Technical Note #1

SECMP0007, DCC CR 1173

Firmware Updates for PPMIDs, IHDs, and HCALCS Design Notes

Version:	**0.21**
Date:	**27th August, 2019**
Author:	**DCC**
Classification:	**DCC PUBLIC**

1 Problem Statement

As part of the Full Impact Assessment (FIA) for SECMP0007, the Service Providers are working on the details of the DUIS and GBCS changes, as well as proposed changes for handling the firmware updates sent to Comms Hubs.

This Tech Note clarifies the usage of Service Requests, and some changes to the GBCS Use Cases. If the proposals are approved, these will be incorporated into the FIA, and any subsequent design work.

Requirements and the solution options for this SEC Modification are held in the PIA for SECMP0007, SECMP0007 CR211 - PIA - Firmware Updates v1.21.docx.

2 SECMP0007 Technical Discussion

2.1 Create New DUIS Service Requests 11.4 Download Firmware and 11.5 Read Firmware specifically for PPMIDs and IHDs

In progressing the FIA for SECMP0007, the team have challenged why the solution should require new DUIS Service Requests 11.4 Download Firmware and 11.5 Read Firmware specifically for PPMIDs and IHDs, as stated in the Requirements for this SEC Mod.

If we look at the requirements for what these two Service Requests (SRs) would actually require in terms of XML inputs and outputs, then they are exactly the same as the existing SR11.1 and SR11.2. The only difference is the device types that are supported.

We have already overloaded the existing SR11.1 to support Firmware Download to SMETS1 Comms Hubs and we have a CR in progress (CR1145) to do the same thing for SMETS1 PPMIDs/IHDs, so we think it would be much more sensible, efficient, and consistent to simply extend SR11.1 to support SMETS2 PPMIDs and IHDs.

Download Firmware is primarily a DSP to CSP interaction, as it is for all existing devices.

Decision is to use the recommendation to switch to 11.1 and 11.2. As a response the CSPs will send an alert through an asynchronous notification.

Re-using and extending the existing SRs will reduce costs and simplify the solution.

2.2 New API to the CSPs for Distribute Firmware to PPMID/IHD

For the firmware download to the Comms Hubs, there needs to be a notification from the CSPs back to the DSP through a custom API, with settings of Success and Fail

This gives information of Activations and confirmation that it is Activated (as this needs to be logged).

Using the Zigbee OTA the Comms Hub issues an "Upgrade End Request", on behalf of the Comms Hub as a mandated command on the Zigbee cluster with translation in the Communications Hub Function (CHF).

There will be an error message if the Comms Hub doesn't have the whole image, and another alert showing when the image is complete and activated.

NOTE: add note to docs that the images >750KB adds significant complexity.

During download there needs to be two new alerts, one for partial delivery, the second for full delivery, with the second alert resent at the end of a successful reboot and activate including a read of the firmware version.

This will need some work from the GBCS Working Group for drafting.

This change is required to allow firmware distribution. It will be added because the appropriate mechanism and alerts were missed from the Requirements.

2.3 Map SR11.2 to new GBCS Use Case with new GBCS Use Case required for the CHF

Service Users will need to be able to read the firmware version with a Service Request. They can't do this at the moment, so the Comms Hub has to be able to execute "Read Firmware Version" in a way similar to SR11.2.

Could change CHF (by adding an Optional Header field)

OR

GBCS header to add forwarding address – Comms Hub then processes and forwards to another device.

Note CGI very nervous about changing headers as there might be backwards compatibility issues. Tom had the action to write up an option for the header change.

Read Firmware for ESME/GSME/CHF is a request goes to the device in question, but this SEC Mod proposes that Read Firmware requests for PPMID and IHD are sent to the CHF and the CHF retrieves the information from the PPMID/IHD (via Zigbee OTA facilities) and then the CHF responds to the request.

In terms of SR11.2, there's a little bit more complexity since a Read Firmware Service Request for a PPMID or IHD would need to map to a (new) GBCS Use Case on the relevant CHF that returns the firmware version data on behalf of the PPMID/IHD. We believe this is the GBCS CS09 command which will be sent back to the Service User, and the Access Control Broker (ACB) command is handled on behalf of user to read the firmware version from ACB to ACB.

There will be an impact on Parse and Correlate , such as when a Service User is trying to ping a device using 11.2 to check.

Will use the Unknown Remote Party (URP) pattern (because Security Credentials are not required).

Note this can be hidden behind the DUIS/MMC XML interface which still has the same inputs (Device ID) and outputs (Firmware Version).

The new GBCS Use Case is required for the CHF to support the request to obtain the Firmware Version for a PPMID or IHD. There is no mention of this in the SECAS requirements.

2.4 HCALCS Options

HCALCS will implement the GBCS Use Cases 11.1., 11.2, and 11.3, using the Use Case for activation in the same way as an ESME. We will assume the ESME buffer gets overwritten so there is no need for an additional buffer. (this needs to be added to Assumptions)