SEC Modification Proposal, SECMP0107

SMETS1 Validation of SRV 6.15.1

Full Impact Assessment (FIA), DCC CR4296

Version:	0.5
Date:	16th August, 2021
Author:	DCC
Classification:	Public

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement MP107 of £254,112 which comprises:
    - £185,743 in Design, Build and PIT costs; and
    - £68,369 in estimated release costs (SIT, UIT, TTO and Systems Integration).
    - an optional one-off data update activity (Requirement 2) to resolve the incorrect certificate data issues on LIVE environment
- The timescale to complete the implementation of six (6) months
- Include SECMP0107 as part of the November 2022 SEC Systems Release.

Problem Statement

If an incorrect Network Operator certificate is placed on SMETS1 device in error, no Network Operator can send any Critical Service Request (SR) including SRV 6.15.1 to that SMETS1 Device. This means, any attempt to replace the incorrect certificate by issuing SRV 6.15.1 will be rejected.

In the equivalent situation on SMETS2 devices, the issue can be overcome by the Network Operator that has certificates on the device sending an SRV 6.15.1. This means that the “wrong” Network Operator can place the correct Network Operator’s certificates on the SMETS2 device.

This is not possible for SMETS1 because Registration Data Provider (RDP) checks are required for all SRs, including Critical SRs.

This Modification solution proposes the DCC shall remove the RDP check for SRV 6.15.1 targeted at SMETS1 devices specifically where it targets Network Operator certificates.

Benefit Summary

The benefits of delivering this change is Network Operator would be able to place correct Network Operator certificate on SMETS1 Devices where there is an incorrect certificate. This would result in:

- routing of SMETS1 alerts to the correct Network Operator.
- Business process related to certificate update process on SMETS1 Devices would be same as SMETS2.

Current estimates suggest that the following numbers of devices are impacted:

- 9024 ESMEs and 18905 GPFs in SMETS1 IOC cohort
- 125 ESMEs and 1226 GPFs in SMETS1 MOC cohort

A DCC managed one-off data update activity is proposed on the appropriate S1SP systems to replace the ‘incorrect’ Network Operator certificate with that of the ‘correct’ Network Operator certificate rather than each DNO having to manually change the certificates which requires signification effort and coordination among Network Operators.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
10/06/2021	0.1	Initial compilation
11/06/2021	0.2	Updated following DCC internal review
14/06/2021	0.3	Updated following further DCC internal review
12/07/2021	0.4	Updated following review from SECAS and the SECMOD Proposer
16/08/2021	0.5	Updated following review from the SECAS

2.2 Associated Documents

This document is associated with the following documents:

#	Title and Originator's Reference	Source	Issue Date
1	MP107-Modification-Report-v0.4	SECAS	23/11/2020
3	SECMP0107 CR1352 - PIA - S1 Validation 6151 v0.5	DCC	25/06/2020

2.3 Document Information

The Proposer for this Modification is Gemma Slaney from Western Power Distribution. Here are the timelines of this Modification.

January 2020	Proposal submitted
April 2020	Preliminary Impact Assessment (PIA) requested of DCC
June 2020	PIA submitted by DCC (DCC Change Request 1352)
November 2020	Full Impact Assessment (FIA) requested of DCC
June 2021	FIA submitted by DCC (DCC Change Request 4296)

Table 1:SECMP0107 Timeline

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 Current Arrangements

Critical Commands in Smart Metering Equipment Technical Specifications 2 (SMETS2) solution do not have any Registered Data Provider (RDP) validation and therefore in order to send Service Reference Variant (SRV) 6.15.1 - 'Update Security Credentials (KRP)' to update certificates on a device, the only requirement is that the Service Request (SR) sender is the owner of the certificate.

For SMETS1 devices, the Network Operator certificates are held by the SMETS1 Service Providers (S1SP). There is an additional RDP validation step to Service Requests including the SRV 6.15.1 used to update the Network Operator certificates. The DSP and S1SPs will validate these Critical Commands against the RDP data. If the user of the Service Request is not the owner of the Meter Point Administration Number (MPAN) for Electricity Smart Metering Equipment (ESME) or Meter Point Registration Number (MPRN) for GSME, that Service Request is rejected.

