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.

SECMP0038 'Sending Commands via PPMIDs'

1st Working Group

8th August 2017 10:00 – 16:00

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ

Meeting Headlines

Attendees:

Organisation	Working Group Member
Utilita (Proposer)	Andy Knowles
British Gas	Rochelle Harrison
SSE	Emslie Law (Teleconference)
SSE	Andrew Warner
Global-365	William Wilson
E.ON	Stacey Brentnall
Landis + Gyr	Elias Hanna
Chameleon Technology	Tom Moore

Representing	Other participants
SECAS	Talia Addy (Chair)
	Selin Ergiden (SECAS Modification Support)
	Caroline Gundu (SECAS Modification Support)
	Kevin Atkin (Technical Support)
DCC	Parmjeet Dayal
	Chris Barlow

Apologies:

Representing	Working Group Member
SSE	Nigel Hullett
SSE	Samantha Cannons

Geotogether	Ferenc Vanhoutte

Modification Proposal overview

SECAS provided an overview of SECMP0038, highlighting the current arrangements and the proposed changes. The modification seeks to require a Communications Hub (CH) to accept any Great Britain Companion Specification (GBCS) Command sent via the Zigbee tunnel from a Prepayment Interface Device (PPMID), rather than only a subset of Commands.

Current arrangements

Currently, Signed Pre-Commands and Non-Critical Service Requests (SRs) are sent by Suppliers to the Data Communications Company (DCC's) Data Service Provider (DSP). If they pass the checks the SEC requires the DCC to carry out, the DSP adds a Message Authentication Code (MAC) to create a fully formed GBCS Command.

There are two options to deliver Commands to a Consumer's Premises:

1. Sending via the DCC's Communication Services Providers (CSPs) (normal option), and / or

2. via Hand Held Terminal (HHT) - if the supplier wishes to do so.

The proposed solution is to extend the HHT mechanism so that Commands can be delivered from a PPMID in the Consumer's premises. The Command would be sent to the PPMID via a route of the Supplier's choice, for example the internet or mobile phone networks.

The WG noted that the Meter to which a Command is addressed is unaware of its delivery route to the Consumer premises and applies the same security checks regardless.

The WG discussed the current arrangements along with the proposed solution, noting that:

- an HHT can only send Commands within an 18-hour window. This is because HHTs are used by installers and will therefore not stay in the Consumer's premises after the installer completes their work

- Smart Meter firmware updates cannot be done via HHT

- there is a need to develop a fall-back solution for customers in no Wide Area Network (WAN) or intermittent WAN coverage areas to ensure Commands can be sent in a timely manner

- there may be security concerns associated with sending Commands over a public network to a PPMID.

    - The WG noted the Security Sub-Committee's (SSC) input and that there may be security concerns but that they may be capable of mitigation.

Working Group consideration of the issue and solution

The WG noted that Suppliers cannot rely on customers having a Wi-Fi connection. Therefore, Suppliers might need to make arrangements with Wi-Fi service providers to use this solution over the internet. However, paying for this service remains another cost Suppliers will have to consider alongside other Supplier operational costs.

The WG deliberated how CPA assurance in relation to PPMIDs might be affected.

The WG noted that Suppliers opting to use this solution will see security assurance through the annual Competent Independent Organisation (CIO) audit.

Next steps

The WG agreed that there will not be any changes made to the proposed solution. Members requested that the discussions carried out during the meeting should be included in relevant modification reports.

ACTION_0808_01 – SECAS to request Preliminary Assessment (PA) from the DCC once the solution design document is agreed.