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.

Smart Energy Code

MP261

‘Extending the Organisation Certificate Validity Period’

Modification Report

Version 1.0

20 December 2023

Corporate member of Plain English Campaign
Committed to clearer communication
592

Gemserv

This document has a Classification of Clear

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 7
7. Assessment of the proposal 8
8. Case for change 8

Appendix 1: Progression timetable 9

Appendix 2: Glossary 10

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:

Kev Duddy

020 3574 8863

kev.duddy@gemserv.com

1. Summary

This proposal has been raised by Bradley Baker from the Data Communications Company (DCC).

Manufacturers use default Certificates, obtained from the DCC, to place on their Devices before they are installed. The expiry date of the Organisation Certificates contained within the first (and current) manufacturing pack is 2026. The DCC therefore needs to issue updated Certificates in a new manufacturing pack.

The DCC would like to align the new manufacture Organisation Certificates with the existing Issuing Organisation Certification Authority (OCA) Certificate, which has an expiry date of 25 years (2041). The DCC is unable to do this currently as Appendix B 'Organisation Certificate Policy' only allows Organisation Certificates to be valid for 10 years.

The Proposed Solution will allow the DCC to create Organisation Certificates for more than 10 years, where it is agreed by the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), having first considered the views of the Security Sub-Committee (SSC). It will also allow the DCC to re-use the existing Public Key information.

This modification will impact the DCC, and Device Manufacturers. The costs are limited to the Smart Energy Code Administrator and Secretariat (SECAS) time and effort to implement and is targeted for the February 2024 SEC Release.

This is a Self-Governance modification.

2. Issue

What are the current arrangements?

What is an Organisation Certificate and what is it used for?

For security reasons, Devices on the Smart Metering network should only be able to communicate with Parties that have the right to do so. To do this, each Device relies on Certificates placed onto the Trust Anchor Cells on the Device. There are multiple Trust Anchor Cells to reflect that Devices need to communicate with Suppliers, Network Operators and the DCC. Those Parties will have their own Organisation Certificates that will match those held on the Device to ensure that only those Parties can communicate.

What is a Manufacturing pack?

When a Device is manufactured, the Network Operator, and potentially the Supplier, will not be known. However, the Trust Anchor Cells cannot be left empty so the Device Manufacturer must place Certificates on them. The DCC issues a default list of Certificates to Device Manufacturers for them to place into the Trust Anchor Cells on their Devices. This ensures that those Devices can be initially communicated with, even though the Manufacturer will not know at the time, where they will be installed or who may operate them.

When do the existing Certificates expire?

Device manufacturing packs hold end-entity certificates signed by the OCA with a lifetime of 10 years. This control is specified in SEC Appendix B 'Organisation Certificate Policy', clause 6.3.2. The certificates in the current manufacturing pack are all original ones signed in 2016, with expiry dates in 2026. Therefore, a new manufacturing pack needs to be created.

What is the issue?

Alignment of expiry dates

The current manufacturing pack contains an Issuing OCA Certificate that expires in 2041, with the Organisation Certificates expiring in 2026. The DCC would like to include Organisation Certificates for the new manufacturing pack with longer expiry dates so that all expiry dates align.

However, the DCC cannot currently create new Organisation Certificates with longer expiry dates due to SEC Appendix B, clause 6.3.2 which specifies the Validity Period of each Organisation Certificate must be 10 years.

For efficiency, and to minimise the impact on SEC Parties, the DCC is proposing to issue a new manufacturing pack only once, expected in Q4 2024. No further manufacturing packs would be issued, until required by either the Issuing Certification Authority or because of any risks posed by Quantum Computing or other future technological advances.

Managing the Device transition

Devices with expired certificates can be installed but will need the appropriate DCC Users to update expired certificates immediately.

During the Install & Commission (I&C) process, the DCC use the default Certificates upon installation to authenticate the Device. If the Certificate on the Device is not the default in the current manufacturing pack, or not previously recorded by the Data Services Provider (DSP) then this can lead to delays in the I&C process as the DSP tries to search for the correct Certificate.

If Certificates for the new manufacturing pack are generated with new key material, this may extend the I&C timescales. Therefore, the DCC is proposing to re-use existing Public Key material for the new manufacturing pack to mitigate the risk of longer installation times.

What is the impact this is having?

If the Organisation Certificate Validity Period is not extended, a new manufacturing pack will need to be created prematurely when considering the residual lifetime of OCA root (set to expire in 2041). This would require the need for multiple manufacturing packs to be created and lead to an unnecessary impact on both DCC and SEC Parties.

If the DCC cannot re-use the existing key material for the new manufacturing pack certificates, this would require re-generating **new** key material and producing new certificates that could extend I&C timescales.

Impact on consumers

Consumers could be negatively impacted as there is currently a risk of extended I&C timescales. This could lead to engineer's being on site for longer periods of time, or failed installs and repeat visits, all at the consumer's inconvenience.

3. Solution

The Proposed Solution will allow the DCC to:

a) Issue an Organisation Certificate that has a longer Validity Period than the current 10 years; and

b) Issue an Organisation Certificate that has the same Public Key as an existing Organisation Certificate for the new manufacturing pack.

Use of these amendments will be subject to approval from the SMKI PMA, and them having considered the views of the SSC.

The current expectation is that the DCC will seek to include new Organisation Certificates within the new manufacturing pack with a Validity Period of 17 years. This would align with the expiry of the Issuing OCA Certificate and prevent DCC needing to issue a new manufacturing pack prematurely.

