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 1.0

22 December 2021

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

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

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 10

Appendix 2: Glossary 10

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex C** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex D** contains the full responses 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 Modification Proposal has been raised by Clive Hallam from the DCC.

Supplier Parties are currently unable to view Service Request Variants (SRVs) or Service Responses which originate from other Service Users that they receive relating to Devices for which they are the Responsible Supplier. 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 the responses 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 all SRVs and Service Responses that have been associated with a Device for which they are the Responsible Supplier or Relevant Network Party. This will allow the User to action the affected SRVs or Service Responses and aid them in investigating the erratic behaviour of the affected Devices.

This modification will affect Suppliers, Network Parties, and the DCC. The total cost to implement the change is £199,839, with a further application support cost (early life support) of £8,346 for a period of two months after the solution is implemented. If approved this modification will be implemented in the November 2022 SEC Release. This is a Self-Governance Modification.

2. Issue

What are the current arrangements?

Supplier Parties receive SRVs and Service Responses for Devices they own (for which they are the Responsible Supplier). However, Supplier Parties are currently unable to view any information around the SRVs or Service Responses submitted by other Service Users on their Devices, even though they may receive Alerts in response to those requests. The other Users in question may be sending SRVs or Service Responses concerning firmware updates or trying to connect Devices on the network the Device is part of.

What is the issue?

A 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 for which they are the Responsible Supplier. Supplier Parties 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 (such as the Relevant Network Party) to the 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 for which a User is the Responsible Supplier or Relevant Network Operator.

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.

Impact on consumers

Currently Suppliers and Distribution Network Parties receive Alerts that are may have been triggered by Parties other than themselves. This means they are unaware of any issues that are being investigated that may be affecting their customer.

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 for which they are the Relevant Supplier or is on their Network. 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 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 (such as the identity of the sender or the contents of the request or response) 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 Change of Supplier (CoS). It will also allow the User to investigate any erratic behaviour from Devices that are showing more activity than usual. From there, a User will be able to diagnose the issue with the affected Device and remediate the issue faster than they would without this information.

The full set of business requirements used for this solution can be found in Annex A and the proposed redlined changes to deliver the solution can be found in Annex C. The Proposed Solution is option 2 within the business requirements.

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

All Supplier Parties and all Network Parties will be positively impacted by the Modification Proposal. The Proposed Solution will allow the User to access the full list of SRVs and Service Responses a Device has either sent or received. By allowing Users to have access to the titles of each SRV or Service Request, it will provide more information to help the User in investigating erratic Device behaviour and remedy any issues with the Device.

Respondents to the Refinement Consultation confirmed there are no SEC Party changes expected.

DCC System

The DCC Systems change are limited only to Self Service Interface (SSI) changes. The DCC will modify the SSI to allow the Responsible Supplier and Relevant Network Party to view the titles of SRVs and Service Responses associated with a Device they are responsible for.

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

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section H 'DCC Services'

The changes to the SEC required to deliver the Proposed Solution can be found in Annex C.

Technical specification versions

There are no changes to any of the Technical Specifications.

Consumers

This change will benefit consumers as there will be improved query resolution and dispute management processes. It will also reduce site visits and delays in dealing with issues and problems.

Other industry Codes

No other industry Codes are impacted by this proposal.

Greenhouse gas emissions

This proposal will have no effects on greenhouse gas emissions

5. Costs

DCC costs

The total cost to the DCC to implement is the Proposed Solution £199,839. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£124,301
System integration testing (SIT) and User Integration Testing (UIT)	£68,967
Implement to Live	£6,571

There is an Application Support cost which has been calculated for a period of two months after the solution has been implemented and are referred to as Early Life Support.

Breakdown of Application Support cost	
Activity	**Cost**
Early Life Support	£8,346

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

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. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

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

SEC Party costs

SEC Parties were asked to provide this as part of the Refinement Consultation. All respondents confirmed that they did not expect any costs to be incurred as a result of this change.

The full response to the Refinement Consultation can be found in Annex D.

6. Implementation approach

Agreed implementation approach

The Change Sub-Committee (CSC) agreed an implementation date of:

- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received on or before 3 February 2022; or
- **29 June 2023** (June 2023 SEC Release) if a decision to approve is received after 3 February 2022 but on or before 29 September 2023.

The earliest SEC Release this modification could be implemented in is the November 2022 SEC Release.

7. Assessment of the proposal

Observations on the issue

The views of the Panel Sub-Committees were sought during the Development Stage. 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 Draft Proposal:

Views of the 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 and Responses, due to CoS events, could be withheld from current Users. Additionally, a member stated that questions over a User's ability to look at Service Requests and Responses from competitors and this would need investigating.

Views of the 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 or 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 or Response. SECAS confirmed after consulting with the Security Sub Committee (SSC) about what data was being used (specifically, the SAT data to access the titles of SRVs and Service Responses rather than data payload), the Proposed Solution would not cause

security breaches or contravene the GDPR. SECAS believed that the Proposed Solution would have utility even if it can't access a SRV or Service Response payload, citing Working Group responses where members believe that just the SAT data would be beneficial for investigations.

