Data Communications Company

SEC Modification Proposal, SECMP0063, DCC CR 1171

Ensuring Correct Network Operator Certificates are Placed on Electricity Smart Meters

Preliminary Impact Assessment (PIA)

Version:	**0.3**
Date:	**1st August, 2019**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Data Communications Company

Contents

1 Document History 3
1.1 Revision History 3
1.2 Associated Documents 3
1.3 Document Information 3
1.4 Problem Statement 3
2 Requirements 5
3 Description of Solution 7
3.1 High Level Solution 7
3.2 DSP Solution 7
3.3 Technical Specification Changes 8
4 Impact on DCC Systems, Processes and People 9
4.1 Security Impact 9
4.2 Request Management 9
4.3 Application Support 9
4.4 Service Impact 9
4.5 Integration Impact 9
4.6 Infrastructure Impact 9
4.7 Safety Impact 10
4.8 Contract Schedules 10
5 Implementation Timescales and Approach 11
5.1 Implementation Approach 11
5.2 Testing and Acceptance 11
6 Costs and Charges 12
6.1 Design, Build, and Testing Cost Impact 12
7 Risks, Assumptions, Issues, and Dependencies 14
7.1 Risks 14
7.2 Assumptions 14
7.3 Issues 14
7.4 Dependencies 14
Appendix: Glossary 15

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
30/07/2019	0.1	Initial version
01/08/2019	0.3	Updates following DCC review

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	SECMP0063 – Request for PIA v0.3	SECAS	29/6/2019

References are shown in this format, [1].

1.3 Document Information

The original Proposer for this Modification was Dean Kelshall of UK Power Networks. The original proposal was submitted in October 2018.

The Preliminary Impact Assessment was requested of DCC in June 2019 after updated requirements were issued by SECAS.

1.4 Problem Statement

To maintain the security of the GB Smart Meter Network, a SMKI (Smart Metering Key Infrastructure) Certificate must be in placed on a Smart Meter during commissioning. During commissioning the Supplier chooses a SMKI certificate to place on the Smart Meter. However, the SMKI Repository does not display the name of the Organisation which owns the Certificate, and this has led to increasing numbers of Smart Meters containing the wrong Network Operator Certificate, preventing the correct Network Operator from communicating with the meter.

The Proposer estimates that over 10% of Electricity Smart Meters have the wrong SMKI Certificate in the Network Operator's slot on the meter and assumes that same proportion of Gas Smart Meters are also affected. Not only does this mean that the Network Operator cannot communicate with the meter, but also requires manual effort for the organisation whose Certificate is in the slot to issue an Update Certificate command. There is also significant effort that needs to go in to communicating, logging and tracking these issues. With multiple Network Operators and many Electricity Suppliers, there will be a significant amount of effort required to track and manage the issues to resolution if the underlying issue is not resolved before installation volumes increase. A 10% error rate could mean volumes in the thousands or tens of thousands per month which is unmanageable using manual methods.

The Working Group have also proposed that for the purposes of validating Certificates for Gas Proxy Functions, that the DCC validate Network Certificates against the registration data held by the Registration Data Provider. The Working Group discussed the potential to validate Network Operator Certificates against the Meter Point Reference Number (MPRN) of the Gas Proxy Function. However, the Working Group were unsure if the MPRN could be mapped to the Network Party and with no Gas Network representatives present they were unable to answer this question. it may be possible to establish which Network the MPRN belongs to by using the registration data held by the Registration Data Providers.

If the DCC are able to fulfil business requirements 1 to 4 for Gas Proxy Functions as well as ESMEs SECAS request the solution is included in their Preliminary Assessment. If not, this should also be called out.

2 Requirements

The requirements and supporting text provided in this section have been provided by the Proposer and the Working Group. The solution design for these requirements and any supporting information from the DCC and DSP are provided in section 3 following.

This modification is expected to address the of issue incorrect Network Certificates being placed on Electricity Smart Metering Equipment (ESME) as a minimum, and business requirements 1 to 4 are specific to them. If a solution mapping a MPRN to a Network Operator is possible, the requirements should be extended to both electricity and gas meters.

The business requirements are as follows.

Requirement 1	The DCC will validate that the Network Operator listed in the SMKI Certificate is the Network Operator for the ESME
Requirement 2	The DCC will block the Certificate from going on the ESME if it fails DCC validation
Requirement 3	If the Certificate is incorrect, the Supplier Party will receive a response advising this
Requirement 4	The DCC will provide reporting to the SEC Panel showing the numbers of incidents where Suppliers have attempted to place incorrect Network Certificates on ESMEs

Requirement 1:The DCC will validate the Network Operator listed in the SMKI Certificate is Network Operator for the ESME

The first two digits of the Meter Point Administration Number (MPAN) core identify the Network Party Organisation for the ESME attached to the MPAN. It is proposed that the DCC validate the Network Operator listed in the Smart Metering Key Infrastructure (SMKI) Certificate (that the Supplier Party attempts to place on the ESME) against the first two digits of the MPAN.

