

SEC Modification Proposal, SECMP0207, DCC CR4875

Allowing Registered Supplier Agents to Maintain Meter Firmware

Preliminary Impact Assessment (PIA)

Version:	0.3
Date:	30th November 2022
Author:	DCC
Classification:	DCC PUBLIC

Contents

1	Executive Summary	3
2	Document History	4
2.1	Revision History	4
2.2	Associated Documents	4
2.3	Document Information.....	4
3	Context and Requirements	5
3.1	Current Arrangements.....	5
3.2	What is the Issue?	5
3.3	Impact of the Issue	5
3.4	Business Requirements	6
4	Description of Solution	8
4.1	Impacts on DSP	8
4.2	Impacts on CSPs	9
4.3	Impacts on S1SPs.....	9
4.4	Impacts on DCC DS&A Reporting	9
5	Impact on DCC Systems, Processes and People	10
5.1	Security Impact.....	10
5.2	Technical Specifications	10
5.3	Integration Impact.....	10
5.4	Infrastructure Impact.....	10
5.5	Service Impact	10
6	Implementation Timescales and Approach.....	11
6.1	Implementation Approach.....	11
6.2	Testing and Acceptance.....	11
7	Costs and Charges.....	11
7.1	Design, Build and Testing Cost Impact.....	11
8	Risk, Assumptions, Issues, and Dependencies	12
8.1	Risks and Issues.....	12
8.2	Assumptions	12
8.3	Dependencies	12
	Appendix A: Glossary	13

1 Executive Summary

The Change Board are asked to approve the following:

- Cost to complete the Full Impact Assessment of **£13,127**.
- The timescales to complete the Full Impact Assessment of 40 working days.
- ROM costs for SECMP0207, up to the end of Pre-Integration Testing (PIT) of £151,000 to £350,000.

Only DSP component impact and cost are included in this PIA. Possible impact on SMETS1 Service Providers (S1SPs), Communications Services Providers (CSPs) and DCC Data Science and Analytics (DS&A) team will be included in the Full Impact Assessment (FIA).

Problem Statement and Solution

Meter Operators (MOPs) and Meter Asset Managers (MAMs) are appointed by Suppliers to maintain a Supplier's portfolio throughout the lifespan of the Devices. MOPs and MAMs can issue Service Requests to the DCC in a Registered Supplier Agent (RSA) user role. As per the current Smart Energy Code (SEC), the responsibility for managing Device Firmware sits solely with Supplier Parties. Each Supplier has to implement varied processes to manage different Device Model Combinations, requiring investment of time and resource which could be outsourced to RSAs. Placing the burden of maintaining meter Firmware versions solely on Suppliers, where a Supplier uses an RSA, causes inefficiencies in the Smart services, as there is an increased risk of Device Firmware becoming outdated.

This Modification is proposing the RSA should be able to deploy firmware updates on behalf of the Supplier without compromising any security, whilst ensuring all relevant parties are able to have an overview of their current Device estate.

Modification Benefits

RSAs being able to deploy the firmware would help mitigate the challenge faced by Suppliers to maintain firmware updated for different Device Model Combinations. This reduces the risk of Devices being out of communications and vulnerable to security breaches.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
29/11/2022	0.1	Initial version, for DCC internal review
29/11/2022	0.2	Updated following DCC internal review
30/11/2022	0.3	Updated following further DCC internal review

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP207 Modification Report v0.4	SECAS	31/08/2022
2.	MP207 Business Requirements v0.5	SECAS	28/09/2022

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Tom Woolley of the SMS Plc. An Initial Modification Report was prepared and published in August 2022.

The Preliminary Impact Assessment (PIA) was requested of DCC on 1st November 2022.

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 Current Arrangements

Supplier Parties authorises Meter Operators (MOPs) and Meter Asset Managers (MAMs) to maintain their Smart Meters including remote and on-site fault resolution and processes such as Install and Commissioning (I&C) procedures. MOPs and MAMs are able to become Data Communications Company (DCC) Users in the 'Registered Supplier Agent' User Role, however, under the Smart Energy Code (SEC), MOPs and MAMs are not able to use the DCC System to remotely manage the meters' Firmware.

