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'

Modification Report

Version 1.0

17 August 2020

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

This document also has nine annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** (attached separately) contains the redlined changes to the GB Companion Specification (GBCS) required to deliver the Proposed Solution.
- **Annex D** (attached separately) contains the redlined changes to the DCC User Interface Specification (DUIS) required to deliver the Proposed Solution.
- **Annex E** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex F** contains the full non-confidential responses received to the first Refinement Consultation.
- **Annex G** contains the full non-confidential responses received to the second Refinement Consultation.
- **Annex H** contains the full non-confidential responses received to the Request For Information (RFI).
- **Annex I** contains the firmware distribution flow diagram.

Contact

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

Joe.hehir@gemserv.com

1. Summary

This proposal has been raised by Robert Williams from E.ON.

Suppliers are responsible for the procurement, installation and maintenance of Smart Metering Equipment Technical Specifications 2 (SMETS2) Devices in customers' premises. Firmware updates are used to keep Devices up to date.

Currently Over-The-Air (OTA) firmware updates via the DCC can only be made to the Communications Hub, Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME). The Proposer of this modification seeks to address the lack of capability to update firmware for other mandated Home Area Network (HAN) Devices.

There is currently no way to execute OTA firmware updates to mandated HAN Devices, specifically In-Home Displays (IHDs), Prepayment Meter Interface Devices (PPMIDs) and HAN Connected Auxiliary Load Control Switches (HCALCSs).

This modification proposes a combination of two OTA firmware update methods; one for PPMIDs and another for HCALCS. IHDs are no longer in scope:

- **OTA method for PPMIDS**

  A ZigBee[1] OTA delivery mechanism will be used to deliver firmware images to PPMIDs. This method introduces the combined distribution and activation of the firmware updates into a single new Service Request (SR). The PPMID will manage and distribute the notification to the Service User upon activation of the firmware.

- **OTA method for HCALCSs**

  The HCALCS will utilise the existing OTA firmware update procedure used by ESME and GSME. This requires a distinct separation between the distribution and activation of the firmware image. This will be achieved by re-using existing SRs 11.1 'Update Firmware' and 11.3 'Activate Firmware' respectively.

This modification will have wide ranging impacts across all SEC Party categories, requiring changes to systems and processes, as well as introducing new capabilities in terms of updating firmware for PPIMDs and HCALCSs. The extent of these impacts has been drawn out through consulting with SEC Parties and other relevant stakeholders. These impacts are summarised further in this report. The total central costs will be approximately £19.7m and, if approved, this modification will be implemented in the November 2021 SEC Release.

[1] ZigBee is an IEEE 802.15.4-based specification for a suite of communication protocols used to create personal area networks with small, low-power digital radios, designed for small scale projects which need wireless connection.

2. Issue

What are the current arrangements?

Currently, the SEC sets out the procedure for OTA firmware updates via the DCC to the Communications Hub, ESME and GSME only.

The SEC does not set out the procedure for OTA firmware updates to IHDs, PPMIDs and HCALCSs as the functionality is not currently available.

What is the issue?

For several years, SEC Parties have advocated the inclusion of an OTA firmware update procedure for mandated HAN Devices. Not having the ability to carry out OTA firmware updates to these Devices will result in significant costs and impacts for Parties associated with:

- Operating multiple OTA and non-OTA update processes;
- Stranded assets that cannot be updated; and/or
- Site visits to locally update firmware or to replace/remove Devices.

What is the impact this is having?

The lack of an OTA firmware update procedure for mandated HAN Devices requires Suppliers to manage multiple processes and systems for updating firmware (OTA for ESME/GSME and non-OTA for other mandated HAN Devices).

There is also a risk that Devices which are not currently OTA upgradable may lose their ability to communicate on the HAN if there is a ZigBee stack[2] upgrade that is mandated, for instance to address a security related issue. This is especially relevant given that:

- IHDs and PPMIDs are key to facilitating consumers' access to information and prepayment functionality; and
- HCALCSs are load affecting Devices and therefore impact consumers' access to energy.

Throughout the progression of this modification Parties have advised on the impacts that could be experienced if nothing is done to address the issue. These are summarised below:

- Security vulnerabilities, although unlikely to occur, would not be able to be addressed via OTA updates and would instead involve suspending Devices;
- The risk of the need to replace PPMIDs and HCALCS due to lack of OTA capability would remain and could cause would high operational impacts; and
- The risk of compatibility issues as CH/ESME/GSME are updated with features that may not be supported by PPMIDs and HCALCS.

[2] ZigBee stacks separate different components and functions into independent modules that can be assembled in different ways. Zigbee is built on the Physical (PHY) layer and Medium Access Control (MAC) sub-layer defined in the IEEE 802.15.4 standard.

These impacts will cause negative consumer experiences and will add a reputational risk to Suppliers and the Smart Metering Implementation Programme (SMIP).

More information on Party impacts can be found on page 8 and more a more detailed assessment on the business case for this modification can be found on page 38.

3. Solution

Proposed Solution

The Proposer seeks to amend the SEC and DCC Systems to include the capability to update firmware OTA for PPMIDs and HCALCSs.

During industry discussions it was agreed that IHDs would be removed from the scope of this modification. Further information regarding these discussions can be found in Section 7.

This modification, developed with extensive industry collaboration, proposes a combination of two OTA firmware update methods: one for PPMIDs and the other for HCALCSs. The steps for each process are summarised below, and summary diagrams can be found in Appendices 1 and 2.

PPMIDs

A flow diagram explaining the proposed OTA PPMID firmware process can be found in Appendix 1 of this document. A further flow diagram can be found in Annex I.

Although the DCC and DCC Service Users can communicate directly with a PPMID, they are only permitted to send a relatively small set of commands none of which facilitate OTA updates. Therefore, the existing ESME/GSME OTA firmware method (which allows Suppliers and Devices to communicate end-to-end) cannot be utilised as PPMIDs to do not contain Supplier Certificates. Instead, they have Access Control Broker (ABC Certificates).

Once a firmware Image has been developed and gone through the appropriate assurance, the Supplier will send a SR 11.4 'Update PPMID Firmware'[3]. This will contain the firmware Image and the list of Extended Unique Identifiers (EUIs) of the target PPMIDs to the DCC. This would be a Non-Critical Command (a 'one-to-many' multicast). The Anomaly Detection Thresholds (ADTs) for the new PPMID Service Request will be counted separately to ESME, GSME and HCALCS SRs as these Devices are load controlling.

In contrast to the ESME/GMSE OTA firmware update procedure, the Service Request will combine both distribution and activation of the firmware within one request. This is because the PPMID is not a load controlling Device whereas the ESME/GSME is and therefore require a distinct GBCS Critical Command for the activation of firmware. Future dated activation of PPMID Manufacturer Images will not be permitted. Therefore, the Service Request will not contain a field for activation date-time.

Once the Service Request is received the DCC will then validate the firmware, calculating the Hash and checking this against the Certified Products List (CPL). Once the DCC has validated the firmware, the following steps will occur:

[3] The title of this new Service Request is yet to be determined. Currently the next available and most logical Service Reference Variant for this Service Request will be 11.4.

1. The DCC will distribute the firmware Image to the Communications Hubs associated with the target Devices.
2. The Device retrieves the new firmware Image from the Communications Hub using ZigBee OTA functionality.
3. Upon successful receipt by the Device of the OTA Upgrade Image, the Communications Hub will instruct the PPMID to immediately activate the new Manufacturer Image.
4. The Communications Hub will subsequently clear the firmware Image from its memory block.
5. After verification of the firmware Image, the Device performs the firmware activation.
6. The PPMID will then create a Device Alert containing its new/current firmware version and send it to the DCC.
7. The DCC will update the Smart Metering Inventory (SMI) if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

HCALCSs

A flow diagram explaining the proposed OTA PPMID firmware process can be found in Appendix 2 of this document. A further flow diagram can be found in Annex I.

The HCALCS will utilise the existing OTA firmware update procedure used by ESME and 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 SR11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

This will be accomplished by extending the following Service Reference Variants to support HCALCS:

- SR 11.1 'Update Firmware'
- SR 11.2 'Read Firmware Version' (note, SR 11.2 will be extended to support PPMIDs as well)
- SR 11.3 'Activate Firmware'

The HCALCS solution has taken this approach because an HCALCS is a load controlling Device and contains Supplier Smart Metering Key Infrastructure (SMKI) Certificates. This means that to activate the firmware on the Device, it must be verified against the Device's security credentials via a GBCS Critical Command. This cannot be achieved with the combined distribution/activation approach being utilised by PPMIDs.

SECAS and the Proposer note that assurance of the overall process will need to be considered. This includes activities such as interface testing with the DCC as well as Device level certification and testing. The Firmware Management Design Note will need updating to reflect changes to the process as specified above.

The business requirements for this solution can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties	✓	DCC

Supplier Parties

Suppliers are responsible for the procurement, installation and maintenance of SMETS2 Devices in customers' premises. They have a responsibility to ensure Devices are operating correctly and efficiently. Therefore, a fit for purpose OTA firmware management process covering all mandated Devices would support Suppliers in delivering their obligation consistently.

In response to the first Refinement Consultation on this modification, several Supplier Parties advised that this modification would require changes to systems and IT infrastructure, as well as business processes. Some respondents noted this as a negative impact due to the effort required to implement these changes. Respondents also noted positive impacts with the increased capability to fix Devices remotely rather than through site visits, and with a greater capability to innovate with PPMIDs and HCALCSs.

The following benefits have also been highlighted by Parties if this modification were to be implemented:

- OTA capability to PPMIDs and HCALCS could serve as a security risk mitigation by addressing security vulnerabilities via firmware updates, instead of suspending and potentially replacing such Devices;
- Savings in costs and resources by preventing the unnecessary replacement of PPMIDs and HCALCSs by maintaining them with OTA firmware updates; and
- Easier to maintain compatibility of HAN Devices by applying OTA firmware updates.

These impacts will inevitably lead to a better consumer experience and therefore feedback for Suppliers.

Electricity Network Parties

In response to the first Refinement Consultation, an Electricity Network Party highlighted that this modification would inevitably impact overall system performance which may have minor knock on effects for Electricity Network Parties. Specifically, this may be in terms of its ability to communicate with a meter whilst an PPMID firmware update is in progress. This could mean that they may have to make minor system changes to facilitate this modification.

Other SEC Parties

PPMID and HCALCS manufacturers will be impacted by this modification as their Devices will be able to receive firmware updates OTA via the DCC's infrastructure. Other impacts also include:

- It is assumed that Manufacturers will notify the SEC Panel of Device Model details and assurance certificates when adding a PPMID or HCALCS to the Central Products List (CPL);
- Suppliers will need to add Manufacturer Image Hashes associated with PPMID and HCALCS CPL entries; and
- Manufacturers will need to digitally sign the association of the Manufacturer Images Hash and the CPL model details.

The full responses received from Parties can be found in Annexes F and G.

DCC System

All the DCC's Service Providers will be impacted as a result of this modification. Service Providers will be required to support additional Alerts, Commands, and Responses. They will also need to support the anticipated changes required for billing and reporting systems/components to incorporate the additional Service Request transaction charges.

The impacted components for each Service Provider have been listed below. The full impacts on DCC Systems and the DCC's proposed testing approach can be found in the DCC Impact Assessment response in Annex E.

Data Service Provider

The Proposed Solution has several impacts across the Data Service Provider (DSP), the components of which are listed below:

Summary of DSP impacts	
Device	**Impact**
PPMID	• Communications Service Provider (CSP) Smart Meter Wide Area Network (SM WAN) Gateway and CSP Interfaces • Changes to the Self-Service Interface (SSI) • Energy Service Interface Inventory Extract • DCC User Gateway Interface Design Specification (DUGIDS), DUIS Service Requests, and Message Mapping Catalogue (MMC) Alerts and Messages • Updates to the CPL • Transform – New GBCS Use Case
HCALCS	• DUGIDS documentation updates for SR11.1, SR11.2 and SR11.3 • Updates to processing of these Service Requests • Changes to GBCS Use Cases

Communications Services Providers

The Proposed Solution has several impacts across the CSPs, the components of which are listed below:

Summary of CSP impacts	
Device	**Impact**
PPMID	• CSP North SM WAN; • CSP/DSP Interfaces; • Communications Hub functionality • Queuing prioritisation
HCALCS	• Requires Design, Build, and Test changes to the CSP solutions to support the delivery of firmware Images for HCALCS Devices to appropriate connected HAN Devices. • Support the delivery of firmware for HAN Devices from the Communications Hub to the connected Device over the HAN • New GBCS Use Cases required

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Schedule 8 'Great Britain Companion Specification'
- Schedule 9 'Smart Metering Equipment Technical Specifications 2'
- Schedule 10 'Communications Hub Technical Specifications'
- Schedule 11 'TS Applicability Tables'
- Appendix E 'DCC User Interface Services Schedule'
- Appendix R 'Common Test Scenarios Document'
- Appendix AB 'Service Request Processing Document'
- Appendix AD 'DCC User Interface Specification'
- Appendix AF 'Message Mapping Catalogue'

The changes to the SEC required to deliver the Proposed Solution can be found in Annexes B, C and D.

Note, the GBCS, DUIS and MMC changes, including the XML Schema changes for the latter two documents, are still being assessed jointly by the DCC and SECAS, and are still subject to change. Any further changes are expected to be minor.

Consumers

This modification will positively impact consumers. The capability for Suppliers to update PPMID and HCALCS firmware OTA will mean less chance of Suppliers having to schedule site visits to maintain

or replace these Devices. This would provide more convenience for consumers as they will not be required to schedule and set aside time to accommodate these site visits.

This modification could indirectly improve consumers' trust in the SMIP, as their Devices would be more likely to be operating on the optimal firmware version with Suppliers able to quickly resolve any bugs. In addition, this modification would enable consumers that have PPMIDs to benefit from new or additional functionality that might be delivered through firmware.

Other industry Codes

This modification will not have an impact on any other Industry Codes.

Greenhouse gas emissions

This modification will not have an impact on greenhouse gas emissions. However, the inability to update the firmware on a Device may lead to additional otherwise unnecessary replacement of functional Devices. The disposal of these Devices may then have a detrimental impact on greenhouse gases.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is £20,800,000. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£13,600,000
Systems Integration Testing (SIT)	£3,800,000
User Integration Testing (UIT)	£1,600,000
Implement to Live	£700,000
Application Support	£1,100,000

More information can be found in the DCC Impact Assessment response in Annex E.

SECAS costs

The estimated SECAS implementation costs to implement this modification is four days of effort, amounting to approximately £2,400. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry; and
- Reviewing and publishing OTA firmware guidance to the industry.

SEC Party costs

All Refinement Consultation and RFI respondents advised that they would incur costs in implementing this modification. These have been summarised below:

- The capability to update firmware OTA may increase the number of firmware updates. Consequently, additional resource may be required to manage the due diligence of firmware updates;
- System and process impacts, with significant testing for every combination of the newly upgradeable HAN Devices with all Communications Hubs; and
- The cost for updating to a new version of DUIS, which would be via a scheduled SEC Release and likely include the implementation of other modifications.

Some respondents also advised that they would see cost savings as a result of this modification. These have been summarised below:

- Parties would experience a dramatic reduction in the risk of a Device irrecoverably failing in the field, which would be a material benefit; and
- Reduced risk of unnecessary costs, because fixes to Devices could be applied remotely without the need for a physical visit to the property and unnecessarily replacing the Device.
- A reduction in customer queries and contact related to Device issues

Note, two Device manufacturers have advised that they have already implemented the Proposed Solution for their Devices, so their extra costs would be minimal and would mainly consist of additional end-to-end testing.

The full Refinement Consultation responses received can be found in Annexes F and G.

The full RFI responses can be found in Annex H.

6. Implementation approach

Approved implementation approach

The Panel has agreed an implementation approach of:

- **4 November 2021** (November 2021 SEC Release) if a decision to approve is received on or before 4 November 2020; or
- **24 February 2022** (February 2022 SEC Release) if a decision to approve is received after 4 November 2020 but on or before 24 February 2021.

The Proposer, Working Group members and the DCC agree that the implementation date for this modification must be as soon as possible to reap the most benefit from it. Therefore, if a decision to approve is not received in time for the November 2021 SEC Release, SECAS recommended that this modification is instead implemented in the February 2022 SEC Release. This will require making this release a SEC Systems Release.

The Proposer and Working Group's preference is to implement the Data Services Provider system changes and all of the SEC legal text, including the CHTS changes, in the November 2021 SEC

Release. The required changes to Communications Hubs would be rolled out later as the updates became available from CSPs, which would not need to happen as part of a SEC Release. This approach would not require a split implementation approach.

7. Assessment of the proposal

Summary

This Proposal has been time consuming and complex. Below is set out the key areas of concern that have been discussed and the changes that have occurred during the Refinement Process. These discussions are summarised below with references to the page numbers in which these discussions can be found:

- Which Devices will this modification apply to: see page 14.
- Should PPMIDs be CPA Certified: see page 16.
- Local firmware updates: see page 16.
- DCC Assessments: see page 19.
- How will a PPMID firmware update be initiated: see page 21.
- Activation date-time of PPMID firmware: see page 23.
- How will Firmware Images be managed: see page 24.
- OTA Firmware Alerts: see page 27.
- Communications Hub impacts: see page 29.
- Forecasting firmware updates: see page 33.
- DCC firmware distribution control: see page 34.
- Liability scenarios: see page 37.
- Implementation approach: see page 37.
- Support for Change: see page 38.
- Business case assessment: see page 39.
- Views against the General SEC Objectives: see page 43.
- Panel views: see page 44.

In order to help the reader follow the development of each issue, a timeline of key meetings and decisions is provided in Appendix 3.

Which Devices will this modification apply to?

Consumer Access Devices

It was initially considered that IHDs, PPMIDs and HCALCS would all be in the scope of this modification. A Working Group member had asked if Consumer Access Devices (CADs) were to be considered as well. However, as the specific format and structure of CADs are unknown and are largely consumer-driven options, it was unclear how the modification could be extended to cover them. As such it was concluded that CADs were excluded from this modification but could be raised under a separate modification if a Party felt it was necessary.

HCALCSs

In the early stages of the Refinement Process, HCALCSs were temporarily removed from the scope of this modification. This was due to perceived security concerns and uncertainty as to the impact their inclusion would have on the business case. The Proposer and the Working Group later re-assessed this and agreed that a considerable number of Parties would require the OTA capability for HCALCSs in the future.

The Security Sub-Committee (SSC) was later asked, in April 2018, for its views on the inclusion of the HCALCS in this modification. The SSC was keen that HCALCSs should be capable of being updated OTA since they are a load controlling Device and have a more critical role than IHDs or PPMIDs.

The SSC agreed that there are no security concerns with extending OTA firmware capability to HCALCSs. It added that there is a greater security risk to HCALCSs if they are not capable of OTA updates, as this would make it harder to apply security updates to the Device.

The SSC advised that the activation of HCALCS firmware must be verified against the security credentials on the Device and hence issued via a GBCS Critical Command. This is due to HCALCS being a load controlling Device subject to CPA Certification.

Considering the view of the Working Group and the SSC, the Proposer opted to include HCALCSs in this modification.

IHDs and PPMIDs

Due to the high costs and complexity of the Proposed Solution, the DCC suggested removing IHDs from the modification in order to explore cost savings. The requirements would be constrained to PPMIDs and HCALCS only. Subsequently, the Proposer briefly opted to remove IHDs from the scope of the modification. The Working Group believed that the vast majority of deployed IHDs are in fact PPMIDs with IHD capability built in, and so this should be acceptable.

However, it was noted that in order to quantify the number of deployed standalone IHDs, Parties would be asked as part of the Refinement Consultation to assess the impact of excluding IHDs from the Proposed Solution. The Working Group pointed out that the removal of IHDs could further reduce the role of the IHD in the market.

The second Refinement Consultation was issued in May 2019. The majority of respondents believed there would be minimal impact to consumers if IHDs were removed from the scope of this modification. However, three respondents made points that indicated consumers would be impacted enough to warrant putting IHDs back in the scope of this modification. Furthermore, the DCC also later advised that excluding IHDs would **not** have a material cost impact on the modification. The Proposer subsequently opted to include IHDs in the scope of the modification.

After the 2019 Refinement Consultation, a Working Group meeting was held in December 2019 to look at ways to reduce the costs of the solution. The DSP noted 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.

Subsequently the Working Group agreed to remove IHDs from the scope of this modification.

Conclusion
Following these discussions, the Proposer has agreed that this modification is applicable to PPMIDs and HCALCSs only.

