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'

19 December 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.

Local firmware updates

SECAS advised the Working Group that the Security Sub-Committee (SSC) had discussed the proposed ban on local firmware updates. The TABASC Chair believed that the proposed ban on local updates to IHDs and PPMIDs imposed by SECMP0007 may present unnecessary constraints on Parties and other participants in the SMART ecosystem in the future. The TABASC Chair subsequently proposed to the SSC that local firmware updates to IHDs and PPMIDs should not be banned, subject to appropriate security controls.

SECAS noted the main concern with local firmware updates was that the current proposed solution would not allow tracking of when an IHD or PPMID has been updated via a non-DCC route. The TABASC Chair proposed two potential options to work around this issue:

- **Option 1 – Supplier periodically reads firmware version**

  Prior to carrying out any maintenance on an IHD/PPMID, Suppliers should request the current firmware version from the Device using SR11.2 'Read Firmware Version'. The Data Services Provider (DSP) will capture the response and update the SMI as a result.

- **Option 2 – DSP periodically reads firmware version**

  The DSP periodically requests firmware versions using SR11.2 and updates the inventory, perhaps once a month. Although this will mean the firmware version will be generally correct on the inventory, it will still be necessary to ask the Device directly before updating the firmware to be sure and so might not deliver much benefit.

Subsequently the SSC advised that it not wish to introduce any delay to the existing approach for the modification. However, it questioned whether the Working Group had considered triage and refurbishment of IHDs and PPMIDs which would require an alternative (local) means of a firmware. In this respect, the SSC considers that local updates are feasible subject to appropriate security controls.

SECAS recommended to the Working Group that it keep the ban on local updates to prevent any further delay to the modification. It noted that this would not prevent a Draft Proposal from being raised to reinstate local updates.

One member agreed with the recommendation to keep the ban to prevent delay to the modification. However, the majority of members disagreed, noting that a there is no ban currently in place and any such ban could not be enforced. Furthermore, members agreed that there is no need to implement a technical solution to automatically read the Device firmware version and subsequently update the SMI.

Decision: The Working Group agreed to remove the proposed ban on local firmware updates. SECAS advised it would issue guidance to Parties advising how to keep the SMI updated following a local firmware update.

Streamlining the proposed solution

SECAS noted the SEC Panel's request for a minimum viable product rather than a gold-plated solution. SECAS, along with the DCC and its Service Providers had identified several options that could streamline the solution, with the intention lower costs and shorten implementation timescales.

Communications Hub memory block rules

The current requirement states that IHD, PPMID and HCALCS firmware shall be able to utilise both blocks on the Communications Hub without distinction. However, it was noted that the use of both blocks will impact the technical architecture, but it is the impacts on testing that would increase costs. The DCC added the number of test cases will decrease with the use of a single block.

A member noted its preference for use of a single block. This would make it easier for Suppliers to know which block the firmware was on and orchestrate their firmware updates.

SECAS noted the increased risk of Image overwrites with the use of a single block. Parties accepted this risk and still preferred the use of a single block.

Members discussed which of the ESME and GSME blocks on the Communications Hub should be used for IHD, PPMID and HCALCS firmware updates. Previous discussions had suggested that if a single block were to be used, that the ESME block be used. This was due to the belief that the ESME block would be available for a longer period of time than the GSME block. However, the TABASC Chair advised that the GSME block might be better utilised for IHD, PPMID and HCALCS firmware updates due to the GSME being updated only once per year. Furthermore, the TABASC Chair noted that the Communications Hub could be supporting four ESME's at any one time, including an Auxiliary Load Control Switch (ALCS), so it would be free for a minimal amount of time.

Decision: The Working Group agreed to restrict PPMID and HCALCS firmware Images to the Gas Smart Metering Equipment (GSME) block of the Communications Hub (for IHDs see below).

Communications Hub Image SLA

SECAS noted the previous Working Group meeting in which the Working Group agreed to remove the two-day Service Level Agreement (SLA) for an Image to remain on the Communications Hub. SECAS advised that as the DCC had been carrying its assessment based on the assumption that the two-day

SLA would remain, this element would require re-assessment. The Working Group noted the update and members clarified that they wanted two-day SLA requirement removed.

Decision: The Working Group agreed to remove the requirement for a two-day SLA for an Image to stay on the Communications Hub. The Image will remain until it is overwritten.

Communications Hub logging of updates

SECAS advised that the current proposed solution contains a requirement in which the Communications Hub shall record the target Device ID and the Upgrade Image File version for up to 15 Devices. The DCC advised that neither of the Communications Service Providers currently do this and that this requirement would subsequently increase costs in development and testing.

