Data Communications Company

SEC Modification Proposal, SECMP0128, DCC CR4382

Gas Network Operators SMKI Requirements

Preliminary Impact Assessment (PIA)

Version:	0.3
Date:	10th August, 2021
Author:	DCC
Classification:	DCC Public

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to complete the Full Impact Assessment of £10,250

- The timescales to complete the Full Impact Assessment of 30 days

- ROM costs for SECMP0128, up to the end of Pre-Integration Testing (PIT) of between £0 and £150,000

Problem Statement and Solution

The SEC does not require GNOs to become DCC Users. 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 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 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.

Modification Benefit

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
29/07/2021	0.1	Initial DCC Review with Service Providers
10/08/2021	0.3	Updated Service Provider version

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP128 Modification Report v0.3	SECAS	6/07/2021
2	MP128 Business Requirements v0.2	SECAS	7/07/2021

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Earl Richards of Cadent Gas.

The Preliminary Impact Assessment was requested of DCC on 13th July 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 Networks 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 Context and Requirements

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

The requirements have been provided by SECAS, the Proposer, and the Working Group.

3.1 Problem Statement

The SEC does not require GNOs to become DCC Users. 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 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. Now Cadent Gas are the GNO for those Devices but National Grid still has its Certificate held in those Devices. This means that Cadent Gas has no access or communications with those Devices as it is not the registered GNO on the Certificate.

Supplier and Network Operator credentials on the Communications Hub (Gas Proxy Function) relate to the supply of gas only. These Trust Anchor Cells on a 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 Access Control Broker certificates so ensuring the Gas Proxy Function (GPF) functionality, apart from Update Security Credentials, is inoperable. 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. 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.

3.2 Business Context

SEC Section B 'Accession' (2.10) currently requires all Network Parties (which includes Gas Networks 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 changes of status should the GNO want to become a DCC User

The SEC does not require GNOs to become DCC Users. Several GNOs who do not wish to be DCC Users have experienced difficulty and disproportionate costs in obtaining SMKI

Organisation Certificates and see no benefit to their organisations by being compelled to make their SMKI Organisation Certificate available in the SMKI Repository.

The Business Proposer is particularly impacted by the Certificates, in cases where National Grid transferred ownership to Cadent Gas. Cadent Gas are not a DCC User, but are the Network Operator for those Devices even though National Grid still has its Certificate held in those Devices. This means that Cadent Gas has no access or communications with those Devices as it is not the registered Network Operator on the Certificate.

This obligation is incurring an unnecessary burden for GNOs where they feel there is no benefit in becoming DCC User, e.g., the Proposer believed this Modification better facilitates SEC Objective (d)1 by providing optionality for GNOs to not undergo the SMKI Repository Entry Process Testing (SREPT). If the current arrangements are not amended, the unnecessary costs and burden on GNOs will continue. Additionally, obligating Suppliers to place Network Organisation Certificates on Devices increases the risk of GNOs being unable to exchange those Certificates if the previous GNO failed to remove its Certificates before a change in organisation.

3.3 Business Requirements

The following table lists the requirements for this Modification and identifies the impacts on various functions.

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 and Impacts 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. This 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 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 Description of Technical Solution

Changes to the DSP are required for this Modification solution.

Req.	DSP Technical Solution
1	Introduces a change in the existing obligation Suppliers have in relation to the GNO SMKI certificate requirements. This does not necessitate any changes to the DCC Data Systems. Network Operator slots are populated with ACB certificates by default during manufacturing.
2	Sets out obligations for the Responsible Supplier and defines the circumstances in which a GNO certificate can be placed on the device. This requires no changes to the DCC Total System.
3	A DCC reporting requirement that has no impact on the DCC Total System
4	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. See below for notes on impacts
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	No impact on the DCC Total System

Table 2: Business Requirements and Impacts for SECMP0128, CR4382

4.1 Requirement 4 and Subsequent System 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.

5　Impact on Systems, Processes and People

This section describes the impact of SECMP0128 on Services and Interfaces that impact Users and/or Parties.

5.1　Data Model

A new table will be required to record the Originator Counter for the GPF Devices.

5.2　Request Management

Request Management requires changes to retrieve the Originator Counter of the Update Security Credentials Response from the GPF Device.

Request Management requires changes to the way in which the Originator Counter of the GBCS Command for SRV6.21 is generated.

5.3　Data Management

Data Management is required introduce a new table solely for the purpose of storing the greatest 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.

Data Management is required to provide interfaces to Request Management to store and lookup the Originator Counter.

5.4　Security Impact

There is no material impact on the security solution as a result of this change. The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams. A more detailed Security impact will be carried out as part of the Full Impact Assessment.

5.5　Infrastructure Impact

There will be no change to the infrastructure design as a result of this change. Additional processing and storage will be required, however, they are not sufficiently large to warrant the procurement of additional compute power or storage.

Note that the aggregated impact of many such changes will ultimately result in a reduction of the available processing headroom assumed as part of the original DSP agreement.

The change does not impact the DSP resilience or Disaster Recovery implementation.

5.6　Service Impact

It is not thought that the change in behaviour of the DSP system from this CR4382 will have a material ongoing service impact. However, a more detailed service impact will be completed as part of the CR4382 Full Impact Assessment.

No changes to SLAs or reporting are expected as a result of this change.

5.7　Safety Impact

No impact is expected, but a Safety Impact Assessment will be carried out as part of the FIA.

6 Implementation Timescales and Approach

This change is expected to be included in a future SEC Release. Design, Build, and PIT is expected to take between two and three months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Testing and Acceptance

There will be an impact to SIT as a result of this change and the System Integrator will be required. No UIT testing is anticipated. Any costs for SIT may be similar to Design, Build, and PIT costs and will be included in the Full Impact Assessment.

7 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result the final offer price may result in a variation.

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

	Design, Build and PIT	Days to Create FIA	Cost to Create FIA
DSP	£0 to £150,000	30	£10,250

Table 2: SECMP0128 Standalone Cost

The phases included are as follows.

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. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
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.

Based on the existing requirements, the fixed price cost for a Full Impact Assessment is **£10,250** and would be expected to be completed in 30 days.

7.1 Contract Schedules

Changes to the following schedules are anticipated as a result of this Modification:

- Updates to Schedule 4.1 as a result of design changes

If required, Contract schedules will be updated as part of a Contract Amendment Note (CAN) following standard processes.

Appendix A: Glossary

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

Acronym	Definition
ACB	Access Control Broker
CAN	Contract Amendment Note
CR	DCC Change Request
DCC	Data Communications Company
DSP	Data Service Provider
FIA	Full Impact Assessment
GBCS	Great Britain Companion Specification
GNO	Gas Network Operator
GPF	Gas Proxy Function
GNP	Gas Network Party
GSME	Gas Smart Metering Equipment
IEDP	Inventory, Enrolment and Decommissioning Procedures
KRP	Known Remote Party
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMHAN, SM HAN	Smart Meter Home Area Network
SMKI	Smart Meter Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SREPT	SMKI Repository Entry Process Testing
SRV	Service Request Variant
SSC	Security Sub Committee
UIT	User Integration Testing

Appendix B: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of any Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of this PIA.

Dependency

The following dependency has been used in the creation of this PIA. Any changes to the assumptions may require DCC to undertake further assessment, prior to the contracting and implementation of this change**.

Ref	Description	Status/Mitigation
MP128-DA1	As DCC owns the Business Scenarios, there is a dependency on DCC to make the updates required to the test scenarios and scripts within the Install & Commission (I&C) and Operational Certificates Business Scenarios for this change before the commencement of SIT.	Open