Much of the discussion within this Section 7 include references to IHDs as these had been included in the scope of the solution at the time.

Should PPMIDs be CPA Certified?

The Working Group questioned whether PPMIDs (which are currently not CPA certified) should be CPA certified if they are to be able to receive OTA firmware updates. This would likely influence the solution for PPMIDs. SECAS asked the Department for Business, Energy and Industrial Strategy (BEIS) for advice regarding the appropriate security level for PPMIDs.

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.

Local firmware updates

Initial views

Concerns were raised with the use of local updates and its impact on the modification. Members highlighted that the continuation of local firmware updates could cause unreliable information being stored in the SMI because the local update process does not directly flow through the DCC's validation checks. Therefore, the DCC is unable to track these updates and if Suppliers do not update the SMI it will be incorrect.

The Working Group discussed the option of using local updates as a backup to OTA updates. Parties would have to proactively make sure firmware for the Device is logged on the CPL for the SMI to be up to date. If a Party carried out a local update without updating the CPL, the firmware version listed on the SMI would not reflect that on the Device. Subsequently, the information gained from SR8.2 'Read Inventory' would be incorrect. Members discussed the option to create governance for this, but it was highlighted that this would involve added costs.

Inaccurate SMI information may not necessarily impact the Supplier updating the Device as it would have initiated the update. However, the impacts of this could be felt more acutely following a Change of Supplier. If for example a gaining Supplier used the SMI to read the firmware version after a local update, the information received would not reflect what is on the Device. Furthermore, the gaining Supplier would not know this. This could only be rectified by a new OTA firmware update or by the gaining Supplier sending SR11.2 'Read Firmware Version'. The Device would then return the correct firmware version and the SMI would be subsequently updated.

The Working Group noted that local firmware updates could not be blocked if carried out locally. This was raised as a security concern. The Proposer decided to ban local updates as part of this modification although noted that this could not be effectively enforced.

geo's proposal to permit local updates

Following on from the DCC's Preliminary Assessment and the subsequent Refinement Consultation, Green Energy Options (geo) raised concerns with the banning of local updates. These were aimed at the impacts this would have on PPMIDs. geo believed that innovation would be severely curtailed if local updates to firmware were not permitted. It also noted that additional features are continually being added to the PPMID and a need for more regular updates to these features.

As Suppliers are not obligated to support firmware on HAN Devices, geo's view was that banning local updates would increase the risk of 'stranding' a Device, especially as Supplier churn increases. geo went on to propose two amendments to the current solution, which would permit the use of local updates to PPMIDs. The advantages and disadvantages for each option are summarised in the tables below:

geo's Proposal 1: Query Next Image Request		
Process	**Advantages**	**Disadvantages**
'Query Next Image Request' command is carried out once every 24 hours by the Device.	24-hour frequency of the process would ensure accuracy of the SMI	At full rollout, all deployed PPMIDs carrying out the 'Query Next Image' could lead to an "Alert Storm".
Upon receipt of the 'Query Next Image Request', the Communications Hub would extract the current firmware version and provide the data to the DCC.		
The process would be repeated after completion of a firmware update (OTA or local) and after locating the Communications Hub.		Communications Hub does not know what firmware version the Device is running. Therefore, the Communications Hub will have to forward the firmware version of that Device to the DCC, even if it has not changed firmware version. To prevent this from happening, it was suggested that the Communications Hub could store the firmware version for the Device. Therefore, it would know on the 'Query Next Image Request' if the Device was reporting a new firmware version and prevent unnecessary Alerts to the DCC. However, SECAS noted this proposal to be a break from the current Proposed Solution; the Communications Hub has been envisaged to transfer firmware information, rather than store it for periods of time. Storing information on the Communications Hub would require additional functionality in the Communications Hub, which would increase costs and complexity.
Communications Hub would respond with either: • No Image available; or • Information concerning the Image available for download by the Device		

geo's Proposal 2: Firmware Changed Alert		
Process	**Advantages**	**Disadvantages**
Upon completion of a firmware update (OTA or local), the Device would send an Alert or notification to the DCC to inform it of the update. The Alert would include the new active firmware version on the Device.	PPMID proactively sending an Alert to the DCC would ensure accuracy of the SMI	Applicable to PPMIDs only, not IHDs. IHDs do not have the capability to send Alerts to the DCC, as they do not have the appropriate Device Certificates. Note, IHDs have since been removed from scope of this modification and subsequently, the Working Group decided to include geo's proposal for PPMIDs to proactively send an Alert to the DCC upon activation of the firmware.

Making sure authorised Parties can carry out local updates

SECAS explained the current firmware process means updates can only be applied by the Responsible Supplier Party. First, the firmware and the Firmware Hash are submitted to the DSP, who validate the Firmware Hash against the CPL. If it is successfully validated, the CSP then sends the firmware to the target Devices. After the activation of the firmware on the Device, the SMI is updated to reflect this. If the Firmware Hash is not on the CPL, the firmware update will not be executed.

The Working Group was unsure how this process could be mirrored using geo's proposals. It was noted that there is nothing to stop a Party from locally updating a Device with firmware not listed on the CPL. This could then create a discrepancy between the CPL and the SMI if, following a local update, a Supplier sends SR11.2 'Read Firmware Version'. This would result in the SMI being updated with the correct firmware version, but consequently it would not reflect what is on the CPL.

Members suggested a DCC gateway screening mechanism could ensure only authorised Parties can locally update firmware. However, this does not currently exist. A DCC gateway screening mechanism would need to be designed and implemented by the DCC, adding additional time and costs to the progress of the modification.

Vote on geo's proposals

The Working Group proceeded to vote on whether to progress geo's proposals as an Alternative Solution under this modification. All Working Group members, other than geo, voted not to take forward these 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 believed that geo had proposed some good ideas and encouraged geo to raise its own Draft Proposal to have its ideas assessed.

SSC consideration of local firmware updates

In November 2019 SECAS advised the Working Group that the SSC had discussed the proposed ban on local firmware updates. The Technical Architecture and Business Architecture Sub-Committee (TABASC) Chair believed that the ban on local updates to IHDs and PPMIDs proposed by this modification may present unnecessary constraints on Parties and other participants in the SMART

ecosystem. 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 Proposed Solution would not be able to track local firmware updates. 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 DSP would 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 would mean the firmware version would be generally correct on the inventory, it would still be necessary to ask the Device directly before updating the firmware to be sure and so might not deliver any benefit.

Subsequently the SSC 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 considered that local updates were feasible subject to appropriate security controls.

In December 2019, 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. The Proposer supported these views.

Conclusion
The Proposer and the Working Group agreed not to ban local firmware updates as there is no ban currently in place and any such ban could not be enforced.

DCC Preliminary Assessments

The first Preliminary Assessment

The DCC provided a high-level Preliminary Assessment in May 2017 which estimated a cost of between £7.3m and £8.2m up to the end of PIT to implement the modification based on the requirements at that time. The DCC also noted that the total cost and implementation lead time may increase following further analysis by its Service Providers.

The Proposer and the Working Group raised questions in relation to the business case of the modification and the high cost to complete a DCC Impact Assessment. They also noted that there was limited information on how many IHDs and PPMIDs will be in use at the time of implementation. It

was noted that some physical Devices may be replaced with applications on consumer Devices such as phones or those connected via Wi-Fi.

Whilst noting that there are assumptions and non-functional requirements outlined in the Preliminary Assessment that require clarification and development, the Proposer and the Working Group agreed that a Refinement Consultation would be the best method to assess the next steps. A second Refinement Consultation was subsequently issued to clarify these areas. These responses were used to inform a second Preliminary Assessment.

The second Preliminary Assessment

The DCC's second Preliminary Assessment contained an assessment of two solution options, one of which had two variants:

- **Option 1:** Original approach using Zigbee OTA delivery
- **Option 2:** Extend existing OTA firmware method
    - **Option 2A:** Including IHDs
    - **Option 2B:** Excluding IHDs

The DCC highlighted going through the CPA procedure under Option 2 would considerably increase the costs on Suppliers to implement the Proposed Solution. The Proposer and Working Group agreed with this assessment.

The DCC stated that although Option 2 had not been requested in the Preliminary Assessment it had been explored as the DCC believed it reduced the complexity of the solution and provided the Proposer with an alternative to the original approach.

Questions were also raised around the £12.3m cost up to the end of PIT given for Option 1. The DCC noted that Option 1 would require different processing patterns for the DSP, CSPs and the Communications Hub. This was due to the requirement for a new Service Request, requiring a change in the DSP and CSP interface in order to accommodate this.

Do the costs of either option present a business case for the change?

Suppliers and Other SEC Parties highlighted that the second Preliminary Assessment only considered the costs for the DCC to test and implement the solution and did not account for the costs on other SEC Parties. These costs would be significant and should be considered as part of the business case due to the emulation testing Parties would have to carry out as part of any solution. Furthermore, the Working Group felt the DCC had not considered the increased costs for Parties to undergo CPA under Option 2.

The Working Group advised that a breakdown of the costs was needed in order to justify them. The DCC noted that it is currently working with the Panel to improve the costs analysis for modifications, making it easier for Parties to determine the business case for every modification.

The DCC noted that the implementation costs given in its Assessment were based upon the assumption that this modification would be implemented as a standalone SEC Release, as the Authority has requested. The DCC acknowledged that this isn't necessarily what Parties would want, and the industry would look to combine several modifications to maximise efficiency and reduce costs. However, a standalone SEC Release could be a possibility.

What did the Proposer agree to take forward?

Partly due to the high costs as well as the complexity of the Proposed Solution, the Working Group agreed that in order to progress the modification, it would seek a combination of the two solutions given in the DCC Preliminary Assessment. The DCC suggested the requirements in Option 1 could be constrained to PPMIDs in order to explore cost savings, and that IHDs could be left out of the solution. The Working Group believed that the vast majority of deployed IHDs are, in effect, PPMIDs with IHD capability, and so this should be acceptable.

However, it was noted that in order to quantify the number of standalone deployed IHDs, the second Refinement Consultation would seek this information from Parties. The Working Group acknowledged that the removal of IHDs from the proposal could further reduce the role of IHDs in the market.

The Proposer noted that they would not remove the HCALCS from the solution, as they anticipated that the demand for OTA capability to these Devices would increase.

Conclusion
As a result, the Working Group agreed to progress with a combination of the two solutions: **1.** Original Approach, Zigbee OTA Delivery for IHDs and PPMIDs **Note**: this solution now only includes PPMIDs. As noted above, IHDs were later removed from the scope of this modification. **2.** Extend Proven ESME/GSME OTA Firmware Method for HCALCSs

How will a PPMID firmware update be initiated?

The following record of the discussions that took place include IHDs as these were included in the solution at the time.

SECAS's and the DCC's views

SECAS and the DCC identified two options for enabling a Supplier to initiate their OTA firmware update to an IHD/PPMID.

The DCC was in favour of using the SR11.1 for IHDs and PPMIDs, rather than creating a new Service Request for these Devices. It believed that using SR11.1 would allow for a faster implementation of the solution whilst also reducing costs. Cost savings would be achieved on the SSI, Service Audit Trail (SAT), SIT/UIT and reporting.

However, it was noted that SR11.1 does not have the functionality to activate firmware. Furthermore, ESME/GSME/HCALCS and IHDs/PPMIDs would each follow different procedures for firmware updates. Therefore, if SR11.1 were to be used for IHDs/PPMIDs, the DCC would need to be able to differentiate between these Devices and ESME/GSME/HCALCS firmware.

SECAS proposed adding a new Service Request, specifically designed for the combined distribution and activation of IHD/PPMID 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 Service Request.

The SSC noted its requirement for the DCC to be able to differentiate firmware updates to IHDs/ PPMIDs from ESME/GSME/HCALCS firmware. This would be essential to enable separate ADT values for IHDs/PPMIDs and ESME/GSME/HCALCS. This would enable anomalies with the potential to affect energy supply (ESME/GSME/HCALCS0 to be detected separately from those for PPMIDs.

The SSC therefore agreed that a new Service Request for the combined distribution and activation of IHD/PPMID firmware would better achieve this. However, it was not against 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 Service Request should be created for firmware updates to IHDs and PPMIDs, noting that a new Service Request would make the process easier to manage as each Device type is following a different procedure. They added that they believed it would likely have lower implementation costs as well.

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

A Working Group member noted that the use of SR11.1 could be easier for the DCC to implement as it would only impact the 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 DUIS for the Service User. However, SECAS noted that a new GBCS Use Case would be required. It added that creating a new Service Request 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 Extensible Markup Language (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 Service Request for what 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. This is that the DCC must be able to differentiate between Device types, as well as be able to apply different ADT values to each Device type.

The IHD/PPMID Service Request was later discussed at the December 2019 Working Group meeting. SECAS advised the Working Group the DSP had since confirmed that creating a new Service Request would be the only way to enable it to achieve the SSC's ADT requirement for IHDs/PPMIDs. However, IHDs were removed from the scope of this modification in the same meeting. Therefore, the new Service Request would only apply to PPMIDs.

Are Users mandated to submit ADTs for PPMIDs?

Section G 'Security' requires Users to submit ADTs for Critical Commands. They may at their own discretion submit ADTs for Non-Critical Commands. As the new Service Request for updating PPMID firmware will be a Non-Critical Command, the SSC was asked to confirm whether Users would be mandated to submit ADTs for this Service Request. The SSC agreed that Users would not be mandated to submit ADTs for PPMID firmware updates, as with other Non-Critical Commands. However, the SSC agreed that DCC guidance should be made available recommending that Users submit ADTs for PPMIDs.

The SSC confirmed its intention was to make sure ADTs for ESME, GSME and HCALCS could be counted separately as these are load controlling Devices. It agreed this would be achieved as PPMIDs will have its own separate standalone Service Request.

Conclusion
The Working Group agreed that a new Service Request will be developed to distribute and activate PPMID firmware. This is in order to facilitate separate ADTs required for PPMIDs and ESME/ GSME/HCALCS.

Activation date-time of PPMID firmware

Enabling future activation date-time

SECAS presented a proposal to the SSC to permit the future activation of IHD and PPMID firmware updates. The SSC advised that there is a security risk posed by allowing Suppliers to set a future activation date-time for the Device. However, the SSC would allow for this requirement, as long as IHDs and PPMIDs are subject to the same ADT regime as EMSE/GSME, but counted separately.

SECAS proposed a six-month limit on future dating firmware updates, in line with the proposal under SECMP0024 'Enduring Approach to Communication Hub Firmware Management'. However, the SSC advised this is too long and the limit must be set to no more than 30 days. This is in order to match existing ADT volume regime as ESME/GSME.

Immediate activation only

After the Panel asked for the solution to be made Minimum Viable Product, SECAS held a meeting with the DCC's Service Providers to find ways in which to streamline the solution. The requirement for future activation date-time was highlighted as having a significant impact on costs and timescales.

This requirement was subsequently discussed at the December 2019 Working Group meeting where the decision was made to remove IHDs from the scope of this modification. 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 firmware Image corruption.

The TABASC Chair advised that they 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 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.

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

How will Firmware Images be managed?

Firmware Image size

The Working Group noted that HAN Devices have a limited capacity for storing firmware Images. A member pointed out that larger Images may slow down the HAN. That said, typically firmware Images for non-meter Devices are small, in the region of 256-512 kilobytes (KB).

CHTS section 4.4.4 requires that the receiving Communications Hubs can buffer Images intended for ESME and GSME. The CSP contracts require Communications Hubs to have the capacity to hold two 750KB Images (to support independent distribution of firmware to one of the ESME and the GSME). The Working Group acknowledged this obligation and agreed that OTA Upgrade Images[4] must be less than or equal to 750KB. Firmware larger than 750KB would be split into single Images less than or equal to 750KB in size. Members agreed there is nothing preventing fragmentation of firmware now, if the Device is built to support it.

Handling firmware[5] larger than 750KB

After the Panel asked for the solution to be streamlined, SECAS, the DCC and its Service Providers held a meeting to discuss options. One of these was the size of firmware Images, specifically how the DCC would handle fragmented updates. The Service Providers proposed to remove the requirement for fragmented Images by limiting firmware updates to 750KB only. They advised that limiting the update size would reduce costs and effort in development, with significantly reduced costs in defining test cases and test execution. Furthermore, they added that fragmentation carried risk, such as image corruption, requiring repeated image sending, and subsequent overwrites. Lastly, the Service Providers believed that fragmentation would require further development to Communications Hubs to manage the fragmentation process.

At the December 2019 Working Group meeting, the Working Group was advised of the DCC Service Providers' proposal to remove fragmentation and to limit the size of any firmware updates to no larger than 750KB in size.

SECAS and the Working Group advised that it would be up to the Device manufactures to fragment their firmware updates into Images of less than or equal to 750KB in size. The Suppliers would subsequently distribute each fragmented firmware Image as a standalone update.

It added that the process does not propose any changes to the way in which the DCC currently manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

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.

[4] Means the concatenation of the OTA Header and the Upgrade Image that is equal to or less than 750KB. This is defined in the GBCS and in the DUIS.

[5] Means a package of firmware which can be made up of a single Manufacturer Image or several Manufacturer Images.

Conclusion
The Working Group agreed that any firmware updates over 750KB in size must be split into separate Images. Each individual Image must be equal to or less than 750KB in size. The Service User must then request distribution of each Image separately.

Activation of fragmented Images

The Working Group questioned how setting the activation date-time to 'zero' would impact the activation of a fragmented Image, specifically any before the final fragmented Image. Further, if doing so would mean that the Image is downloaded by the Device and stored until the second part of the Image is downloaded.

Note, the concept of setting an activation date-time no longer exists as the capability for future activation was removed by the Working Group. However, as firmware will now only be activated immediately, this question still applies. The DCC confirmed that both parts of the Image would be activated on the activation 'date-time' specified in the last Command where there are fragmented Images.

Suppliers will not receive an Alert with the new firmware version until all the fragmented Images have successfully been activated.

Each Manufacturer will provide specific guidance on how to activate multiple Images within a release note.

Rejected firmware Images

PPMIDs

The DCC advised that a provision could be built in to the 'UpgradeEndResponse' Command from the IHD (now removed from this modification) and PPMID to the Communications Hub. This Zigbee Cluster Library (ZCL) Command would specify whether the Image has been successfully downloaded. If the download is unsuccessful, the Communications Hub would then create a Device Alert containing an indication that the Image was invalid and send it to the DCC. The DCC would forward the Device Alert to all Responsible Suppliers.

HCALCS

Questions were raised as to how the Device would inform the Communications Hub if an Image was rejected due to, for example, not being able to verify the signature in the Image. The DCC advised that the Device would send a corresponding Alert to the appropriate Supplier.

Failed firmware Images

It was noted that the Communications Hub can only communicate with the target Devices when they are switched on. Consequently, the Devices cannot download or activate firmware Images when they are switched off.

Switched off Devices leads to two possible scenarios:

1. **Failed distribution**

   If the Device is switched off during the distribution of the Image from the Communications Hub to the Device, the distribution will fail. The Image will remain on the Communications Hub until it is overwritten by a new Image for the same Device or by a GSME Image. However, this could lead to a scenario where the Image occupies the memory block for a considerable amount of time, or indefinitely, if it does not reach the Device or isn't overwritten. In this scenario, the Image is essentially 'pending'.

   The discussions held for pending Images are found in the 'Communications Hub memory blocks' section of this report below.

2. **Failed activation**

   If the Image is successfully distributed to the Device, but the Device is subsequently switched off before the Image is activated, the activation will fail. At any point once the Device is switched back on, the Image may automatically be activated if the Device can support this.

Dual Supplier scenarios

SECAS noted that it was the Working Group's intention for the dual Supplier requirements developed under SECMP0024 'Enduring Approach to Communication Hub Firmware Management' to apply to this modification as well. SECMP0024 introduces the requirement whereby in a dual Supplier scenario, both the Import and Gas Suppliers need to coordinate firmware updates. It was proposed that both Suppliers need to agree to proceed in the event that one Supplier wishes to deploy a firmware update. However, this approach was not taken forward due to the streamlining of the solution carried out in December 2019. Specifically, the requirement for immediate activation only meant there would be no benefit in allowing Responsible Suppliers to coordinate as they wouldn't have a window for which to agree the timing of a firmware update.

The Energy and Utilities Alliance (EUA) also asked if a firmware update with fragmented Images would succeed in a Change of Supplier (CoS) event. It was advised that the new Supplier may not have access to the Images as it may not have an established relationship with the Manufacturer. SECAS advised that the Supplier would have the following options if a CoS were to take place during a firmware update:

- The gaining Supplier could simply choose to do nothing and leave the firmware on the Device as it is;
- The gaining Supplier could pick the update up from where it left off; or
- The gaining Supplier could overwrite the already distributed Images with a new firmware update.