The TABASC Chair suggested that such logging was not necessary, and that Service Users could simply check the progress of their firmware updates reading the firmware version on the Device.

Decision: The Working Group agreed to remove the requirement for the Communications Hub to log the progress of up to 15 Devices in the Upgrade Image list.

Firmware updates over 750KB

SECAS advised that current requirements are to fragment any firmware updates larger than 750KB in size. The DCC proposed to remove this requirement and to limit the size of any firmware updates to no larger than 750KB in size. This would reduce costs in testing and development. Furthermore, fragmentation increases the risk of Image corruption which requires repeated Image sending and overwrites.

The Working Group clarified the requirement and advised that it would be up to the Device manufactures to fragment their firmware updates into Images of no larger than 750KB in size. The Suppliers would subsequently distribute each fragmented firmware Image as a standalone update. Therefore, there is no requirement for the DCC to fragment the firmware updates or orchestrate their delivery to the Device.

The Service Providers advised that they had previously misunderstand this requirement and that with this clarification would reassess the impact on the solution. However, they noted the this would likely not have as much impact on development or testing as had been anticipated.

Decision: The Working Group agreed that any firmware updates over 750KB in size must be split into separate Images. Each Image can be no larger than 750KB in size. The Service User must then request distribution of each Image separately.

Future-dated Update Activation

SECAS noted the current requirement to allow for a Supplier to set a future activation date on their firmware updates. This date could be no further than 30 days into the future, in order to meet the Anomaly Detection Thresholds (ADTs).

The DCC proposed that firmware updates to IHDs, PPMIDs and HCALCSs be limited to immediate activation only. This would significantly reduce costs in defining test cases and test execution. It added that with future activation, as the activation date goes further into the future there is an increased risk of Image corruption.

The TABASC Chair advised that he did not see any considerable benefit in Suppliers being able to future activate their firmware updates. Two Device manufacturers advised that they saw a benefit in being able to future activate firmware, in that it would allow Suppliers to synchronise their firmware updates, especially when there are major updates to the Technical Specifications for which they must upgrade to. However, both manufacturers agreed that this benefit does not warrant any considerable increased costs or implementation timescales on the solution.

Decision: The Working Group agreed to limit firmware updates to immediate activation only. Therefore, the requirement for future dated activation has been removed.

Service Request for PPMID firmware updates

SECAS advised that there had always been a requirement to develop a new Service Request for IHD and PPMID firmware. However, the Service Provides had suggested using existing SR11.1 'Update Firmware' for IHDs and PPMIDs.

SECAS advised that since then, the SSC introduced a requirement that IHDs and PPMIDs must have separate ADT values to ESME and GSME. As a result, the DSP have confirmed that creating a new Service Request would enable them to achieve this. However, this element will require re-assessment.

Decision: The Working Group agreed that a new Service Request shall be developed in order to distribute and activate PPMID firmware. This is in order to facilitate separate ADTs required for PPMIDs.

In-Home Displays

SECAS clarified that the scope of the modification currently includes IHDs. It noted that removing IHDs had been discussed at previous meetings and that a consultation had been carried to understand the impacts of removing them. IHDs subsequently remained in the scope of the modification, as it was believed that removing them would have no material impact.

The DSP have since proposed removing IHDs as it believes that 95% of all deployed displays are PPMIDs. Furthermore, it noted that some of the 5% listed as an IHD, are wrongly listed as an IHD and are in fact a PPMID. The DSP added that IHDs have no firmware version listed in the SMI. Therefore, including them would require development in order to achieve this.

One Device manufacturer advised that it saw no benefit in including IHDs within this modification. Another Device manufacturer advised that it has already deployed a number IHDs but would accept not being able to update these Devices OTA as they would be able to update PPMIDs.

Decision: The Working Group agreed to remove IHDs from the scope of this modification.

Alerts and notifications

SECAS advised that the current SEC Schedule 8 'Great Britain Companion Specification' (GBCS) draft legal text introduces several Alerts during the process of OTA firmware updates:

- Image Discarded
- Hardware Version Mismatch
- File Transfer Failure

- File Transfer Success
- Firmware Read Failure
- Firmware Read Success

The DCC proposed to reduce the number of Alerts and Notifications, suggesting that the modification should be used as a transport mechanism only. However, it noted that this would not have large impacts on development and have minimal impacts on testing.

A member suggested that if some of these Alerts were removed, they could be added at a later date, after the implementation of the modification, as an enhancement. However, the majority of the Working Group agreed that these Alerts were beneficial to have now and noted the limited impact these Alerts would have on development and testing.

