

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Smart Energy Code

MP107 'SMETS1 Validation of SRV 6.15.1'

Modification Report

Version 0.4

18 November 2020

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	4
4. Impacts	5
5. Costs	6
6. Implementation approach	7
7. Assessment of the proposal	7
Appendix 1: Progression timetable	9
Appendix 2: Glossary	10

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the full Data Communications Company (DCC) Preliminary Assessment response.
- **Annex D** contains the full response received to the Refinement Consultation.

Contact

If you have any questions on this modification, please contact:

Khaleda Hussain

020 7770 6719

Khaleda.Hussain@gemserv.com

1. Summary

This proposal has been raised by Gemma Slaney from Western Power Distribution (WPD).

To send a Critical Command to a Smart Metering Equipment Technical Specification (SMETS) 1 Device, the User must be the owner of the relevant Certificate on the Device and the owner of the Device in the Registered Data Provider (RDP) data. The Certificates are held by proxy (not on the Device) by the SMETS1 Service Provider (S1SP). The Data Service Provider (DSP) and S1SP will perform the additional validation against the RDP data when a Critical Command is sent to a SMETS1 Device.

If an incorrect Network Operator Certificate is placed on a SMETS1 Device in error, the correct Certificate cannot be sent to replace the incorrect one. This is because the Service Request to update the Certificate (Service Reference Variant (SRV) 6.15.1) is a Critical Command, therefore it will be rejected if:

- The Device owner sends SRV 6.15.1 as they are not the owner of the (incorrect) Network Operator Certificate; and
- The owner of the (incorrect) Network Operator Certificate sends SRV 6.15.1 as they are not the owner of the Device as validated using the RDP data.

The solution is to remove the DSP 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 in future. This is a SMETS1-only SRV and is not carried out for SMETS2 Critical Service Requests.

The S1SP system will also be updated to remove the RDP check for SRV 6.15.1 specifically where it targets Network Operator certificates. The existing RDP checks will remain for all other SRVs; and will remain for an SRV 6.15.1 that targets Supplier certificates.

This modification will impact the DCC and Network Operator Parties. It will cost around £200,000 and take around three months to progress up to the end of Pre-Integration Testing (PIT); costs and timescales for the subsequent implementation stages will be confirmed during Impact Assessment. SECAS is recommending this is a Self-Governance Modification and, if approved, implemented in the June 2022 SEC Release.

2. Issue

What are the current arrangements?

Critical Commands in SMETS2 do not have any RDP validation. Therefore in order to send Service Reference Variant (SRV) 6.15.1 'Update Security Credentials (KRP)' to update the Certificates on a Device, the only requirement is that the sender is the owner of the Certificate.

For SMETS1 Devices, the Network Operator Certificates are held by proxy within the S1SP and there is an additional RDP validation step to Service Requests including the Service Request used to update the Network Operator Certificates. The DSP will validate these Critical Commands against the RDP data. If the sender is not the owner of the Meter Point Administration Number (MPAN) their request is rejected.

What is the issue?

If an incorrect Network Operator Certificate is placed on a Device (stored in the S1SP) in error, the correct Certificates cannot be sent to replace the incorrect one. If the owner of the Certificates tries to send the correct Network Operator Certificates, their request would be rejected as they are not the Network Operator for that MPAN.

There is the potential that a Network Operator (the correct Network Operator, according to the RDP data, and the owner of the Certificates currently associated with the meter) could send another Network Operator's Certificates to be stored in the S1SP. The Service Request sent in order to do this would be accepted and the Certificates updated. However, if this were to happen there is currently no mechanism for either Network Operator involved to correct the Certificates due to the RDP validation.

The additional validation on SMETS1 Critical Service Requests are defined in SEC Appendix AB 'Service Request Processing Document' (SRPD) section 6.1:

- (f) *subject to Clause 6.2, in the case of Non-Critical Service Requests and SMETS1 Critical Service Requests, confirm (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) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request:*
 - (i) *for all times within any date range requested.*
 - (ii) *where there is no such date range, at the specified time for execution; or*
 - (iii) *where there is no date range and no date for execution is specified, at the time at which the check is being carried out.*

This has been raised at the Technical and Business Design Group (TBDG) Enrolment and Adoption (E&A) Subgroup and discussion had with the DCC. It was agreed to raise this as a SEC Modification.