Device manufacturers would have to explain all three options via release notes.

At the December 2019 Working Group meeting, SECAS sought a decision from the Working Group on how to handle dual Supplier scenarios for PPMIDs. SECAS recommended that only the Lead Supplier should be able to carry out firmware updates in a dual Supplier scenario. The DCC would 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 to PPMIDs. 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.

Note, only the Lead Supplier as defined in the DUIS shall be able to update HCALCS firmware OTA.

Conclusion
The Working Group agreed that in a dual Supplier scenario, both Responsible Suppliers shall be able carry out firmware updates to PPMIDs, and that only the Lead Supplier (as defined in the DUIS) shall be able to update HCALCS firmware.

OTA Firmware Alerts

What Alerts will Suppliers receive?

It was acknowledged that Suppliers will need to receive Alerts at various stages during the process. The Working Group agreed that Suppliers would receive the following Alerts:

1. The first Alert would be sent to all Responsible Suppliers (except for the sender as the sender would receive a Service Response) once the DCC has processed the Service Request to distribute the Image. The Alert would include a list of specific Device IDs that were referenced in the original Service Request.
2. The second Alert would be generated by the Communications Hub and sent to all Responsible Suppliers with confirmation of success/failure of distribution to the Devices. This would confirm one of the following;
    a. Image Discarded
    b. Hardware Version Mismatch
    c. File Transfer Failure
    d. File Transfer Success
3. The third Alert will be a Device Alert sent to all Responsible Suppliers confirming the firmware version on the Device. The discussions around the mechanism for this Alert can be found in section ‘firmware activation Alert mechanism’ sub-section below.

SECAS, the DCC and its Service Providers identified potential cost-savings. One of these was the reduction in Supplier Alerts. The Service Providers suggested that the solution be used as a transport mechanism only, rather than a way to deliver, monitor, and confirm the status of the update. However, the DCC acknowledged that there have been requests from Suppliers to receive more information, such as diagnostics around firmware updates in order to improve reliability.

At the December 2019 Working Group meeting, the Working Group were advised on the DCC’s Service Providers proposal to reduce Supplier Alerts. A member suggested that if some of these Alerts were removed, they could be added at a later date, after the implementation of this modification. 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.

Conclusion
The Working Group agreed to keep the original proposed Alerts.

Firmware activation Alert mechanism

Initial approach

The delivery of the success/failure Alert to the Supplier was initially proposed to be managed and driven by the Communications Hub. IHDs don't have Supplier or Access Control Broker (ACB) SMKI Certificates. Therefore, IHDs cannot communicate end-to-end with Suppliers. In order to enable IHDs to hold these Certificates would require costly and timely development. Furthermore, IHDs would also have to undergo CPA certification due to the security implications, which can be a lengthy process.

To facilitate this, the Communications Hub would set a reminder 10 minutes from the point the Image had successfully been distributed to its target Device. It would also record the IHD/PPMID Device ID against that reminder. When that time has passed, the Communications Hub would read the firmware version from the target Device and send a Device Alert containing the subsequent value to the DCC. The DCC would then update the SMI if the firmware version had changed and forward the Device Alert to Responsible Suppliers recorded to receive the Alert. This Alert would indicate delivery of the Image and that the IHD/PPMID successfully activated the Image.

New approach

The Working Group opted to remove IHDs from the scope of this modification in December 2019. As a result, the TABASC Chair proposed an alternate firmware activation Alert method for PPMIDs. This was considering the initial approach had been designed to cater for IHD limitations.

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 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 a simpler solution for the PPMID as it minimises the impact on the Communications Hub. They also noted that the reason for the using the Communications Hub to manage the Alert was because the IHD doesn't have the capability to determine its Supplier.

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 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. The Working Group agreed that manufacturers needed to ensure that the first OTA firmware update to already deployed PPMIDs following the implementation of SECMP0007 needed to include the functionality implemented by this modification. If this initial OTA firmware update were to fail, the sending Supplier will not receive an Alert confirming this as the Device will not have the capability to do so.

Subsequently, SECAS initiated discussions with three PPMID Manufacturers in January 2020, two of which responded. Both manufacturers agreed to the new approach and requirements were updated for the DCC to proceed with its Impact Assessment.

Conclusion
Due to the removal of IHDs, PPMIDs will generate the Device Alert for success/failure of activation to the Responsible Suppliers. The Communications Hub will not manage this process and will not be required to record the activation date-time of the Image.

Communications Hub impacts

Memory block management

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

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

The DCC currently use dedicated memory blocks on the Communications Hub for ESME and GSME firmware. It 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 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. Considering these impacts, the DCC proposed that IHD/ PPMID/HCALCS firmware should be restricted to the ESME block only.

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 the Sub-GHz band. 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 on the WAN. Consequently, it increases the risk of the Communications Hub creating a bottleneck for firmware updates, increasing pressure on the WAN.

SECAS noted the current estimates for the timescales of GSME firmware updates:

- GSME firmware is likely to be updated once per year; and
- Each GSME 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 proposed 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.

Suppliers raised concerns with the use of both memory blocks as it would not be possible 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. However, SECAS advised that Supplier Alerts will be generated, advising whether firmware updates have been successfully downloaded and activated. At any point in time, SR11.2 ‘Read Firmware Version’ can be utilised in order to read the firmware version for the Device.

A Working Group member advised that IHD/PPMID 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 added that it plans to add functionality to the DSP, flagging when firmware updates are in progress. It could use this information to notify the Service User if there is an update in process, preventing firmware Images from being overwritten.

In later discussions between SECAS, the DCC and its Service Providers, the use of memory blocks was again identified as an option to streamline the solution. All of the DCC Service Providers preferred the use of a single block for IHD, PPMID and HCALCS firmware. They advised that the use of both blocks would impact the technical architecture, and that the testing is the driver of increasing costs. The number of test cases would increase, and the behaviour when a new update arrives is more complicated.

At the December 2019 Working Group meeting, SECAS sought a decision from the Working Group on which, if not both, memory blocks should be utilised by PPMID and HCALCS firmware.

Members repeated their preference for use of a single block, making it easier for Suppliers to orchestrate 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 two blocks, ESME or GSME, on the Communications Hub should be used for PPMID and HCALCS firmware. Previous discussions had suggested that if a single block were 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 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 ESMEs at any one time, including an Auxiliary Load Control Switch (ALCS), so it would be free for a minimal amount of time.

Conclusion
The Working Group agreed to restrict PPMID and HCALCS firmware Images to the GSME block of the Communications Hub.

Additional memory space

The Communications Hub currently has two memory blocks: one for the ESME and one for the GSME. The Working Group questioned why additional memory on the Communications Hub had not been considered. The DCC stated that this is possible but will cost considerably more to implement. The Proposer also stated that they would not want to propose additional memory as part of this modification. The Working Group agreed that this should be addressed under a separate modification if another Party saw this as necessary.

Conclusion
No additional buffer space on the Communications Hub is being proposed.

Device prioritisation

PPMID and HCALCS firmware Images will utilise the GSME memory block. The Working Group agreed that ESME and GSME updates are of higher priority than PPMID and HCALCS updates, although ESME is not impacted due to its memory block not being utilised. Therefore, if a GSME Image arrives whilst a PPMID or HCALCS Image in progress, the PPMID or HCALCS Image will be overwritten by the GSME Image.

The Working Group agreed that PPMID and HCALCS will not have priority over one another. Therefore, if another PPMID or HCALCS Image arrives whilst a PPMID or HCALCS update is in progress, the newly arrived Image will overwrite the one in progress at any point in time.

A Working Group member questioned whether there would be a greater advantage for allowing the PPMID or HCALCS Image process to complete. This would prevent two Suppliers competing to update simultaneously. However, another member advised that the overall process would take approximately 10-15 minutes. Therefore, the probability of two Suppliers simultaneously sending firmware Images to a PPMID or HCALCS is unlikely.

Pending firmware Images

Initial solution

In relation to the 'failed firmware Images' section above, SECAS noted the DCC's proposal to prevent Images occupying a memory block indefinitely. The DCC proposed a two-day service level agreement (SLA) for an Image to occupy a memory block without initiating its distribution to the Device. If distribution had not commenced after two days, the Communications Hub would remove the Image and free up the memory block.

The Working Group was 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 IHDs and PPMIDs to be switched off for long periods of time, in some cases up to six months or more. It also questioned the benefit of clearing the memory blocks if they are eventually overwritten. The Working Group agreed that it is up to Suppliers to manage their firmware and to plan updates in a logical order to prevent this from happening. Therefore, if a customer has their PPMID switched off during a firmware update, the Image will still be available on the Communications Hub for download and activation once the Device is switched back on, unless it has been overwritten.

Limitations and proposed workaround

During the Impact Assessment, the CSP North Service Provider found that leaving the Image indefinitely on EDMI Communications Hubs (as used in the CSP North) will negatively impact the Communications Hub Flash memory and shorten the life of the Communications Hub.

SECAS and the DCC proposed that when the firmware update is sent to the Communications Hub, it would initially be stored in the flash memory for up to a week. If the Image has not been sent to the PPMID after one week, it would be moved to the Communications Hub Random Access Memory (RAM). The image would remain in the RAM until the Communications Hub reboots or until it is overwritten. In both cases the Communications Hub would generate an Alert that the image has been discarded.

Note that Communications Hub reboots may occur at a random time when any of the following take place:

- A new ESME firmware update
- A Communications Hub fault
- A power outage
- A Communications Hub firmware update

To prevent repeated Image attempts from Service Users, SECAS will develop a firmware guidance note as part of this modification. This will recommend that Suppliers carry out a Firmware Read using SR 11.2 before attempting a firmware update for any Device. If they get a positive response, they should update that Device; if not, they should try again in one month's time. As noted in the example above, if a PPMID is not connected, this would prevent wasting network capacity by attempting a firmware update. This procedure requires the PPMID to support the Read Firmware Command and excludes currently installed PPMIDs.

In addition, where a Service User has initiated a firmware update, it should wait until it gets an Alert for a successful transfer/image discarded before attempting another firmware update.

Second workaround and agreed approach

After completing its assessment of this modification, EDMI concluded that storing the image in the Communications Hub RAM after it is deleted from Flash would not be feasible, due to the sector sizes that are available in the RAM. As a compromise, EDMI proposed holding the Image in the Communications Hub Flash memory for a minimum of two weeks, instead of one. After two weeks, the image could be permanently deleted.

Members sought clarity on the SLA and whether this mean all Images would be removed from the Communications Hub after two weeks. SECAS advised that it is a minimum SLA and that the Image could remain in the Communications Hub flash memory for longer. The GBCS wording has been drafted to accommodate this.

SECAS noted drawback of the previous idea of storing the image in the RAM would have been an informal way of extending the storage duration on the Communications Hub, as the Communications Hub could re-boot at any time, subsequently clearing the RAM.

SECAS also noted that the GBCS drafting places a requirement on the Communications Hub to send an Alert for each Device associated with an image when the image has:

- successfully transferred to the target Device;
- failed to transfer to the target Device after all retries (at ZigBee level) have been exhausted; or
- been discarded due to a time-out.

The Supplier will then know the status of the file transfer and whether the image needs resending. If the image is discarded after the mandated storage duration, then the PPMID may not be operational.

As noted above, a Supplier could read the firmware version (SR 11.2) on the PPMID (after initial upgrade or new installation of a PPMID which supports this SR). The absence of a response would indicate that the PPMID isn't operational and the Supplier should not attempt to update the firmware on the Device.

Conclusion
The Image shall remain on the Communications Hub a minimum of two weeks, after which it may be discarded.

Logging of updates

Initial drafts of the GBCS legal text specified that the Communications Hub would log the progress of up to 15 Devices in the Upgrade Image list. The DCC and its Service Providers identified this requirement as one that could possibly be removed in order to streamline the solution.

SECAS highlighted this at the December 2019 Working Group meeting. The DCC advised that neither of the CSPs currently carry out such logging and that the 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 by reading the firmware version on the Device.

Conclusion
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.

Forecasting firmware updates

Size and frequency of firmware updates

In December 2019, the DCC asked the Working Group to estimate the following in relation to PPMIDs and HCALCSs:

- How many Devices there will be at full deployment
- The frequency of updates to these Devices per year
- 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 very few HCALCSs, if any, 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 hold 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 it plans to move from three to two firmware updates a year to its PPMIDs. It also acknowledged the potential for a Supplier to reject a firmware update if it doesn'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 its firmware updates would be around 300KB. The DCC added that if the average size is around 300-350KB, there would be less traffic on the WAN than had been anticipated.

In 2020, the DCC again sought feedback on PPMID volumes. 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:

DCC forecast of PPMID volumes		
SMETS2 Device	**Today**	**At scale (end of 2024)**
PPMIDs	2.4 million	17.9 million
Communications Hub Function (CHF)	2.7 million	20.3 million
Current proportion of PPMIDs to CHFs		88%

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.

Request For Information responses

SECAS issued a RFI in late July/early August 2020 which included a question for Parties to advise how many times they expect to update the PPMIDs in their estate each year. Those who were able to advise responded with either once or twice a year. No Parties believed that PPMIDs would be updated any more than twice per year. This is consistent with the feedback noted above from the Working Group meetings.

However, there were varying responses as to how the updated would be spread across the year. Two respondents believed the updates would be made in a single batch, whereas two other respondents believed the updates would be spread throughout the year.

The full responses received from Parties can be found in Annex H.

DCC 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 requested these proposals be delivered in combination, not in isolation. The TABASC and the Working Group considered these proposals and their views on each are provided below.

Firmware Distribution Control 1: In Progress Check

The DCC proposed a Device-Based Control mechanism. When a Service User requests a firmware update, the 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 CSP to the Communications Hub, 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 DUIS.

A TABASC member questioned in the event of a timeout under validation rule 2, whether a User would be notified or if it would have to manually check this. The DCC advised that the firmware tracking mechanism provided by the DSP would address this and ensure Users have a view of where in progress their firmware updates are. The SMI will automatically update with the subsequent firmware version and Users will receive Alerts which will systematically update Users on the progress of their firmware updates.

The TABASC asked the DSP to clarify whether the ‘In Progress Check’ is carried out against Device IDs or the Communications Hub for the given HAN. The DSP confirmed that this check would be carried out against the target Device ID, not the Communications Hub. This was due to feedback from the Working Group and previously from the TABASC that an ‘In Progress Check’ against the Communications Hub would not be favourable.

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.

The TABASC questioned whether Users will know why their firmware update has failed in the event of the CSP “too busy” scenario. The DSP noted that the only User impact as a result of this firmware distribution control would be after four days from the CSP “too busy” response, the DSP would generate an N22 ‘Failure to deliver Update Firmware Command to CSP’ Alert to the User. The TABASC agreed that this Alert would provide Users with enough information.

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 Communications Hub 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 Communications Hubs in a batch.

The TABASC questioned whether this firmware distribution control was adding significant complexity onto the DCC Systems and consequently adding costs. The DSP advised that this control is not a significant driver of cost for it to change its Systems for this modification.

The TABASC also questioned whether the DCC had considered a new “batched Alert” as a result of the CSPs batched notifications to the DSP. The DSP advised that a new “batched Alert” could add considerable cost onto the Proposed Solution and had therefore not been considered.

Conclusion
Firmware Distribution Controls 1, 2 and 3 will be put in place if SECMP0007 is approved.

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 request (SR 11.1 or 11.4), it should wait until it receives an Alert to tell them the Image has been successfully transferred or discarded by the Communications Hub 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.

The DCC also proposed a managed schedule be agreed between the DCC and appropriate Parties. However, the TABASC preferred that the DCC actively contacts those Users overloading the network whenever this happens. The Working Group agreed with this approach.

Working Group’s views

Working Group members had no comments on the Firmware Distribution Control. However, one Member questioned how much these changes 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.

Liability scenarios

Liability scenarios were raised in order to facilitate discussion on the existing liability limitations, loss recovery provisions and dispute resolution procedures. It was highlighted that the SEC does not currently extend Supplier responsibilities to Devices that form part of other Smart Metering Systems (SMSs) in the same premise for which the Supplier is not the Responsible Supplier. This means that if an Import Supplier damaged a GSME by upgrading the firmware on an IHD/PPMID/HCALCS that forms part of both the Gas SMS and the Electricity SMS, it would not be liable for the damage to the GSME, and vice versa. However, it was noted that that if a Supplier damages a Communications Hub that forms part of a SMS for which it is the Responsible Supplier, it would be liable to the DCC for that damage.

The Working Group agreed the liability for physical damage should lie with the sender of the Image but questioned how a Supplier would know who the sender was. The DCC advised that it would keep this in its audit trail. However, there are constraints on the information that can be shared. The Working Group suggested that the affected Supplier should raise an incident in such an event and request that the DCC advise on the sender of the Image.

SECAS asked the Working Group whether liabilities for damage to physical property should remain as currently set out in the SEC (limited to £1million per incident) and the Working Group agreed to the provision. It was also noted that disputes and appeals can be raised with the SEC Panel, in line with the current procedures for a larger scale problem.

Implementation approach

The DCC provided four possible approaches to implementing SECMP0007:

DCC implementation approaches	
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 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 Communications Hub 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 Communications Hub 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.

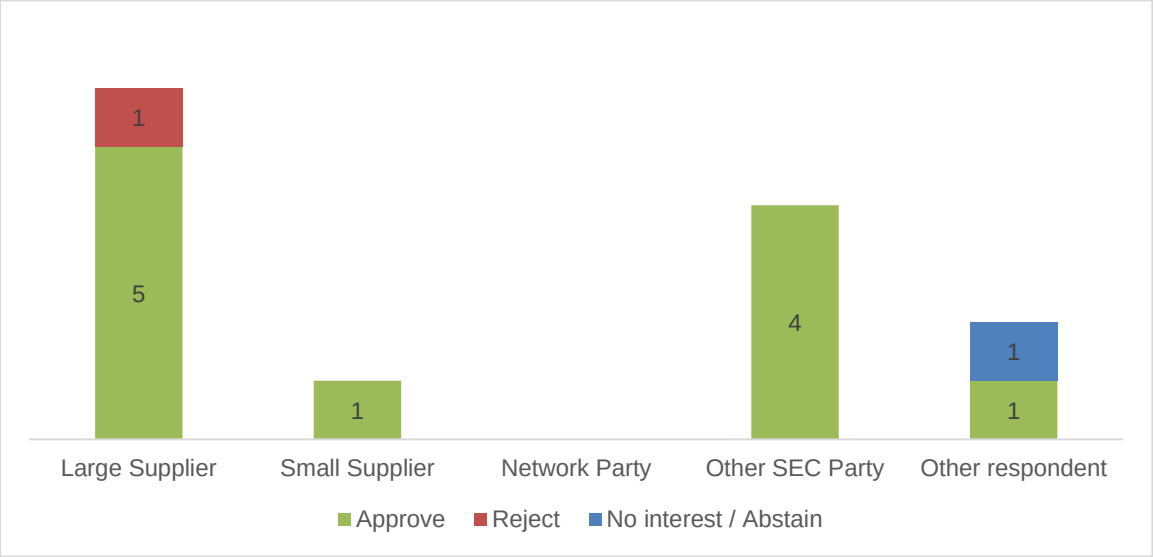
Conclusion
The Working Group's preference is to implement the DSP system changes and all of the SEC legal text, including the CHTS changes, in the November 2021 SEC Release. The required changes to CHs would be rolled out later as the updates became available from CSPs, which would not need to happen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

Support for change

Refinement Consultation responses

Views on the solution

The below graph shows the responses to the second Refinement Consultation (2019) question 1 'Do you agree with the solution put forward?':



Ten respondents agreed with the solution put forward by this modification, noting that it would prevent unnecessary site visits and limit the risk of stranded Devices. These respondents also agreed with the different approaches for PPMIDs and HCALCSs. Two of the supportive respondents raised points in their responses. One advised that although it agreed with the solution, it was concerned the costs noted in the DCC's Preliminary Assessment. Another advised that the solution needs to be compatible with existing Devices. It added that this is necessary to maximise the benefits to be gained from making this change and minimise the number of Devices that would remain exposed to the risk of stranding. Note, two PPMID manufacturers have since advised that they have designed their SMETS2 PPMIDs on the assumption that SECMP0007 is approved and would therefore be able to support OTA firmware updates. However, some of the existing Devices may not be able to support the additional Alerts introduced by this modification.

