SEC
Smart Energy Code

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP251

'Transfer of Secret Key Material'

Modification Report

Version 1.0

18 October 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

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

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

Elizabeth Woods

020 4566 8335

elizabeth.woods@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Smart Meter Key Infrastructure Policy Management Authority (SMKI PMA).

To complete the migration from Transitional Change of Supplier (TCoS) to the Enduring Change of Supplier (ECoS) to the timetable set by the Implementation Managers Forum (IMF), the Data Communications Company (DCC) needs to transfer the TCoS Private Key from the Data Service Provider (DSP) to the new ECoS Service Provider. The Department for Energy Security and Net Zero (DESNZ) made specific provision in the SEC for this to happen in Section G2.22F – G22I. These clauses were written so that the arrangements can be applied to other Secret Key Transfers in the future, subject to permissions from the SMKI PMA (after consulting with the Security Sub-Committee (SSC)) (e.g. DSP re-procurement).

The DCC has presented a proposed method of transfer to the SMKI PMA and to SSC which, after several iterations, the SMKI PMA approved on 2 October 2023. The Transfer needs to be secured by a Certificate from a different Root Private Key than SMKI. Therefore, the DCC proposes to use a DCC Key Infrastructure (DCCKI) Certificate to secure the transfer of the TCoS Private Key from the DSP to the ECoS Service Provider. The SMKI PMA and the SSC recognise that this is a sensible and secure means of authenticating the transfer using a known Public Key Infrastructure (PKI) that is subject to SEC governance rather than using an alternative PKI that is not.

However, SEC Appendix S 'DCCKI Certificate Policy' restricts the use of DCCKI to establishing Transport Layer Security (TLS) communications over the DCC Gateway and signing Security Assertion Markup Language (SAML) assertions for the Self-Service Interface (SSI).

The Proposed Solution is to allow the DCC to use a DCCKI Certificate to secure the transfer of the TCoS Private Key from the DSP. This method has been reviewed and approved by the SMKI PMA and SSC, and the timescales signed off by the Technical and Business Design Group (TBDG) and IMF.

This modification will impact the DCC directly as this change will allow them to use a DCCKI Certificate to secure the TCoS to ECoS Private Key Transfer. No other SEC Parties are impacted by this change. The cost to implement will be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort. This is a Self-Governance Modification and, if approved, will be implemented in an ad-hoc SEC Release, ten Working Days after decision.

2. Issue

What are the current arrangements?

The SEC Appendix AS (ECoS Transition and Migration Approach Document) Section 1.3 requires:

"Subject to Clause 1.4, the DCC shall attempt ECoS Migration for all eligible TCoS Devices as soon as reasonably practicable."

To complete the migration from TCoS to the ECoS to the timetable set by the IMF,, the DCC must arrange for the TCoS Private Key to be transferred from the DSP (the current holder) to the ECoS Service Provider. TCoS Private Key is used to digitally sign and encrypt Service Requests from the

TCoS Component of the DSP to a Device, in order to update the security credentials on that Device so it can communicate with the gaining Supplier. The DCC plans to transfer the TCoS Private Key from its current location at the DSP to the new ECoS Service Provider so Devices can continue to progress through the Change of Supplier (CoS) process as TCoS is decommissioned.

DESNZ made specific provision in the SEC for this to happen through the designation of SEC Section G2.22F – G22I. These clauses were written to allow the arrangements to be applied to other Secret Key Transfers in the future subject to permission from the SMKI PMA (after consulting with SSC) (e.g. DSP re-procurement).

What is the issue?

The DCC has presented a proposed method of transfer to the SMKI PMA and to the SSC and, after several iterations to improve the security of the Transfer, the SMKI PMA approved this on 2 October 2023. The DCC proposes to use a DCCKI Certificate to secure the transfer of the TCoS Private Key from the DSP. The SMKI PMA and the SSC recognise that this is a sensible and secure means of authenticating the transfer using a known PKI that is subject to SEC governance rather than using an alternative PKI that is not.

However, SEC Appendix S 'DCCKI Certificate Policy' Clause 1.4.1(b) restricts the use of DCCKI Certificates to two specific scenarios:

> *(ii) for the purposes of:*
>
> > *(1) establishing TLS communications with the DCC over a DCC Gateway Connection; or*
> >
> > *(2) the signing of SAML assertions of a User that chooses to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not provided by the DCC.*

The DCC, with support from SMKI PMA and SSC wish to sanction the use of DCCKI to authenticate and secure the Transfer of Secret Key Material as set out in SEC Section G2.22F to G2.22I.

It is noted that when Appendix S was drafted, the SEC provisions for the Transfer of Secret Key Material in Section G2.22 had not been drafted. They were included recently by DESNZ to support TCoS to ECoS Private Key Transfer and any future transfers of Secret Key Material.

What is the impact this is having?

The current wording of Appendix S prevents the DCC from using a SEC governed method to secure the Transfer of Secret Key Material. Updating the remit of the DCCKI Certificates would reduce security risks by avoiding the use of a PKI that is not governed by the SEC.

Impact on consumers

There is no impact on consumers.

3. Solution

The Proposed Solution is to allow the DCC to use a DCCKI Certificate to secure the transfer of the TCoS Private Key from the DSP. This method has been reviewed and recommended by the SMKI PMA and SSC, and the timescales signed off by the TBDG and IMF.