The Working Group advised that Service Requests 6.15.1 ‘Update Security Credentials (KRP)’ and 6.21 ‘Request Handover Of DCC Controlled Device’ are used to update the security credentials for Smart Meters, but that Service Request 6.21 is used more commonly by Supplier Parties during the post-commissioning process. Taking this into consideration the Working Group proposed that an additional response code to Service Request 6.21 could be used to validate the Certificate against the first two digits of the MPAN, whilst ensuring the DCC would still be able to place recovery keys on the Smart Meter.

Requirement 2: The DCC will block the Certificate from going on the ESME if it fails DCC validation

Where a Network Operator Certificate fails validation, the DCC shall block the Network Operator Certificate from being placed on the ESME. In this scenario the Supplier Party will be required to make another attempt to comply with SEC Appendix AC, 5.2 (a) and

place the correct security credentials for the Network Operator on the ESME within seven working days of commissioning the ESME.

However, this must not prevent Network Parties who are not associated with the MPAN from invoking Service Request 6.15.1. This allows for a Network Operator to correct where their Certificate has erroneously been placed on a meter.

Requirement 3: If the Certificate is incorrect, the Supplier Party will receive a response advising this

Where a Network Operator Certificate that a Supplier Party attempts to place on an ESME fails validation, the DCC shall respond with an error code notifying the Supplier Party.

Requirement 4: The DCC will provide reporting to the SEC Panel showing the numbers of incidents where Suppliers have attempted to place incorrect Network Certificates on ESMEs

The Working Group requested that as part of the solution the DCC provide Network Certificate reporting to the SEC Panel. This would include;

- The number of invalid Network Certificate error codes that are generated;
- The Supplier Party for which the error code(s) were sent to; and
- The quantities of each error code being sent to each Supplier Party.

The SEC Panel would consider the results and act on a Supplier case by case basis where they deemed necessary.

3 Description of Solution

Knowing which Smart Meter is installed to which Network Operator's system is very simple as the first two digits of the MPAN map directly to the Network Operator's SEC Party or Distribution Area. DCC has access to the MPAN as well as the SMKI Certificates. DCC can therefore validate the command that the Energy Supplier issues to the Smart Meter to place the Network Operator certificate on the meter. Where DCC knows which MPAN is assigned to the Smart Meter they can verify that the Certificate being placed in the Network Operator slot is for the Network Operator associated with that MPAN. Should the MPAN be unknown, DCC systems can revert to default functionality and trust that the Supplier is updating to the correct Certificate. DCC already validate the Service Request which is used to update the Certificates for a range of other invalid scenarios and thus there is an existing design pattern (precedent) for this method.

Based on the discussions at the Working Group and the Business Requirements as provided, DCC consider the requirements for SECMP0063 to be **STABLE**.

3.1 High Level Solution

DCC systems would require an additional logic step to compare the Network Operator Public Certificate with the MPAN to ensure alignment. This would have to be done pre-signing. This would be consistent with other pre-validation checks that are already done. Some of the checks are described in DUIS section 3.8.66.3.

The change will need to be tested to ensure that when a Supplier Party submits a Service Request to install an invalid Certificate, an appropriate error code is generated, while valid Service Requests are processed correctly.

3.2 DSP Solution

To satisfy the above requirements, the DCC Data System will be amended as follows.

The DCC Data System will perform a new validation check when it receives the following Service Requests (SR) submitted by the Energy Suppliers (EIS or GIS):

- SRV 6.15.1 Update Security Credentials (KRP): required only when it is targeted at an ESME
- SRV 6.21 Request Handover Of DCC Controlled Device: required for the target device types ESME and GPF

The validation check is required on SRV 6.15.1 since it is possible that some suppliers may request ESME devices to be manufactured with Supplier certificates in the Network Operator Trust Anchor Cell and these can only be replaced by the Supplier using SRV 6.15.1.

Note that this validation will not be applied if SRV6.15.1 is submitted by a Network Operator, since it must remain possible for one Network Operator to place another Network Operator's certificate on the device.

SRV 6.21 is used when Access Control Broker (ACB) certificates are placed in the Device at manufacture, which is the most common scenario for ESME devices and is the only scenario for Gas Proxy Function (GPF) devices. SRV 6.21 is only available to Suppliers.

The validation checks for both SRVs will verify that the Network Operator certificate included in the Service Request belongs to the Network Operator Party that is recorded in the DSP's copy of Registration data as being the responsible Network Operator for the MPAN or MPRN associated with the target device. This provides a common and standard solution for both ESME and GPF devices.

If validation fails, the Service Request will be rejected, and the Service Users will be notified using a specific error code. This requires changes to the DUIS definition which must be aligned with the SEC Modification implementation.

The details of a rejected Service Request (Message ID, Service User ID, Error Code, Timestamp etc.) will be recorded in the SAT log, from which DCC will be able to extract the data required to meet the reporting requirement (#4). Therefore this PIA assumes that DSP is not required to produce a separate data extract for the incorrect Network Operator certificates.

3.3 Technical Specification Changes

DUGIDS definitions for the SRVs 6.15.1 and 6.21 will be updated to include the newly introduced error code.