One respondent did not agree with the solution put forward. This was due to the ban on local firmware, which has since been removed. They added that they disagreed with one of the assumed benefits of the solution; providing a more reliable and an up to date SMI. They added that their experience with the current firmware ESME/GSME firmware solution, which the HCALCS Proposed

Solution relies on, is that it is not reliable. The respondent also raised concern with the longer-term use of the solution. They believed that they could be undermined by new technology.

Views on the modification, noting the costs and benefits

Seven respondents to the second Refinement Consultation (2019) agreed this modification should be approved, noting the costs and benefits. They advised that the benefits of this modification outweighed the high costs given in the Preliminary Assessment. Respondents said that the costs to industry to maintain the system through Device replacement are prohibitively high compared to the costs to implement OTA capability through this modification. Another advised that the volumes of Devices, especially PPMIDs, that are being installed means that the risk of stranding such Devices is significant and will increase as the rollout accelerates. OTA firmware updates will prevent these Devices from being stranded.

One respondent noted their concern at the high costs of this modification and its value for money. However, they acknowledged this modification represents important functionality that would provide significant value to consumers and needs to be approved promptly.

Noting the costs and benefits of this modification, three respondents did not agree that this modification should be approved. Those who provided rationale advised that this is due to the high implementation costs associated with this modification.

The full responses received can be found in Annex G.

Working Group attendees

Frequent Working Group attendees strongly advocate the implementation of this modification as soon as possible, especially in the case of PPMIDs. Common feedback has been that this modification is need by Manufacturers and Suppliers as a matter of urgency, noting this modification was raised in 2016.

The SSC

The SSC is keen that HCALCSs should be capable of being updated remotely since they are load controlling and have a more critical role than IHDs or PPMIDs. The SSC noted that there is a greater security risk if HCALCSs are not capable of being updated OTA.

At the latter stages of the DCC's Impact Assessment, the SSC commissioned a risk assessment against HCALCS and OTA capability. The SSC highlighted that the HCALCS has the same security profile as the ESME as it can affect the supply of energy. Therefore, the security risks associated with updating an HCALCS OTA should be no different from updating an ESME OTA. The Proposed Solution for the HCALCS has been designed to align with the ESME OTA process for this reason. However, at present, the CPA Security Characteristics will prevent OTA capability and will therefore need to be amended if this modification is approved.

Business case assessment – Party feedback

Towards the end of the Refinement Process SECAS sought feedback from Parties for the business case of this modification. Five Parties responded, two Large Suppliers and three Other SEC Parties,

all of which believe the modification does have a business case although no specific costs have been provided.

Their feedback can be put into four categories:

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

Security impacts

If a security risk/vulnerability is to be found with a PPMID of HCALCS, currently a Supplier would have to disconnect or suspend the Device on the SMI. This could also lead to all the Devices for a given model/version to be disconnected from the HAN or suspended on the SMI.

One Party advised that, given the functionality of the PPMID, the type of issue that is most likely to arise is a security issue or vulnerability. It noted that while it is relatively easy to quantify the impact of such a widespread issue arising, it is hard to know how likely it is that such an issue, one that would require PPMIDs to be disconnected or suspended, would occur.

Therefore, OTA capability would provide a significant risk mitigation in this respect, as it would allow Device manufacturers to develop a firmware update that could resolve the vulnerability and be rolled out remotely.

Compatibility impacts

Parties advised that that lack of OTA capability for PPMIDs and HCALCS could lead to increased interoperability issues with other Devices on the HAN.

A Supplier advised that smart metering is complex with a variety of Device types and Device manufacturers all needing to work together. As much testing as might be done before the rollout of Devices begin, it is hard to identify all issues, and impossible to test Devices with every possible combination of equipment that might be found in a customer's home. It noted at least one issue where a PPMID and meter have issues communicating with each other, but when either is paired with another manufacturer's Device, they both work fine. In this case both manufacturers could be construed as aligning to the technical specifications, but with a slightly different interpretation. If the Device that is 'at fault' is the PPMID, it would be more efficient to resolve that Device, rather than having to apply a fix to the meter to make it work with the PPMID.

A Device manufacturer also noted the impacts of OTA capability and mitigating interoperability issues. It outlined two possible scenarios with incompatibility issues between a PPMID and Communications Hub with each Device being at fault.

If the Communications Hub was at fault and without OTA capability, the Communications Hub manufacturer would be required to develop, test and release an update to the Communications Hub, stalling other updates/fixes that are part of the same release. However, with OTA capability, the PPMID manufacturer could test and release an update to the PPMID instead which may be faster and cheaper. This might allow the Communications Hub release to proceed with lower overall cost to the industry.

If the PPMID was at fault and without OTA capability, either the Communications Hub manufacturer would need to introduce a new release or the impacted PPMIDs would need to be recalled and replaced. However, with OTA capability, a new firmware update that resolves the incompatibility could be prepared by the PPMID manufacturer and a roll-out plan developed to ensure maximum uptake of the update to the affected PPMIDs.

Ultimately, if a PPMID or HCALCS does become incompatible with other Devices on the HAN, without OTA capability, the Device may need replacing.

Operational impacts

As noted above, the lack of OTA capability to PPMIDs and HCALCS increases the risk of these Devices being replaced. A Supplier noted significant impacts for replacing these Devices:

- Contact centre appointment booking costs;
- Technician time (if required): 1-1.5 hours;
- Replacement PPMID hardware costs;
- Triage costs; and
- Disposal cost if the Device is scrapped.

One Party estimated that it is a minimum of £75-£90 for each replacement PPMID. Therefore, a delivery of 10,000 replacement PPMIDs could cost between £750,000 and £900,000 for a given Party. This cost could escalate quite quickly where an issue affects many Devices across many Parties.

Consumer impacts

All of the above impacts will have inevitable impacts on consumers:

- Making time to book site visits;
- Disposing of old Devices;
- Loss of faith in smart metering Devices; and
- Lack of updates to the User Interface and other consumer benefiting features.

A Party advised that this modification would enable customers that already have these Devices to benefit from new or additional functionality that might be delivered through firmware. Another Party advised that without OTA capability to PPMIDs and HCALCS, the risks will result in a negative consumer experience and will add a reputational risk to Suppliers and the Smart Metering Implementation Programme (SMIP). Considering these impacts, the overall benefits argument for smart metering will be lessened.

Costs and cost-savings

In addition to the feedback received above, SECAS also issued a RFI in late July/early August 2020 which included a question for Parties to advise if their organisation would incur any costs and/or realise any cost savings in implementing SECMP0007.

There were seven respondents, six of which advised they would see cost savings, either directly or indirectly. These Parties advised the following:

- A decreased risk in their Devices irrecoverably failing
- A reduction in engineer site visits; one Party advised this could reduce by around 10%
- A reduction in customer queries and contact related to Device issues

The growing cost of doing nothing

One Supplier noted the unsustainability of the growing number of PPMID firmware combinations due to the lack of OTA capability. It estimated that based on a £20 cost for a PPMID, a change requiring the upgrade of firmware to 10% of its estate could equate to £1.1m to replace all PPMIDs.

It provided another example based on its predominant Device provider. It currently has six different firmware versions on the same model. To get them all up to the latest version, it would need to replace just under 50% of the Devices. Based on its portfolio, this could equate to £4.5m. It added in the worst possible situation, it needed to upgrade just those on that model, it would equate to £10m for just that given Device model.

Lastly, the Supplier advised that in the period of 1 August 2019 to 31 July 2020, it sent out over 16,000 replacement Devices. This equates to £320,000 in a year.

Another Supplier advised that based on the volumes of PPMIDs that are installed, it would require a relatively low percentage of them to need to be replaced to get to a benefit equivalent to the DCC implementation costs.

Additional Party costs of SECMP0007 is implemented

The majority of respondents advised that they would not incur significant additional cost as a result of SECMP0007.

Additional costs would include:

- The cost for updating to a new version of DUIS, which would be via a scheduled SEC Release and likely include the implementation of other modifications
- Additional end-to-end testing that comes from having PPMIDs and HCALCSs support OTA capability
- Additional IT costs to support and manage the implementation of OTA capability, though not expected to be excessive

The full responses received from Parties can be found in Annex H.

Views against the General SEC Objectives

Proposer's views

Objective (a)[6]

The Proposer believes that SECMP0007 will better facilitate SEC Objective (a). The Proposed Solution will provide for a fit for purpose, efficient and effective process for updating firmware for IHDs, PPMIDs and HCALCSs. It would additionally allow Energy Suppliers to avoid unnecessary costs relating to replacement of Devices and site visits thus helping to ensuring the sustainability of Devices for the longer term.

Objective (c)[7]

The Proposer believes that SECMP0007 will better facilitate SEC Objective (c). This modification would allow consumers to better manage their energy usage by having sustainable most-up-to-date Devices that provides them with energy related information.

Objective (d)[8]

The Proposer believes that SECMP0007 will better facilitate SEC Objective (d). The Proposed Solution would allow Energy Suppliers to use a fit for purpose, efficient and effective process for updating firmware on IHDs, PPMIDs and HCALCSs. This process would be consistent between all Energy Suppliers and the HCALCS process will be aligned to the ESME/GSME firmware process.

Objective (f)[9]

The Proposer believes that SECMP0007 will better facilitate SEC Objective (f). The Proposed Solution will use a fit for purpose, efficient and effective process for updating firmware on these Devices. This would cover any potential security vulnerabilities on the IHD, PPMID or HCALCS that may need be addressed via a firmware update.

Industry views

Ten respondents to the second Refinement Consultation agreed that this modification would benefit at least one of the SEC Objectives, with all ten in unanimous agreement that it would benefit Objective (a). They noted reasons such as increased interoperability of PPMIDs and the avoidance of unnecessary costs in replacing these Devices.

The majority of the ten respondents in support advised that this modification would benefit Objective (c). They advised this modification would maintain the Devices' ability to enable Consumers to manage their use of electricity and gas. This is because the Devices would remain as up to date as could be.

---

[6] To facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.

[7] To facilitate Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems.

[8] To facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy.

[9] To ensure the protection of Data and the security of Data and Systems in the operation of this Code.

Two respondents agreed this modification would benefit SEC Objective (d). They believed that this modification would provide an industry standard process for updating firmware on PPMIDs.

Three respondents agreed that this modification would benefit SEC Objective (f) as it would enable Suppliers to patch any security vulnerabilities that arise in PPMIDs in a quicker and more manageable fashion to current processes where OTA is not available.

One respondent thought that this modification would also benefit SEC Objective (e)[10] which had not been noted by the Proposer. The respondent believes this modification will facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy.

One respondent did not believe this modification would benefit any SEC Objectives. It specifically noted this against Objective (a), advising that the cost effectiveness of this modification is finely balanced and, in its opinion, negative. It noted the costs of the modification and the implementation timescales as reasons for its views why SECMP0007 does not better facilitate the SEC Objectives.

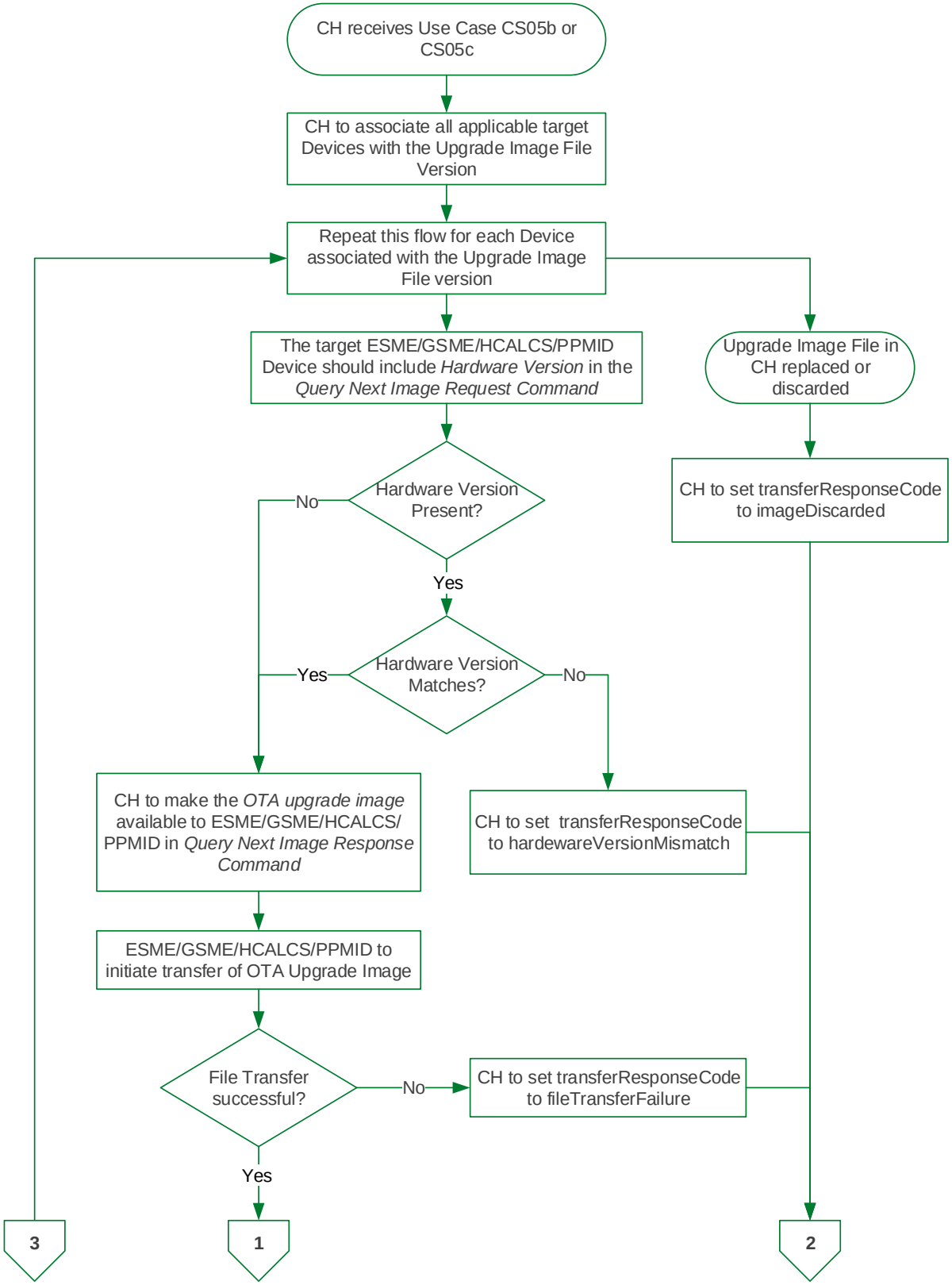
The full responses can be found in Annex G.

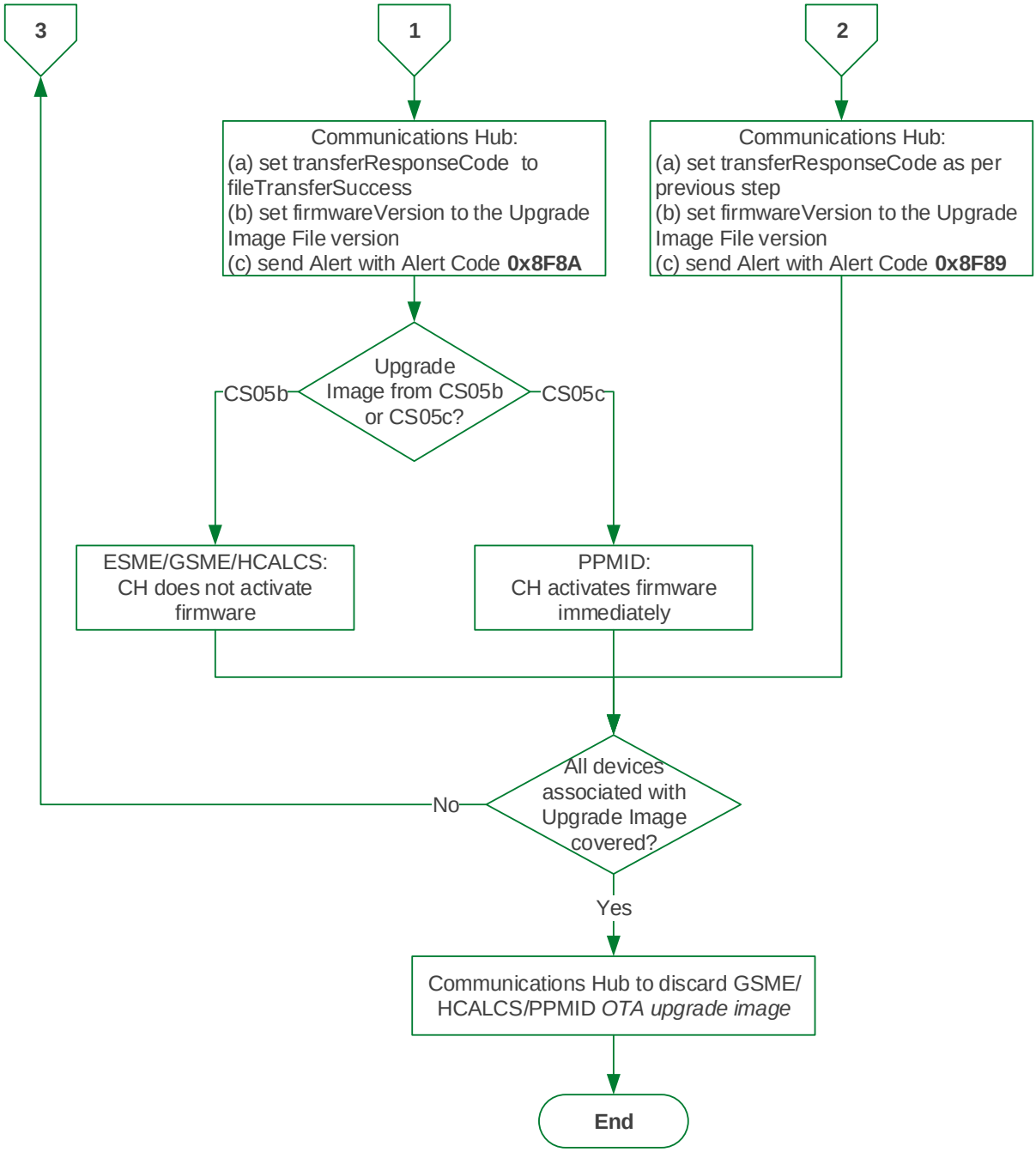
Panel views

The Panel agreed that this modification is ready to progress to final decision and should be progressed as an Authority Determined Modification.

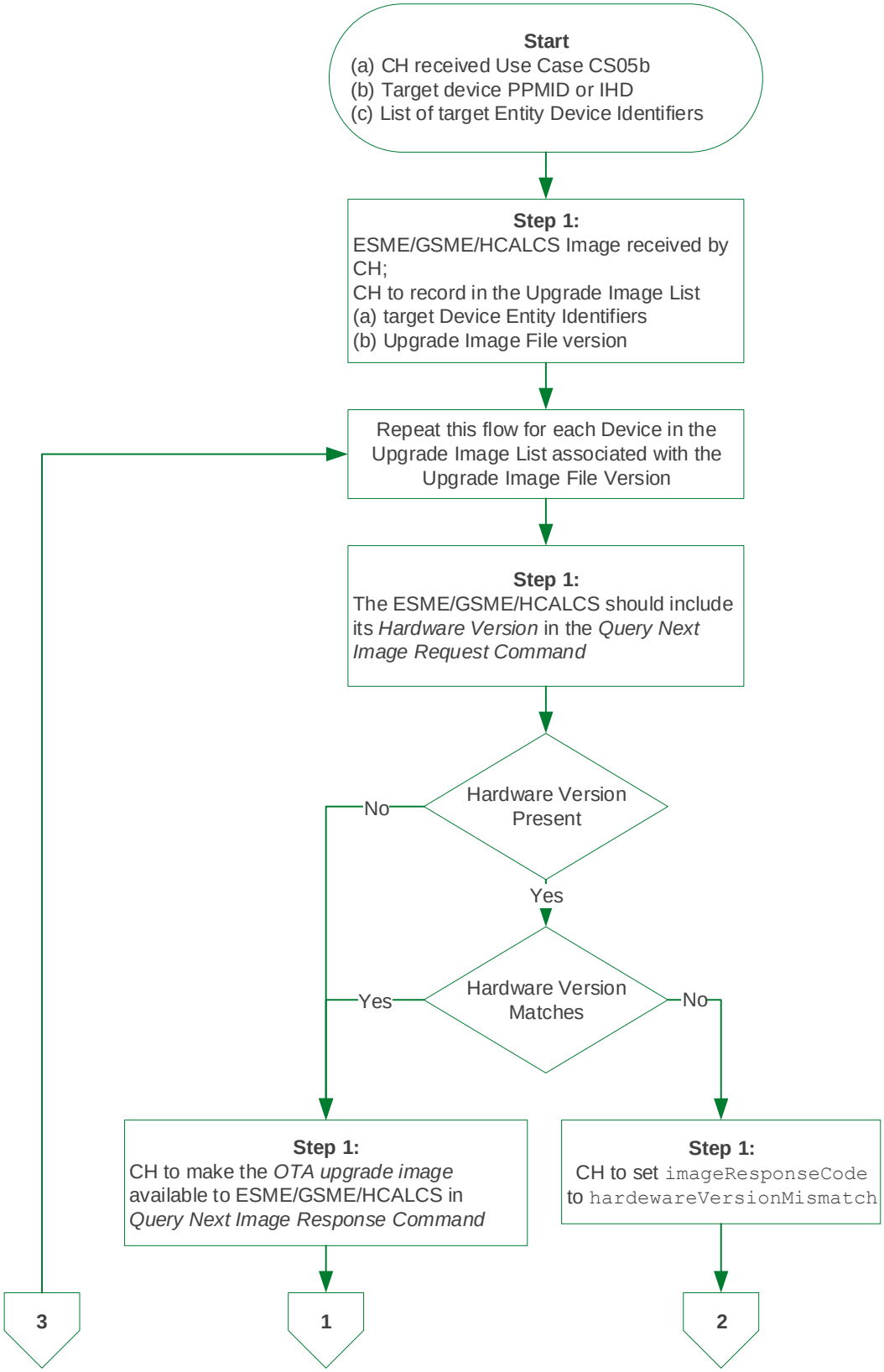
[10] To facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy.

