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'

November 2019 Working Group Meeting summary

SECMP0007 overview

SECMP0007 'Firmware updates to IHDs and PPMIDs' proposes to provide the capability to update firmware Over-The-Air (OTA) for In-Home Displays (IHDs), Prepayment Meter Interface Devices (PPMIDs) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs) via the Data Communications Company (DCC) infrastructure.

IHD and PPMID proposed solution

A ZigBee OTA delivery mechanism will be used to deliver firmware images to the IHD and PPMID Devices, the processing of which differs from that of other Devices. This mechanism requires new GBCS use cases to distribute and activate the firmware and return the Device firmware version. As this solution is intended for ZigBee capable Devices only, the solution cannot communicate directly with the Devices and cannot re-use the existing capability for distribution and activation of HAN Device firmware. As part of this option the Communications Hub is to manage the activation of firmware and manage the notification to the Service User upon activation.

HCALCS proposed solution

The HCALCS will utilise the existing OTA firmware update procedure used by Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME). This requires a distinct separation between the distribution and activation of the firmware image. As with ESME and GSME firmware updates, distribution will be carried out via Service Request (SR)11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter using a GBCS Critical Command.

SR for distribution/activation of PPMID/IHD firmware

SR11.1 will be used to distribute firmware to the HCALCS. However, the DCC and SECAS have differing views over the SR to be used for the combined distribution and activation of PPMID/IHD firmware. Both sets of views were discussed in the meeting starting with the DCC's.

The DCC's views

SECAS began by summarising the DCC's views which are in favour of using the existing SR11.1 for PPMIDs and IHDs, rather than creating a new SR for these Devices. The DCC believe that re-using SR11.1 will allow for a faster implementation of the proposed solution whilst also reducing costs. Cost savings would be achieved on the Self-Service Interface (SSI), Service Audit Trail (SAT), System and User Integration Testing (SIT/UIT) and reporting. SECAS noted that if SR11.1 were to be used for

PPMIDs/IHDs, the DCC would have to be able to differentiate between ESME/GSME and PPMID/IHD firmware. This is due to the two Device types following different methods of firmware activation.

SECAS's views

SECAS noted that the functionality of SR11.1 does not include the ability to activate firmware. Furthermore, ESME/GSME and PPMIDs/IHDs are each following different procedures for firmware updates. It is for these reasons that SECAS propose adding a new SR, specifically designed for the combined distribution and activation of PPMID and IHD firmware. This would prevent any risk of issues with amending SR11.1 which already works for ESME/GSME. It would also create a clear distinction for the DCC and the Service User as to which Device type is contained in each SR.

The Security Sub-Committee's (SSC's) view on the SR for PPMID and IHD firmware was given. This is that the SSC require the SR for the distribution/activation of the PPMID/IHD firmware to be differentiated from the activation of ESME/GSME firmware. This is to enable separate Anomaly Detection Threshold values for ESME/GSME and PPMIDs/IHDs. The SSC therefore agree with SECAS that a new SR for the distribution/activation of the PPMID/IHD firmware would achieve that. However, they would not prevent SR11.1 from being used, as long as it could also achieve separate anomaly detection for each Device type.

Working Group discussions

The Proposer agreed with SECAS's view that a new SR should be created for firmware updates to IHDs and PPMIDs, noting that a new SR would make the process easier to manage as each Device type is following a different procedure. They added that it would likely have lower implementation costs as well.

Both PPMID/IHD manufacturers present at the meeting were indifferent as to which SR is used, as their Devices don't validate against the SR reference.

A Working Group member noted that the use of SR11.1 could be easier for the DCC to implement as it would only impact its Data Service Provider (DSP). They added that it could be easier for Service Users as well, as using SR11.1 wouldn't result in a change to the DCC User Interface Specification (DUIS) for the Service User. However, SECAS noted that a new GB Companion Specification (GBCS) Use Case would be required. SECAS added that creating a new SR wouldn't result in any more changes than re-using SR11.1, as it would simply use the same structure as SR11.1, with a line added to the XML schema.

A Working Group member preferred the use of SR11.1 for PPMIDs/IHDs, noting that it would simply be extending its scope to additional Devices. They didn't see the benefit in creating a new SR for what their view is the same job as SR11.1. Furthermore, the Party already has operational processes in place that are based upon the use of SR11.1. However, the Party did note that either way, they will have to make changes to their interface with the DCC.

It was noted that evidence is needed for SR11.1 being able suffice the SSC's statement that the solution must be able to differentiate between Device types as well as be able to apply different Anomaly Detection values.

Next steps

Overall, the Working Group did not believe there were any negative consequences resulting from using SR11.1 or a new SR. They agreed that there are several variables that need to be investigated, but that the most practical approach needed to be taken. The DCC subsequently agreed to raise a Change Request against creating a new SR in order to assess the following:

- Cost impact
- Impact to implementation timescales
- Clarify if SR11.1 would be able to facilitate the SSC's statement; and
    - be able to differentiate between each Device type; and
    - apply different Anomaly Detection values to each Device type.

Communications Hub memory block usage

During the development of the solution, SECAS and the DCC have identified two options for using the memory blocks on the Communications Hub:

- Restriction of PPMID/IHD/HCALCS firmware to the ESME block only
- Use of both the ESME and GSME blocks for PPMID/IHD/HCALCS firmware

SECAS noted that the current requirement is for PPMID/IHD/HCALCS firmware to utilise both memory blocks on the Communications Hub, with ESME and GSME firmware taking priority. This is in order to maximise efficiency and minimise demand on the Wide Area Network (WAN).

