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'

25 January 2021 Requirements Workshop – meeting summary

Attendees

Attendee	Organisation
Harry Jones	SECAS
Ali Beard	SECAS
David Kemp	SECAS
Anik Abdullah	SECAS
Khaleda Hussain	SECAS
David Walsh	DCC
Chun Chen	DCC
Remi Oluwabamise	DCC
Steve Bull	CGI
Julian Hughes	TABASC

Heading

Issue and Proposed Requirements

The issue the Modification Proposal looked to address was explained to the members. This was that Service Request Variants (SRVs) and Service Responses that the Responsible Supplier can't view on a Device that they are responsible for need visibility so an informed decision can be made whether or not to action them. The business requirements that were presented stated that the Responsible Supplier and the Network Party responsible for the affected Device should be able to request and view the SRVs/Service Responses. This would be achieved using the Service Audit Trail (SAT) data, so therefore wouldn't use the payload and prevent confidential information being obtained.

One question raised about the business requirements was that the requirements mentioned Devices which were "owned" by a Supplier or Network Party, which one member believed should be revised to "be responsible for" when referring to the Supplier relationship with the Device. The other business requirements workshop members agreed with this revision and SECAS stated the requirements would be updated accordingly. This also led to questions about the role of a Responsible Supplier where members asked why this hadn't been split into an Import and Export Supplier roles. SECAS confirmed that the Working Group had been asked on this question earlier in the process, and that they wanted the role merged to cover both. It was suggested that the requirements be updated to clarify the differences between these two roles to state how they would be affected if the Import and Export Suppliers are different for a premise.

A question was raised over the second business requirement which specified that a Network Parties would be able to view the SRVs/Service Responses for a Device. In particular, the rationale as to why a Network Parties would need visibility of the contents of a Device. SECAS raised that a Network Parties had contacted them during the Development Stage noting that they would benefit from the visibility. The business requirements workshop members believed that the rationale for extending the scope of this visibility to the Network Parties needed exploring further and that clarity was needed.

One member enquired into the possible General Data Protection Regulation (GDPR) concerns that any Proposed Solution would need to deal with if any confidential Device data was being viewed from Supplier Parties previously responsible for them. SECAS clarified this by stating the use of SAT data to acknowledge where an SR had been sent or a Service Response received rather than the SR/Service Response payload would be the only data used. This was highlighted in the copy of the business requirements under the General section, and SECAS agreed that this information would be mentioned in each individual business requirement to prevent this detail being overlooked.

One member asked about the scale of the issue for the Modification Proposal as to how many Devices or Suppliers this affected. SECAS stated that the DCC as the Proposer of the Modification Proposal had raised it as it was brought to them as action to follow up on. The DCC clarified that the Modification Proposal was raised following a Technical Specification Issue Resolution Subgroup (TSIRS) meeting where the issue had been raised by its members concerning not being able to view the relevant SRVs/Service Responses.

One member asked whether there was any time limit specified in the business requirements to how far back a Responsible Supplier could access the SRs/Service Responses. The reason for this was that the member believed a Responsible Supplier would only need to go back a month or so at best to find SRs/Service Responses which needed actioning. SECAS confirmed that at present there were no limits mentioned in the requirements as to how far back a Responsible Supplier could request the SAT data. The Data Service Provider (DSP) was asked whether a limit was needed for the amount of data that could be returned and in what length of time to prevent an ‘interactive screen’ used on the Self Service Interface (SSI) from timing out. The DSP confirmed that the requests used for the SAT data would not create a substantial impact on the overall volume or SRV/Service Response traffic in the DCC Systems if it were retrieving between one and three months’ worth of data, but suggested testing should take place to see what additional traffic this would likely create. The DSP also stated that SSI changes would be needed as the Modification Proposal would change the access controls within the SSI for concerning who has visibility rights of the affected SRVs/Service Responses.

Next Steps

The following actions were agreed on after the questions proposed by members were answered:

- SECAS would update the business requirements to reflect the change of “ownership” to “responsibility” for Supplier Parties, enquire further into the rationale for extending the requirements to include Network Parties and amend the requirements to include details on the SAT data being used.
- SECAS will then circulate these updated requirements to the Working Group and TABASC for comment prior to a Preliminary Assessment being sought.