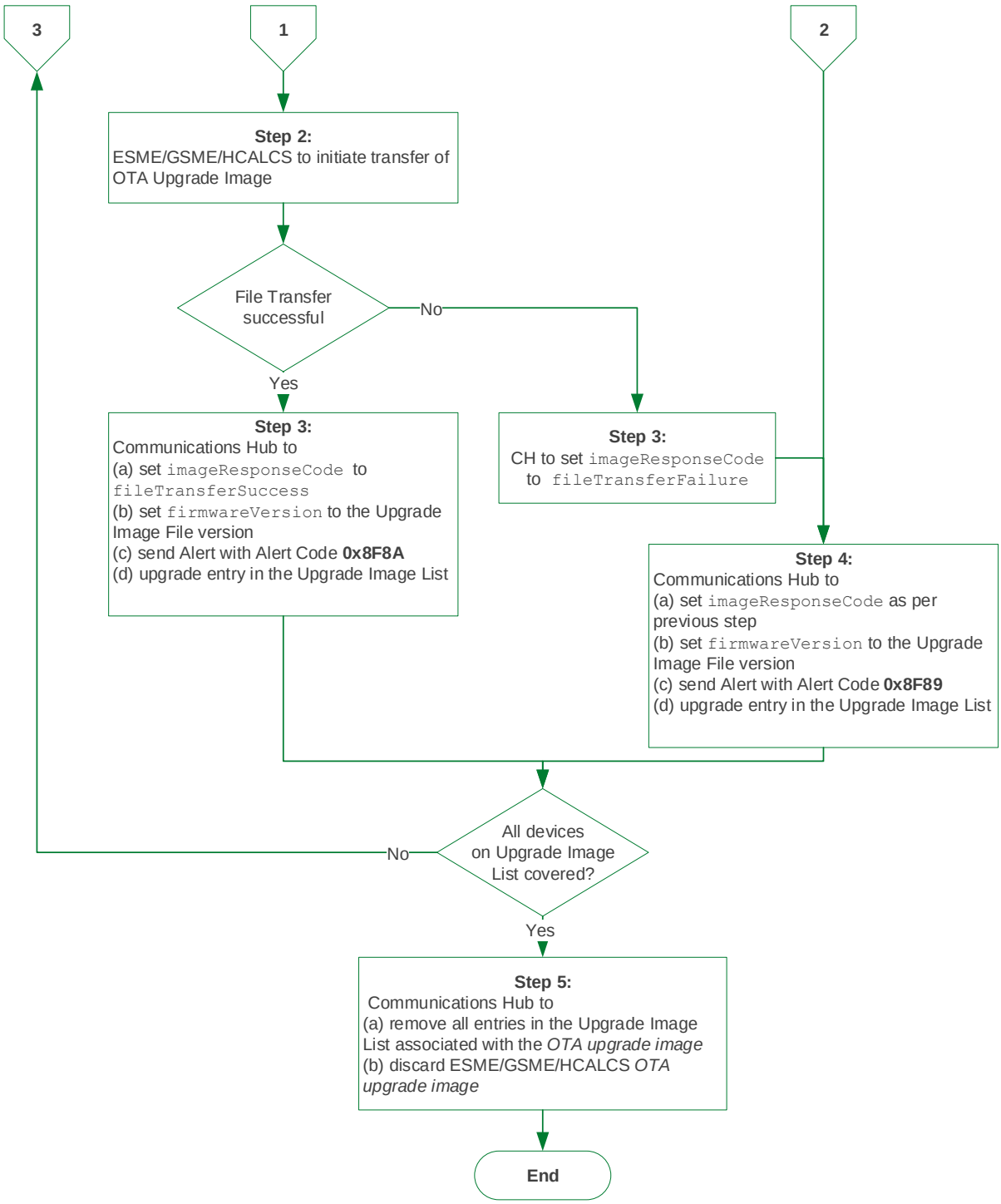
Appendix 1: Proposed PPMID OTA firmware process




3
1
2
Communications Hub:
(a) set transferResponseCode to fileTransferSuccess
(b) set firmwareVersion to the Upgrade Image File version
(c) send Alert with Alert Code 0x8F8A
Communications Hub:
(a) set transferResponseCode as per previous step
(b) set firmwareVersion to the Upgrade Image File version
(c) send Alert with Alert Code 0x8F89
Upgrade Image from CS05b or CS05c?
CS05b
CS05c
ESME/GSME/HCALCS: CH does not activate firmware
PPMID: CH activates firmware immediately
All devices associated with Upgrade Image covered?
No
Yes
Communications Hub to discard GSME/ HCALCS/PPMID OTA upgrade image
End

Appendix 2: Proposed HCALCS OTA firmware process




3
1
2
Step 2:
ESME/GSME/HCALCS to initiate transfer of OTA Upgrade Image
File Transfer successful
No
Yes
Step 3:
Communications Hub to
(a) set imageResponseCode to fileTransferSuccess
(b) set firmwareVersion to the Upgrade Image File version
(c) send Alert with Alert Code 0x8F8A
(d) upgrade entry in the Upgrade Image List
Step 3:
CH to set imageResponseCode to fileTransferFailure
Step 4:
Communications Hub to
(a) set imageResponseCode as per previous step
(b) set firmwareVersion to the Upgrade Image File version
(c) send Alert with Alert Code 0x8F89
(d) upgrade entry in the Upgrade Image List
All devices on Upgrade Image List covered?
No
Yes
Step 5:
Communications Hub to
(a) remove all entries in the Upgrade Image List associated with the OTA upgrade image
(b) discard ESME/GSME/HCALCS OTA upgrade image
End

Appendix 3: Progression timetable

This table summarises the timeline of events that this modification taken.

Timeline	
Activity	**Date**
Modification Proposal raised	1 Mar 16
Panel considers Initial Modification Report	11 Mar 16
Initial DCC Preliminary Assessment	10 Jun 16 – 17 May 17
First Refinement Consultation	17 Oct 17 – 8 Nov 17
Firmware industry workshop	29-30 Jun 18
The SSC considers the inclusion of the HCALCS into the modification • **Outcome**: The SSC approves the inclusion of the HCALCS into the modification, as long as activation is carried out via a Critical Command	11 Apr 18
Second DCC Preliminary Assessment	5 Jul 18 – 11 Apr 19
Second Refinement Consultation	24 May 19 – 17 Jun 19
Green Energy Options (geo) proposed alternative solution options • geo suggest the removal of the proposed ban on local firmware updates	17 Jul 19
The Working Group considered geo's proposed solutions • **Outcome**: The Proposer and the Working Group agree to reject geo's proposed solutions and proceed with the Proposer's Proposed Solution	7 Aug 19
SECAS publishes first draft of the GBCS legal text	29 Aug 19
An Other SEC Party proposes legal text changes • It suggests making the inclusion of the hardware version in the 'Query Next Image Request Command' optional The Proposer accepts this proposal	30 Aug 19
The DCC raises a change to the cost for the Impact Assessment, rising from £187,703 to £392,785. The Change Board agrees to this revised cost.	13 Sep 19
SECAS and the DCC identified options for the legal text detail: • Service Request for combined distribution and activation of PPMID/IHD firmware • Rules for the use of Communications Hub memory blocks	23 Sep 19
The SSC considers the Proposed Solution • **Outcome**: The SSC agreed with the PPMID/IHD approach, as long as it matches the existing ADT volume regime as applied to ESME and GSME • **Outcome**: The SSC agreed with the HCALCS approach	9 Oct 19

Timeline	
Activity	**Date**
The Proposer[11] raises an amendment to the solution, preferring a different Service Request for combined distribution and activation of PPMID/IHD firmware	15 Oct 19
The Working Group discuss the outstanding questions on the solution • **Outcome**: The DCC is to proceed with its Impact Assessment as-is • **Outcome**: The DCC is to ask its Service Providers to provide cost impacts on the use of different Service Requests as well as the use of memory blocks on the Communications Hub	6 Nov 19
SEC Panel ask for the solution to be streamlined to provide a Minimum Viable Product	15 Nov 19
SECAS, the DCC and its Service Providers discuss potential options that could be used to streamline the solution	28 Nov 19
The Working Group discuss options to streamline the solution • **Outcome**: Several elements of the solution are removed • **Outcome**: Considering the changes made, the TABASC Chair proposes a change to the approach for the PPMID	19 Dec 19
Agreement reached with all PPMID manufacturers to progress the TABASC Chair's proposed PPMID method	22 Jan 20
New business requirements are agreed with the DCC and its Service Providers are instructed to proceed with the Impact Assessment	6 Feb 20
DCC draft Impact Assessment received	14 Jul 20
DCC's draft Impact Assessment considered by the TABASC	23 Jul 20
DCC's draft Impact Assessment considered by the Working Group	28 Jul 20
Final DCC Impact Assessment received	5 Aug 20
DCC's firmware distribution control proposals considered by the TABASC	6 Aug 20
Modification Report approved by Panel	14 Aug 20
Modification Report Consultation	17 Aug 20 – 8 Sep 20
Change Board Vote	23 Sep 20
Authority decision (anticipated date)	30 Oct 20

[11] There was a change in Proposer due to the original named sponsor leaving their organisation.

Appendix 4: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary – Acronyms	
Acronym	**Full term**
ADT	Anomaly Detection Thresholds
BEIS	Department for Business, Energy and Industrial Strategy
CAD	Consumer Access Device
CHF	Communications Hub Function
CHTS	Communication Hubs Technical Specification
CoS	Change of Supplier
CPA	Commercial Product Assurance
CPL	Certified Products List
CSP	Communications Service Provider
DCC	Data Communications Company
DSP	Data Services Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
EUA	Energy and Utilities Alliance
EUI	Extended Unique Identifier
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
IDTS	Industry Draft Technical Specification
IHD	In-Home Display
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch
MMC	Message Mapping Catalogue
OTA	Over-The-Air
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
RFI	Request For Information
SSC	Security Sub-Committee
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SM WAN	Smart Meter Wide Area Network
SMETS	Smart Metering Equipment Technical Specifications
SMI	Smart Metering Inventory
SMIP	Smart Metering Implementation Programme

Glossary – Acronyms	
Acronym	**Full term**
SMS	Smart Metering System
SR	Service Request
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
UIT	User Integration Testing
XML	Extensible Markup Language
ZCL	Zigbee Cluster Library

This table lists key terms used in this document and their definitions.

Glossary – Terms	
Term	**Meaning**
firmware	Means a package of firmware which can be made up of a single Manufacturer Image or several Manufacturer Images. This term will NOT be capitalised.
Manufacturer Image	Means a full firmware Image or one part of a firmware Image as defined in the GBCS.
Upgrade Image	The Manufacturer Image concatenated with additional information as defined in the GBCS.
OTA Upgrade Image	Means the concatenation of the OTA Header and the Upgrade Image that is equal to or less than 750KB. This is defined in the GBCS and in the DUIS.

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'

Annex A

Business requirements – version 1.31

About this document

This document contains the business requirements for this Modification Proposal. It provides detailed information on the business requirements for the Proposed Solution agreed by the Proposer, with input from the Data Communications Company (DCC) and Sub-Committees. It also provides the considerations and assumptions for each business requirement with respect to this Modification Proposal.

Note: Contrary to the title of this modification, the scope of this modification is only applicable to Prepayment Meter Interface Devices (PPMIDs) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs). As agreed by the Proposer and the Working Group, In-Home Displays (IHDs) have been dropped from the Proposed Solution and are no longer within the scope of this modification.

Version history

Revision date	Revision	Summary of changes
19 Jul 19	1.0	First submission based on the initial Proposed Solution. This included IHDs, PPMIDs and HCALCSs.
6 Jan 20	1.2	Following on from the Working Group meeting held on 19 December 2019, amendments were made to reference the Working Groups decisions. This includes removing IHDs from the scope of the modification.
3 Feb 20	1.3	This version incorporates the TABASC Chair's proposal made at the Working Group meeting held on 19 December 2019. This is to have the PPMID generate the success/failure Alert to the DCC. This removes the following Communications Hub requirements: • to record the activation date-time plus [X] minutes; and • to subsequently read the firmware version on the Device.
28 Feb 20	1.31	Inclusion of the SSC's decision on ADT rules for HCALCSs.

Definitions

Term	Definition
firmware	Means a package of firmware which can be made up of a single Manufacturer Image or several Manufacturer Images. This term will NOT be capitalised.
Manufacturer Image	Means a full firmware Image or one part of a firmware Image as defined in the GBCS.
Upgrade Image	The Manufacturer Image concatenated with additional information as defined in the GBCS.
OTA Upgrade Image	Means the concatenation of the OTA Header and the Upgrade Image that is equal to or less than 750KB. This is defined in the GBCS and in the DUIS.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	**Requirement**
1	Manufacturer Image Hashes associated with PPMIDs and HCALCSs to be added to the CPL
2	Suppliers to be able to send firmware updates to PPMIDs and HCALCSs OTA
3	The DCC to notify all Responsible Suppliers at certain stages during the processing of firmware updates
4	The DCC and Responsible Suppliers will check the latest firmware version on PPMIDs and HCALCSs
5	The Communications Hub will be able to support the prioritisation of firmware Images to all HAN Devices
6	Upon firmware Image activation, the DCC will update the SMI with the new firmware version for the updated Device
7	Additional Communications Hub functionality to support the distribution of OTA Upgrade Images to PPMIDs and HCALCSs
8	Firmware update support capability will need to be mandated on PPMIDs installed after this modification is implemented

2. Summary of OTA firmware solutions

2.1 Updating PPMID firmware

A ZigBee Over-The-Air (OTA) delivery mechanism will be used to deliver firmware to PPMIDs. This method introduces the combined distribution and activation of the Manufacturer Image into one single Service Request. This will be a new Non-Critical Service Request created specifically for the PPMID. The Communications Hub is to manage the activation of PPMID firmware. The PPMID itself will manage the notification to the Service User upon activation of the firmware.

The distribution and activation of firmware to PPMIDs is detailed in section 4.

2.2 Updating HCALCS firmware

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. As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 ‘Update Firmware’ and activation via SR11.3 ‘Activate Firmware’, the latter via a Great Britain Companion Specification (GBCS) Critical Command.

The distribution and activation of firmware to HCALCSs is detailed in section 5.

3. Considerations and assumptions

3.1 Scope of the modification

This Modification Proposal will only apply to PPMIDs and HCALCSs.

3.2 Forecasting firmware updates – Non-functional requirements

PPMID firmware is expected to be typically less than 750KB in size and updates will occur no more than two times per year. Device manufacturers have advised that their firmware updates are likely to be no larger than 350KB in size. However, the customisation of PPMIDs with graphics will increase the firmware size; this may happen going forward and require the mechanism for delivering firmware greater than 750KB. In any case, any single OTA Upgrade Image must be less than or equal to 750KB.

HCALCS firmware is expected to be much smaller and with a very low upgrade frequency. It may be possible that HCALCSs do not need updates at all unless changes to the ZigBee version are required.

3.3 Adding PPMID/HCALCS Manufacturer Image Hashes to the CPL

For a Manufacturer Image to be added to the Central Products List (CPL), additional details in relation to that Image will need to be provided to the SEC Panel.

The Supplier will need to confirm to the Panel that the firmware update does not affect how the PPMID or HCALCS communicates using ZigBee.

If the firmware update impacts how the PPMID or HCALCS communicates using ZigBee and requires re-testing, a new ZigBee Assurance Certificate will need to be provided to the Panel before the firmware can be updated.

The CPL Requirements Document specifies the additional details in relation to the Manufacturer Image that must be provided to the Panel:

- the Hash of the Manufacturer Image;
- the identity of the organisation that created that Image; and
- a digital signature created by the creator of the Image across the communication containing the CPL entry details.

The digital signature used to sign the communication between the submitter and the Panel needs to be the same as the one received from a Public Key Infrastructure (PKI) chosen by the Panel to check the signature

A template for submitting CPL entries has been published on behalf of the Panel, which sets out the approach to digital signing taken by the Panel.

In addition to the above, HCALCSs must comply with the Commercial Product Assurance (CPA) Security Characteristics as per the Smart Metering Equipment Technical Specification (SMETS). Changes to HCALCS firmware may require either the inclusion of the new firmware version in the existing CPA certificate or a new CPA certificate. For HCALCSs, this CPA certificate must be submitted to the Panel when adding a new firmware version to the CPL.

3.4 Communications Hub memory considerations

No additional buffer space on the Communications Hub is being proposed. Only the GSME memory block will be used for storing PPMID and HCALCS Images. The ESME memory block will not be used to store PPMID and HCALCS Images.

GSME Images will take priority over PPMID and HCALCS Images. Therefore, a PPMID or HCALCS Image will be overwritten by a GSME Image if one arrives whilst a PPMID or HCALCS update is in progress at any point in time.

If another PPMID or HCALCS Image arrives whilst a PPMID or HCALCS update is in progress, the newly arrived Image will overwrite the one in progress at any point in time.

3.5 Dual Supplier Scenarios

Both Responsible Suppliers shall be able carry out firmware updates to PPMIDs in dual Supplier scenarios. The Proposer and the Working Group accept that this may increase the risk of firmware updates being overwritten by each of the Responsible Suppliers in a dual Supplier scenario.

Only the Import Supplier shall be able to carry out firmware updates to the HCALCSs.

3.6 Anomaly Detection Thresholds

The Security Sub-Committee (SSC) have stated that Service Requests to update firmware for PPMIDs must be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME. However, PPMIDs must be counted and reported separately to enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs.

The SSC also stated that Service Requests to update firmware for HCALCSs should subject to the same ADT procedures as ESME and GSME since similar risks to the supply of energy apply to HCALCSs.

3.7 Activation date-time

Future dated activation of PPMID Manufacturer Images will not be permitted. Upon successful receipt of the OTA Upgrade Image by the PPMID, the Communications Hub will instruct the PPMID to immediately activate the new Manufacturer Image.

HCALCS Manufacturer Images are activated using the existing Service Request 11.3, which must be adjusted to include HCALCS as valid target Device Type.

4. Sending PPMID firmware Images

This section outlines how the process will work for PPMIDs if firmware is made up of a single Manufacturer Image or several Manufactures Images. HCALCSs are covered in Section 4 'Sending HCALCS Manufacturer Images' below.

Note: An OTA Upgrade Image must be less than or equal to 750KB in size.

4.1 Sending a single Manufacturer Image to a PPMID

This section details the steps that will need to be taken to update PPMID firmware. It is assumed that a Manufacturer provides a Manufacturer Image to the Supplier and a new CPL entry has been created. The resulting OTA Upgrade Image will be less than or equal to 750KB in size.

Sending a Manufacturer Image to a PPMID will require a new Non-Critical Service Request 'Send PPMID Firmware'[1]. Currently the next available and most logical Service Reference Variant for this Service Request will be 11.4.

4.1.1 Supplier preparations

Before sending the new Service Request to the DCC for a PPMID firmware update, the Supplier will be required to follow several steps. These will be similar in initiating a firmware update to the DCC for a Meter:

Obtain the following information:

1. The Manufacturer Image;
2. OTA Header, which should include:
    a. Manufacturer ID;
    b. Model to which it can be applied;
    c. Firmware Version contained in the Image; and
    d. Minimum and maximum hardware version to which it can be applied.
3. A Hash of the Manufacturer Image.