3.2 Problem Statements

During the enrolment phase of a SMETS1 Installation, a Network Operator Smart Meter Key Infrastructure (SMKI) Organisation certificate can be provided by:

- the Supplier via Migration Authorisation or via the response of Dormant Meter Migration Notification process,
- the DCC's Migration Control Centre Team for the SMETS1 ESME where the Supplier has not provided the Network Operator certificate, or
- the Supplier using SRV 6.21 where Network Operator certificate is not provided by any of the above methods.

If an incorrect Network Operator certificate is placed (stored at S1SP) in error, then the Network Operator cannot send a Critical SR including SRV 6.15.1 to the SMETS1 Device. This is currently enforced by the following validations:

#1 DSP performs RDP validation adhering to clause 6.1(f) of Smart Energy Code (SEC) Appendix AB - Service Request Processing Document (SRPD).

#2 S1SP performs RDP validation adhering to clause 16.1 of SRPD.

#3 S1SP validates the certificate owner with the Business Originator ID as per clause 4.2 of SEC Appendix AM - SMETS1 Supporting Requirements (S1SR).

This means that SRV 6.15.1, sent from the current Network Operator to update the incorrect certificate, is rejected due to validation #3 because the Business Originator ID of the SR does not match with the Entity Identifier of the certificate associated with the device.

SRV 6.15.1 from the Network Operator whose certificate was incorrectly associated with the device is also rejected because they fail the RDP checks as per validation #1 and #2.

In the equivalent situation on SMETS2 devices, the issue can be overcome by the Network Operator provided they have certificates on the device sending an SRV 6.15.1 because validation #1 is not applied. This is not blocked by the DSP since it is a Critical request and the device will accept matching certificates. This means that the "wrong" Network Operator can place the correct Network Operator's certificates on the SMETS2 device.

This is not possible for SMETS1 because RDP checks are required for all SRVs, including Critical SRs.

N.B. In this context Network Operator means both the Electricity and Gas Network Operators.

3.3 Business Requirements for this Modification

This section contains the considerations and assumptions for business requirement.

Req.	Requirement
1	Remove the additional Registered Data Provider validation step for Service Reference Variant (SRV) 6.15.1 'Update Security Credentials (KRP)' for SMETS1 Devices.
2	(Optional) DCC to undertake corrective action to fix the incorrect Network Operator's certificate(s) as one-off activity on the SMETS1 Device's virtual anchor slots.

Table 2: Business Requirements for SECMP0107, CR4296

3.3.1 Requirement 1

This requirement obligates the DCC to remove the additional Registered Data Provider validation step at the DSP and S1SPs for Service Reference Variant (SRV) 6.15.1 'Update Security Credentials (KRP)' targeted at SMETS1 Devices.

3.3.2 Optional Requirement 2

DCC voluntarily included an optional requirement to resolve the incorrect certificate data issues on LIVE environment should the impacted Parties wishes to.

This means, DCC to undertake corrective action to fix the incorrect' Network Operator's certificate(s) as one-off activity on the SMETS1 Device's virtual anchor slots (database at S1SP systems) in LIVE environment following the deployment of Requirement 1 if the impacted Parties deem it worthwhile to do so given the numbers of devices involved.

The rationale behind voluntarily including this optional requirement are:

- following the delivery of Requirement 1, 'incorrect' Network Operator need to place the 'correct' Network Operator certificates on SMETS1 device's virtual anchor slots. This approach is similar to SMETS2 and can be considered as enduring solution to fix any future incorrect Network Operator certificate issue. However, resolving the current incorrect certificate data issue requires signification effort and coordination among Network Operators.

- considering the numbers of impacted SMETS1 devices in LIVE environment, Network Operators may consider DCC managed single solution to fix all the current incorrect certificate data issue on behalf of all Network Operators.