Only the following newly generated Certificates will have their Validity Period extended in the new manufacturing pack:

- "recovery";
- "transitionalCoS";
- "wanProvider"; and
- "accessControlBroker".

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
	DCC Other Users		MAPs/ MAMs

The DCC will be positively impacted by this change as it will allow them to align the Organisation Certificates with the Issuing OCA Certificate, to enable them to issue a single update to the manufacturing pack.

Device Manufacturers will be positively impacted by the assurance of Certificates remaining the same in future iterations of the manufacturer pack, as well as by managing a single updated pack.

Suppliers and Meter installers will be positively impacted as the risk of extended I&C timescales will be mitigated, which would reduce the likelihood of additional inconvenience for their consumers through repeat visits.

DCC Systems

DCC System changes

This modification will not impact the DCC System.

DCC System traffic

This modification will not impact DCC System traffic.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section L 'SMKI and DCC Key Infrastructure (DCCKI)'
- Appendix B 'Organisation Certificate Policy'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Devices

There is no impact to Device behaviour.

Consumers

Consumers could be positively impacted as the solution will mitigate a risk of extended I&C timescales.

Other industry Codes

This modification does not impact other industry Codes.

Greenhouse gas emissions

This modification does 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 are no SEC Party costs associated with this modification.

6. Implementation approach

Approved implementation approach

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

- **29 February 2024** (February 2024 SEC Release) if a decision to approve is received on or before 15 February 2024; or
- **Ad-hoc SEC Release** (one Working Day after decision) if a decision to approve is received after 15 February 2024.

The Proposed Changes are required to ensure that the DCC can start generating Certificate Signing Requests (CSRs) and start to test the new manufacturing pack at the end of February 2024.

This document has a Classification of **Clear**

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	Approval of the legal text and solution
SSC	Approval of the legal text and solution
TABASC	None

Solution development/ Discussion points

The Proposed Solution has been developed with input from the DCC, the SMKI PMA and the Department for Energy Security and Net Zero (DESNZ).

8. Case for change

Business case

This modification is a document only change and will allow the DCC to streamline the creation of the manufacturing packs. That will benefit Manufacturers and Suppliers who will have confidence their Devices will be able to be installed without issue throughout the Smart Metering Implementation Programme (SMIP).

Views against the General SEC Objectives

Proposer's views

The Proposer believes this modification better facilitates SEC Objective (a)[1] as it will ensure Devices manufactured on existing Certificates will still be able to be installed once the new manufacturing pack is in effect.

[1] facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain

Views against the consumer areas

Improved safety and reliability

There will be no impact from this modification in this consumer area.

Lower bills than would otherwise be the case

There will be no impact from this modification in this consumer area.

Reduced environmental damage

There will be no impact from this modification in this consumer area.

Improved quality of service

There will be a positive impact in this consumer area as a risk of extended installation times is being mitigated.

Benefits for society as a whole

There will be no impact from this modification in this consumer area.

Final conclusions

This legal text for this modification has been drafted with support from DESNZ, SMKI PMA and the SSC. The SMKI PMA has recommended it the modification proceeds, in line with the proposed implementation approach.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	14 Dec 2023
CSC converts Draft Proposal to Modification Proposal	19 Dec 2023
Modification Report approved by CSC	19 Dec 2023
Modification Report Consultation	20 Dec 2023 – 15 Jan 2024
Change Board Vote	24 Jan 2024

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**
CSC	Change Sub-Committee
CSR	Certificate Signing Requests
DCC	Data Communications Company
DCCKI	DCC Key Infrastructure
DESNZ	Department for Energy Security and Net Zero
DSP	Data Services Provider
I&C	Install & Commission
OCA	Organisation Certification Authority
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMIP	Smart Metering Implementation Programme
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee

This document has a Classification of **Clear**

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.

MP261 'Extending the Organisation Certificate Validity Period'

Annex A

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

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

These changes have been redlined against Section L version 21.0.

Amend Section 11.4 as follows:

Certificate Signing Requests

L11.4 No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

(b) subject to Section 11.4A, an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or

(c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate.

L11.4A Subject to 11.4B, the DCC may submit a Certificate Signing Request for, and may Issue, an Organisation Certificate that has the same Public Key as an existing Organisation Certificate.

L11.4B The circumstances in which 11.4A applies are:

(a) that the SMKI PMA (having taken into account the views of the Security Sub-Committee) has given approval for a Certificate to be Issued that contains the same Public Key as an existing Organisation Certificate; and

(b) the Remote Party Role Code for that Certificate is either: "recovery", "transitionalCoS", "wanProvider", or "accessControlBroker".

This document has a Classification of **Clear**

Appendix B 'Organisation Certificate Policy'

These changes have been redlined against Appendix B version 8.0.

Amend Section 6.3 as follows:

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The OCA shall ensure that it archives OCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an Organisation Certificate, 10 years or, a different duration in circumstances approved by the SMKI PMA (having taken into account the views of the Security Sub-Committee);

(ii) in the case of an Issuing OCA Certificate, 25 years; and

(iii) in the case of a Root OCA Certificate, 50 years.

(B) For the purposes of paragraph (A), the OCA shall set the `notAfter` value specified in Annex B in accordance with that paragraph.

(C) The OCA shall ensure that no OCA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.