SEC Modification Proposal, SECMP0128A, DCC CR4382
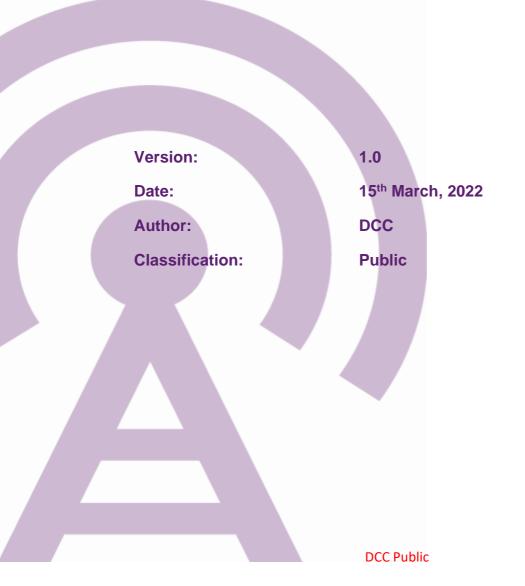
Gas Network Operators SMKI Requirements

Full Impact Assessment (FIA)

Version:	**1.0**
Date:	**15th March, 2022**
Author:	**DCC**
Classification:	**Public**

Contents

1 Executive Summary

The Change Board are asked to approve:

- Total cost to implement SECMP0128 of £158,050 which comprises:

  - £69,639 in Design, Build and PIT costs

  - £88,411 in post-PIT Release costs (SIT and TTO)

- A timescale to complete the implementation of 7 months

- Include SECMP0128A in the June 2023 SEC Release

Problem Statement

The SEC does not require a Gas Network Operator (GNO) to become a DCC User. Several GNOs who do not wish to be DCC Users have experienced difficulty and disproportionate costs in obtaining Smart Meter Key Infrastructure (SMKI) Organisation Certificates.

The solution seeks to provide optionality to GNOs to place their Organisation Certificate in the SMKI Repository. The solution will also amend the obligation on Suppliers in SEC Appendix AC to make the requirement optional and to clarify that, where a SMKI Organisation Certificate for a GNO that is a DCC User exists, then the Supplier should put it onto the Device Post Commissioning. Where there is no Network Operator Organisation Certificate available in the SMKI Repository, the Supplier shall leave the Access Control Broker (ACB) Certificate on the Device. The solution also adds an obligation for GNOs to submit a Certificate Revocation Request and to not subscribe to any further Organisation Certificates if it no longer intends to be a DCC User.

To replace the GNO certificate, a GNO will continue to use SRV6.15.1 Update Security Credentials (KRP) with an ACB certificate as the replacement certificate. However in the case where an ACB certificate is placed on a Gas Proxy Function (GPF) by a departing GNO, any subsequent SRV6.21 request to place a new GNO certificate on that device will need to pass device anti-replay checks for the Network Operator Trust Anchor Cell. A change in the DSP will detect that the Security Credentials of a GNO in a GPF has been successfully replaced with the ACB Security Credentials, and the Originator Counter of the message will be recorded. A change in SRV6.21 will ensure the Originator Counter is greater than the recorded number, thus ensuring that the command will be accepted by the device.

Benefit Summary

The Modification intends to provide an enduring solution for all GNOs such that they do not need to become SEC Parties to obtain and maintain SMKI Organisation Certificates.

If the DSP change is not made, and the tracking of the Originator Counter is not carried out by the DSP then the DSP will be unable to create a command that passes device anti-replay checks and it will not be possible to put a valid GNO certificate on that device at any point in the future.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
1/02/2022	0.1	Initial compilation
25/02/2022	0.2	Updated following internal review

2.2 Associated Documents

This document is associated with the following documents:

#	Title and Originator's Reference	Source	Issue Date
1	MP128A Modification Report v0.5	SECAS	6/12/2021
2	MP128A Business Requirements v0.3	SECAS	14/12/2021
3	SECMP0128 CR4382 - PIA - Gas Network Operators SMKI Requirements v0.4	DCC	1/08/2021

2.3 Document Information

The Proposer for this Modification is Earl Richards of Cadent Gas, although it should be noted that the SMKI PMA have been closely engaged with this development. The original proposal was submitted on 24th August 2020.

The Preliminary Impact Assessment was requested of DCC on 13th July 2021 and completed on 1st August 2021. A Full Impact Assessment was requested on 21st December, 2021, although Service Providers did not start work on this Modification until 6th January, 2022.

