MP134B Alternative Solutions Workshop minutes **19 May 2022**

Background

- SECAS summarised the purpose and issue to the modification is trying to resolve.

Purpose of the meeting

SECAS stated that the Refinement Consultation responses and Sub-Committee discussions had highlighted the following issues with the Proposed Solution:

- Industry Parties were concerned that as well as the modification being expensive, Shared Resource Providers (SRPs) would also incur high costs, and these would be passed through to Suppliers (suppliers would pay 'double bubble')
- Industry Parties believed that most Supplier failures were not disorderly and only one of these events had occurred in the last year, with no PPM consumers involved
- Industry Parties believed that most Suppliers that were going to fail had done so already and there would be fewer in future
- Industry Parties suggested the costs should not be expended even on the DCC Impact Assessment as the solution was unlikely to be used
- Suppliers had concerns about putting consumers into credit mode for several reasons (accumulation of debt while in credit mode, confusion when 'unable' to top up etc.)
- Parties were content with the solution which MP134A delivered and believed it to be working well and didn't see any need for MP134B.

In response to these points SECAS highlighted that in discussions it was clear that respondents had not considered the manual work involved with MP134A solution which involves the SMKI Chair to physically check emails continuously and how the process breaks the Security Trust model.

The DCC advised that the reason the costs are so high is due to impacts on both SMETS1 and SMETS2 Devices.

SECAS stated that this meeting was to discuss whether the solution could be amended or made more appealing to industry Parties. MP134B would need to pass Change Board to progress to Impact Assessment. A member queried if the Change Board had any representatives from the Security Sub-Committee. SECAS advised that the Change Board is made up of Industry Parties, not Sub-Committee representatives but the Change Board is guided by Sub-Committee feedback.

Discussions

SRP PoV - Environments

- An SRP member advised impacts on SRPs were dependant on each SRPs business architecture. The concern was raised of exactly how many certificates would be required (would it be one SoLR Contingency cert for each Supplier that the SRP serviced?) They questioned if there would be additional certificates which organisations would need to consider storing. They highlighted their organisation uses Hardware Security Model (HSM) which is a system which stores the certificates and is limited to a certain number of certificates it can store. The TABASC Chair advised a single certificate would be required for a single SRP.

- An SRP queried how the DCC would know which SRP certs related to which customers (Suppliers) to confirm the SRP can act on their behalf? The TABASC Chair noted that separate reference data would need to be provided by the DCC and SMKI PMA on which were the valid SRPs for a particular failed Service User.

- The SSC Chair questioned how this would fit the Security Trust model if the SRP was still using the Supplier Signing key. They clarified that the GBCS message would be signed with the (failed) Supplier key and the Service Request would be signed with the SRP key, ensuring the Security Trust model was adhered to.

SRPs relations with customers (Suppliers)

- An SRP also advised there are Suppliers that use multiple SRPs. The TABASC Chair advised there is nothing to prevent the use of multiple keys in this situation. It was advised either to consider extending the storage in the HSM to store more certificates or develop an application to facilitate this. An SRP member advised it was more a case of how many clients they had rather then how many keys were used. It was summarised that it would be up to the organisation and the architecture they want to implement. An SRP advised in their initial response to the consultation they had an estimated 100k-200k across roughly 40 customers (Suppliers). He also highlighted it would take 18-24months to implement the change due to the complexity and size of the change. They would also need to go through a qualification process where they are able to design and implement the system and then have it rolled across to every client. It was suggested the 18–24-month timings will align with DSP re-procurement.

S1SPs Preliminary Assessments

- The TABASC Chair referred to the Preliminary Assessment and queried if it was necessary to make all the changes outlined in the PA. He questioned if SMETS1 Service Providers (S1SPs) are validating the Service Requests coming from the Data Service Provider (DSP), specifically do messages received from those acting on behalf of a Supplier need to be validated too. A member questioned if the S1SP repeat validations already carried out by the DSP? And whether it would reduce cost removing this step. It was suggested to confirm that the 'Access Control check' with the new User Role is necessary.

- The DCC advised originally the business requirement was 'XML signature checks will be changed, so the Business Originator can still be the failing Supplier (validated against a list) but the entity that owns the XML signing cert can be the SRP itself'.

- It was highlighted it would be beneficial to understand if it made any material changes to the costs and as the work was conducted previously by Phil Twiddy (SECAS) it was worth revisiting and re-sharing with the SSC.

SRV 1.6 options

- SECAS highlighted that Suppliers had concerns about using SRV 1.6 as it would confuse customers as well as allow consumers to build up a debt whilst in credit mode. This may then cause consumer angst and additional costs when they were later required to pay the money back. SECAS queried whether SRPs could send the non-disconnect calendar. It was noted the SSC were agnostic about the SR sent. There were several actions that could make a customer safe and maintain continuity of supply. It was suggested that the Anomaly Detection Attributes (ADAs) was a generic issue where SRPs would suddenly

start sending SRs which then fall outside previously agreed levels. It was highlighted from a security perspective the current MP134B solution served a purpose but from a Supplier perspective looking at cost and how customers will be at a disadvantage being put in a credit mode they will accrue debt and will get billed for when they were in credit mode and unable to top up.

- SECAS queried if the non-disconnect calendar could be updated. It was highlighted that the non-disconnect calendar is not an SR in itself but part of SRV 2.1 'Update Prepay config'. This SR has seven mandatory fields including 'set debt recovery rate' and 'set credit limit'. It was advised that these are not individually configurable and allowing SRPs access to this SR would allow them to change any of the parameters within it. It was also noted that it would be difficult to apply ADAs to individual elements contained in SRV 2.1 in the signed pre-command and would require the DSP to process the entire message rather than just the XML signed command. SECAS advised it was worth revisiting to make sure all avenues have been explored. It was suggested a 'fixed format' could be 'matched'. SECAS will check if a revised set of business requirements is required or not which are then to be included in the revised PA request. SECAS will check if both of these are required.

Business case for this change

- From a cost perspective it was highlighted, there has been so far only one disorderly exit in the last four years. It was suggested that this was a Security concern and industry need to drive progress to FIA.

- It was queried if there was a clear response why MP134A was not a good enough solution. A member advised it was regarding the principle from a security perspective. MP134A was not to be used as an enduring solution but rather an interim solution until MP134B was implemented. It was highlighted an immediate solution was required at the time, and as a result the modification was split into two parts. Members advised it was important to put this point across at Change Board to ensure the FIA was requested. Furthermore, MP134A is reliant on one person checking emails, including out of hours.

- It was suggested MP134A should be removed from the SEC. SECAS advised if MP134B is implemented then we could potentially look at taking MP134A out.

Next steps

- SECAS to work with the DCC to reassess S1SP costs to see if they can be reduced.
- SECAS to work with the DCC and DSP to assess if any other Service Requests can be a workable option.
- SECAS to consider resending MP134B out for a second Refinement Consultation once the previous two actions have been addressed.
- SECAS to check if revised business requirements are required along with revised DCC PA request.