Decision: The Working Group agreed to keep the Alerts and Notifications referenced in the SEC Schedule 8 'Great Britain Companion Specification' (GBCS) draft legal text. For clarity, this requirement is unchanged.

TABASC Chair PPMID proposal

As a result of the Working Groups decision to remove IHDs from the scope of this modification, the TABASC Chair proposed an alternate firmware activation Alert method for PPMIDs. Upon successful firmware activation, instead of the Communications Hub managing the Alert for successful activation, the PPMID would send this Alert directly to the Supplier. The Alert would be directed to the Access Control Broker (ACB) on the Device. The ACB, using registration data, would then validate that the Supplier the Alert is addressed to is the Supplier for the Device.

The TABASC Chair believed this to be simpler solution for the PPMID as it minimises the impact on the Communications Hub. The TABASC Chair also noted that the reason for the using the Communications Hub to manager the Alert was because the IHD doesn't have the capability to determine its Supplier. However, IHDs have now been removed from the scope of the modification.

The DSP agreed with the TABASC Chair's points but noted that this would create an additional Alert for them to develop and test. However, the DSP agreed that this would reduce the complexity for the Communications Hub. Both Communications Services Providers (CSPs) agreed that the TABASC Chair's proposal would achieve a simpler implementation for them.

A Device manufacturer noted that the TABASC Chair's proposal would only apply to future updates. No existing devices could support this until after a successful update had been applied.

Forecasting firmware updates

SECAS advised that the DCC had requested the Working Group provide the following information in relation to PPMIDs and HCALCSs:

- To estimate how many Devices there will be at full deployment
- How many times they're expected to be updated per year; and
- To estimate the average size of each firmware update.

The DCC advised that the CSPs wanted to understand the number of firmware transactions per second to identify the impacts on the Wide Area Network (WAN).

A member noted that there are none or very few HCALCSs deployed so it is hard to estimate how many there will be at full deployment. However, the Working Group agreed that the DCC should take a ratio-based approach to identify how many PPMIDs there will be at full deployment as the DCC holds the current deployment data. Furthermore, the ratio of deployed Communication Hubs to PPMIDs is unlikely to change so could this be used to estimate future numbers.

A Device Manufacturer advised that they plan to move from three to two firmware updates a year to their PPMIDs. It also acknowledged the potential for a Supplier to reject a firmware update if they don't need the improvements that the manufacturer has applied. The other two Device Manufacturers agreed that they would carry out a maximum of two updates per year to their PPMIDs.

A Device Manufacturer advised that the average size of their firmware updates would be around 300KB. The DCC added that if the average size is around 300-350KB, this would be less traffic on the WAN than had been anticipated.

Dual Supplier scenarios

SECAS recommended that only the Lead Supplier should be able to carry out firmware updates in a dual Supplier scenario. The DCC should then forward the Alerts for the firmware update to the other Responsible Supplier.

Members noted that this would be unfair on Gas Suppliers as they would be reliant on Electricity Suppliers to carry out their updates. The Working Group deemed this requirement an unnecessary constraint and stated their preference for both Responsible Suppliers to be able to carry our firmware updates on their Devices. The Working Group accepted the risk that this may increase the of firmware updates being overwritten by the other Responsible Supplier in a dual Supplier scenario.

Decision: The Working Group agreed that in a dual Supplier scenario, both Responsible Suppliers shall be able carry out firmware updates to PPMIDs and HCALCSs.

Update on the implementation approach

SECAS advised that this modification is targeted for one of the 2021 SEC Releases. If the DCC Impact Assessment is returned in time, and the DCC has enough lead time, the modification could be targeted for the June 2021 SEC Release. However, the DCC advised that it could not guarantee it could meet the June 2021 SEC Release.

SECAS also advised that the implementation of this modification is dependent on two DCC Change Requests which are currently ongoing. The DCC clarified that it had since determined that this statement was not true and the SECMP0007 is not dependant on any Change Requests in order to be implemented.

Next steps

SECAS advised the immediate next steps will be to update the business requirements document in line with the Working Groups decisions. The DCC will subsequently re-assess the proposed solution against the new requirements set by the Working Group.

SECAS noted that both the SSC and the TABASC will review the Impact Assessment, with the SSC also intending to carry out a risk assessment on the Impact Assessment response.

Actions

- SECAS will update the business requirements document in line with the Working Groups decisions.
- The DCC will subsequently re-assess the proposed solution against the new requirements set by the Working Group.