3.4 Business Case

The Modification looks to address the following issue:

If an incorrect Network Operator certificate is placed on SMETS1 device in error, any attempt to replace the incorrect certificate by issuing SRV 6.15.1 by the Network Operator will be rejected.

In the equivalent situation on SMETS2 devices, the issue can be overcome by the Network Operator that has certificates on the device sending an SRV 6.15.1.

As provided by the Proposer and SECAS, the impact is currently low due to the way that SMETS1 Devices are enrolled to the DCC and the Network Operator certificates validated during enrolment, coupled with the fact that not all Network Operators are currently using Appendix AD ‘DCC User Interface Specification’ version 3.0/3.1 (DUIS 3). However, there is the potential that in the future the problem could become much larger.

DCC identifies the impact of incorrect Network Operator certificate is limited to SMETS1 ESME for alert routing.

This impacts the SEC Parties as follows:

Network Operators	1. Network Operator can follow SMETS2 process to correct certificate on SMETS1 Device on ongoing basis on ongoing basis if incorrect certificate is placed in error. 2. If Requirement 2 is not included in the scope, Network Operators need to take corrective action to update certificate on enrolled SMETS1 Devices with incorrect certificate.

In summary, this Modification would provide ability to resolve incorrect Network Operator certificate issues on SMETS1 Devices resulting in security improvement and more accurate alert routing to Network Operators.

4 Solution Overview

This Modification impacts the DSP and three S1SP component of the DCC Total System.

4.1 DSP Solution Overview

The DSP will be updated to remove the RDP check for SRV 6.15.1 where the sender is a Network Operator. RDP checks will remain for a SMETS1 6.15.1 from a Supplier or any other type of service user. This change does not affect SMETS2 SRV processing.

DSP will implement a single feature switch to enable the functionality covering all S1SPs. Therefore, the preference is for all S1SPs and DSP to deliver the change in a co-ordinated release to avoid inconsistent processing across S1SPs.

If the change isn't managed through a coordinated release, then a request could be allowed by the DSP but rejected by an S1SP (using the standard S1SP Alert mechanism). There will be no impact on the DCC Service Management System.

4.2 S1SP Solution Overview

4.2.1 Solution for Requirement 1

All three S1SPs will disable the RDP check for SRV 6.15.1, when sent from a Network Operator, to allow the 'incorrect' Network Operator to be able to place the 'correct' Network Operator certificates on device's virtual anchor slots.

This would then enable the 'correct' Network Operator to own and communicate with the meter as they are now the Known Remote Party (KRP) to the device.

Once this has happened, the 'incorrect' Network Operator will no longer be able to talk to the device or alter the certificates further as they will receive an S1VE64 error as their security credential is no longer on the device.

This RDP validation change (i.e. disable S1VE4) is only applicable to SRV 6.15.1 targeting the Network Operator Certificate when sent from a Network Operator (Electricity Distributor and Gas Transporter). Other SRVs as well as SRV 6.15.1 when sent from a Supplier are not impacted by this change.

4.2.2 Solution for Requirement 2

At the time of drafting this FIA, following are the numbers of SMETS1 Devices where the certificate in the Network Operator anchor slot belongs to a Network Operator who is **not** the registered owner of the device.

- **9024** ESMEs and **18905** GPFs in SMETS1 IOC cohort
- **125** ESMEs and **1226** GPFs in SMETS1 MOC cohort.
- No data available for FOC cohort yet due to very low number of enrolled devices at the time of this FIA.

DCC will run a one-off data update (Organisation Certificates are stored on S1SP system unlike SMETS2 devices) activity on appropriate S1SP systems to replace the 'incorrect' Network Operator certificate with that of the 'correct' Network Operator certificate. The correct Network Operator will be identified from RDP data and their certificates that are shared by Network Operator for SMETS1 Enrolment and available on SEC website (Engineering Recommendation M31).

This data update option is completely separate and independent from the solution of requirement 1 and have no impact to Service Users whilst running.

