DP107

‘SMETS1 Validation of SRV 6.15.1’

Modification Report

Version 0.1

About this document

This document is a draft Modification Report. It currently sets out the background, issue, 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 4

Appendix 1: Progression timetable 6

Appendix 2: Glossary 7

Contact

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

Jordan Crase

020 3574 8863

jordan.crase@gemserv.com

1. Summary

This Draft Proposal was raised by Gemma Slaney of Western Power Distribution.

To send a Critical Command to a Smart Metering Equipment Technical Specification 1 (SMETS1) 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 Data Service Provider (DSP) and the SMETS1 Service Provider (S1SP), where the DSP 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 by proxy on a SMETS1 Device in error, the correct certificates cannot be sent to replace the incorrect one. This is as 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 (wrong) Network Operator Certificate; and
- The owner of the (wrong) Network Operator Certificate sends SRV 6.15.1 as they are not the owner of the Device as validated using the RDP data.

2. Issue

What are the current arrangements?

Critical Commands in Smart Metering Equipment Technical Specifications 2 (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 DSP and 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 by proxy on a Device (stored in the S1SP and the DSP) 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 DSP and 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 Smart Energy Code (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 Data Communication Company (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.

Appendix 1: Progression timetable

This Proposal will go to the Change Sub-Committee (CSC) for initial discussion. It is then expected that it will be taken to the SEC Sub-Committees to comment before returning to the CSC.

Timetable	
Action	**Date**
Initial comments from SEC Parties	W/B 20 Jan 2020
Taken to CSC for decision	25 Feb 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
E&A	Enrolment and Adoption
MPAN	Meter Point Administration Number
RDP	Registered Data Provider
S1SP	SMETS1 Service Provider
SEC	Smart Energy Code
SMETS1	Smart Metering Technical Specifications 1
SMETS2	Smart Metering Technical Specifications 2
SRPD	Service Request Processing Document
SRV	Service Reference Variant
TBDG	Technical and Business Design Group