What is the impact this is having?

The impact is currently low due to the way that SMETS1 Devices are migrated and the Network Operator Certificates validated on migration, coupled with the fact that not all Network Operators are currently using SEC 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.

For SMETS2 Devices, if the incorrect Network Operator Certificates are placed on the Device, the owner of the Certificate can currently send the relevant Service Request to the Device to correct the Certificates. SMETS2 Devices are therefore not affected by this issue.

3. Solution

Proposed Solution

The solution seeks to remove the additional Registered Data Provider validation step at the DSP for Service Reference Variant (SRV) 6.15.1 'Update Security Credentials (KRP)'.

The DCC confirms the S1SP system will be updated to remove the RDP check SRV 6.16.1 specifically where it targets Network Operator certificates. The existing RDP checks will remain for all other SRVs; and will remain for an SRV 6.15.1 that targets Supplier certificates.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
	Other SEC Parties	✓	DCC

Electricity Network Operators and Gas Network Operators are impacted as SRV 6.15.1 RDP validation from Network Operators will be updated at DSP and all S1SP systems.

DCC System

The DCC confirms the implementation will be security assured during the implementation phase. This will include 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 DCC Impact Assessment. Regarding any impacts on Technical Specification the DCC confirms there will be no changes to the DUIS, the GB Companion Specification (GBCS) or any other Technical Specification apart from proposed changes to the SRPD.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex C.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AB 'Service Request Processing Document'

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

Consumers

Consumers would benefit from the Modification as it would allow Smart Metering system to be updated by the correct Network Operator. The impact on consumers from the incorrect certificated would mean a negative experience from Suppliers as the only fix in correcting the issue would be for Supplier to conduct a site visit and manually swap out the meter.

Other industry Codes

There are no impacts on other industry Codes from this modification.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions from this modification.

5. Costs

DCC costs

The estimated DCC implementation costs up to the end of PIT to implement this modification is £193,125. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build and Pre-Integration Testing (PIT)	£193,125
Systems Integration Testing (SIT)	N/A
User Integration Testing (UIT)	N/A
Implement to Live	N/A
Application Support	N/A

The estimated standalone costs for SIT, UIT and Implement to Live will be assessed as part of the DCC Impact Assessment.

More information can be found in the DCC Preliminary Assessment response in Annex C.

SECAS costs

The estimated Smart Energy Code Administrator and Secretariat (SECAS) implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

The majority of Refinement Consultation respondents advised they would not incur any costs in implementing MP107. However, one respondent requested for quantitative analysis to be included in the consultation before they could answer if their organisation would incur any costs in implementing MP107.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **30 June 2022** (June 2022 SEC Release) if a decision is received on or before 30 September 2021.
- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received after 30 September 2021 but on or before 3 February 2022.

The DCC has provided an estimated lead time of three months up to the end of PIT to develop the DSP and S1SP changes. A further six months has then been allowed for the post-PIT stages. As this requires a DCC System change (but no change to the Technical Specifications or the DUIS) the first possible SEC Release it could be included in is the June 2022 SEC Release.

7. Assessment of the proposal

Observations on the issue

Views of the Change Sub-Committee

Change Sub-Committee (CSC) members agreed the impact of this issue is currently low. As this is the case, the CSC wanted to have a cost benefit analysis performed on this Proposal. The Preliminary Assessment identified the cost and as part of the Refinement Consultation it was requested to provide details of any benefits or disadvantages and any associated costs.

Currently no meters are impacted. However, the Proposer believes there could be a potential issue in the future for all SMETS1 Devices which would have the incorrect Network Operator certificate on them due to the additional step added to the SMETS1 infrastructure which is different to SMETS2 Devices. The Proposer added once the Device has migrated the incorrect certificate and if a Service Reference Variant (SRV) is attempted, there is an additional validation in place for SMETS1 Devices which cannot be corrected by any party. Resources will be impacted if the issue is not fixed as it would require a site visit by a Supplier to manually swap out the meter which would cause negative experience for consumers.