Note that a separate Modification, MP128B, Incorrect Gas Network Operator Certificates, was implemented in November 2021.

Note that the terms Gas Network Party (GNP), Gas Network Operator (GNO), and Network Operator were used interchangeably in documents [1] and [2] supplied by SECAS. Gas Network Operators and Gas Transporters are collectively known as GNPs. This document aims to use the term GNO for consistency, but understands there may be cases where the other terms should be used.

3   Solution Requirements and Overview

In this section, the context of the Modification, assumptions, and the requirements are stated.

The problem statement and requirements have been provided by SECAS and the Proposer.

3.1   Problem Statement

Smart Energy Code (SEC) Section B 'Accession' (2.10) currently requires all Network Parties (which includes Gas Network Operators (GNOs) and Gas Transporters) to become SMKI Subscribers. Suppliers have an obligation in SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' to place Supplier and Network Operator SMKI Certificates on Devices Post Commissioning of Smart Metering Equipment Technical Specifications (SMETS) 2+ Devices.

The original policy intent was to include an obligation on GNOs, to ensure that the relevant SMKI Organisation Certificates can be placed by Suppliers and held on Devices. This allows:

- a Supplier to know the correct Network Operator
- future status changes should the GNP want to become a DCC User

The SEC does not require GNOs to become DCC Users. If a GNO who does not wish to be a DCC Users they would experience difficulty and disproportionate costs in obtaining SMKI Organisation Certificates and see no benefit to their organisations or wider smart metering by being compelled to make their SMKI Organisation Certificate available in the SMKI Repository.

Once a Network Operator Certificate is placed on a Device, it can only be changed by the Network Operator for the given Certificate and only if the Network Operator systems are capable of doing so.

This is particularly relevant where National Grid transferred ownership to Cadent Gas. Cadent Gas are now the GNO but National Grid still has its Certificate held in those Devices. This means Cadent Gas has no access or communications with those Devices as it is not the registered GNO on the Certificate. Note this Modification will provide an enduring solution rather than a fix for one GNO.

GPFs are manufactured with ACB Certificates already loaded in the GNO slot of the Device. If an ACB Certificate is in the GNO slot in the GPF, then it will be possible in the future to enable that to be replaced with a GNO Certificate, should a GNO wish to become a DCC User and to communicate with the Device.

3.2   Business Context

Supplier and Network Operator credentials on the Comms Hub GPF relate to the supply of gas only. These Trust Anchor Cells on the Comms Hub are still required and valid where there is no Gas Meter (GSME) connected to the Smart Meter HAN (SMHAN), but the stores should be populated with ACB certificates so ensuring the Gas Proxy Function (GPF) functionality is inoperable, apart from Update Security Credentials. GPFs are manufactured with ACB Certificates already loaded in the GNO slot of the Device. Where an ACB Certificate is in the GNO slot in the GPF, in future it will be possible for that to be replaced with a GNO Certificate, should a GNO wish to become a DCC User and to communicate with the Device. As part of the GSME installation, the Supplier can then send Service Request 6.21 to the GPF to change from ACB certificates to the Network Operator certificates.

Once a Network Operator Certificate is placed on a Device, it can only be changed by the GNO for the given Certificate and only if the GNO is a DCC User.

3.3 Business Requirements

This section contains the considerations and assumptions for each business requirement.

Req.	Requirement
1	Suppliers will no longer be permitted to install Devices with Gas Network Operator (GNO) Certificates in the GNO slot of SMETS2 Gas Proxy Functions (GPFs) and they must ensure that within seven days of commissioning the GPF, the GNO slot contains an Access Control Broker (ACB) Certificate
2	A Responsible Supplier will place the GNO Certificate in a commissioned SMETS2 GPF only if the GNO is a DCC User and has its Certificate available in the SMKI Repository
3	The DCC will update its Post Commissioning reporting to reflect that Suppliers are able to leave the ACB Certificate in the GNO slot of a GPF
4	Where a GNO that is a DCC User intends to cease to be a DCC User, it must replace its Organisation Certificates on the Devices with an ACB Certificate prior to ceasing to be a DCC User
5	A GNO shall submit a Certificate Revocation Request and shall not subscribe to any further Organisation Certificates if it no longer intends to be a DCC User
6	It will be optional, not mandatory (as it is currently) for Gas Networks to become Subscribers for Organisation Certificates

Table 1: Business Requirements for SECMP0128, CR4382

The solution will be applied to SMETS2 GPFs only.

