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 0.2

17 August 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

This document also has two 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.

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.

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 by the SMETS1 Service Provider (S1SP), where 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 implement. We are recommending this is a Self-Governance Modification and, if approved, implementation in the June 2021 SEC Release.

2. Issue

What are the current arrangements?

Critical Commands in SMETS2 do not have any RDP validation and 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 you are not the owner of the Meter Point Administration Number (MPAN) your 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 and it was agreed to raise 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 would be able to send the relevant Service Request to the Device to correct the Certificates.

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)'. DCC confirm 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

There is no impact on DCC systems in this modification.

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

There are no impacts on Consumers in this Modification.

Other industry Codes

There are no impacts on other industry codes in this Modification.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions in this Modification.

5. Costs

DCC costs

The estimated DCC implementation costs 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

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

SECAS costs

The estimated SECAS implementation costs to implement this modification is 2 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.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **24 June 2021** (June 2021 SEC Release) if a decision to approve is received on or before 24 March 2021; or
- **4 November 2021** (November 2021 SEC Release) if a decision to approve is received after 24 March 2021 but on or before 4 August 2021.

As this requires a DCC System change (but no change to the Technical Specifications or DCC User Interface Specification (DUIS)) the first possible SEC Release it could be included in is the June 2021 SEC Release.

7. Assessment of the proposal

Observations on the issue

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 has identified the cost and as part of this Refinement Consultation we ask that you provide details of any benefits or disadvantages and costs associated with these.

Views against the General SEC Objectives

Proposer's views

SEC Objective (a)[1]

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

Appendix 1: Progression timetable

Following this Refinement Consultation, the business case will be assessed, and we will liaise with the Proposer on the next steps.

Timetable	
Action	**Date**
Initial comments from SEC Parties	20 January 2020
Taken to CSC for decision	25 February 2020
Panel convert Draft Proposal to Modification Proposal	13 March 2020
Request DCC Preliminary Assessment	30 March 2020
Modification discussed with Working Group	5 August 2020
Refinement Consultation	14 September – 3 October 2020
Business Case analysis	5 October – 14 October 2020

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**
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
DUIS	DCC User Interface Specification

[1] Facilitate the efficient provision, installation, operation and interoperability of smart metering systems 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.

Glossary	
Acronym	**Full term**
E&A	Enrolment and Adoption
MPAN	Meter Point Administration Number
RDP	Registered Data Provider
S1SP	SMETS1 Service Provider
SEC	Smart Energy Code
SMETS	Smart Metering Technical Specifications
SRPD	Service Request Processing Document
SRV	Service Reference Variant
TBDG	Technical and Business Design Group