



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.

Stage 03: Final 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

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 unanimously believes that SECMP0052 should be:



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

Impacts



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

SECMP0052

Final Modification
Report

11th 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?	5
3. Proposed Solution	7
4. Impacts	9
5. Costs	10
6. Implementation	11
7. Panel views	12
Appendix 1: Glossary	13

About this Document

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

The Change Board will consider this modification at its meeting on 20th June 2018, where it will determine whether SECMP0052 should be approved.

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 2 of 13

This document is
classified as **White**

© SECCo 2018

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 to SEC Parties** due to the implementation of this Modification, as it 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.

Implementation Costs

The estimate cost to implement SECMP0052 is approximately £1,200 will be limited to SEC time and effort to deliver the necessary document changes.

Implementation Date

SECAS recommends an implementation date of:

- **1st November 2018** (as part of the November 2018 SEC Release) if a decision to approved is received on or before 25th October 2018.

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

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 3 of 13

This document is
classified as **White**

© SECCo 2018



Panel conclusions

The Panel **unanimously** agreed that SECMP0052 should progress to Modification Report Consultation as a Path 3: Self-Governance Modification Proposal.

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 4 of 13

This document is
classified as **White**

© SECCo 2018

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:

- The DCC Gateway Connection;
- The Self-Service Interface; and
- The 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 a number of observations aimed at ensuring that the DCCKI Service is carried out in accordance with Good Industry Practise.

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 5 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.

SECMPO052

Final Modification
Report

11th May 2018

Version 1.0

Page 6 of 13

This document is
classified as **White**

© SECCo 2018

3. Proposed Solution

Proposed Solution

The DCC raised [SECMP0052 'Updates to the DCCKI CP and DCCKI RAPP'](#) on 26th 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 19th 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

Final Modification
Report

11th May 2018

Version 1.0

Page 7 of 13

This document is
classified as **White**

© SECCo 2018



- **Objective (d)**¹: 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)**²: 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.

SECMPO052

Final Modification
Report

11th May 2018

Version 1.0

Page 8 of 13

This document is
classified as **White**

© SECCo 2018

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

² Ensure the protection of Data and the security of Data and Systems in the operation of this Code



4. Impacts

The following section sets out our assessment of impacts should SECMP0045 be approved and implemented.

SEC Party impacts

There are no direct impacts to SEC Parties due to the implementation of this Modification, as it 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 impacts

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

Testing

There is no testing required as part of this modification.

SEC and Subsidiary Document impacts

The documents set out below require changes as part of this modification:

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

Impacts on other industry codes

There are no impacts on other industry codes arising from this modification.

Greenhouse Gas Emission impacts

There are no impacts on Greenhouse Gas Emissions.

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 9 of 13

This document is
classified as **White**

© SECCo 2018

5. Costs

SEC Implementation costs

The total estimated implementation cost to delivery SECMP0052 will be limited to the Code Administration time and effort for:

- making the necessary amendments to the SEC;
- releasing a new version of the SEC to SEC Parties; and
- releasing a new version of the SEC to SEC Parties

SEC costs

The estimated SEC implementation cost is detailed in the table below:

SECAS implementation costs		
Implementation Activity	Effort (man days)	Cost
Application of approved changes to the SEC. Publication of new version of the SEC on the SEC Website and issuance to SEC Parties. Review and updated any impacted SEC guidance materials.	Two	£1,200 ³

³ SEC man day effort based on a blended rate of £600 per day.



6. Implementation

Recommended implementation date

The Panel has agreed an implementation date for SECMP0052 of:

- **1st November 2018** (as part of the November 2018 SEC Release) if a decision to approved is received on or before 25th October 2018.

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

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 11 of 13

This document is
classified as **White**

© SECCo 2018



7. Panel views

Panel conclusions

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.

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 12 of 13

This document is
classified as **White**

© SECCo 2018

Appendix 1: Glossary

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

Term	Acronym
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

SECMP0052

Final Modification
Report

11th May 2018

Version 1.0

Page 13 of 13

This document is
classified as **White**

© SECCo 2018