Note the above requirements will not resolve those Devices already experiencing the issue highlighted in section 3.2 above. However, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) has agreed to carry out a Recovery Event as defined in SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' which will resolve the Devices in the Cadent Gas area. The Recovery Event does not require a SEC Modification.

3.3.1 Notes on the Requirements

Requirement 1: Suppliers will no longer be permitted to install Devices with GNO Certificates in the GNO slot of SMETS2 GPFs and they must ensure that within seven days of commissioning the GPF, the GNO slot contains an ACB Certificate.

With it being optional for GNOs to become DCC Users, Suppliers shall leave the ACB Certificate in the GNO slot of the GPF. This will require amendments to SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' (IEDP). This is expected to be a non-DCC System impacting requirement.

Requirement 2: A Responsible Supplier shall place the GNO Certificate in a commissioned SMETS2 GPF only if the GNO is a DCC User and its Certificate is available in the SMKI Repository.

A GNO may choose to become a full DCC User and therefore hold Organisation Certificates. Only a Supplier Party can load the GNO Certificates onto the Device and

therefore, if the GNO Certificate is available in the SMKI Repository the Supplier place it on the Device.

Requirement 3: The DCC shall update its Post Commissioning reporting to reflect Suppliers being able to leave the ACB Certificate in the GNO slot of a GPF.

In accordance with IEDP 5.3, the Responsible Supplier must place the SMKI Certificates for the given Network Operator in the SMETS2 Device within seven days from being commissioned. If the Supplier were to leave the ACB Certificate in the GNO slot of the Device, this would count as a failure against the obligation.

If Requirement 1 is implemented, this obligation must be amended to allow Responsible Suppliers to leave the ACB Certificate in the GNO slot of the Device. The DCC would consequently need to update its reporting on post-commissioning obligations to reflect this.

Requirement 4: Where a GNO that is a DCC User intends to cease to be a DCC User, it shall replace its Organisation Certificates on the Devices with an ACB Certificate prior to ceasing to be a DCC User.

This requirement will ensure that where a change in organisation of a GNO occurs, the incoming organisation will be able manage the GNO security credentials on its Devices, if that organisation is a DCC User and chooses to do so.

This will prevent the scenario in which a GNO has placed Organisation Certificates in the SMKI Repository but then transfers ownership to another GNO but did not remove its Organisation certificates. Such an action would leave a large number of Devices with the incorrect GNO Certificate on the Device and no means of changing them through normal business operations.

Requirement 5: A GNO shall submit a Certificate Revocation Request and shall not subscribe to any further Organisation Certificates if it no longer intends to be a DCC User.

This requirement shall ensure that GNO Organisation Certificates are only held on GPFs where the GNO is a DCC User. This requirement will need to be reflected in SEC Appendix B 'Organisation Certificate Policy', section 4.9.1 (A) 'Circumstances for Revocation'. This would require an additional third sub-bullet (iii) to ensure a Subscriber requests to revoke its Certificates if it no longer intends to be a DCC User.

Requirement 6: It shall be optional instead of mandatory for Gas Networks to become Subscribers for Organisation Certificates.

As noted previously, SEC Section B 'Accession' (2.10) requires all Network Parties to become SMKI Subscribers for those Organisation Certificates which pertain to it. They must do this as soon as reasonably practicable after their accession to the SEC.

The Proposer believes this is a very expensive process for Gas Network Parties that do not have the infrastructure to create and maintain the SMKI Keys and to complete SMKI Repository Entry Process Testing (SREPT). They also consider this obligation provides no benefit to Gas Network Parties since they do not receive Alerts. Consequently, the Proposer feels that Gas Network Parties currently have no benefit in becoming DCC Users. Gas Network Parties that wish to become SMKI Subscribers must be DCC Users because otherwise they will be unable to replace their Organisation Certificates at the end

of life or if there is a SMKI Recovery Event since it requires a Critical Command to replace security credentials which can only be sent by DCC Users.

3.4   Proposed Solution

Based on current arrangements, there are no grounds for a GNO having a mandatory obligation to place their SMKI Organisation Certificates in the SMKI Repository. The solution seeks to provide optionality to GNOs to place their Organisation Certificate in the SMKI Repository. During discussions with the Working Group and the Security Sub-Committee (SSC) it was agreed that flexibility must be provided as there may be GNOs who do wish to become DCC Users either now or in the future. Additionally, there is a possibility that, GNOs may be required to become DCC Users in the future.