Following the deployment of core solution for requirement 1, DCC would agree a production run schedule with S1SPs prior to final change approval for this data update exercise.

To be clear, requirement 2 is optional and included in this Modification voluntarily to offer as one-off data update exercise option by the DCC instead of correcting the data by individual Network Operators if the impacted Parties deem it worthwhile to do so given the numbers of devices involved.

4.3 SEC Changes

The DCC and Service Providers have proposed the following legal text changes in the SEC Appendix AB - Service Request Processing Document for the requirement 1.

Clause 6.1(f) of the SRPD requires DCC (which, through clause 16.1, includes S1SP as well as DSP) shall check Registration Data for incoming SRVs. However, it says that the check is "subject to Clause 6.2" which lists exceptions. Suggested changes to Clause 6.2 are highlighted below:

SRPD Clause 6.2

The step set out at Clause 6.1(f) shall not apply in the following circumstances (and, where it is necessary to identify a Responsible Supplier, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory):

(a) *an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function;*
(b) *an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or*
(c) *the Service Request has been sent by a User acting in the User Role of 'Other User'.*
(d) *a SMETS1 Service Request with Service Reference Variant 6.15.1 (Update Security Credentials) received from an Electricity Distributor or Gas Transporter.*

No SEC changes required for optional requirement 2.

4.4 Deliverables

The deliverables of this Modification are described in the table below.

Phase Deliverables	Deliverable	Changes Required
Design	SD2.1.1 Functional Specification Instant Energy	Changes required due to change in validation for SRV 6.15.1
	SD4.1 DCC User Gateway Interface Design Specification	
	SD2.2.1.6 Component Design Spec – Security	
	Design Document for respective S1SP component	
PIT Completion	System Test and FAT Completion Report	To be created

4.5 Impact on DSP Component

The following sub-systems and components of the DSP are impacted by this change.

4.5.1 Request Management (Security)

RDP checks will be updated so that checks are not applicable to SRV6.15.1 issued to update the Network Operator Certificate if the sender is a Network Operator and the target is a SMETS1 Device.

4.6 Impact on S1SP Components

4.6.1 S1SP Validation

RDP checks will be removed so that checks are not applicable to SRV6.15.1 issued to update the Network Operator Certificate if the sender is a Network Operator.

5 Testing Considerations

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

5.1 Pre-Integration Testing

5.1.1 DSP and S1SPs for Requirement 1

Pre-Integration Testing (PIT) will be required to align DSP and S1SPs functionality of requirement 1 and the functionality described above. The PIT phase of implementation will be subject to standard test phases and level of DCC assurance as defined in previous releases. Specifically, the development team will carry out unit testing and the build will be subject to continuous build and automated testing to identify build issues at the earliest opportunity. The implementation team will carry out system testing consisting of positive and negative path testing which will culminate in a short period of Factory Acceptance Testing (FAT), witnessed by DCC test assurance at DSP offices. The FAT tests will be a subset of System Tests.

Acceptance will be defined by:

1. An agreed set of design documentation.
2. DCC approving the Factory Acceptance Testing outcome in accordance with pre-agreed criteria, which shall not be unreasonably delayed or withheld.
3. Meeting Schedule 6.2 PIT exit criteria.
4. Approval for a MAC to be issued will be authorised by DCC's Test Assurance Board.

5.1.2 S1SPs for Requirement 2

If requirement 2 is approved by the stakeholders to be included in scope, Pre-Integration Testing (PIT) will be required to check that the functionality described above can be executed independently as a database script.

Acceptance will be defined by for both Requirement 1 and Requirement 2:

1. Relevant PIT testing results are precisely captured and shared with DCC.
2. DCC Test assurance reviews and approves the PIT testing results for SIT entry.

5.2 System Integration Testing and User Integration Testing

The complexity of integration testing is low. The SIT and UIT test approach for SECMP0107 will be to send SRV6.21 to DCC enrolled devices that forms part of an installation of a migrated device set, with the incorrect certificate for User Role “Network Operator”. Thereafter, to execute SRV6.15.1 by the Network Operator owning the current certificate can associate the correct certificate on the device. This will verify the RDP check is not being applied.