Undertake the following checks on that information:

1. The Hash the Supplier has calculated over the Manufacturer Image is the same as that provided by the person who created the Manufacturer Image (in this case the Manufacturer); and
2. Check that the Manufacturer Image is associated with one or more Device Models on the CPL. The check should include that:
    a. The Hash is recorded on the CPL against one or more entries;
    b. The OTA Header Manufacturer ID, model and Firmware Version fields match identically with one of the entries identified at step (a); and

[1] The title of this new Service Request is yet to be determined.

c. The hardware version in that CPL entry is between OTA Header minimum and maximum hardware version, inclusively.

4.1.2 Supplier creation of a 'Send PPMID Firmware' Service Request

Having obtained the information and upon the above checks being successful, the Supplier will create a 'Send PPMID Firmware' Service Request. The Service Request will include the following information:

1. Image: The Image to be sent composed of a base64 encoded version of the concatenation:

   OTA Header || Manufacturer Image

2. List of Device IDs

Up to 50,000 PPMIDs will be able to be listed within the Service Request.

4.1.3 The DCC checks on the 'Send PPMID Firmware' Service Request

On receipt of the 'Send PPMID Firmware' Service Request, the DCC will follow the following steps:

1. Check whether the OTA Upgrade Image contained within the Service Request is less than or equal to 750KB in size;
2. Calculate the Hash of the Manufacturer Image contained within the Service Request;
3. Check whether the Hash the DCC has calculated is on the CPL, and identify CPL entries with that Hash;
4. For each of the Device IDs in the Service Request:
   a. Check the Device is a PPMID;
   b. From the Smart Metering Inventory (SMI), identify the Device's current Device Model, and ensure that the Manufacturer ID, model and hardware version fields for that current Device Model equate to one of the entries identified at step 3;
   c. Identify, from the SMI, the Communication Hub Function (CHF) ID to which the Device is associated; and
   d. Check that the Supplier is the Responsible Supplier for one of the Smart Meters Associated with that CHF ID.

If this and all preceding checks succeed, the DCC will identify (and temporarily record against the Device ID) the details of all Responsible Suppliers Associated with the CHF ID. This temporary record will be used to populate the DCC Alerts at the next step.

4.1.4 DCC response to the 'Send PPMID Firmware' Service Request

The DCC will be required to notify all Responsible Suppliers at different stages of the Service Request processing. The first notification will happen when the DCC receives the 'Send PPMID Firmware' Service Request:

1. Upon the DCC receipt of the 'Send PPMID Firmware' Service Request, the requesting Supplier will receive a Service Response. If some of the Device IDs in the Service Request failed any of the checks at step 4 under 4.1.3 (above), the DCC will send a Service Response to the requesting Supplier listing all the Device IDs that failed and the reason for the failure in each case. The DCC will carry on processing the firmware distribution for those Device IDs that passed the check.
2. Upon the DCC completing the processing of the 'Send PPMID Firmware' Service Request, each Responsible Supplier identified in 4.1.3 will receive a DCC Alert containing:
    a. The Hash of the Manufacturer Image in the Service Request (to identify the CPL entry); and
    b. A list of Device IDs to which the Image is being sent.

4.1.5 DCC Distribution of the 'Send PPMID Firmware' Service Request

If the checks are successful, the DCC will distribute the Image from the Service Request (having decoded from base64 encoding) to the Communications Hub associated with each of the PPMIDs in the List of Device IDs where the Device ID passed the validation.

SEC Schedule 10 'Communication Hub Technical Specifications' (CHTS) 4.4.4 requires that the receiving Communications Hubs can buffer Images intended for ESME and GSME. The Communication Services Provider (CSP) contracts require Communications Hubs to have the capacity to hold two 750KB Images (to support independent distribution of firmware to one of the ESME and the GSME).

Upon successful transfer of the OTA Upgrade Image to the Communications Hub, the Communications Hub will send an Alert to the DCC which will be forwarded to the Supplier.

4.1.6 Communications Hub notification of Image availability to the PPMID

Once the Image arrives at the Communications Hub, the Communications Hub will need to:

1. Record OTA Header details
2. Notify the PPMID by sending a message to it/them ('the Communications Hub shall send a Zigbee Smart Energy (ZSE) Image Notify command').

4.1.7 PPMID request for the details of the Image

The PPMID will then, in line with the ZigBee OTA specification, send a message (a 'QueryNextImageRequest' ZSE command containing Manufacturer ID (manufacturer code), model (Image type), current Firmware Version, and optionally hardware version) to ask the Communications Hub if there is an Image that may be suitable for it.

The ZSE Image Notify Command may not be received by the PPMID. Therefore, to mitigate this risk, the PPMID will carry out the 'QueryNextImageRequest' no more than once per day.

4.1.8 Provision of Image details by the Communications Hub to the PPMID

For the Communications Hub to decide that the Image is suitable for the PPMID, the ZigBee OTA specification details a recommended, default policy to determine its response, specifically to:

'send back a response that indicates the availability of an Image that matches the manufacturer code, Image type, and the highest available file version of that Image on the server. However, the server may choose to upgrade, downgrade, or reinstall clients' Image, as its policy dictates. If client's hardware version is included in the command, the server shall examine the value against the minimum and maximum hardware versions included in the OTA file header'

Note that 'server' in the above refers to the Communications Hub and 'client' refers to the PPMID.

The Communications Hub will send back a 'QueryNextImageResponse' accordingly.

4.1.9 PPMID download and authentication of the Image

The PPMID will then download the Image from the Communications Hub, if one is available for it.

When the PPMID has downloaded the Image, it will check the Manufacturer signature (or equivalent) within it. This confirms the Manufacturer Image is as created by the Manufacturer. The PPMID will then store the Manufacturer Image from within the Image sent, so that it is available for activation[2]. The PPMID will then send a 'UpgradeEndRequest' to the Communications Hub.

4.1.10 Activation of the firmware Image

The Communications Hub will then send a 'UpgradeEndResponse' with the activation date-time set to 0x00000000 for immediate activation in line with the ZigBee specifications. The PPMID will immediately activate the Image.

The PPMID will then create a Device Alert containing its firmware version and send it to the DCC. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

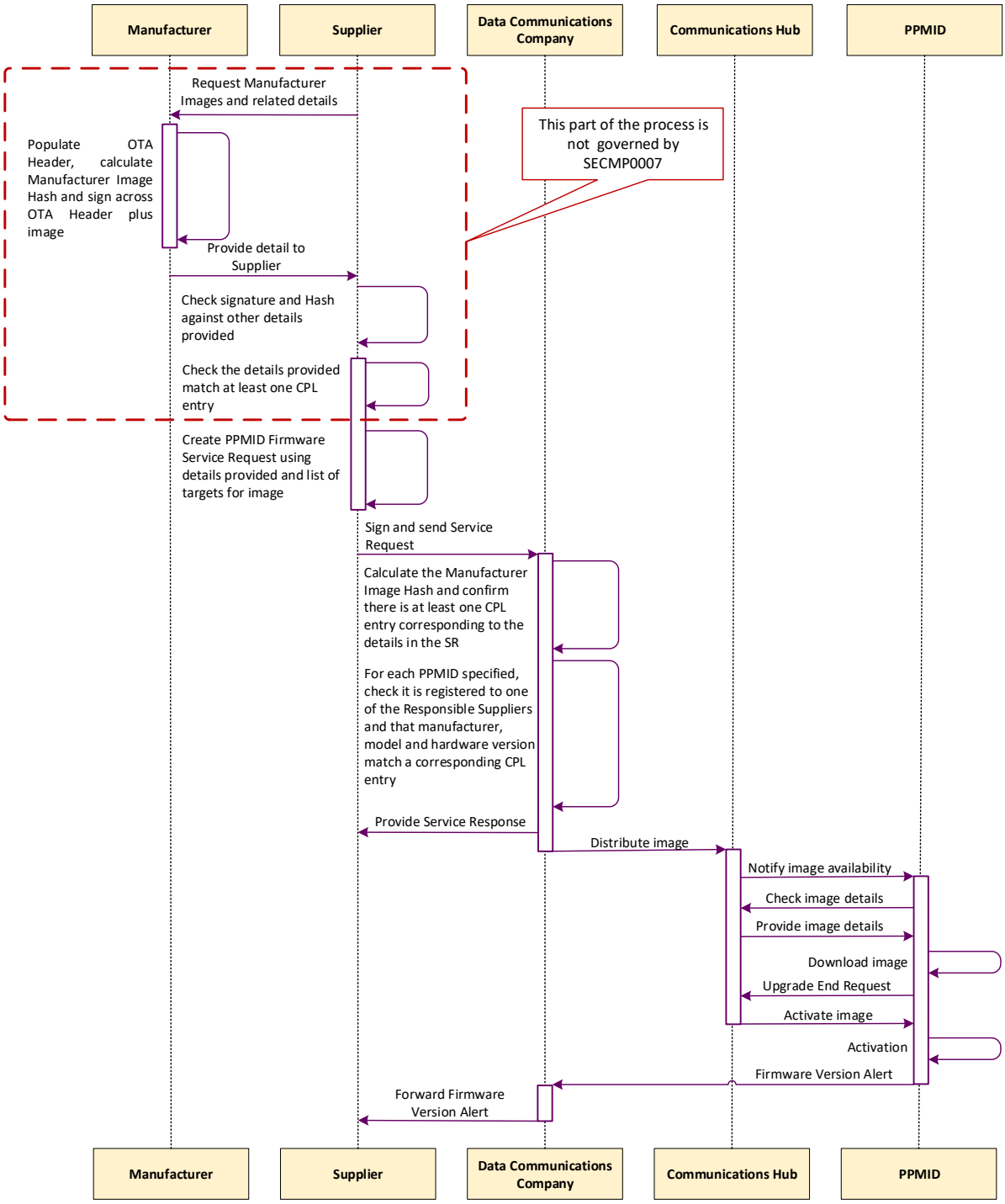
If the Device Alert is not received, the Supplier can send SR11.2 to the DCC. This will result in a Command to the PPMID to respond with its active firmware version. The DCC will forward the Response to the Supplier and update the SMI if the firmware version in the SMI is different. SR11.2 can also be sent at any time by a Responsible Supplier if desired.

4.1.11 Process for updating PPMID Firmware comprised of a single Manufacturer Image

The process described above for processing PPMID firmware updates comprised of a single Manufacturer Image is presented in Figure 1 'Process for updating a single PPMID Manufacturer Image' below.

[2] Note these checks are Manufacturer specific. Their detail will not be mandated in the specifications, as they do not need to be implemented in the same way across Manufacturers.

Figure 1 'Process for updating a single PPMID Manufacturer Image'



4.2 Updating PPMID firmware comprised of multiple Manufacturer Images

Impacts: The process set out in this section is for the benefit of Manufacturers and Suppliers. This process does not propose any changes to the way in which the DCC currently manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

The expectation is that PPMID firmware is typically below 750KB. However, it may be possible for PPMID firmware to exceed this in the future. This section illustrates how to activate firmware comprised of multiple OTA Upgrade Images that are less than or equal 750KB in size.

The operating firmware version in this example is 0x10, which is reflected in the CPL entry example in Table 1 below.

A PPMID is to be updated to firmware version 0x20. This requires two Images to be sent to the PPMID, to provide all the changed firmware/configuration data required for firmware version 0x20.

The Manufacturer has split this upgrade data into two Images:

- **Image 0x15**: this contains the first part of the upgrade data and contains Manufacturer instructions for the PPMID to only store this first part on activation
- **Image 0x20**: this contains the second part of the upgrade data and contains Manufacturer instructions for the PPMID to check that Image 0x15 has already been activated. Activating this Image causes the functionality of the PPMID to be upgraded to firmware version 0x20.

New CPL entry:

Table 1: Example New CPL Entry for firmware comprised of multiple Manufacturer Images

Manufacturer identifier	Model identifier	Hardware version	Hardware version revision	Firmware version	Hash
FF: FE	AA:BB	01	01	00:00:00:10	(Hash of Image 10)
FF: FE	AA:BB	01	01	00:00:00:15	(Hash of Image 15)
FF: FE	AA:BB	01	01	00:00:00:20	(Hash of Image 20)

To upgrade firmware for a PPMID, the Supplier will follow the following process:

1. Having undertaken the necessary checks, the Supplier will create a 'Send PPMID Firmware' Service Request to distribute Image 0x15.
2. The DCC will distribute Image 0x15 to the Communications Hub and the PPMID will download the Image. The PPMID will then send a Device Alert containing its firmware version. Note that this value will still be 0x10 (in line with the Technical Specification Issue Resolution Sub-Group (TSIRS) decision). Therefore, the Device Alert will only indicate delivery of the Image. It will NOT indicate that the PPMID has successfully validated the

Image. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

3. On receipt of the Device Alert from the DCC containing the PPMID's firmware version, the sending Supplier will send Image 0x20. If this Device Alert was not received the Supplier can only resend Image 0x15 (since the TSIRS decision means, there is no mechanisms to discover if the PPMID had that Image).
4. The DCC will distribute Image 0x20 to the Communications Hub. When the PPMID has downloaded the Image, the PPMID will send a Device Alert containing its firmware version. Note that this value will, if activation was successful, now be 0x20 (in line with the TSIRS decision). Therefore, this Device Alert will indicate delivery of the Image and that the PPMID successfully activated the Image. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.
5. The Supplier can only resend Image 0x20 if this Device Alert is not received. However, it should verify this first by sending SR11.2 to the PPMID. The DCC will then update the SMI if the firmware version has changed and forward the Device Response for SR11.2 to the Supplier.

The result is that the PPMID (excluding where the OTA firmware upgrade process cannot be completed e.g. where there is no Wider Area Network (WAN) connectivity), will be operating firmware version 0x20.

The above process is explained in detail in Figure 2 and Figure 3: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2 (parts 1 and 2 respectively) below.

Figure 2: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 1

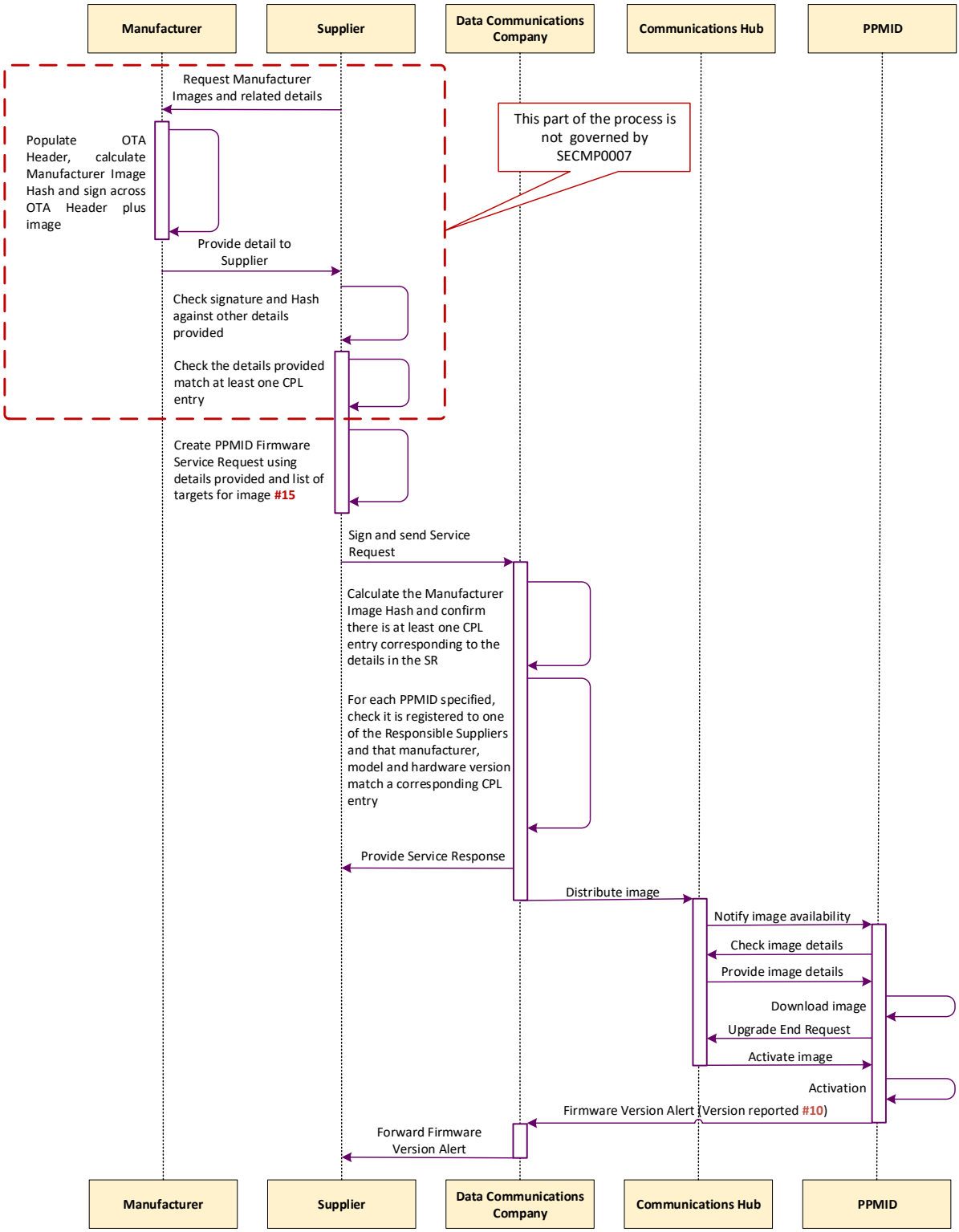
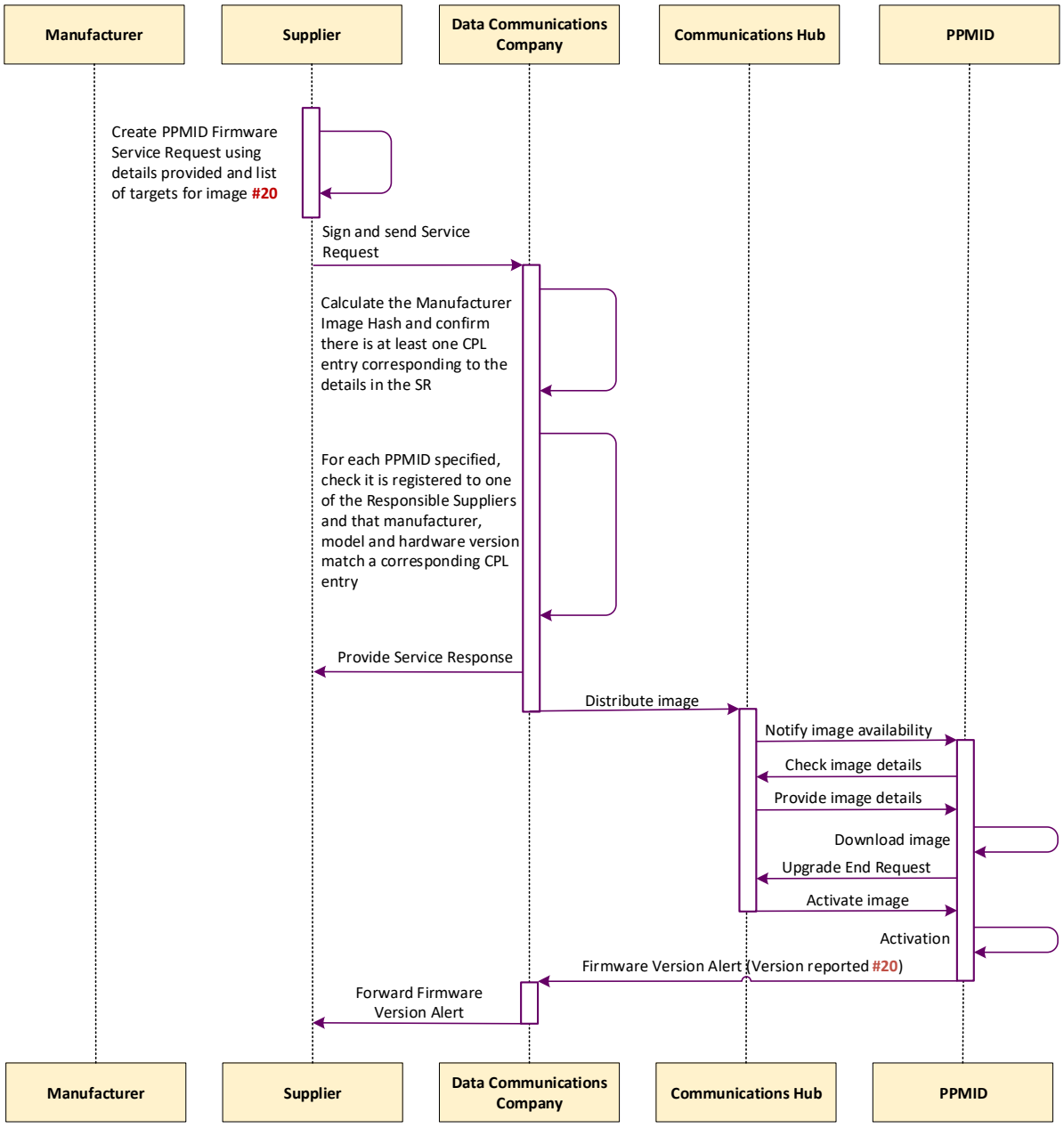


Figure 3: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2



5. Sending HCALCS Manufacturer Images

The process for the OTA upgrade of HCALCSs aligns with the current Technical Specifications and the Great Britain Companion Specification (GBCS) for the Supplier to distribute and activate firmware on the ESME and GSME. This will be accomplished by adding the HCALCS as a target Device Model to the existing Service Reference Variants.