The solution will also amend the obligation on Suppliers in SEC Appendix AC to make the requirement optional and to clarify that, where a SMKI Organisation Certificate for a GNO that is a DCC User exists, then the Supplier should put it onto the Device Post Commissioning. Where there is no Network Operator Organisation Certificate available in the SMKI Repository, the Supplier shall leave the ACB Certificate on the Device.

The solution also adds an obligation for GNOs to submit a Certificate Revocation Request and to not subscribe to any further Organisation Certificates if it no longer intends to be a DCC User.

4   Solution Overview

Changes to the DSP and DCC Technical Operations Centre are required for this Modification solution.

4.1   Requirement 4 and Subsequent DSP Changes

To replace the GNO certificate held within the Network Operator Trust Anchor Cell of a GPF device, the GNO will need to use SRV6.15.1 Update Security Credentials (KRP) with an ACB certificate as the replacement certificate. This is currently supported by the DCC Total System and therefore no changes are required to the DSP solution to meet this aspect of the requirement.

GBCS also supports this scenario for the CS02b Update Security Credentials Command on the GPF. However, in this scenario where an ACB certificate has been placed on a GPF by a departing GNO, then any subsequent SRV6.21 request to place a new GNO certificate on that device at any point in the future will need to pass device anti-replay checks for the Network Operator Trust Anchor Cell.

For this to be possible, the DSP will need to be aware of the Originator Counter that was used by the GNO when it submitted the SRV6.15.1 that placed the ACB certificate on the device.

The northbound processing of SRV6.15.1 will therefore be amended such that when the DCC Total System detects that the Security Credentials of a GNO in a GPF has been successfully replaced with the ACB Security Credentials, the Originator Counter of the message will be recorded.

Southbound processing of SRV6.21 will then also be amended to ensure that the Originator Counter generated by the DCC Total System is greater than the recorded number, thus ensuring that the command will be accepted by the device.

If this tracking of the Originator Counter is **not** carried out by the DSP then the DSP will be unable to create a command that passes device anti-replay checks and it will no longer be possible to put a valid GNO certificate on that device at any point in the future.

4.1.1   Request Management

Where a SRV6.15.1 response from a GPF shows that the certificate in the GNO slots now belongs to the ACB, changes to the Request Management component are needed to store the Originator Counter of the Update Security Credentials Response from the GPF Device.

Changes to Request Management requires changes to the way in which the Originator Counter of the GBCS Command for SRV6.21 is generated for a GPF so that, if there is a stored Originator Counter which is larger than the ACB generated counter, the stored counter should be incremented and used.

4.1.2   Data Management

Data Management will be modified to introduce a new table to store the highest Originator Counter of the Network Operator Trust Anchor Cell of a Device where it has had an ACB certificate placed in that Trust Anchor Cell.

4.1.3   Technical Specifications and Documentation

There are no changes to any of the Technical Specifications.

4.1.4 Application Support

There is no impact to infrastructure as part of this Modification.

4.1.5 Security

On the basis that there are no changes to infrastructure and no changes to interfaces, it will not be necessary to perform any security testing (e.g. penetration testing).

4.2 DCC Technical Operations Centre Impact

Development and testing for reporting at the TOC would take two months. However the TOC have suggested their preferred way forward is to implement SECMP183 for certificate-based checking and amend the reporting logic to accommodate the SECMP128A change. This would reduce the development and testing to roughly half the time and cost. This approach is seen as fundamentally a more robust approach as it is natively relying upon slot certificate inspection.

SECAS and the Business Proposer have agreed to this approach, so TOC reporting is now out of scope for this Modification.

5   Testing Considerations

This Full Impact Assessment includes the cost to develop, fully test and deliver this SEC Modification.

5.1   Pre-Integration Testing

The DSP PIT team will design and implement the functional updates required to the DSP for the change. PIT Testing will be carried out to prove that the functionality specified in the Design has been implemented against agreed acceptance criteria. Both manual and automated testing is in scope. The DSP PIT System Test team create manual tests (and data). Test execution covers manual testing and automated regression test packs.

Once PIT Complete status is achieved, the PIT team will support post PIT activities in the form of technical support and defect fixes to allow DSP to achieve its test exit obligations.

The updates to the DSP system and the timing of the PIT exit will be agreed with the DCC through updates, submission and review of the Solution Design documents.

5.2   System Integration Testing (SIT)

The expected integration activities are documented below. All testing is expected to be carried out as part of June 2023 SEC Release testing on the DSP "B Stream" environments, in accordance with existing practices for SEC releases.

