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'

Working Group meeting summary – 28 July 2020

SECMP0007 overview

SECMP0007 'Firmware updates to IHDs and PPMIDs' proposes to provide the capability to update firmware Over-The-Air (OTA) for Smart Metring Equipment Technical Specifications (SMETS) 2+ Prepayment Meter Interface Devices (PPMIDs) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs) via the Data Communications Company (DCC) infrastructure.

OTA firmware rules

Device prioritisation

SECAS advised that PPMID and HCALCS firmware shall only be able to occupy the Gas Smart Metering Equipment (GSME) memory block on the Communications Hub (CH), with GSME firmware taking priority.

A DCC Service Provider questioned if a GSME Image would overwrite a PPMID or HCALCS Image if the Image had already started transferring to the CH. SECAS advised that the GSME Image would overwrite the PPMID/HCALCS Image in this scenario as the GSME Image takes priority.

CH Image SLA

SECAS explained the original proposal it put forward to Working Group members in April 2020 following consultation with the DCC's Service Providers:

1. Once a firmware Image is distributed to the CH, the Image would initially be stored in the flash memory for up to one week
2. If the Image had not been transferred to the PPMID after one week, it would be moved to the CH Random Access Memory (RAM)
3. The image would then remain in the RAM until the CH reboots or until it is overwritten

SECAS noted a CH could reboot at any time due to several scenarios, and so there was a high risk of an Image being discarded from the CH RAM.

However, SECAS had since received information from the DCC's Service Providers that storing the Image in the CH RAM would not be feasible and so a new approach is being proposed. This approach is as follows:

1. Once a firmware Image is distributed to the CH, the Image would be stored in the flash memory for **at least two weeks**
2. After two weeks, the image **may be** permanently deleted

Members sought clarity on the service level agreement (SLA) and whether this mean all Images would be removed from the CH after two weeks. SECAS advised that it is a minimum SLA and that the Image could remain in the CH flash memory for longer. The GB Companion Specification (GBCS) wording has been drafted to accommodate this.

PPMID volumes

Forecasted volumes of PPMID firmware updates

The DCC noted the advice it had previously received from Parties on volumes of firmware updates to PPMIDs:

- A maximum of two updates per PPMID per year
- The average size of each update is 350KB with a maximum of 750KB
- A Variance of ±10% over the year

A Large Supplier believed it would be very rare to have more than one firmware update to each PPMID per year. However, a Device manufacturer advised that it wouldn't be surprised to initially see two firmware updates per year to each PPMID in the shorter-term following implementation. Over the longer term, it expected this to drop to one firmware update per year.

Forecasted rollout of PPMIDs

The DCC presented its forecast of PPMID volumes from now until the end of 2024:

SMETS2 Device	Today	At scale (end of 2024)
PPMIDs	2.4 million	17.9 million
CHF	2.7 million	20.3 million
Current proportion of PPMIDs to CHFs		88%

Again, Members thought these forecasts may have been overestimated. A Large Supplier advised that for SMETS1 Devices, customers were not as interested in receiving firmware updates to their PPMIDs and that only 25% of its SMETS1 PPMIDs remained connected to the HAN. A member didn't believe that what had happened for SMETS1 would necessarily apply for SMETS2. However, another member cautioned against disregarding SMETS1 experiences. It acknowledged that SMETS1 and SMETS2 experiences differ, but that many aspects of the SMETS1 experience (both from the Supplier and the consumer) are still relevant.

Firmware distribution control

The DCC presented its proposals to mitigate against repeated firmware requests overloading the network in the form of firmware distribution control. The DCC is requesting these proposals be delivered in combination, not in isolation.

Firmware Distribution Control 1: In Progress Check

The DCC proposed a Device-Based Control mechanism. When a Service User requests a firmware update, the Data Service Provider (DSP) would check whether the User already has a firmware update in progress to the same HAN Device. This would apply to all HAN Devices (e.g. ESME, GSME, PPMID and HCALCS).

This prevents excessive repeated downloads from the Communications Service Provider (CSP) to the CH, preventing an “accidental Denial of Service”.

Two validation rules were proposed:

1. The DSP cannot send another firmware update to the HAN Device until the first update is complete. Those that are rejected due to this validation will generate a failure code and a list of Devices to the applicable Service Users.
2. A Device can only stay in the ‘In Progress’ status for a limited time to avoid any erroneous deadlocks, thus allowing Service Users to send new firmware update requests. The tracking timeout will be managed as a configurable duration of time.

These validation rules would be documented in the DCC User Interface Specification (DUIS).

Firmware Distribution Control 2: Too Busy

The DCC also proposed a “too busy” response from the CSP to the DSP to prevent CSP system overload. There is currently a “not available” response already in place for ESME and GSME and this would be extended to PPMIDs and HCALCSs.

Currently if the DSP receives a “not available” response it carries out an immediate retry and then carries out a retry every hour for 24 hours followed by a timeout.

The DCC proposed to extend this behaviour to the new “too busy” response and invoke the same “long retry” design pattern. It recommends that in all cases the "long retry" design pattern is extended to four days instead of the current 24 hours.

Firmware Distribution Control 3: Batch Status

The DCC anticipates a high volume of Alerts notifying the status of a firmware update over the Smart Meter Wide Area Network (SM WAN). The DCC therefore proposed that the notifications from the CSPs of success/failure of distribution to the CH should be batched on the interface between the CSP and the DSP, to potentially minimise the load on both the CSP and DSP systems.

This would result in Service Users receiving several DCC Alerts in short succession when the CSP notifies many CHs in a batch.