As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

The expectation is that HCALCS firmware is typically below 750KB. However, the existing ESME/GSME OTA firmware upgrade mechanisms contained in the GBCS allow manufacturers to split firmware into multiple OTA Upgrade Images less than or equal to 750KB in size; this method can be employed in case HCALCS firmware exceeds the size of 750KB.

The following Service Requests will be enhanced to support the OTA upgrades of HCALCS:

- SR 11.1 'Update Firmware'
- SR 11.2 'Read Firmware Version'
- SR 11.3 'Activate Firmware'

Additional GBCS Use Cases will be introduced to support the distribution and activation of firmware Images for HCALCSs.

In the SMETS the HCALCS sections must be updated to reflect the HCALCS capability of receiving and activating new firmware.

6. Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
ADT	Anomaly Detection Threshold
CHF	Communication Hub Function
CHTS	Communication Hub Technical Specifications
CPA	Commercial Products Assurance
CPL	Central Product List
DCC	Data Communications Company
ESME	Electricity Smart Metering Equipment
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch
IHD	In Home Display
OTA	Over-The-Air
PKI	Public Key Infrastructure
PPMID	Prepayment Meter Interface Device
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specification
SMI	Smart Metering Inventory
SSC	Security Sub-Committee

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'

Annex B

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2'

These changes have been redlined against Schedule 10 version 1.3.

Add Section 7.4.7 as follows:

7.4.7.5 Firmware

A PPMID shall be capable of activating Firmware when instructed by the Communications Hub (as set out in *Section 7.5.2.5*).

Add Sections 7.5.2.5 and 7.5.2.6 as follows:

7.5.2.5 Activate Firmware

The PPMID shall be capable of installing new Firmware using a mechanism that is robust against failure and loss of data.

The new Firmware shall include version information. Where new Firmware is successfully installed, the PPMID shall be capable of recording the version information of that new Firmware in *Firmware Version (7.6.4.1)*.

7.5.2.6 Receive Firmware

The PPMID shall be able to receive Firmware from the Communications Hub.

Add Section 7.6.4 as follows:

7.6.4 Operational data

Describes data used by the functions of the PPMID for output of information.

7.6.4.1 Firmware Version

The active version of Firmware of the PPMID.

Amend Section 8.4.4.1 as follows:

8.4.4 Security

8.4.4.1 General

An HCALCS shall be designed taking all reasonable steps to ensure that any failure or compromise of its integrity shall not compromise the Security Credentials stored on it or compromise the integrity of any other Device to which it is connected by means of a Communications Link.

An HCALCS shall be capable of securely disabling Critical Commands other than those Commands set out in Section 8.5 that are Critical Commands.

An HCALCS shall be capable of verifying its Firmware at power-on and prior to activation of the Firmware, to verify that the Firmware, at that time, is in the form originally received. On

failure of verification an HCACLS shall be capable of generating and sending an Alert to that effect via its HAN Interface.

Add Section 8.4.4.5 as follows:

8.4.4.5 Firmware

An HCALCS shall only be capable of activating Firmware on receipt of an Activate Firmware Command (as set out in *Section 8.5.1.7*).

Add Sections 8.5.1.7 and 8.5.1.8 as follows:

8.5.1.7 Activate Firmware

A Command to activate Firmware.

In executing the Command the HCALCS shall be capable of installing new Firmware using a mechanism that is robust against failure and loss of data.

The new Firmware shall include version information. Where new Firmware is successfully installed, the HCALCS shall be capable of recording the version information of that new Firmware in *Firmware Version (8.6.3.1)*.

8.5.1.8 Receive Firmware

A Command to receive Firmware.

In executing the Command the HCALCS shall be capable of:

i. only accepting new Firmware from an Authorised and Authenticated source;

~~i.~~ii. and verifying the Authenticity and integrity of new Firmware before installation.

Add Section 8.6.3 as follows:

8.6.3 Operational data

Describes data used by the functions of the HCALCS for output of information.

8.6.3.1 Firmware Version

The active version of Firmware of the HCALCS.

These changes have been redlined against Schedule 10 version 1.3.

Amend Section 4.4.4 as follows:

Buffering

A CHF shall be capable of Buffering all Commands intended for GSME with Security Credentials recorded in the *CHF Device Log (4.6.2.1)*.

A CHF shall be capable of prioritising the forwarding of any GSME Add Credit Commands and GSME Activate Emergency Credit Commands.

A CHF shall be capable of Buffering a Command to receive Firmware intended for ESME.

A CHF shall be capable of Buffering a Command to receive Firmware intended for a PPMID or a HCALCS.

A CHF shall be capable of Buffering Responses and Alerts to be sent via the WAN interface.

Under normal operating conditions, a CHF shall be capable of Buffering at all times:

i. *CHF Device Log (4.6.2.1)* Alerts;
ii. Device Commissioning Alerts;
iii. Responses to Critical Commands; and
iv. other Critical Alerts.

Appendix E ‘DCC User Interface Services Schedule’

These changes have been redlined against Appendix E version 3.0.

Amend Service Reference 11.1 ‘Update Firmware’ as follows:

Service Reference	Service Reference Variant	Description	Eligible Users	SMETS2+ Target Response Time	SMETS1 Target Response Time	Non-Device Services	Notes
11.1	11.1	Update Firmware	Import Supplier, Gas Supplier	24 ~~H~~hours	24 hours	✓	In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within 5 days of receipt of the Service Request.

Add Service Reference 11.4 'Update PPMID Firmware' as follows:

Service Reference	Service Reference Variant	Description	Eligible Users	SMETS2+ Target Response Time	SMETS1 Target Response Time	Non-Device Services	Notes
11.4	11.4	Update PPMID Firmware	Import Supplier, Gas Supplier	24 hours	n/a	✓	In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within 5 days of receipt of the Service Request.

Add Service Reference 11.4 'Update PPMID Firmware' to the Monthly Service Metrics table as follows:

Monthly Service Metric applies to Users acting in the following User Roles**	Monthly Service Metric applies to Service Requests for the following Services	Monthly Service Metric (excluding SMETS1 Service Requests and SMETS1 SMS)	Monthly Service Threshold
Import Supplier Gas Supplier	3.1 Display Message	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	24
Import Supplier Gas Supplier Export Supplier	4.8 Read Profile Data	The number of Service Requests in month m; divided by the number of Smart Metering Systems for which that User is a Responsible Supplier on the 15th day of month m.	The number of days in month m

Import Supplier Gas Supplier	11.1 Send Firmware	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	6
Electricity Distributor Gas Transporter	4.8 Read Profile Data	The number of Service Requests in month m; divided by the number of Smart Metering Systems for which the User is the Electricity Distributor or Gas Transporter on the 15th day of month m.	10^{-3} x 48 x the number of days in month m
Electricity Distributor Gas Transporter	4.8 Read Profile Data	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	4
Electricity Distributor	4.10 Read Network Data	The number of Service Requests in month m; divided the number of Smart Metering System for which the User is the Electricity Distributor or Gas Transporter on the 15th day of month m.	10^{-3} x the number of days in month m

Electricity Distributor	4.10 Read Network Data	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	4
Import Supplier Gas Supplier	11.4 Update PPMID Firmware	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	6

Appendix R 'Common Test Scenarios Document'

These changes have been redlined against Appendix R version 2.0.

Amend Table 8.1.5 as follows:

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	IS
11.4	11.4	Update PPMID Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS

Update the total values for Table 8.1.5 as follows:

Count of N/A	5~~2~~3	102	100~~1~~1	101~~2~~2	7~~4~~5	8~~1~~2	102~~3~~3	105~~6~~6	104~~5~~5	92	
Count of Mandatory	36	2	0	0	19	0	0	0	0	8	65
Count of Mandatory SMETS 2	18	3	6	5	13	25	4	1	2	~~6~~7	8~~3~~4
									Total Tests	148~~8~~9	

Amend Table 8.1.6 as follows:

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	GS
11.4	11.4	Update PPMID Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS

Update the total values for Table 8.1.6 as follows:

Count of N/A	3~~8~~9	8~~1~~2	7~~7~~8	~~79~~80	6~~1~~2	6~~5~~6	8~~1~~2	8~~2~~3	8~~1~~2	68	
Count of Mandatory	30	~~0~~1	0	0	18	0	0	0	0	8	5~~6~~7
Count of Mandatory SMETS 2	14	1	5	3	3	17	1	0	1	~~6~~7	51
									Total Tests		10~~7~~8

Appendix AB 'Service Request Processing Document'

These changes have been redlined against Appendix AB version 3.0.

Amend Section 2 as follows:

2 Obligations of Users: Suspended Devices and Firmware

2.1 A User shall take all reasonable steps to ensure that it does not send Service Requests in relation to Devices that have an SMI Status of 'suspended', other than where:

(a) the Service Requests will (if Successfully Executed) result in the Device's Device Model becoming one that is listed on the Central Products List;

(b) it is necessary to do so in order to update the Device Security Credentials following a change of Responsible Supplier; or

(c) for SMETS1 Devices only, the User is requesting only the production of UTRNs for return to that User.

2.2 A User shall only send an 'Update Firmware' Service Request or an 'Update PPMID Firmware' Service Request in respect of a Device or a SMETS1 CH if:

(a) the User has received the following information:

(i) the OTA Header and the associated replacement Manufacturer Image;

(ii) a Digital Signature, created by the person who created the Manufacturer Image, across the concatenation of the OTA Header and the associated replacement Manufacturer Image; and

(iii) the Hash of the replacement Manufacturer Image;

(b) the User has successfully confirmed that the Digital Signature across the concatenation is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party);

(c) the User has generated its own Hash from the replacement Manufacturer Image, and confirmed that the Hash that the User has generated is the same as the Hash provided; and

(d) the User has confirmed that a Device Model associated with the replacement Manufacturer Image (as determined by the Hash and the information in the OTA Header) is currently on the Central Products List.

Amend Section 6 as follows:

6 Obligations of the DCC: Processing Service Requests

6.1 Subject to Clause 18 (Obligations of the DCC: Non-Device Service Requests), where the DCC receives a Service Request from a User, the DCC shall send an Acknowledgement to the User, and (whether before or after such Acknowledgement is sent) apply the following checks:

(a) Verify the Service Request;

(b) confirm that the Service Request has been sent by a User whose right to send that Service Request has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for that Service Request;

(c) in the case of Non-Critical Service Requests (other than an 'Update Firmware' Service Request, an 'Update PPMID Firmware' Service Request, a 'CoS Update Security Credentials' Service Request or a 'Top Up Device' SMETS1 Service Request with a Command Variant value of 2) and SMETS1 Critical Service Requests, confirm that the SMI Status of the Device identified in the Service Request is: (i) 'commissioned'; (ii) 'installed not commissioned'; (iii) 'whitelisted'; or (iv) 'pending';

(d) Check Cryptographic Protection for the Service Request;

(e) Confirm Validity of the Certificate used to Check Cryptographic Protection for

the Service Request;

(f) subject to Clause 6.2, in the case of Non-Critical Service Requests and SMETS1 Critical Service Requests, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request:

(i) for all times within any date range requested;

(ii) where there is no such date range, at the specified time for execution; or

(iii) where there is no date range and no date for execution is specified, at the time at which the check is being carried out;

(g) in the case of a 'CoS Update Security Credentials' Service Request, confirm that the User ID contained within each of the Organisation Certificates included within the Service Request is associated with the User submitting the Service Request and that the MPRN or MPAN included within the Service Request is Associated with the Device identified within the Service Request;

(h) in the case of a 'Restore HAN Device Log' or a 'Restore Gas Proxy Function Device Log' Service Request, confirm that the Device Log Data to be restored originates from a Communications Hub Function or Gas Proxy Function that forms (or formed immediately prior to its replacement) part of a Smart Metering System for which the User making such Service Request is (or, immediately prior to its replacement, was) the Responsible Supplier;

(i) in the case of an 'Update Firmware' Service Request or an 'Update PPMID Firmware' Service Request, confirm that the Hash calculated across the Manufacturer Image contained within the Service Request is the same as the entry within the Central Products List (as identified by the Device ID, information in the Smart Metering Inventory and the firmware version specified in the Service Request);

(j) in the case of any Service Request that contains any Certificates, Confirm Validity of those Certificates;

(k) in the case of an 'Update HAN Device Log' Service Request requesting the addition of a Smart Meter to the Device Log of a Communications Hub Function confirm (using the Registration Data and the MPRN or MPAN in the Service Request) that the User sending the Service Request is a Responsible Supplier in respect of that MPRN or MPAN;

(l) in the case of a 'Set CHF Sub GHz Configuration' Service Request, that the settings requested would only allow a CHF to use Sub GHz Available Channels (as defined in the GBCS); and

(m) in respect of a SMETS1 Critical Service Request, a 'Request Handover of DCC Controlled Device' SMETS1 Service Request, a 'CoS Update Security Credentials' SMETS1 Service Request or a 'Top Up Device' SMETS1 Service Request, confirm that the Service Request is not a Replay.

Housekeeping amendment to Section 12.4 as follows:

12.4 Where the DCC applies Threshold Anomaly Detection (other than in relation to a value of the type referred to in (b)(ii) of the definition of Anomaly Detection Threshold) to a Signed Pre-Command, Transformed Service Request or SMETS1 Service Request (for the purposes of this Clause, each being a "**Relevant Communication**"), the DCC shall:

Amend Section 18 as follows:

18 Obligations of the DCC: Non-Device Service Requests

18.1 Where the DCC receives a Non-Device Service Request from a User, the obligations of the DCC under this Appendix shall be modified as follows (and where a Non-Device Service Request is not specifically identified below, they shall be applied un-modified):

(a) the DCC shall not send an Acknowledgement in respect of the Service Request;

(b) the checks set out in Clause 6.1 shall be modified as follows:

(i) the check set out in Clause 6.1(c) does not apply to the following Service Requests:

(A) 'Update Inventory';

(B) 'Read Inventory';

(C) 'Request WAN Matrix';

(D) 'Device Pre-notification';

(E) 'Communications Hub Status Update- Install Success';

(F) 'Communications Hub Status Update - Install No SM WAN';

(G) 'Communications Hub Status Update – Fault Return'; and

(H) 'Communications Hub Status Update – No Fault Return'; and

(ii) the check set out in the Clause 6.1(f) does not apply to the following Service Requests:

(A) 'Read Inventory';

(B) 'Request WAN Matrix';

(C) 'Device Pre-notification';

(D) 'Communications Hub Status Update- Install Success';

(E) 'Communications Hub Status Update - Install No SM WAN';

(F) 'Communications Hub Status Update – Fault Return'; and

(G) 'Communications Hub Status Update – No Fault Return';

(c) the DCC shall not, in any event, be required to apply Threshold Anomaly Detection in relation to Non-Device Service Requests;

(d) where the checks set out in Clause 6.1 (as modified by this Clause 18) are satisfied, the DCC shall not Transform the Service Request or Countersign a Countersigned Service Request (as would otherwise be required by Clause 6) and shall instead send the User a Service Response notifying the User whether or not the Non-Device Service Request has been successful, and where successful:

(i) in the case of any Non-Device Service Request that changes or creates information held (or intended to be reflected) on the DCC Systems (including the Smart Metering Inventory), update the information held on DCC Systems accordingly; and/or

(ii) in the case of a 'Read Inventory' or 'Request WAN Matrix' Service Request, include within the Service Response the relevant information requested by the Service Request;

(iii) in the case of a 'Device Pre-Notification' Service Request, add the relevant Device to the Smart Metering Inventory with an SMI Status of 'pending';

(iv) in the case of a 'Create Schedule' Service Request,

(A) create a schedule of the Service Request type identified in the 'Create Schedule' Service Request;

(B) include within the Service Response the identifier of any schedule that has been successfully created;

(C) at each point in time set out in the schedule (and subject to the further arrangements set out in the DCC User Interface Specification), create a Service Request (without a Digital Signature from the User) of the appropriate type and in relation to the relevant Device (in each case as specified in the original 'Create Schedule' Service Request);

(D) process the Service Requests referred to in (C) above in accordance with Clause 6 as if they had been received from the User that sent the original 'Create Schedule' Service Request, provided that the checks identified under Clause 6.1(c) and 6.1(d) do not apply;

(v) in the case of a 'Read Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, include within the Service Response details of the relevant schedule(s) so identified (and otherwise reject the 'Read Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vi) in the case of a 'Delete Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, delete the relevant schedule(s) so identified (and otherwise reject the 'Delete Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vii) in the case of a 'Decommission Device' Service Request:

(A) set the SMI Status of the relevant Device to 'decommissioned';

(B) where the relevant Device is a Smart Meter, disassociate the Device in the Smart Metering Inventory from any MPRN or MPAN with which it is Associated; and

(C) where the relevant Device is a Communications Hub Function, set the SMI status of the associated Gas Proxy Function to 'decommissioned'; or

(viii) in the case of an 'Update Firmware' Service Request:

(A) include within the Service Response the details of any Devices

that were listed within the Service Request to which, by virtue of the checks DCC has carried out, DCC does not propose to send a communication to update the firmware; and

(B) to all other Devices so listed, send a communication to update the firmware of those Devices ensuring that the communication reaches the SMETS1 CHF (in the case of updates to a SMETS1 CHF) or (in the case of updates to all other Devices) the Communications Hub Functions associated with all such Devices (in each case, within the timescales specified in the DCC User Interface Services Schedule)~~.~~; or

(ix) in the case of an 'Update PPMID Firmware' Service Request:

(A) include within the Service Response the details of any Devices that were listed within the Service Request to which, by virtue of the checks DCC has carried out, DCC does not propose to send a communication to update the firmware; and

(B) to all other Devices so listed, send a communication to update the firmware of those Devices ensuring that the communication reaches the Communications Hub Functions associated with all such Devices (in each case, within the timescales specified in the DCC User Interface Services Schedule).

Appendix AF 'Message Mapping Catalogue'

These changes have been redlined against Appendix AF version 3.1.

Note, the XML Schema changes will be made during the design phase, post-decision of this modification.

Amend Table 8 'ASN.1 Response Codes' as follows:

4.1.3.3 Status Response Codes

For the GBCS Use Cases that are encoded in the ASN.1 format, the error statuses shall be embedded in the SMETSData element group, rather than using a separate DebugInfo element. In such structures, the MMC Output Format shall include the response code and response code name as set out in Table 8 immediately below.

