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.

SECMP0007 'Firmware updates to IHDs and PPMIDs'

August 2019 Working Group Meeting summary

SECMP0007 'Firmware updates to IHDs and PPMIDs' proposes to provide the capability to update firmware Over-The-Air (OTA) for In-Home Displays (IHDs), Pre-Payment Meter Interface Devices (PPMIDs) and Home Area Network (HAN) Auxiliary Load Control Devices (HCLACSs) via the Data Communications Company (DCC) infrastructure. The solution includes the banning of local updates once the OTA solution is implemented. The Working Group discussed a proposal from Green Energy Options (geo) to allow use of local firmware updates for PPMIDs in parallel to OTA firmware updates.

geo's views on the Modification Proposal

geo stated that they strongly support SECMP0007 in order to provide the capability for OTA firmware updates to mandated HAN Devices via the DCC infrastructure. This would avoid the risk of costly site visits to update firmware as well as provide greater capacity to deal with security incidents that could be addressed via firmware updates.

The banning of local updates

However, geo is concerned with the proposal that all local firmware updates will be banned following the implementation of this modification, most notably for the PPMID. geo noted the additional features that are being added to the PPMID and the need for more regular updates to these features. The Department for Business, Energy and Industrial Strategy's (BEIS's) recent funding granted to add functionality to the PPMID was noted as an example of this already happening.

geo's view is that by banning local updates you would increase the risk of 'stranding' a Device, especially as Supplier churn increases, because Suppliers are not obligated to support firmware on HAN Devices. They went on to propose some amendments to the current solution options for SECMP0007 as outlined below.

geo's proposed solutions

geo gave a summary for each of their two proposals[1] noting that changes to SEC Schedule 10 'Communications Hub Technical Specifications' (CHTS) and Schedule 8 'Great Britain Companion Specification' (GBCS) are already needed with their proposals not requiring any additional changes to the SEC.

A Working Group member noted a step in geo's process diagrams had been missed off, being the stage whereby the firmware Image enters the Certified Products List (CPL) listing gateway. geo noted the missing step.

geo presented a quote from BEIS;

[1] The meeting materials, including geo's summary of their proposals can be found here.

'BEIS noted that the Communications Electronics Security Group (CESG) supported the removal of PPMIDS from the scope of the CPA scheme. This was due to the industry evidence showing that the PPMID cannot be used to disable a supply, even if its security was to be compromised. It was therefore noted that PPMIDs would not need to be CPA certified, and therefore the Working Group would not need to approach the CESG for further input.'

Contrary to this view, the May 2019 Working Group meeting agreed that if the IHD and PPMID were able to communicate directly with the Communications Hub, those Devices would probably be required to undergo CPA certification and have the relevant Device Certificates added.

geo also noted the following benefits of their proposals:

- allows feature sets for non-Smart Metering Equipment Technical Specifications (SMETS) functions to evolve
- expands the use of smart meter data to energy services providers
- faster and cheaper to upgrade Devices

Working Group discussions on the proposed solutions

A DCC gateway screening mechanism was suggested as a way of ensuring only authorised Parties can locally update firmware. However, this does not currently exist and would need to be designed and implemented by the DCC.

The Smart Energy Code Administrator and Secretariat (SECAS) presented the Working Group with the following questions to consider with regard to geo's proposed solutions:

- How can we ensure local updates can only be carried out using firmware listed on the CPL?
- How will the Smart Meter Inventory be updated with the firmware version following local firmware updates?
- How will the information given in SR8.2 'Read Inventory' be affected?
- Should the Communications Hub be required to store firmware information and/or forward it on?
- Could the proposed daily Alert from the IHD/PPMID to the Communications Hub constitute an Alert storm? If so, how could this be addressed?

The SECAS Technical Lead explained the current firmware update method whereby updates can only be applied by authorised subscribers. First, the firmware and the Firmware Hash are submitted to the Data Service Provider (DSP) who validate the Firmware Hash. The DSP then check that the Firmware Hash is on the CPL and, if it is, sends the firmware to the target Devices. After the activation of the firmware on the Device the Smart Metering Inventory (SMI) is updated to reflect this. If the Firmware Hash is not on the CPL, then the firmware update will not be executed. The Working Group were unsure how this process could be mirrored using geo's proposed solutions. A Working Group member also noted the negative impact an SMI with out of date firmware versions would have on SR8.2 'Read Inventory'.

SECAS noted geo's proposal to store the IHD/PPMID firmware version in the Communications Hub would be a break from the original concept the current proposed solution is been based upon. The Communications Hub has been envisaged to transfer firmware information, rather than store it for periods of time, and that to do so would require building in functionality to the Communications Hub.

The Working Group also discussed geo's other proposal requiring the Communications Hub to forward the IHD/PPMID firmware version to the DCC in a suggested daily routine. However, this proposal was noted as leading to high numbers of Alerts generated to the DCC when considering if every IHD/PPMID were to do this.

The Working Group asked geo how many updates to PPMIDs they were likely to carry out a year. geo advised updates to PPMIDs would be very limited, but potentially every three months for the other functions on the Device.

Next steps and vote on the progression

What are the next steps if geo's proposals are taken forward?

SECAS advised the following progression plan if geo's proposed solutions were to be taken forward:

- consideration by the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC)
- finalise the business requirements
- undergo a DCC Preliminary Assessment
- Working Group to consider DCC Preliminary Assessment
- Change Board review cost of DCC Impact Assessment
- undergo a DCC Impact Assessment (if agreed by the Working Group and Change Board)

The DCC also noted geo's proposed solutions would add additional costs and time to the modification process.

Working Group vote on an Alternative Solution

The Working Group proceeded to vote on whether to progress geo's proposals as an Alternative Solution under SECMP0007. All Working Group members but geo voted not to take forward geo's proposals as an Alternative Solution. This was due to the desire not to cause any undue delays to SECMP0007, given that Parties wanted this implemented as soon as possible. However, several members were of the view that geo proposed some good ideas and encouraged geo to raise their own Draft Proposal to have their ideas assessed.