SIT activities will include the creation of two new GNO Service Users with the relevant Organisation Certificates. SIT will make updates to the existing test scenarios and scripts as required for this change.

The functional testing scope will be executed against a single-band (SBCH) Comms Hub variant from each of the two SMETS2 CSPs. SIT is expected to last 22 days.

5.3   User Integration Testing (UIT)

No UIT is anticipated for this Modification.

6   Implementation Timescales and Releases

This Modification is expected to be included in a SEC Release in June 2023. Implementation timescales will be finalised as part of the relevant SEC Release Change Request.

6.1   Change Lead Times and Timelines

From the date of approval (in accordance with Section D9 of the SEC), to implement the changes proposed DCC requires a lead time of approximately **seven** months.

The broad breakdown of the testing regime is shown in the following table in months after an approval decision date (D).

Phase	Duration
SECAS agreement on scope of release	
CAN signature	D + 1 Month
Design, Build and PIT Phase	3 Months
SIT and UIT Phase, aligned with Release Dates	3 Months
Transition to Operations and Go Live	D + 7 Months

6.2   SEC Release Allocation and Other Code Impacts

This Modification is expected to be implemented as part of the June 2023 SEC Release, however the allocation to a release may be dependent on other Modification timings and the suitability of a release. No functionality overlap with other Modifications has been identified at the time of undertaking this Impact Assessment.

6.3 Costs and Charges

This section indicates the quote for all phases of application development stage for this Modification. Note these costs assume a release of just this SEC Modification without any other Modifications or Change Requests in the release, which is not truly reflective of what the post-PIT test costs or programme duration will look like. A calculation of those costs will be carried out when the contents of the future Release are finalised, and the post-PIT costs determined through a "Grouping CR" also referred to as a "Release CR".

£	Design, Build and PIT	SIT, UIT and TTO	Total
SECMP0128A	£69,639	£88,411	**£158,050**

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.
Systems Integration Testing (SIT)	All the Service Provider's PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.
Implementation to Live (TTO)	The solution is implemented into production environments and made ready for use by Users as part of a live service.

As part of the Release CR charges for June 2023, it is expected that the SIT and Implementation costs will be shared amongst other Modifications and CR in the same release, and consequently are expected to be lower.

6.3.1 Application Support Costs

Application Support costs have been calculated for a period of 16 months after the solution is implemented, additional four Low Complexity calls per month on average relating to additional functionality. The service will run from July 2023 for a period of 16 months.

SECMP0128A	£988 per month

6.3.2 Changes to the DSP Contract

The contract updates will be detailed within the CAN and will impact the following schedules:

- Schedule 2.1 (DCC Requirements): update to reflect the addition of new Requirements to enable achievement of the activities and / or deliverables under this Modification

- Schedule 3 (DCC Responsibilities): update to reflect the addition of new DCC Responsibilities to enable achievement of the activities and / or deliverables under this Modification

- Schedule 4.1 (Contractor Solution): Solution Design documents will need to be updated as per section 4.1

- Schedule 6.1 (Implementation Planning): addition of new milestones

- Schedule 7.1 (Charges and Payment): revisions to incorporate the charges and payment applicable for Modification

Appendix A: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of the Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of the Full Impact Assessment. DCC requests that the Working Group considers this section and considers any material matters that have been identified. Changes may impact the proposed solution, implementation costs and/or implementation timescales.

Risks

Ref	Description	Status/Mitigation
MP128-R1	There is no time contingency in the high-level plan and therefore, although reasonable efforts will be made to adhere to the plan, there is a risk to the planned dates.	Open

Appendix B: Glossary

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

Acronym	Definition
ACB	Access Control Broker
Comms Hub	Communications Hub
CR	DCC Change Request
DCC	Data Communications Company
DSP	Data Service Provider
FIA	Full Impact Assessment
GNO	Gas Network Operators
GNP	Gas Network Party
GPF	Gas Proxy Function
GSME	Gas Smart Meter Equipment
HAN	Home Area Network
I&C	Installation and Commissioning
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
RSA	Registered Supplier Agent
SAT	Service Audit Trail
SBCH	Single-band Comms Hub
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SMHAN, SM HAN	Smart Meter Home Area Network
SMKI	Smart Meter Key Infrastructure
SMKI PMA	Smart Meter Key Infrastructure Policy Management Authority
SREPT	SMKI Repository Entry Process Testing
SRV	Service Request Variant
SSI	Self Service Interface
TOC	Technical Operations Centre
UIT	User Integration Testing