Additional firmware guidance

The DCC also proposed that additional guidance is made available to Service Users to mitigate the risk of wasted OTA firmware update attempts. The DCC proposed the following guidance:

- After a Supplier sends an initial update firmware Service Request (SR) (SR 11.1 ‘Distribute Firmware’ or 11.4 ‘Update PPMID Firmware’), it should wait until it receives an Alert to tell

them the Image has been successfully transferred or discarded by the CH before it resends the SR or send a subsequent SR.

- After sending SRV 11.4, the Supplier should wait for an activation Alert or failure message from the PPMID before re-sending the firmware update.
- A statement within the guidance that firmware updates must be limited to a gap of at least five days between attempts. This would reduce the loads on the CSP networks.

Working Group's views

Working Group members had no comments on the proposal themselves. However, one Member questioned how much these proposals were impacting the overall cost of SECMP0007. They believed that the issue of unnecessary repeated firmware updates already exists, regardless of whether PPMIDs are given OTA capability. They also questioned whether distribution control mechanisms should be handled separately from SECMP0007. The DCC advised that providing OTA capability to PPMIDs has a direct impact on network capacity and therefore must be addressed via SECMP0007.

Business case assessment

SECAS had sought further feedback from Parties on the business case for this modification, and had received five responses. The feedback was split into four categories:

- Security impacts
- Operational impacts
- Compatibility impacts
- Consumer impacts

Security impacts

SECAS noted that if a security risk or vulnerability is to be found with a PPMID or a HCALCS, the Device model would currently need to be disconnected or suspended. Therefore, OTA capability would provide a significant risk mitigation in this respect as a firmware update could be used to resolve the security vulnerability.

Operational impacts

A Large Supplier had given feedback on the operational impacts due to the lack of OTA capability for PPMIDs. These were:

- Contact Centre appointment booking costs
- Technician time (1 – 1.5 hours)
- Replacement PPMID hardware costs
- Triage costs
- Disposal cost if the PPMID is scrapped

The Party estimated a minimum of £75-£90 for each replacement PPMID. Therefore, a single delivery of 10,000 replacement PPMIDs to a single Supplier could cost between £750,000 and £900,000.

Compatibility impacts

Parties advised that the lack of OTA capability to PPMIDs and HCALCSs could lead to increased compatibility issues, for example when updating legacy PPMID firmware following firmware updates to ESME, GSME and/or the CH. PPMIDs may need replacing if these Devices become interoperable. Alternatively, an interoperable Device may require a CH manufacturer to develop, test and release an update to the CH.

The ability to update PPMIDs and HCALCSs OTA would mitigate against these risks. Members agreed SECMP0007 would provide an alternative method to addressing issues with Devices via CH updates.

Consumer impacts

SECAS advised that all of the impacts noted above would have inevitable impacts on consumers:

- Making time to book site visits
- Disposing of old Devices
- Loss of faith in smart metering Devices
- Lack of updates to the User Interface

Furthermore, SECMP0007 would enable customers that already have these Devices to benefit from new or additional functionality that might be delivered through firmware updates.

A Member advised that the overarching benefit from SECMP0007 will come when it prevents from having to unnecessarily replace Devices. Another Member noted that a previous “Alert storm” in the CSP North Region could have been addressed more effectively and quickly had there been OTA capability to PPMIDs.

Working Group views

Members asked if it was known whether existing SMETS2+ PPMIDs could support the SECMP0007 Proposed Solution. Two PPMID manufacturers advised that they had designed their Devices to support the SECMP0007 solution and would be able to receive OTA firmware updates. However, they noted that the new PPMID Device Alerts would not be supported by any PPMIDs already deployed.

A Member questioned whether Suppliers would be obligated to support the SECMP0007 Proposed Solution, noting that if they didn’t then this may impact the business case. Members advised that Suppliers already have an obligation to maintain their Devices and that this is dictated by the Maintenance Validity Period (MVP) in the Technical Specification Applicability Tables (TSAT).

Implementation approach

The DCC provided four possible approaches to implementing SECMP0007:

Ref.	Option
1	Do nothing/modification rejected
2	Release the entire modification in the June 2022 SEC Release
3	Deliver the DSP requirements in the November 2021 SEC Release and the CSP requirements in the June 2022 SEC Release
4	Defer the November 2021 SEC Release until the February 2022 SEC Release and deliver the DSP and the CSP South & Central requirements in this release, with the CSP North requirements delivered in the June 2022 SEC Release

The TABASC Chair advised a further option where the entirety of the SECMP0007 legal text, including the DUIS and the Communications Hub Technical Specifications (CHTS) changes, be implemented in the November 2021 SEC Release. This would include the DSP System changes. They noted that this method would allow the CSPs to implement their system and CH changes at later dates as soon as they passed all of the testing requirements. Furthermore, there would be no requirement for the CSPs to implement their CH changes in a scheduled SEC Release as the CHTS requirements would already be in effect; they could be rolled out as soon as testing had been completed and signed off. Members agreed that this would be the best approach and the DCC agreed to investigate this further.

The SSC Chair noted that a threat mapping exercise is currently underway for the HCALCS and that the Security Characteristics require updating as a result. This needs to be achieved before SECMP0007 is implemented.

Conclusion: The Working Group's preference is to implement the DSP system changes and all of the SEC legal text, including the CHTS changes, in the November 2021 SEC Release. The required changes to CHs would be rolled out later as the updates became available from CSPs, which would not need to happen as part of a SEC Release.

Next steps

SECAS advised the TABASC will further review the DCC's firmware distribution control proposals on Thursday 6 August.

SECAS will also issue a Request For Information (RFI) to better understand PPMID volumes and SEC Party implementation costs.

SECAS is aiming to complete the Modification Report and present this to the Panel at its meeting on 14 August 2020 for progression to the Report Phase.

Actions

- SECAS will issue an RFI gathering views on the remaining questions for the modification
    - Note, this RFI has now been issued and closes on Thursday 6 August 2020.