Solution development

When asked about how they would benefit from the Proposed Solution, the Working Group members believe there is more of a use case for the Proposed Solution in investigating erratic behaviour from Devices they are responsible for, rather than actioning previous SRVs or Service Responses on Devices acquired through CoS. The Working Group stated that there would be additional benefits that would be realised if the Proposed Solution was implemented, such as investigations being completed, and decisions made at a faster rate than current.

The Working Group was asked about whether the Proposed Solution should only consist of Requirement 1 in the business requirements to reduce costs (i.e. not extended to Network Parties). Some members believed that there wasn't a clear case for Network Parties also having this access. The Working Group members rejected this. Members believed that if Requirement 2 would add little cost, this should be included it if it provides a benefit to the Network Parties. The DCC's Impact Assessment noted there would be an incremental cost of around £41,000 to include Requirement 2 (Option B) compared to delivering just Requirement 1 (Option A).

In the Refinement Process SECAS asked the Working Group if there was a preferred solution option to progress the modification forward with. The Working Group members confirmed they wished to progress with is the option to allow the Responsible Supplier and the Relevant Network Operator to see all SRVs and Service Responses sent by all Users to a Device. On nomenclature, the Woking Group suggested and agreed 'Responsible Supplier' and 'Relevant Network Party' should be used for clarity instead of 'owner', and this has been reflected as a footnote into the business requirements. The DCC confirmed this would not impact the solution.

SECAS presented the outcomes of the Impact Assessment, including reported costs for both Options A and B. SECAS highlighted the Working Group had opted to progress Option B. The TABASC remarked that costs were higher than initially expected but the benefits of implementing it made sense given the extra changes required to provide network operators visibility were good value for money and could be met in the same lead time. The TABASC requested that that this change would also need to be reflected via an update to the Business Architecture Document (BAD). Overall, the TABASC supported the modification progressing under Option B. The CSC agreed the modification should be progressed to the Report Phase.

Support for Change

The Working Group was supportive of this change as the ability to view this information would assist Parties in resolving consumers' issues.

Five out of six Refinement Consultation respondents were supportive, again believing that understanding the reason a message was initiated would assist in consumer issue resolution.

Business case

This change will benefit Suppliers and Network Operators as it will allow them to view SRVs and Service Responses early to resolve issues. This will improve query and resolution management process and reduce site visits and improve customer service in dealing with issues and problems.

Views against the General SEC Objectives

Proposer's views

The Proposer believes the Modification Proposal better facilitates General SEC Objective (a)[1], where it would contribute to the better operation of Devices at a premise that are experiencing unusual activity and require investigating. The Proposer also believes that it will provide additional benefits in the form of faster decision making for Users, which in turn provides greater efficiency and may pass through on to consumers.

Industry views

The Refinement Consultation responses were generally positive, with five out of six respondents (two Large Suppliers and three Network Operators) believing this information would help with effective management of consumers issues. Only one respondent (a Large Supplier) was not supportive. They believed that this change was a 'nice to have' feature but found it difficult to see any value for resolution of consumer issues. They did not believe that DNOs having sight of this information would resolve any issues.

Views against the consumer areas

Improved safety and reliability

Consumers may experience improved reliability as any issues they are experiencing which trigger an Alert may be more easily visible to the SEC Party that can resolve the issue.

Lower bills than would otherwise be the case

This modification is neutral against this area.

Reduced environmental damage

This modification is neutral against this area.

Improved quality of service

Consumers may experience improved quality of service as any issues they are experiencing which trigger an Alert may be more easily visible to the SEC Party that can resolve the issue.

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

Benefits for society as a whole

Where a consumer is experiencing an issue which prompts a SEC Party to issue a Service Request to investigate the problem, any Alerts or Responses received by another Party should be more easily interpreted to allow the speedy resolution of the consumer's issue.

Appendix 1: Progression timetable

Following the Modification Report Consultation (MRC) the modification will be presented to the Change Board for vote under Self-Governance on 26 Jan 2022.

Timetable	
Event/Action	**Date**
Draft Proposal raised	20 Aug 2020
Presented to Change Sub-Committee (CSC) for initial comment	25 Aug 2020
Proposal discussed with Sub-Committees	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
Business Requirements developed with the Proposer	19 Oct 2020 – 23 Oct 2020
Business Requirements discussed at Working Group	4 Nov 2020
Modification discussed with TABASC	5 Nov 2020
Modification discussed with TABASC	7 Jan 2021
Modification discussed at Requirements Workshop	25 Jan 2021
Modification discussed with TABASC	4 Mar 2021
Preliminary Assessment requested	5 Mar 2021
Preliminary Assessment returned	9 Apr 2021
Modification discussed at Working Group	5 May 2021
Refinement Consultation	17 May 2021 – 7 Jun 2021
Impact Assessment requested	24 Jun 2021
Impact Assessment returned	19 Aug 2021
Modification Report presented to CSC	21 Dec 2021
Modification Report Consultation	22 Dec 2021 – 17 Jan 2022
Change Board vote	26 Jan 2022

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
BAD	Business Architecture Document
DCC	Data Communications Company
GDPR	General Data Protection Regulation
HAN	Home Area Network
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