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.

DP141

'SRV Visibility for Devices on SSI'

Modification Report

Version 0.2

22 September 2020

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

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 which lack visibility or information, which is causing issues where they may be high priority or have security implications.

2. Issue

What are the current arrangements?

Supplier Parties receive SRVs and Service Responses for Devices they own. However, only the individual User who 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 Parties 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 off 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.

Supplier Parties have acknowledged that it will not be possible to view the payload of these SRVs and Service Responses. Therefore, a change has been requested to alter the Self Service Interface (SSI) and to provide the SAT information for all SRVs and Service Responses to or from any meter a User owns.

SEC Section H8 'DCC Services' details the requirements which the SSI follows, which will need to be amended. This is found in Sections H8.15-H8.18, where H8.16(b) states the following:

> "*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*".

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. Assessment of the proposal

Observations on the issue

When the Draft Proposal was initially taken to the Change Sub Committee (CSC), the members present took note of it and agreed this would be an issue. They noted that further detail and input would be required before proceeding to recommend conversion to a Modification Proposal.

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

TABASC

The Technical Architecture and Business Architecture Sub Committee (TABASC) reviewed the Draft Proposal and agreed that it would be of interest to it. Its rationale was that it raises the issue of Service Requests/Responses that, due to Change of Supplier (CoS) events, could be withheld from current Users. Additionally, a member raised that questions would be had over a User's ability to look at Service Requests/Responses from competitors and it needs investigating if the proposal is taken to the Refinement Process.

Operations Group

The Operations Group stated its interest in the Draft Proposal. One member stated that any solution created wouldn't 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 Draft Proposal was raised at the CSC on 25 August 2020 for initial comment. It was then taken to the Operations Group, the SSC and the TABASC for further analysis. It is being returned to the CSC on 29 September 2020 for recommendation on the way forward. SECAS is recommending the Draft Proposal is ready for conversion to a Modification Proposal and sent to the Refinement Process so a solution can be developed.

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

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
SAT	Service Audit Trail
SEC	Smart Energy Code
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