Solution development

The proposed solution presented to the Working Group was to remove the additional Registered Data Provider validation step at the DSP for Service Reference Variant (SRV) 6.15.1 'Update Security Credentials (KRP)'. The Working Group members supported the solution idea for the validation of SMETS1 SRV 6.15.1 to be updated and to remove the Registered Data Provider validation check specifically when it targets Network Operator certificates.

Support for Change

Working Group views

The Working Group members agreed the issue was clear and should progress further. SECAS presented the findings of the DCC Preliminary Assessment which included the cost for delivering the changes and services required to implement this modification expected to cost £193,125 and a full DCC Impact Assessment to cost £22,596.58 with a duration of 30 days. The Working Group members noted the DCC Preliminary Assessment findings and supported the cost and implementation time.

Business case

Proposer's views

The Proposer has advised at this moment, fortunately, no meters are impacted. However, if the issue did occur, the only way to fix the problem would be through a site visit by a Supplier to manually swap out the meter. This would cause resource impacts on Suppliers and a negative experience for consumers.

Party feedback

Noting the costs and benefits of this modification, three respondents to the Refinement Consultation believed this modification should be approved.

One Large Supplier who believed MP107 should not be approved added, while they agreed with the principles of the change, they believed there was no evidence the benefits to Network Operators of making this change would outweigh the costs.

Views against the General SEC Objectives

Proposer's views

SEC Objective (a)¹

The Proposer believes this Modification better facilitates SEC Objective (a) by ensuring smart metering systems can be operated by the correct Network Operator.

SEC Objective (c)²

The Proposer believes this Modification better facilitates SEC Objective (c) by ensuring that the information from the smart metering systems is provided to the correct Network Operator.

¹ Facilitate the efficient provision, installation, operation, and interoperability of smart metering system at energy consumers premises within Great Britain.

² Facilitate energy consumers management of their use of electricity and gas through the provision of appropriate information via smart metering systems.

Industry views

Five responses were received from the Refinement Consultation. Three Large Suppliers agreed the modification would better facilitate SEC Objective (a), as it would allow Smart Metering system to be updated by the correct Network Operator, and SEC Objective (c), as it would allow information from the Smart Metering systems to be sent to the correct Network Operator. One Network Party supported the Modification stating the Modification better facilitates SEC Objective (a) and (c). One Network Party questioned the lack of clarity to the actual scale of the problem within the consultation and requested for further information from the Proposer.

Appendix 1: Progression timetable

This Modification will be presented to the Change Board for a DCC Impact Assessment request. The DCC Impact Assessment findings will then be presented to the Working Group for discussion before the Modification Report is presented to the Panel.

Timetable	
Action	Date
Draft Proposal raised	13 Jan 2020
Presented to CSC for initial comment	28 Jan 2020
Initial comments from SEC Parties	20 Jan 2020
Presented to CSC for final comment and recommendations	25 Feb 2020
Panel converts Draft Proposal to Modification Proposal	13 Mar 2020
Preliminary Assessment requested	20 Apr 2020
Preliminary Assessment returned	25 Jun 2020
Modification discussed with Working Group	5 Aug 2020
Refinement Consultation	14 Sep 2020 – 3 Oct 2020
Business Case analysis	5 Oct – 14 Oct 2020
Request DCC Impact Assessment from Change Board	25 Nov 2020
Impact Assessment requested	26 Nov 2020
Impact Assessment returned	13 Jan 2021
Modification discussed with Working Group	3 Feb 2021
Modification Report presented to Panel	12 Mar 2021

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
CSC	Change Sub-Committee
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
DUIS	DCC User Interface Specification
E&A	Enrolment and Adoption
MPAN	Meter Point Administration Number
PIT	Pre-integration Testing
RDP	Registered Data Provider
S1SP	SMETS1 Service Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Technical Specifications
SRPD	Service Request Processing Document
SRV	Service Reference Variant
TBDG	Technical and Business Design Group