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.

MP141

‘SRV Visibility for Devices on SSI’

Modification Report

Version 0.4

8 January 2021

Corporate member of Plain English Campaign
Committed to clearer communication
592

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 3
3. Solution 4
4. Assessment of the proposal 4

Appendix 1: Progression timetable 5

Appendix 2: Glossary 5

Contact

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

Harry Jones

020 7081 3345

harry.jones@gemserv.com

1. Summary

This proposal has been raised by Clive Hallam from the Data Communications Company (DCC).

Supplier Parties are currently unable to view Service Request Variants (SRVs) or Service Responses from other Service Users that they receive on their Devices. This is due to an obligation in the Smart Energy Code (SEC) that states only an individual User can view the SRVs and Service Responses they send or receive. This therefore leads to SRVs and Service Responses being received by Users without visibility or information of the triggering requests, which is causing issues where they may be high priority or have security implications.

The Proposed Solution is to allow Supplier Parties and Network Operators to view all the titles of SRVs and Service Responses that have been associated with a Device that they own.

2. Issue

What are the current arrangements?

Supplier Parties receive SRVs and Service Responses for Devices they own. However, only the individual User who currently owns that Device can access these SRVs and Service Responses. This means that SRVs and Service Responses sent by other Users can't be viewed if they are sent to a Device they own, regardless of the payload or significance of the SRV/Response.

What is the issue?

Supplier stated in the Technical Specification Issue Resolution Subgroup (TSIRS) forum that it would be desirable to be able to view all the SRVs and Service Responses that are sent to a meter they own. Supplier Parties have raised the issue that they will receive Alerts based on SRVs sent by other Service Users to their meters. Currently, they have no visibility of this activity through the Service Audit Trail (SAT) data they have access to. They need to know which SRVs have been sent by a Service User to their meters so that they can make an informed decision of whether to ignore or action the Alerts they receive.

SEC Section H8 'DCC Services' details the requirements which the Self Service Interface (SSI) follows, which will need to be amended. This is found in Sections H8.15-H8.18, where H8.16(b) states the SSI must (as a minimum) allow:

> "*a record of the Service Requests and Signed Pre-Commands sent by each User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to that User*".

Therefore, a change is required to alter the SSI and to provide the SAT information for all SRVs and Service Responses to or from any meter a User owns.

What is the impact this is having?

The current lack of visibility and information for SRVs and Service Responses means Supplier Parties are receiving security related Alerts with no accompanying information or rationale.

3. Solution

Proposed Solution

The Proposed Solution is to allow Supplier Parties and Network Operators to view all the titles of SRVs and Service Responses that have been associated with a Device that they own. By allowing this functionality, it will allow a Network Operator or a Responsible Supplier of a Device to check the Device for any SRVs or Service Responses that need to be actioned, or will assist for the purpose of auditing. The Devices that will be affected by this Proposed Solution will be any Device connected to the Home Area Network (HAN).

The Proposed Solution will ensure that only the SAT data is used for viewing any SRVs or Service Responses. This is so that any confidential data will remain undisclosed during any such audits or during a business process of checking for SRVs or Services Responses that need to be actioned from when the Device was owned by a previous Supplier prior to CoS.

4. Assessment of the proposal

Observations on the issue

The Change Sub Committee (CSC) agreed this is an issue. One CSC member stated that they wanted to see the scope extended in the Refinement Process so that it would consider the views of Network Parties and Other SEC Parties, not just Supplier Parties as originally outlined. SECAS agreed this would form part of the discussions in the Refinement Process if converted to a Modification Proposal.

The other Panel Sub Committees had the following views to give on the Modification Proposal:

TABASC

The Technical Architecture and Business Architecture Sub Committee (TABASC) agreed that it would like to be kept updated on the progress of this Proposal. The rationale was that Service Requests/ Responses, due to Change of Supplier (CoS) events, could be withheld from current Users. Additionally, a member raised that questions over a User's ability to look at Service Requests/ Responses from competitors and this would need investigating if the proposal is taken to the Refinement Process.

Operations Group

The Operations Group confirmed its interest in the Draft Proposal. One member stated that any solution created must not allow the payload of these Service Requests/Responses to be viewed as it

may constitute a breach of security and the General Data Protection Regulation (GDPR). Another member questioned the effectiveness of any solution which wouldn't allow a User to view the payload of the Service Request/Response.

Appendix 1: Progression timetable

The Panel agreed on 16 October 2020 to convert the Draft Proposal into a Modification Proposal and entered the Refinement Process. The business requirements have been discussed with the Proposer and the Working Group before being taken to the TABASC for input. Following comments received from the TABASC in January 2021, it was decided that the business requirements will be discussed at an upcoming Requirements Workshop. Following the outcomes of this workshop, it will be returned to the TABASC for decision before requesting the Preliminary Assessment.

Timetable	
Event/Action	**Date**
Draft Proposal raised	20 Aug 2020
Presented to CSC for initial comment	25 Aug 2020
Sub Committee input given	1 Sep 2020 – 9 Sep 2020
Presented to CSC for final comment and recommendation	29 Sep 2020
Presented to Panel for conversion to Modification Proposal	16 Oct 2020
Discuss Business Requirements with the Proposer	19 Oct 2020 – 23 Oct 2020
Discuss Business Requirements at Working Group	4 Nov 2020
Presented at TABASC meeting	5 Nov 2020
Presented at TABASC meeting	7 Jan 2021
Take to Requirements Workshop	25 Jan 2021
Present at TABASC meeting	4 Mar 2021
Request Preliminary Assessment	5 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
CoS	Change of Supplier
DCC	Data Communications Company
GDPR	General Data Protection Regulation
HAN	Home Area Network

Glossary	
Acronym	**Full term**
SAT	Service Audit Trail
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SRV	Service Request Variant
SSC	Security Sub Committee
SSI	Self Service Interface
TABASC	Technical Architecture and Business Architecture Sub Committee
TSIRS	Technical Specification Issue Resolution Subgroup