Service Request	Response Code Name	Response Code
All ASN.1 SRs except 6.11, 8.1.1, 11.2	success	0
6.11 (gas only), 8.1.1 (gas only)	reliable	0
6.11 (gas only), 8.1.1 (gas only)	invalid	1
6.11 (gas only), 8.1.1 (gas only)	unreliable	2
6.15.1, 6.21, 6.23, 8.5	badCertificate	5
6.15.1, 6.21, 6.23, 8.5	noTrustAnchor	10
6.15.1, 6.21, 6.23, 8.5	insufficientMemory	17
6.24.1	trustAnchorNotFound	25
6.15.1, 6.21, 6.23, 8.5	resourcesBusy	30
6.15.1, 6.21, 6.23, 6.24.1, 8.5	other	127
6.15.2	invalidCertificate	1
6.15.2	wrongDeviceIdentity	2
6.15.2	invalidKeyUsage	3
6.15.2	noCorrespondingKeyPair	4
6.15.2	wrongPublicKey	5
6.15.2	certificateStorageFailed	6
6.15.2	privateKeyChangeFailed	7
6.17	invalidKeyUsage	1
6.17	keyPairGenerationFailed	2
6.17	cRProductionFailed	3
6.24.2	invalidKeyUsage	1
6.24.2	noCertificateHeld	2
6.24.2	certificateRetrievalFailure	3
8.7.1, 8.7.2	invalidMessageCodeForJoinMethodAndRole	1
8.7.1, 8.7.2	invalidJoinMethodAndRole	2
8.7.1, 8.7.2	incompatibleWithExistingEntry	3
8.7.1, 8.7.2	deviceLogFull	4
8.7.1, 8.7.2	writeFailure	5
8.7.1, 8.7.2	keyAgreementNoResources	6
8.7.1, 8.7.2	keyAgreementUnknownIssuer	7

Service Request	Response Code Name		Response Code
8.7.1, 8.7.2	keyAgreementUnsupportedSuite		8
8.7.1, 8.7.2	keyAgreementBadMessage		9
8.7.1, 8.7.2	keyAgreementBadKeyConfirm		10
8.7.1, 8.7.2	invalidOrMissingCertificate		11
8.7.1, 8.7.2	noPartnerLinkKeyReceived		12
8.7.1, 8.7.2	noCBKEResponse		13
8.8.1, 8.8.2	otherDeviceNotInDeviceLog		1
8.8.1, 8.8.2	otherFailure		2
8.12.2	incompatibleWithExistingEntry		3
8.12.2	deviceLogFull		4
8.12.2	writeFailure		5
11.2	firmwareReadSuccess		0
11.2	firmwareReadFailure		1
11.3	noImageHeld		1
11.3	hashMismatch		2
11.3	activationFailure		3
All ASN.1 Service Response	notKnown	*Any Response Code where the Response Code/Service Request combination is not listed above*	

Table 8 : ASN.1 Response Codes

Amend Section 4.2 as follows:

Device Alerts

The *Body* element of the MMC Output Format in respect of a successful Device Alert shall contain an element named *DeviceAlertMessage* with an underlying element *DeviceAlertContent* containing the XML elements and element groups as set out in **Table .**

Device Alerts containing encrypted data shall be initially processed using the *GBCSData* element of the *DeviceAlertMessage* element, once decrypted (as set out in section **Error! R eference source not found.** of this document) the *DeviceAlertContent* structure is used.

The execution of a future dated Service Request may generate one or more Device Alerts to the User in response where the same Service Request executed on demand would generate a Service Response to the User.

All Device Alerts as set out in Sections **Error! Reference source not found.** to ~~6.4~~6.7 shall c ontain a Payload XML element with underlying elements specific to the Device Alert.

Data Item	Description	Type	Mandatory	Valid Values
GBCSHexAlertCode	The Alert Code corresponding to the Alert defined in GBCS	xs:hexBinary	Yes	Values in 16 bit hexadecimal, as set out in GBCS
AlertDescription	Description of the Alert as defined in GBCS	xs:string (maxLength = 250)	Yes	As set out in GBCS
Timestamp	The Device Alert timestamp as sent by the Device, (UTC)	xs:dateTime	Yes	UTC Date-Time
Payload	This is additional data specific to the GBCS Use Case, where there is data additional to the Alert Code, as set out in Sections 6.1 to 6~~.4~~6.7 of this document	ra:DeviceAlertMessagePayload	No	As set out in Section **Error! Reference source not found.** of this document

Table 9 : Data Items within the DeviceAlertContent element

Where encrypted data is contained within a Device Alert message, such encrypted data shall be contained within the GBCS Payload data item. Where such encrypted data is contained within the GBCS Payload, the *DeviceAlertContent* element group shall not be included within the MMC Output Format. In order to decrypt such data, a User may conduct the steps as set out in Section 4.3 of this document.

Amend Sections 5.106 and 5.107 as follows:

5.106 Read Firmware Version

5.106.1 Service Description

Service Request Name	ReadFirmwareVersion
Service Reference	11.2
Service Reference Variant	11.2

5.106.2 MMC Output Format

The xml type within the SMETSData element is ReadFirmwareVersionRsp. The header and body data items appear as set out immediately below.

5.106.2.1 Specific Header Data Items

GBCS v1.0:

Data Item	Electricity Response	Gas Response
GBCSHexadecimalMessageCode	0x0059	0x0084
GBCS Use Case	ECS52	GCS38
SupplementaryRemotePartyID	ra:EUI (see clause 2.4.1) Where originator is Unknown Remote Party	
SupplementaryRemotePartyCounter	xs:nonNegativeInteger Where originator is Unknown Remote Party	

Table 242 : Read Firmware Version MMC Output Format Header data items

GBCS v4.x[1]:

Data Item	Electricity Response (ESME)	Gas Response	PPMID and HCALCS
GBCSHexadecimalMessageCode	0x0059	0x0084	0x0129
GBCS Use Case	ECS52	GCS38	CS08
SupplementaryRemotePartyID	ra:EUI (see clause 2.4.1) Where originator is Unknown Remote Party		
SupplementaryRemotePartyCounter	xs:nonNegativeInteger Where originator is Unknown Remote Party		

Table 242 : Read Firmware Version MMC Output Format Header data items

5.106.2.2 Specific Body Data Items

Data Item	Description / Valid Set	Type	Units	Sensitivity
FirmwareVersion	Current version number in manufacturer format. The Firmware version as held in the Central Products List and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F. This data item matches the value on the Central Products List (excluding the colon separator between octet values)	xs:string	N/A	Unencrypted

Table 243 : Read Firmware Version MMC Output Format Body data items

5.107 Activate Firmware

5.107.1 Service Description

Service Request Name	ActivateFirmware
Service Reference	11.3
Service Reference Variant	11.3

5.107.2 MMC Output Format

The xml type within the SMETSData element is ActivateFirmwareRsp. The header and body data items appear as set out immediately below.

5.107.2.1 Specific Header Data Items

GBCS v1.0:

Data Item	Electricity Response	Gas Response
GBCSHexadecimalMessageCode	0x0012	0x0012
GBCS Use Case	CS06	CS06

[1] The version of the GBCS for which these changes will apply to will be decided post-decision of this modification.

Timestamp	xs:dateTime

Table 244 : Activate Firmware Version MMC Output Format Header data items

GBCS v4.x[2]:

Data Item	Electricity Response (ESME)	Gas Response	HCALCS
GBCSHexadecimalMessageCode	0x0012	0x0012	0x0012
GBCS Use Case	CS06	CS06	CS06
Timestamp	xs:dateTime		

Table 244 : Activate Firmware Version MMC Output Format Header data items

5.107.2.2 Specific Body Data Items

Data Item	Description / Valid Set	Type	Units	Sensitivity
ActivateImageResponseCode	Outcome of the request for each replacement, with valid values: • success; • noImageHeld; • hashMismatch; or • activationFailure Optional – will not be present in responses to future dated Service Requests	ra:StatusASN1 As set out in section 5.58.2.2.2 of this document	N/A	Unencrypted
FirmwareVersion	A unique identifier representing a firmware image that has been approved by the User for release. The Firmware version as held in the Central Products List and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F. This data item matches the value on the Central Products List (excluding the colon separator between octet values). Optional – will not be present in responses to future dated Service Requests	ra:FirmwareVersion *(ra: data type is identical to the corresponding sr: data type, except that in ra: all the components are optional within the schema, although items may be mandatory within the business process)* (xs:string,where maxLength = 8)	N/A	Unencrypted

Table 245 : Activate Firmware MMC Output Format Body data items

[2] The version of the GBCS for which these changes will apply to will be decided post-decision of this modification.

SEC Modification Proposal, SECMP0007, DCC CR 211

Firmware Updates to Mandated HAN Devices (PPMIDs and HCALCS)[1]

Full Impact Assessment (FIA)

Version:	**0.76**
Date:	**5th August, 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

[1] PPMID = PrePayment Meter user Interface Devices, HCALCS = HAN Connected Auxiliary Load Control Switch

Contents

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
10/07/2020	0.4	Initial responses with DCC first review
22/07/2020	0.55	Release to Working Group
30/07/2020	0.71	Incorporated feedback from TABASC and Working Group
04/08/2020	0.76	Included overall costs

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	SECMP0007 – Solution Design Note 0.7	SECAS	07/08/2018
2	Updated Requirements and Preliminary Impact Assessment (PIA) version 1.21	DCC	05/08/2019
3	SECMP0007 Firmware updates to IHDs and PPMIDs' Business requirements – version 1.31	SECAS	04/02/2020

References are shown in this format, [1].

An initial draft of changes to the Great Britain Companion Specification (GBCS) with changes related to this Modification was shared with the Service Providers by SECAS.

1.3 Document Information and Modification History

The Proposer for this Modification is now Robert Williams, E.ON.

An Early Impact Assessment was requested of DCC in July 2016, after updated requirements were issued by SECAS, with the first Preliminary Impact Assessment (PIA) supplied in July 2018.

A full review of the PIA was carried out based on the expiry of the original design and cost estimates in the original PIA. The second version of the PIA (0.60) submitted in April 2019, includes a full listing of the requirements and two options for a solution approach; solution 1 using Zigbee Over The Air was covered in the previously issued PIA, but a new solution 2 for implementing firmware upgrades using the existing ESME approach was proposed. The document was used by the Service Providers as the basis for a high-level solution design with associated, revised costings.

That document was then reviewed to reflect the findings of the Working Group, and the Refinement Consultation, which included a check on the scope of the Modification.

A first Full Impact Assessment was requested by SECAS on 24th July 2019, but approval to proceed was not issued until 20th August, 2019, and the document was not fully completed.

In December 2019, a streamlining review designed to generate a minimum viable product including the Working Group, Service Providers, and BEIS met. A modified and reduced scope was defined, and the Service Providers were asked to complete a FIA against the new requirements in April 2020.

Note that a section highlighting design decisions made during the development of this solution has been added in Appendix D: Design Decisions.

1.4 Terminology

Note the terms "Device” and "HAN Devices" are used interchangeably with the phrases "PPMID / HCALCS" and "PPMID and HCALCS" in this document. The terms PPMIDS, PPMIDs, and HCALCSs were used in the Business Requirements and may appear in this FIA.

The terms "updates” and "upgrades" relating to firmware updates are used interchangeably in this document.

Additional terms specific to this Modification have been added to Appendix A: Glossary at the end of this document.

2 Introduction

This section gives context to the required solution and includes both the high-level business requirements and detail of the proposed solution. Most of this section is taken verbatim from the business requirements document [3] published by SECAS.

2.1 Context

Over-The-Air (OTA) firmware updates through the DCC Total System are currently supported only for the Communications Hub (CH), Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) devices. This modification aims to enable Suppliers to send Manufacturer produced Firmware updates to PPMIDs and HCALCS via the DCC, and for the HAN devices to be able to activate those updates, subject to Manufacturer specific checks that updates are valid (i.e., from the Manufacturer; valid for the Device's current Device Model etc.).

It should be noted there are already a large number of PPMID devices in the field that will require firmware updates, and this number will have increased by the time this Modification is implemented.

2.2 Requirements

Based on the discussions at the Working Group and the Business Requirements as set out in the Solution Design Document [1], DCC understands the outcomes this modification wants to achieve the business requirements that can be summarised as follows.

1.	Manufacturer Image Hashes associated with PPMIDs and HCALCSs to be added to the Central Products List (CPL)
2.	Suppliers to be able to send firmware updates to PPMIDs and HCALCSs over the air (OTA)
3.	The DCC to notify all Responsible Suppliers at certain stages during the processing of firmware updates
4.	The DCC and Responsible Suppliers will check the latest firmware version on PPMIDs and HCALCSs
5.	The Communications Hub will be able to support the prioritisation of firmware Images to all HAN Devices
6.	Upon firmware Image activation, the DCC will update the Smart Metering Inventory (SMI) with the new firmware version for the updated Device
7.	Additional Communications Hub functionality to support the distribution of OTA Upgrade Images to PPMIDs and HCALCSs
8.	Firmware update support capability will need to be mandated on PPMIDs installed after this Modification is implemented

Table 1 High L:evel Business Requirements:

2.3 Detailed Requirements and Business Processes for Firmware Upgrades

A detailed breakdown of the requirements, supporting information, and potential business process solutions for the requirements follows.

2.3.1 Adding PPMID/HCALCS Manufacturer Image Hashes to the CPL

For a Manufacturer Image to be added to the Central Products List (CPL), additional details in relation to that Image will need to be provided to the SEC Panel.

The Supplier will need to confirm to the Panel that the firmware update does not affect how the PPMID or HCALCS communicates using ZigBee.

If the firmware update impacts how the PPMID or HCALCS communicates using ZigBee and requires re-testing, a new ZigBee Assurance Certificate will need to be provided to the Panel before the firmware can be updated.

The CPL Requirements Document specifies the additional details in relation to the Manufacturer Image that must be provided to the Panel:

- the Hash of the Manufacturer Image;
- the identity of the organisation that created that Image; and
- a digital signature created by the creator of the Image across the communication containing the CPL entry details.

The digital signature used to sign the communication between the submitter and the Panel needs to be the same as the one received from a Public Key Infrastructure (PKI) chosen by the Panel to check the signature

A template for submitting CPL entries has been published on behalf of the Panel, which sets out the approach to digital signing taken by the Panel.

In addition to the above, HCALCSs must comply with the Commercial Product Assurance (CPA) Security Characteristics as per the Smart Metering Equipment Technical Specification (SMETS). Changes to HCALCS firmware may require either the inclusion of the new firmware version in the existing CPA certificate or a new CPA certificate. For HCALCSs, this CPA certificate must be submitted to the Panel when adding a new firmware version to the CPL.

2.3.2 Communications Hub Memory Considerations

No additional buffer space on the Communications Hub is being proposed. Only the GSME memory block will be used for storing PPMID and HCALCS Images. The ESME memory block will not be used to store PPMID and HCALCS Images.

PPMID and HCALCS Images will be overwritten by GSME Images if one arrives whilst a PPMID or HCALCS update is in progress. If another PPMID or HCALCS Image arrives whilst a PPMID or HCALCS update is in progress, the newly arrived Image will overwrite the one in process.

Changed requirement: There will be no Service-Level Agreement (SLA) for how long a firmware Image can be stored in the Communications Hub before it is overwritten. The Image will remain on the Communications Hub until it is overwritten.

The Communications Hub shall make the PPMID / HCALCS image available for fourteen (14) days unless a new PPMID / HCALCS / GSME image is available.

If a PPMID / HCALCS / GSME Upgrade Image is discarded or replaced prior to having been successfully transported over the HAN, the Communications Hub shall send an Alert for each target Device Entity Identifier associated with the Upgrade Image File

GBCS drafting places a requirement on the CH to send an Alert for each device associated with an image when the image:

(a) has transferred to the target successfully

(b) failed to transfer after all retries (at ZigBee level) have been exhausted

(c) is discarded.

The Supplier will then know status of the file transfer and whether the image needs resending. If the image is discarded after the mandated storage duration ((c) above) then there is a fair chance that the PPMID isn't operational. A Supplier could send the read firmware version command to the PPMID (after initial upgrade or new installation of a PPMID which supports the feature), but the absence of a response would simply confirm that the PPMID isn't operational; just much quicker.

2.3.3 Dual Supplier Scenarios

Both Responsible Suppliers shall be able carry out firmware updates to PPMIDs in dual Supplier scenarios. The Proposer and the Working Group accept that this may increase the risk of firmware updates being overwritten by each of the Responsible Suppliers in a dual Supplier scenario.

Only the Import Supplier shall be able to carry out firmware updates to the HCALCSs.

2.3.4 Anomaly Detection Thresholds

The Security Sub-Committee (SSC) have stated that Service Requests to update firmware for PPMIDs must be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME. However, PPMIDs must be counted and reported separately to enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs.

The SSC also stated that Service Requests to update firmware for HCALCSs should subject to the same ADT procedures as ESME and GSME since similar risks to the supply of energy apply to HCALCSs.

2.3.5 Activation date-time

Future dated activation of PPMID Manufacturer Images will not be permitted. Upon successful receipt of the OTA Upgrade Image by the PPMID, the Communications Hub will instruct the PPMID to immediately activate the new Manufacturer Image.

Changed requirement: The Communications Hub will no longer be required to record the activation date-time plus [X] minutes. This is due to the decision made at the Working Group meeting held on 19 December 2019, to have the PPMID generate the Device Alert for success/failure of the firmware update. This Alert will go from the PPMID to the Supplier, via the Access Control Broker (ACB).

HCALCS Manufacturer Images are activated using the existing Service Request 11.3, which must be adjusted to include HCALCS as valid target Device Type.

2.4 Sending PPMID Firmware Images

This section outlines how the process will work for PPMIDs if firmware is made up of a single Manufacturer Image or several Manufactures Images. HCALCSs are covered in Section 4 'Sending HCALCS Manufacturer Images' below.

Note: An OTA Upgrade Image must be less than or equal to 750KB in size.

2.4.1 Sending a single Manufacturer Image to a PPMID

This section details the steps that will need to be taken to update PPMID firmware. It is assumed that a Manufacturer provides a Manufacturer Image to the Supplier and a new CPL entry has been created. The resulting OTA Upgrade Image will be less than or equal to 750KB in size.

Sending a Manufacturer Image to a PPMID will require a new Non-Critical Service Request 'Send PPMID Firmware'. Currently the next available and most logical Service Reference Variant for this Service Request will be 11.4.

Supplier Preparations

Before sending the new Service Request to the DCC for a PPMID firmware update, the Supplier will be required to follow several steps. These will be similar in initiating a firmware update to the DCC for a Meter:

Obtain the following information:

1. The Manufacturer Image

2. OTA Header, which should include:

    a. Manufacturer ID;

    b. Model to which it can be applied;

    c. Firmware Version contained in the Image; and

    d. Minimum and maximum hardware version to which it can be applied.

3. A Hash of the Manufacturer Image.

Undertake the following checks on that information:

1. The Hash the Supplier has calculated over the Manufacturer Image is the same as that provided by the person who created the Manufacturer Image (in this case the Manufacturer); and

2. Check that the Manufacturer Image is associated with one or more Device Models on the CPL. The check should include that:

    a. The Hash is recorded on the CPL against one or more entries;

    b. The OTA Header Manufacturer ID, model and Firmware Version fields match identically with one of the entries identified at step (a); and

    c. The hardware version in that CPL entry is between OTA Header minimum and maximum hardware version, inclusively.

Supplier creation of a 'Send PPMID Firmware' Service Request

Having obtained the information and upon the above checks being successful, the Supplier will create a 'Send PPMID Firmware' Service Request. The Service Request will include the following information:

1. Image: The Image to be sent composed of a base64 encoded version of the concatenation:

OTA Header || Manufacturer Image

2. List of Device IDs: Up to 50,000 PPMIDs will be able to be listed within the Service Request.

The DCC checks on the 'Send PPMID Firmware' Service Request

On receipt of the 'Send PPMID Firmware' Service Request, the DCC will follow the following steps:

1. Check whether the OTA Upgrade Image contained within the Service Request is less than or equal to 750KB in size;

2. Calculate the Hash of the Manufacturer Image contained within the Service Request;

3. Check whether the Hash the DCC has calculated is on the CPL, and identify CPL entries with that Hash;

4. For each of the Device IDs in the Service Request:

    a. Check the Device is a PPMID;

    b. From the Smart Metering Inventory (SMI), identify the Device's current Device Model, and ensure that the Manufacturer ID, model and hardware version fields for that current Device Model equate to one of the entries identified at step 3;

    c. Identify, from the SMI, the Communication Hub Function (CHF) ID to which the Device is associated; and

    d. Check that the Supplier is the Responsible Supplier for one of the Smart Meters Associated with that CHF ID.

If this and all preceding checks succeed, the DCC will identify (and temporarily record against the Device ID) the details of all Responsible Suppliers Associated with the CHF ID. This temporary record will be used to populate the DCC Alerts at the next step.

DCC response to the 'Send PPMID Firmware' Service Request

The DCC will be required to notify all Responsible Suppliers at different stages of the Service Request processing. The first notification will happen when the DCC receives the 'Send PPMID Firmware' Service Request:

1. Upon the DCC receipt of the 'Send PPMID Firmware' Service Request, the requesting Supplier will receive a Service Response. If some of the Device IDs in the Service Request failed any of the checks at step 4 under 4.1.3 (above), the DCC will send a Service Response to the requesting Supplier listing all the Device IDs that failed and the reason for the failure in each case. The DCC will carry on processing the firmware distribution for those Device IDs that passed the check.

2. Upon the DCC completing the processing of the 'Send PPMID Firmware' