04 | Decision            |

### SECAS Contact:

**Name:**

Mertcan Agir

**Number:**

020 7090 7747

**Email:**

[SEC.change@gemserv.com](mailto:SEC.change@gemserv.com)

## Summary

This modification proposes to make changes to the Data Communications Company (DCC) Key Infrastructure (DCCKI) Certificate Policy (CP) and Registration Authority Policies and Procedures (RAPP) to ensure that the governance provisions under the SEC are aligned with the current operational practises.

## Panel views

The Panel have determined that this modification should be:

- Progressed as a Path 3: Self-Governance Modification Proposal; and
- submitted for Modification Report Consultation.

## Potential Impacts



- There are no impacts on SEC Parties identified.
- There are no impacts on DCC Central Systems and/or Party interfacing systems.

SECMP0052  
Initial Modification  
Report

11<sup>th</sup> May 2018

Version 1.0

Page 1 of 13

This document is  
classified as **White**

© SECCo 2018

## Content

|                         |    |
|-------------------------|----|
| 1. Summary              | 3  |
| 2. What is the issue?   | 4  |
| 3. Solution             | 6  |
| 4. Potential Impacts    | 8  |
| 5. Potential Costs      | 9  |
| 6. Proposed Progression | 10 |
| 7. Implementation       | 11 |
| 8. Panel views          | 12 |
| Appendix 1: Glossary    | 13 |

## About this Document

This is an Initial Modification Report (IMR). This document contains details of the issue, solution, potential impacts and costs as well as the proposed progression for SECMP0052.

This document has three attachments:

- Attachment A contains the SECMP0052 Modification Proposal Form; and
- Attachments B and C contain the draft legal text changes to support this modification.

The Panel considered this IMR at its meeting on 11<sup>th</sup> May 2018 and determined that SECMP0052 should be progressed as a Path 3 Self Governance Modification and submitted directly to Modification Report Consultation.



## 1. Summary

### What is the issue?

An independent audit of the DCCKI Services was carried out in January 2017. The DCC commissioned the audit to gain reasonable assurance that the DCCKI Services were compliant with applicable requirements of the DCCKI Document Set.

The auditor raised a number of observations aimed at ensuring that the DCCKI Service is carried out in accordance with Good Industry Practise.

### What is the Proposed Solution?

The modification aims to make changes to the DCCKI CP and DCCKI RAPP to bring these SEC subsidiary documents into alignment with the current operational practises.

### Potential impacts

#### Party

There are **no direct impacts on SEC Parties** due to the implementation of this Modification, as it only intends to align the SEC with the current operational practises. SEC Parties are not expected to take any action in response to this modification.

#### System

There are no impacts on DCC Central Systems or on Party interfacing systems

### Potential implementation costs

We believe that the cost to implement SECMP0048 will be limited to SEC time and effort to deliver the necessary document changes.

### Proposed progression

This Modification Proposal is recommended to be:

- progressed as a Path 3: Self-Governance Modification Proposal; and
- submitted directly to Modification Report Consultation.

## 2. What is the issue?

### What is the DCCKI?

The DCC Key Infrastructure is a cryptography related service that provides the GB Smart Metering industry with a secure and effective means of ensuring that messages to and from Smart Metering Equipment are properly authenticated, provide integrity and (where applicable) provide non-repudiation using Public Key cryptography and Certificates.

The DCCKI is used to secure the link between DCC Users and DCC interfaces including:

- DCC Gateway Connection;
- Self-Service Interface; and
- Registration Interface and the DCC User interface.

The Public Key Infrastructures (PKIs) refer to components such as software, hardware and policy processes that are required to create, manage, store and revoke these Certificates. PKIs are used in the SMKI DCCKI, which enables the binding of Public Keys to user identities by means of a Certificate Authority. This includes the Public or Private Key Pair owner to show sufficient proof of identity. Once the Certificate Authority can confirm that the User is who they claim to be, a Certificate is issued which incorporates the Public Key within a set of Credentials that affirm the identity of the owner and that of the issuer.

### What is the DCCKI RAPP and DCCKI CP?

The SEC requires Parties and Registration Data Providers (RDPs) to first become an Authorised DCCKI Subscriber in order to submit DCCKI Certificate Signing Requests (CSRs). This is done by following the relevant procedures as set out in the DCCKI Certificate Policy (CP) (SEC Appendix S) and the DCCKI Registration Authority Policies and Procedures (RAPP) (SEC Appendix W) documents. Annex B of the DCCKI CP specially outlines the metadata and cryptographic values required to request and create DCCKI Certificates.

### What is the issue?

An independent audit of the DCCKI Services was carried out in January 2017. The DCC commissioned the audit to gain reasonable assurance that the DCCKI Services were compliant with applicable requirements of the DCCKI Document Set.

The auditor raised several observations aimed at ensuring that the DCCKI Service is carried out in accordance with Good Industry Practise.

SECMPO052  
Initial Modification  
Report

11<sup>th</sup> May 2018

Version 1.0

Page 4 of 13

This document is  
classified as **White**

© SECCo 2018



This modification seeks to bring the SEC into alignment with current operational practice by making amendments to the DCCKI CP and the DCCKI RAPP as a result of the findings of the audit.

## 3. Solution

### Proposed solution

The DCC raised [SECMP0052 'Updates to the DCCKI CP and DCCKI RAPP'](#) on 26<sup>th</sup> April 2018.

The proposed solution seeks to make changes to the DCCKI CP and DCCKI RAPP. Most of these changes relate to the Certificate Profiles contained in Annex B of the DCCK CP which fall into the following categories:

- mandatory changes required to implement the DCCKI service;
- recommended changes required to comply with common PKI practice; and
- cosmetic changes and document corrections.

In addition to making changes to the existing DCCKI Certificate Profiles, this Modification Proposal adds a new Certificate Profile to support the SubjectAltName (SAN) attributes for Transport Layer Security (TLS) communication. This is required in response to changes to the internet browsers Chrome and Firefox that require Certificates to specify the hostname(s) to which they apply in the SubjectAltName field; values in the Subject field will be ignored. If impacted, a blocking page is displayed when a HTTPS site is accessed. In line with this change a new Certificate Profile is required to support TLS communication. This Certificate profile will be added to the DCCKI CP and all subsequent TLS certificate requests must be issued in accordance with this certificate profile. For the avoidance of doubt, DCCKI Service Users will not be required to change current Certificates should this modification be approved and implemented.

### SMIKA PMA consideration

At its meeting on 19<sup>th</sup> December 2017, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) reviewed and approved the DCC's proposed changes to the DCCKI CP and DCCKI RAPP, which now form the legal text changes for the modification.

### Draft legal text changes

The proposed legal text changes to SEC Appendices S (DCCKI CP) and W (DCCKI RAPP) are provided in **Attachments B and C** respectively.

### Views against the General SEC Objectives

The Proposer believes that this Modification Proposal better facilitates General SEC Objectives (d) and (f) for the following reasons:

SECMP0052  
Initial Modification  
Report

11<sup>th</sup> May 2018

Version 1.0

Page 6 of 13

This document is  
classified as **White**

© SECCo 2018



- **Objective (d)<sup>1</sup>:** The modification will improve the clarity of the Certificate Profiles to be used to enable connectivity to DCC Total Systems Interfaces, and will ensure that the SEC requires Users to adhere to Good Industry Practice regarding the use of Certificate Profiles.
- **Objective (f)<sup>2</sup>:** The Modification will bring the SEC into alignment with Good Industry Practice regarding the use of PKI in accordance with the recommendations made by the independent auditor.

For the avoidance of doubt, the Proposer believes that this modification is neutral against the remaining Objectives.

---

<sup>1</sup> Facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy

<sup>2</sup> Ensure the protection of Data and the security of Data and Systems in the operation of this Code



## 4. Potential Impacts

The following section sets out the initial assessment of likely impacts should SECMP0052 be approved and implemented.