3.2 What is the Issue?

SEC Appendix E 'DCC User Interface Services Schedule' (UISS) and SEC Appendix AD 'DCC User Interface Specification' (DUIS) both state that only Parties with either the DCC User Role 'Import Supplier' or 'Gas Supplier' can send Service Reference Variant (SRV) 11.1 'Update Firmware', SRV 11.3 'Activate Firmware' and SRV 11.4 'Update PPMID Firmware'. Parties with the User Role 'Registered Supplier Agent' are unable to send these SRVs, and therefore unable to manage the Firmware version on Smart Metering Equipment Technical Specifications (SMETS) 2+ Devices they are registered to.

The responsibility for managing Device Firmware therefore sits solely with Supplier Parties when it may be beneficial to outsource some of this functionality to RSAs.

Firmware management is essential for Suppliers and the wider industry, which relies on Smart Meter data for day-to-day processes and for the success of future programmes, such as Market-wide Half Hourly Settlement (MHHS) and achieving net-zero. It is also critical for asset funders, such as Meter Asset Providers (MAPs) and their investors, which rely on meters being installed and operated for many years.

3.3 Impact of the Issue

Each Supplier has to implement varied processes to manage different Device Model Combinations, requiring investment of time and resource which could be outsourced to RSAs.

Placing the burden of maintaining meter Firmware versions solely on Suppliers, where a Supplier uses an RSA, causes inefficiencies in the Smart service, as there is an increased risk of Device Firmware becoming outdated. In addition, this can have a negative impact on the interoperability of Devices. This in turn increases the risk of disruption to message process pathways if Devices are not communicating as expected over the Home Area Network (HAN) or Wide Area Network (WAN). Out-of-date Firmware versions may also be more vulnerable to security breaches.

Also outdated Firmware can impact the interoperability of HAN Devices such as In-Home Displays (IHDs) and Prepayment Meter Interface Devices (PPMIDs), negatively affecting consumers' access to information and prepayment functionality. The financial investment in time and resources required for Suppliers to manage Firmware versions across all their

Devices may be greater than if they were able to outsource this functionality to RSAs, resulting in a higher cost to consumers for providing this service.

3.4 Business Requirements

The business requirements are as follows.

Ref.	Requirement
1	Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to Update Firmware on SMETS1 and SMETS2+ Devices (ESME and GSME only).
2	Validation of Devices which the appointed RSAs are responsible for and have permission to manage
3	Current firmware management security requirements must be maintained
4	Reporting mechanism to monitor and ensure Energy Suppliers are aware of the current state of their Device portfolio
5	RSAs can access Alerts that are triggered by updating firmware

Requirement 1: Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to Update Firmware on SMETS1 and SMETS2+ Devices (ESME and GSME only).

RSAs are being instructed to maintain the meters, however, currently only an Energy Supplier is able to update or activate firmware for their Device portfolio. By allowing RSAs to update firmware, they are able to assist the Energy Supplier to ensure the correct firmware is on Devices within their portfolio, and therefore better able to maintain their meters in the process. Targeted Smart Metering Equipment Technical Specifications 1 (SMETS1) and SMETS2+ Devices are only for Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) due to Prepayment Meter Interface Device (PPMID) Update Firmware SRV automatically Activates Firmware. Energy Suppliers will still be required to activate the firmware.

Requirement 2: Validation of Devices which the appointed RSAs are responsible for and have permission to manage

RSAs are contracted by Energy Suppliers to maintain the Devices within their portfolio. Validation will be needed to ensure that only the correct RSA has access to Devices which are within the Energy Supplier's portfolio and restricted from those for which they are not appointed. This would ensure Devices are not being accessed by unauthorised Parties.