The legal text to implement these changes can be found in Annex A.

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

As this would be used at part of the TCoS to ECoS Private Key Transfer, it will impact the DCC directly.

DCC System

There will be no impacts on the DCC System from this modification.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix S 'DCCKI Certificate Policy'

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

Devices

The issues outlined in this proposal do not impact Devices.

Consumers

The issues outlined in this proposal do not impact consumers.

Other industry Codes

The issues outlined in this proposal do not impact other industry Codes.

Greenhouse gas emissions

The issues outlined in this proposal do not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. 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.

SEC Party costs

There will be no other costs for SEC Parties from this modification.

6. Implementation approach

Timescales

The TBDG and IMF have approved the timescales for the Secret Key Transfer in September 2023, but the transfer needs to take place no later than February 2024, before the next scheduled SEC Release. Therefore, the latest the modification could need to be implemented at least one month prior (i.e. January 2024). SECAS recommends this modification for an Ad-Hoc Release.

Agreed implementation approach

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

- **Ten Working Days after decision**.

The next available scheduled release date is 29 February 2024 (February 2024 SEC Release). This is after the agreed dates of the transfers has passed. Therefore, this modification will be implemented in an ad-hoc release to ensure they meet the timescales approved by TBDG and IMF. If this

modification is approved under Self-Governance, the implementation date will be ten Working Days following the end of the Self-Governance referral window.

As this is a text-only change, the modification can be implemented ten Working Days following decision.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	We do not believe this has any operational impacts
SMKI PMA	The SMKI PMA, as has an obligation under SEC Section G2.22I to approve the method of transfer. They have recommended the Proposed Solution be implemented
SSC	The SSC has approved this approach and required legal text change.
TABASC	We do not believe this has any Technical or Business Architecture impact.

Observations on the issue

The changes in this modification report have been identified by the DCC and endorsed by the SMKI PMA. Both the SMKI PMA and SSC approved the method proposed by the DCC. The SMKI PMA and SSC recognise that this is a sensible and secure means of authenticating the transfer using a known PKI that is subject to SEC governance rather than using an alternative PKI that isn't subject to SEC governance.

Change Sub-Committee

One CSC member requested clarity on the difference between Secret Key Material and Private Key Material. The Proposer advised that the difference was just terminology, the SEC refers to Secret Key Material as a generic term to cover current and future Transfers of Secret Key Material. The TCoS Private Key is a specific instance of Secret Key Material that needs to be transferred and there are likely to be other instances of different Private Keys to be transferred in the future. They both fall under Secret Key Material and SMKI PMA is giving approval for the DCCKI to be used on this occasion, although they are concerned that the current process may not be secure enough to transfer a different key in the future.

Another CSC member queried how important is this issue to be resolved and considered whether it is seen as a risk rather than an issue. The Proposer noted that if this change does not go ahead, DCC will not be able to meet the TCoS to ECoS migration timetable. They added that the DCC is under pressure to migrate from TCoS to ECoS by mid-2024. The proposals have been discussed at SMKI PMA in June and July 2023, as well as held two workshops in August and September 2023 to ensure a secure means of transfer of Secret Key Materials. The Proposer added that there has been a great deal of analysis on how it can be achieved with input from the SMKI Specialist, DESNZ and the

TABASC Chair, and if DCC uses a PKI which is not governed by the SEC, SEC Parties are carrying the risk if this is not changed.

The CSC appreciated the background provided by the Proposer and agreed that the modification should proceed to Report phase.

Solution development

Legal Text

The intent is to ensure that the DCC obtains SMKI PMA approval for any uses of DCCKI that aren't listed in SEC Appendix S, Clause 1.4.1.b) (ii) 1, 2 and 3. Following DESNZ feedback, the legal text was amended to explicitly call out that "other than in the cases specified in 1.4.1(a) to (c) above, subject to SMKI PMA approval.".

8. Case for change

Business case

The purpose of the proposed changes to have a secure SEC governed method for the Transfer of Secret Key Material. There is minimal cost to implement these changes.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that this Modification Proposal will better facilitate SEC Objectives (f)[1] as it will reduce security risks by using a SEC governed method for the Transfer of Secret Key Material.

Industry views

The SMKI PMA and the SSC have agreed with the DCC and endorse this modification.

Views against the consumer areas

Improved safety and reliability

This change is neutral in this area.

Lower bills than would otherwise be the case

This change is neutral in this area.

[1] Ensure the protection of Data and the security of Data and Systems in the operation of this Code.

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

SMKI PMA endorses that this modification be implemented, and the timelines for this approach have been signed off by TBDG and IMF.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	5 Oct 2023
CSC converts Draft Proposal to Modification Proposal	17 Oct 2023
Modification Report approved by CSC	17 Oct 2023
Modification Report Consultation	18 Oct – 7 Nov 2023
Change Board Vote	22 Nov 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**
CoS	Change of Supplier
CSC	Change Sub-Committee
DCC	Data Communications Company
DCCKI	Data Communications Company Key Infrastructure Certificate
DESNZ	Department for Energy Security and Net Zero
DSP	Data Service Provider

Glossary	
Acronym	**Full term**
ECoS	Enduring Change of Supplier
IMF	Implementation Managers Forum
OPSG	Operations Group
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TBDG	Test Build and Design Group
TCoS	Transitional Change of Supplier
TLS	Transport Layer Security