This test should be executed for each S1SP. If the S1SP has not implemented the change, and DSP has, DCC expect SRV 6.15.1 to be rejected by the S1SP for Service User role of Network Operator.

A new negative scenario and test script will verify where a SRV 6.15.1 is processed where the incorrect Service User Role of “Supplier” or any other role other than Network Operator is used as the SU to process the SRV therefore the SRV will be rejected by DSP.

If requirement 2 is approved by the stakeholders to be included in scope, the System Integration effort will be required to ensure the data update scripts specific to individual S1SPs are tested by as part of System Integration Testing.

6 Implementation Timescales and Releases

This Modification was expected to be included in a SEC release in November 2022. 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 **six 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 (functional changes only), aligned with Release Dates	2 Months
Transition to Operations and Go Live	D + 6 Months

6.2 SEC Release Allocation and Other Code Impacts

The allocation to any release may be dependent on other Modification timings and the suitability of a release. No functionality overlaps with other Modifications has been identified.

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 standalone release of just this SEC Modification without any other Modifications or Change Requests in the release, which is not truly reflective of what the 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	PIT	SIT	UIT	TTO	SP Total
Phase Total for Requirement 1 (core solution)	32,281	63,579	51,333	48,001	13,682		**208,876**
Phase total for Requirement 2 (**optional** data update activity by DCC for S1SP 1, S1SP2 and S1SP 3)	38,550			6,686			**45,236**

Please note, System Integrator’s costs are not fully factored in and they might increase as part of the Release cost.

As part of the DCC negotiation with the DSP regarding the Contract Extension, some charges may be reduced for post-PIT phases. The negotiation is expected to be completed in October 2021.

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.

6.3.1 Application Support Costs

This change will not result in a material increase in application support required.

6.4 Impact on Contracts and Schedules

At a minimum, the following schedules will be updated as a result of the changes introduced by this Modification:

- Schedule 4.1 - to reflect solution changes
- Schedule 6.1 - to reflect delivery milestones
- Schedule 7.1 - to reflect payment milestones under this 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.

6.5 Risks

Ref	Description	Status/Mitigation
MP107-R1	If the release of this change is not coordinated across the DSP and all S1SPs under a single SEC release, it may lead to additional time and cost to deliver the CR in multiple releases.	Accepted

6.6 Assumptions

These assumptions have been used in the creation of this Full Impact Assessment. 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
MP107-A1	SECMP0107 will be included in the November 2022 SEC Release. The price breakdown, and work start-date is based on November 2022 Release.	Accepted
MP107-A2	This change does not materially increase processing, data storage or data exchange within the DSP and S1SP solution. As such, it is assumed the change on its own does not warrant the procurement of additional infrastructure.	Accepted
MP107-03	For Requirement 2, S1SP3 cost is included for completeness by averaging the cost of other 2 S1SPs. If no incorrect certificate data is identified related to S1SP 3, this cost will be removed. See Annex document for details.	Accepted

6.7 Issues

None at this time.

6.8 Dependencies

None at this time.

Appendix B: Glossary

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

Acronym	Definition
CAN	Contract Amendment Note
CR	DCC Change Request
DCC	Data Communications Company
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FAT	Factory Acceptance Testing
FIA	Full Impact Assessment
FOC	Final Operating Capability
GPF	Gas Proxy Function
GSME	Gas Smart Metering Equipment
IOC	Initial Operating Capability
KRP	Known Remote Party
MOC	Middle Operating Capability
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
RAID	Risks, Assumptions, Issues, and Dependencies
RDP	Registration Data Provider
SAT	Service Audit Trail database in the DSP
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SMIP	The Smart Meter Implementation Programme
SP	Service Provider
SR	Service Request
SRV	Service Request Variant
UIT	User Integration Testing
UTS	User Testing Services