For example, check could be performed by the DCC, to provide an indication that the Device is for a contracting Party, in this case an Import Supplier, and the RSA is the appointed Party for said Import Supplier.

Requirement 3: Current firmware management security requirements must be maintained

In order to maintain current security requirements, the Proposer is only pursuing deployment of firmware due to implications of firmware activation being a critical command. By only allowing RSAs to deploy firmware, no additional User Competent Independent Organisation (CIO) Assessments would be needed and that the Supplier would remain accountable for the mitigation of this risk, as they are under the current model.

If firmware activation is added to the scope, it would need a new User Role to be needed to help facilitate the Firmware management by appointed RSAs. This new role would also be added to the Trust Anchor Cells to ensure Security is maintained and no malicious activity occurs.

Requirement 4: Reporting mechanism to monitor and ensure Energy Suppliers are aware of the current state of their Device portfolio

As Energy Suppliers who use RSAs to manage their Device portfolio, it would be ideal if the exact state of their Device portfolio is known and an obligation added to the Smart Energy Code (SEC) to facilitate this. This is to ensure there is a up to date report to understand and determine the exact state of all Devices at any one time. Ideally current reports should be used if the appropriate information is provided.

Requirement 5: RSAs can access Alerts that are triggered by updating firmware

Currently Energy Suppliers are sent these Alerts, however, to enable RSAs to effectively manage an Energy Supplier's Device portfolio, they will need access to Alerts which will be triggered following any updating of firmware on Devices. This modification does not intend to stop Alerts being received by Energy Suppliers, but allow RSAs access to these Alerts as well. Without these Alerts, the RSA would need to obtain this information from the Energy Supplier and this would impede their management of the Device portfolio effectively and in a timely manner.

4 Description of Solution

The primary change to the DCC solution is on Data Services Provider (DSP) component. Communications Service Providers (CSPs), SMETS1 Service Providers (S1SPs) and DCC's Data Science and Analytics (DS&A) team could also be impacted.

4.1 Impacts on DSP

The following changes are required to the DSP solution to meet the requirements mentioned in section 3.4

Requirement 1

Allow a Registered Supplier Agent (RSA) to send Service Request Variant (SRV) 11.1 to ESME and GSME devices.

Requirement 2

Extend SRV 11.1 authorisation check to include the RSA role.

Requirement 3

No impact – activation of firmware is not in scope.

Requirement 4

No impact – likely impact the DCC's DS&A team.

Requirement 5

Update the Self Service Interface (SSI) component such that both the Supplier and their appointed RSA can see each other's SMETS2 firmware tracking data.

Deliver copy of firmware receipt alerts (8F72 & 8F1C) to RSAs.

Add RSAs to recipients for DCC Alerts N49 N50 N51 N52 where these relate to ESMEs or GSMEs.

Amend SRV 11.3 processing to send N49 to RSAs when the firmware on an ESME or GSME is updated to an active version.

In summary, this change adds the capability for RSAs to send 11.1s to ESMEs and GSMEs where they are the appointed RSA for the meter. RSAs will receive all the alerts related to the distribution as they are the sender of the 11.1, and will also receive copies of the firmware receipt device alerts sent from the device to the Supplier.

RSAs and Suppliers will be able to see the firmware tracking for devices where the other party has sent the SRV 11.1 using SSI.

RSAs will receive DCC Alerts relating to changes of firmware on devices.

The definition of invalid device check W110101 (used when device does not exist or sender is not the registered supplier) to be extended to include checking that an RSA is appointed to the device (which must be an ESME or GSME).

Note that it may also be necessary to create a new DUIS error code to report validation failures when an RSA attempts to download firmware to a device type for which they are not authorised. This could result in a requirement to revise the DUIS schema. This will need to be discussed with the Business Proposer and Working Group prior to the Full

Impact Assessment (FIA). A decision to create a new error code could increase costs and extend the project duration.