4 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0063 on DCC Services and Interfaces that impact Users and/or Parties.

4.1 Security Impact

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.

There are no material changes to interfaces or the security solution as part of this change and as such, a penetration test is not required in response to this CR. There will not be any changes to the DSP protective monitoring solution as result of this CR.

4.2 Request Management

Request Management will need to implement the new validation check for the SRVs 6.15.1 and 6.21.

4.3 Application Support

On the basis that updates to configuration will be charged under separate Operational Change Requests, it is not expected that there will be any change to ongoing levels of support as a result of the change. There will need to be some updates to service procedures in advance of the new solution being deployed to the Production system.

4.4 Service Impact

This change introduces new functionality within the DCC Data Systems. As such, the Operational Service will require an uplift in order to support and maintain the solution. Immediately after Go Live, DSP expects to provide an uplifted level of support to ensure any unexpected issues are rectified quickly and to allow the service to bed in.

4.5 Integration Impact

It is assumed that the change will be implemented and tested as part of a major release. The functionality will need to validate both in the SIT and UIT environments and will require integration tests that involve both DSP and CSPs as a minimum. It is assumed that it will be integrated as part of a wider release with other changes to spread the costs of regression testing major supplier solutions.

4.6 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change. This change does not warrant procurement of additional compute power or storage. Note that the aggregated impact of many such changes to the DSP solution will ultimately result in a reduction of the available processing headroom assumed as part of the original DSP agreement. As such, DSP reserves the right to raise a CR for the provision of additional infrastructure should the DCC Data System experience performance problems that are the direct result of such changes.

The change does not impact the DSP resilience or DR implementation.

It will be necessary to deploy the revised DUIS schema to Data Power devices.

4.7 Safety Impact

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

4.8 Contract Schedules

Schedules will require modification to reflect the changes necessitated under this Modification. Contract schedules will be updated as part of a Contract Amendment Note (CAN) which combines schedule updates from other relevant CRs.

A minor change to one DSP contract is expected.

5 Implementation Timescales and Approach

Notwithstanding in which release this change is implemented, based on the currently stated requirements, the elapsed time for Service Provider implementation will be between 3 – 6 months following the provision of full commercial cover.

The release lifecycle duration will be confirmed as part of the Full Impact Assessment (FIA). As currently planned , the standard ongoing major release model will provide drops to the production environment in November 2020.

5.1 Implementation Approach

Within the Smart Meter Implementation Programme (SMIP), the Implementation Approach is referred to as Transition to Operations (TTO).

This change will be implemented as part of a larger release. It is assumed that the activities required for TTO will be minimal following completion of contractual test phases.

Any required environment uplifts will take place outside of business hours.

5.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release. The System Integration Test (SIT) team will carry out necessary testing to validate the following aspects of the solution:

- Configuration parameter settings scenarios
- SLA reporting

There is no perceived need to test this change separately in the User Integration Testing (UIT) environment.

6 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 here describes indicative costs to implement the functional requirements as assumed now. The price is presented as a +/-15% range and 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 outside of the indicative range.

6.1 Design, Build, and Testing Cost Impact

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

Implementation Costs							
SECMP0063	**Design**	**Build**	**Pre-Integration Testing**	**System Integration Testing**	**User Integration Testing**	**Implement to Live**	**Total**
Cost	*£550,000*			*Not included*	*Not included*	*Not included*	**£550,000**

Supplementary Information	
Implementation cost assumptions	*A. Costs are exclusive of VAT and any applicable finance charges* *B. Majority of the costs above represent labour costs.* *C. Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers with specific exclusions of costs as identified above. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* *D. Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design 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.*

	• *System Integration Testing (SIT): All Service Providers' PIT-complete solutions are brought together and tested as DCC's Total Solution, ensuring all Service Provider 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: The solution is implemented into Production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

For the existing requirements, the fixed price cost for a Full Impact Assessment is **£15,056.26** and would be expected to be completed in 30 days.

7 Risks, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

It is possible that further Risks, Assumptions, Issues, and Dependencies will be established as part of the Working Group reviews and FIA.

7.1 Risks

Ref.	Area	Description	Outcome

7.2 Assumptions

Ref.	Area	Description	Accept
MP63-AD01	SIT, UIT, TTO	Assume that the change will be implemented and tested as part of a major DCC release.	Accepted

7.3 Issues

Ref.	Description	Mitigate?
MP63-ID01	We do not believe a solution linking a MPRN to a Network Operator is possible, and an alternative solution is proposed	Accept

7.4 Dependencies

Ref.	Area	Dependency	Impact

Appendix: Glossary

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

.Acronym	Definition
ACB	Access Control Broker
CAN	Contract Amendment Note
CR	Change Request
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GPF	Gas Proxy Function
MPAN	Meter Point Administration Number
MPRN	Meter Point Reference Number
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SIT	Systems Integration Testing
SMKI	Smart Metering Key Infrastructure
SMIP	Smart Metering Implementation Programme
SP	Service Provider
SR	Service Request
TTO	Transition to Operations
UIT	User Integration Testing