### SEC Party impacts

There are **no direct impacts on SEC Parties** due to the implementation of this Modification, as it intends only to align the SEC with current operational practises. SEC Parties are not expected to need to take any action in response to this modification.

### Central System impacts

There are no central system or user system changes required to implement this modification.

### Testing

There is no testing required as part of this modification.

### SEC and Subsidiary Document impacts

The following SEC Subsidiary Documents will be impacted:

- SEC Appendix S 'DCCKI Certificate Policy'
- SEC Appendix W 'DCCKI Registration Authority Policies and Procedures'

### Impacts on other industry codes

There will be no impact on other industry codes.

### Greenhouse Gas Emission impacts

There will be no impact on Greenhouse Gas Emissions

## 5. Potential Costs

### Implementation costs

The costs to implement SECMP0052 is expected to be limited to the SEC Code Administration time and effort for:

- making the necessary amendments to the SEC;
- releasing a new version of the SEC to SEC Parties; and
- publication of this on the SEC website.

#### SECAS implementation costs

| Implementation activities   | Effort               | Cost                |
|---|----------------------|---------------------|
| <p>Application of approved changes to the SEC.</p> <p>Publication of new version of the SEC on the SEC Website and issuing this to SEC Parties.</p> <p>Review and update any impacted SEC guidance materials.</p> | Two Man Days maximum | £1,200 <sup>3</sup> |

<sup>3</sup> Based on a blended rate of £600 per day.

## 6. Proposed Progression

### Modification Path

The Proposer and SECAS recommend that SECMP0052 be progressed as a Path 3: Self-Governance Modification Proposal as it does not meet any of the criteria for needing an Authority determination listed under SEC Section D2.6.

### Proposed progression

The Panel agreed the following progression timetable.

| Activity                          | Date                  |
|-----------------------------------|-----------------------|
| Modification Proposal raised      | 26 Apr 18             |
| IMR presented to Panel            | 11 May 18             |
| Panel reviews Modification Report | 11 May 18             |
| Modification Report Consultation  | 11 May 18 – 04 Jun 18 |
| Change Board vote                 | 20 Jun 18             |

The Panel also agreed to progress this modification directly to Modification Report Consultation. The draft legal text has already been reviewed and approved by the SMKI PMA in December 2017. The modification is intended only to bring the relevant SEC documents in line with current operational practice, and is not expected to have any impact on any SEC Parties.



## 7. Implementation

### Recommended implementation date

The Panel agreed an implementation date of **1<sup>st</sup> November 2018** (as part of the November 2018 SEC Release) if a decision to approve is received on or before 25<sup>th</sup> October 2018.

This is the earliest SEC Release that this modification can be included in.



## 8. Panel views

### Panel discussions

The Panel **unanimously** agreed that SECMP0052 should progress to Modification Report Consultation.

The Panel also agreed that SECMP0052 is a Path 3 – Self Governance Modification Proposal and that the draft legal text changes to the SEC deliver the intention of the modification.

### Panel decisions

The Panel by majority/unanimously:

- **AGREED** that this modification should be submitted to Modification Report Consultation;
- **AGREED** the progression timetable set out in Section 6; and
- **AGREED** that SECMP0052 should be progressed as a Path 3 Modification Proposal.

## Appendix 1: Glossary

The table below provides definitions of the terms used in this document.

| Acronym    | Defined Term  |
|------------|---|
| CA         | Certificate Authority   |
| CSR        | Certificate Signing Requests  |
| DCC        | Data Communications Company   |
| DCCKI      | DCC Key Infrastructure  |
| DCCKI CP   | DCC Key Infrastructure Certificate Policy                             |
| DCCKI RAPP | DCC Key Infrastructure Registration Authority Policies and Procedures |
| PKI        | Public Key Infrastructure   |
| RDPS       | Registration Data Providers   |
| SEC        | Smart Energy Code   |
| SAN        | SubjectAltName  |
| SMKI PMA   | Smart Metering Key Infrastructure Policy Management Authority         |
| TSL        | Transport Layer Security  |