4.2 Impacts on CSPs

SECMP0007 already introduced validation on SRV 11.1 to check that there is no firmware update already in progress to a given Device when an SRV 11.1 is submitted and this validation is not User specific. This existing validation should prevent the scenario where Supplier and RSA are invoking the same firmware download request which could have impact Communications Services Providers (CSPs). Any other impact of inclusion of *SR11.1-Update Firmware* for SMETS1 and SMETS2+ Devices in RSA role on CSPs will be assessed as part of the FIA.

4.3 Impacts on S1SPs

Inclusion of *SR11.1-Update Firmware* for SMETS1 Devices in RSA role are likely to impact SMETS1 Service Providers. This will be assessed as part of the FIA.

4.4 Impacts on DCC DS&A Reporting

Inclusion of *SR11.1-Update Firmware* in RSA role are likely to impact reporting produced by the DCC Data Science and Analytics (DS&A) team. This will be assessed as part of the FIA.

5 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0207 solution on DCC Services and Interfaces that impact Users and/or Parties.

5.1 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.

A more detailed security impact will be carried out as part of the Full Impact Assessment.

5.2 Technical Specifications

There will be changes in DUIS and corresponding changes in DUGIDS for the changes in DUIS. The DUIS Guidance document may need to be updated.

5.3 Integration Impact

An appropriate level of Systems Integration and User Integration Testing (SIT and UIT) will be carried out prior to progressing the release of this change to the Production environment, but this is not included in the PIA. A more detailed integration impact will be carried out as part of the Full Impact Assessment to evaluate CSPs and SMETS1 Service Providers need to carry out any integration testing or not.

5.4 Infrastructure Impact

No infrastructure impact is expected from this Modification. It should be noted 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 Agreement. As such, it may be necessary for DSP to raise a Business as Usual (BAU) CR for the provision/ of additional infrastructure to ensure the DCC Total System does not experience performance problems that are the direct result of the accumulation of such changes.

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

5.5 Service Impact

The changes noted above are not expected to alter traffic volumes significantly, nor to add to message processing time but amends functionality of core DSP processing components. No changes to Service Level Agreements (SLAs) or reporting are expected as a result of this change.

A detailed service impact will be completed as part of the Full Impact Assessment.

6 Implementation Timescales and Approach

This Modification is expected to be implemented in a future SEC Release. Design, Build, and PIT is expected to take approximately four months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release and will include release based regression testing in SIT and UIT.

7 Costs and Charges

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. 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. As a result, the final offer price may result in a variation.

7.1 Design, Build and Testing Cost Impact

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
SECMP0207	£151,000 to £350,000

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by the DSP is **£13,127** and would be expected to be completed in 40 working days.

8 Risk, Assumptions, Issues, and Dependencies

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

8.1 Risks and Issues

Ref.	Assumption	Impact
MP207-IS1	This PIA draft includes DSP component impact only. Other DCC components (such as S1SPs, CSPs and DS&A Reporting) could be impacted and this will be assessed prior to the FIA.	Total cost of the Modification and the price to complete the FIA may increase based on wider impacts.

8.2 Assumptions

None at this time.

8.3 Dependencies

Ref.	Dependency	Impact
MP207-AD1	Adding new error code may have impact on DUIS schema as mentioned in Section 4.1	This should be discussed with the Business Proposer and Working Group to agree or avoid the DUIS schema change.

Appendix A: Glossary

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

Acronym	Definition
BaU, BAU	Business As Usual
CAN	Contract Amendment Note
CR	DCC Change Request
CSP	Communications Services Provider
DCC	Data Communications Company
DS&A	Data Science and Analytics
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
FIA	Full Impact Assessment
HAN	Home Area Network
IHD	In-Home Display
MAM	Meter Asset Manager
MOP	Meter Operator
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
RAID	Risks, Assumptions, Issues, and Dependencies
ROM	Rough Order of Magnitude (cost)
RSA	Registered Supplier Agent
S1SP	SMETS1 Service Provider
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
SR	Service Request
SRV	Service Request Variant
SSI	Self Service Interface
UIT	User Integration Testing
WAN	Wide Area Network