The views of each were presented and the pros and cons discussed with the Working Group.

The DCC's views

The DCC are currently using dedicated memory blocks on the Communications Hub for ESME and GSME firmware. They advised that using both blocks will require changes to the Communications Hub design to build in the required logic to prioritise both ESME and GSME firmware, as well as distribute firmware to the available blocks. The Communications Service Provider (CSP) would be required to test all the possible combinations of firmware on the Communications Hub. Noting this, the DCC advised that the use of both blocks would increase implementation timescales as well as costs.

The DCC propose that PPMID/IHD/HCALCS firmware should be restricted to the ESME block in order to speed of the up the implementation of this modification and to minimise any costs impacts.

SECAS's views

SECAS noted several constraints with restricting PPMID/IHD/HCALCS firmware to the ESME block. The transfer of firmware from the Communications Hub to the target Device may take considerably longer if the target Device is operating on Sub-GHz. If another firmware update is sent during this time, this would increase the length of time the firmware image is waiting for a free block the WAN. Consequently, it increases the risk of the Communications Hub creating a bottleneck for firmware updates, increasing pressure on the WAN.

SECAS went on to discuss the current estimates relating to GSME firmware updates. These are that GSME firmware is likely to be updated once per year and that each update will take no longer than two weeks to complete. Using these estimates, the GSME block on the Communications Hub is likely to be free for 50 weeks (96%) of the year. It is for these points that SECAS propose using both memory blocks on the Communications Hub without distinction. This would reduce the pressure on the WAN and avoid the need to invest in additional WAN capacity.

Working Group discussions

Two-day SLA firmware Image limit

A Working Group member noted that if PPMID/IHD/HCALS firmware is restricted to the ESME block, this increases the chances that the image would have been overwritten by next ESME firmware update. In this case the Supplier would have to attempt the firmware update again. SECAS advised that a two SLA is proposed for the time a firmware Image can be pending on the Communications Hub before it is removed. Once the two-day SLA is exceeded, the Communications Hub would remove the Image and free up the memory block.

The Working Group were not in favour of this requirement and noted that this is not how the SMETS1 firmware update procedure works. In SMETS1, the Image will sit on the Communications Hub until it has failed, been activated or is overwritten with another Image. Working Group members advised that it is common for PPMIDs/IHDs to be switched off for long periods of time, possibly up to six months. The Working Group also questioned the benefit of clearing the memory blocks if they eventually get overwritten anyway. Members agreed that it is up to Suppliers to manage their firmware and to plan updates in a logical order.

The Working Group agreed that it must be ensured the Image is available on the Communications Hub for as long as possible. Therefore, once the customer turns on their Device the Image is still available in the Communications Hub for download and activation.

Memory block usage

If both memory blocks are used, it is not possible for Suppliers to distinguish which block each firmware Image is on. Therefore, they would not know if the Image has been overwritten or not. Noting this, the Working Group agreed that using both memory blocks on the Communications Hub could make it harder for Suppliers to manage their firmware updates. SECAS advised the Communications Hub will send Alerts informing the Supplier whether firmware updates have been successfully transferred to the IHD/PPMID and in a second Alert whether the firmware has been activated successfully or not. At any point in time SR11.2 ‘Read Firmware Version’ can be utilised for the PPMID/IHD/HCALCS, in order to read the firmware version for the Device.

A Working Group member advised that PPMID/IHD firmware updates are usually consequential from ESME updates. Therefore, an ESME firmware update is likely to be the first to be applied, decreasing the risk of Images being overwritten. The DCC also noted it plans to add functionality to the DSP, flagging when firmware updates are in progress. They could then use this information to notify the Service User if there is an update in process, preventing firmware Images from being overwritten.

Next steps

The Working Group agreed to progress Impact Assessment as-is, with the assumption that both blocks on the Communications Hub will be utilised. However, they asked the DCC to investigate with their CSP's the impacts of restricting PPMID/IHD/HCALCS firmware updates to the ESME block.

Modification next steps

SECAS advised that both the SSC and the Technical Architecture and Business Architecture Sub-Committee (TABASC) will review the Impact Assessment, with the SSC also intending to carry out a risk assessment on the Impact Assessment response. SECAS will also organise another Working Group meeting, to give Working Group members a chance to discuss the Impact Assessment.

Regardless of whether these actions have been completed by this time, SECAS intend to present the Modification Report to the Panel on 13 December 2019.

Actions

- The DCC are to raise a Change Request against the modification for creating a new SR in order to assess the following:
    - Cost impact
    - Impact to implementation timescales

- The DCC are to clarify if SR11.1 would be able to facilitate the SSC's statement:
    - Be able to differentiate between each Device type
    - Apply different Anomaly Detection values to each Device type

- The DCC are to raise a Change Request against the modification to investigate the impacts of restricting PPMID/IHD/HCALCS firmware updates to the ESME memory block:
    - Cost impact
    - Impact to implementation timescales

- The DCC will remove the two-day SLA window for which a firmware Image can remain on the Communications Hub

- SECAS to publish guidance and support materials for the OTA firmware update process once the solution is confirmed