



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

Joint SECMP0010 'Introduction of triage arrangements for Communication Hubs' and SECMP0013 'Smart meter device diagnostics and triage'.

Date and location

24 September, 2018, (10:00 – 13:00).

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

Summary of SECMP0010 and SECMP0013 Working Group Meeting

- The Working Group concluded the original solution proposed for SECMP0013 should be accompanied by an alternate solution following a consideration of the potential costs to users of implementing the original solution. Members highlighted that the original solution could be simplified into an alternate solution in order to reduce the costs, but this would result in some limitations, namely:
 - A dependency on National Cyber Security Centre (NCSC) allowing the use of local communication ports – note the original proposal would not require this
 - Some manufacturers have designed their meters without local communication ports, or these have been disabled – note the original proposal would work with any SMETS2 meter
 - Suppliers would not be able to triage meters which came from a manufacturer for whom they did not have a triage tool – note the original proposal would work with any SMETS2 meter
 - The alternate solution does not directly deliver the ability to perform install and uninstall in a QA environment although this could be done if there was access to dummy MPxNs and a SECMP0010 solution
- Additionally, the original solution for SECMP0013 could allow for both meter triage and reset to be carried out by either a Supplier or a Registered Supplier Agent (RSA) – assuming access control were set to allow RSA as an eligible

What stage is this document in the process?

01	Initial Assessment
02	Refinement Process
03	Modification Report
04	Decision

SECAS Contact:

Name:

Cordelia Grey

Number:

020 7090 1072

Email:

SEC.Change@gemserv.com

SECMP0010 and
SECMP0013

Working Group
Meeting Summary

24 September 2018

Version 0.1

Page 1 of 2

This document is
classified as **White**

© SECCo 2018



User for these Service Requests, with Members acknowledging that not all MAPs were RSA's, and therefore would need an external party to send the new Service Requests.

- The new proposed alternate solution would require, at a minimum, the ability for the meter to have its SMKI Certificates reset, set to re-join using ZigBee Installation Code and have all consumer data unavailable, effectively resetting and returning the meter to its original state. Diagnostics could be carried out via an optical port and/or VPN or another method and the Working Group acknowledged that there may be security implications to be aware of which would be put forward to the National Cyber Security Centre (NCSC). Members stressed the fact that meter diagnostics would not take place in a consumer's premise and should be taken into account. Additionally, the Members highlighted the importance in progressing with a solution for both meters and CH's to avoid assets becoming single-use and allowing for them to be reused as a full value asset.
- Finally, the Working Group highlighted that Users may wish to perform alternative analysis/ diagnostics to rule out HAN or WAN issues.

The Working Group agreed on the following actions:

- **Action:** SECAS to issue a Request for Information (RFI), possibly as part of the Working Group Consultation, to allow for the industry to submit information on the numbers of returned Communication Hubs, SMETS1 electricity and gas meters between June 2017 – June 2018. The information requested would include how many were returned that required resetting and how many were returned which were found to have no fault. The objective is to gain the latest information to support the development of a business case for change.
- **Action:** SECAS to contact Security Sub-Committee (SSC) and NCSC and request clarification on the security implications surrounding using an optical port and/or VPN or another method to connect to the meter to carry out basic diagnostics and not using Service Requests to carry out triage and QA, as proposed by SECMP0013 originally.
- **Action:** Suppliers to find out via Gas Distributors whether dummy MPRNs exist for gas and if they can be used in the same way as electricity dummy MPANS for the purpose of triage and QA.
- **Action:** SECAS to issue the Working Group Consultation documents for SECMP0010 to the Working Group for review.

SECMP0010 and
SECMP0013

Working Group Meeting
Summary

24 September 2018

Version 1.0

Page 2 of 2

This document is classified
as **White**

© SECCo 2018