



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.

Stage 02: Working Group Meeting Summary

SECMP0010 ‘Introduction of triage arrangements for Communication Hubs’ and SECMP0013 ‘Smart meter device diagnostics and triage’

Date and location

31st October 2018, 14:30 – 17:00.

Gemserv offices, Jubilee Room, 5th Floor, 8 Fenchurch Place, London, EC3M 4AJ.

Summary of SECMP0010 and SECMP0013 Working Group Meeting

Discussions

The Working Group discussed the outcome of the Request for Information (RFI) for both SECMP0010 and SECMP0013 for the number of returned SMETS1 meters and CHs. The results showed that the total numbers of devices with No Fault Found (NFF) were much greater than the number of devices returned that were faulty (an average of 70% for NFF was shown for all returns, from five respondents data).

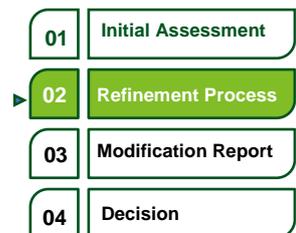
Additional areas to note from the RFI were:

- Suppliers can perform triage themselves on SMETS1 devices and if there was found to be a fault with a device then it would be sent back to the manufacturer
- Some CHs and SMETS1 meters were sent back together making it difficult to differentiate which of the two was potentially at fault
- Early indications of SMETS2 CH returns showed higher volumes when compared to SMETS1 which was suggested to be a cause of SMETS2 CH not being a mature product
- Change of Supplier was not always excluded from the number of returned SMETS1 devices which would affect whether these results would be representative of SMETS2

It was noted that the costs involved (average avoided cost per unit and other avoided cost, such as logistics) that had been provided were not consistent across all respondents.

The Working Group discussed the Security Sub-Committee (SSC) views on the alternate solution for SECMP0013 for SMETS2 and advised that the request to the SSC was for their views on performing triage in an off-site facility, and with the device offline, which would negate the need for a change to security characteristics. The SSC feedback stated that the proposed triage mechanism could require a change to the security characteristics as there could be issues with the tampering seal needing to be replaced.

What stage is this document in the process?



SECAS Contact:

Name:

Cordelia Grey

Number:

020 7090 1072

Email:

SEC.Change@gemserv.com

SECMP0010 and SECMP0013

Working Group Meeting Summary
13 November 2018

Version 1.0

Page 1 of 3

This document is classified as **White**

© SECCo 2018



Additionally, Members of the Working Group noted that the DCC solution would involve an online system where the meter would be joined to a test CH in a test facility using dummy MPANs (or MPxNs).

It was confirmed that, under current governance for SMETS2, performing triage by anyone other than manufacturers, would not be possible. Members stated that in some cases, it would also not be possible for the manufacturer to perform triage either.

Members acknowledged there was no requirement on manufacturers to have an optical port as part of a meter specification meaning it would not be possible to use an optical port as a means of triaging a meter. It was suggested that each meter manufacturer would have, and need, their own proprietary solution. It was confirmed the bronze solution would be a proprietary solution and the gold solution would be the Data Communication Company (DCC) solution.

Members agreed that triage was mostly carried out on meters that were returned upon installation, not meters that were five-plus years old, for example. Members noted that Meter Asset Providers (MAPs) may see benefit in triaging a meter that was older but not Suppliers, especially if Suppliers had a meter that required triage that they did not fit themselves. Additionally, it was noted that, as well as Suppliers triaging a meter first, MAPs may also perform triage before sending it back to the manufacturer, therefore many meters may be triaged more than once by multiple parties.

Members acknowledged there was a need for all manufacturers to reach an agreement that an alternate solution was required, other than the DCC solution that had been assessed against in the Preliminary Assessment, to ensure that the triaging of meters was possible for SMETS2. Members also agreed that the National Cyber Security Centre (NCSC) needed to provide confirmation that additional security would not be required to allow the triaging of meters in a proprietary solution.

From a Distribution Network Operator (DNO) perspective, it was raised that, should a meter be removed, then the DNO would need to be notified. It was advised that, should a meter be removed from a premise, then the credentials would need to be wiped and a factory reset performed so that it could be reinstalled anywhere.

Members noted that some manufacturers had previously advised they were unable to perform factory resets, resulting in meters being scrapped, whereas other manufacturers stated they could perform resets and reuse meters. Current CPA requirements mandate meters to only support interfaces for standard operations; the use of engineering mode, additional interfaces or user interface menus allowing access to meter functionality other than defined by the technical specifications is not permitted. Where implemented by manufacturers, access to these functions is behind the secure perimeter of the meter. Accessing these functions requires breaking the tamper seals; re-use of the meter mandates re-sealing the device. The Working Group agreed a formal view would need to be provided by the NCSC on what was permitted.

The Working Group agreed the business requirements for SECMP0010 'Introduction of triage arrangements for Communication Hubs' were still correct, but questioned whether the proposed costs of implementing a solution were still valid when compared to the number of returned CHs. It was decided that the Proposer for SECMP0010 would seek views internally on the numbers of CHs they sent back and whether there was still a business case for the modification. DCC also stated they would re-confirm the costs in the Preliminary Assessment, with their Service Providers, and send these through once available. Members stated there were expectations of additional CHs being returned once DBCHs were rolled out because existing CHs might be replaced in order to provide mesh coverage and overall better coverage for certain premises, which would indicate current SMETS1 return rates were even more unrepresentative of SMETS2.

The Working Group agreed to the removal of references to optical ports and to replace with "a local means of connecting the device". All Members were also in agreement that

SECMP0010 and
SECMP0013

Working Group Meeting
Summary

13 November 2018

Version 1.0

Page 2 of 3

This document is classified
as **White**

© SECCo 2018



they should be engaging with meter manufacturers to establish how they were proposing to perform meter triage.

Actions

- CL to seek statistics internally on the number of CHs returned and the costs involved, taking into account the business case for the modification, and to provide a view on the next steps for the modification when convenient.
- DCC to seek confirmation of the costs involved to implement SECMP0010 from DCC Service Providers and update SECAS/Proposer/Working Group when available.
- DL to arrange a meeting with BEIS to seek their views on SECMP0013, and the associated benefits case for a triage tool, the security considerations and the impact of failing to deliver meter triage tools. Meeting to ideally take place on Monday 12th November.
- Following the meeting with BEIS, a workshop should take place with manufacturers, DCC, Suppliers, MAPs/MOPs/MAMs, NCSC and BEIS to determine the feasibility of a solution for triaging meters.

SECMP0010 and
SECMP0013

Working Group Meeting
Summary

13 November 2018

Version 1.0

Page 3 of 3

This document is classified
as **White**

© SECCo 2018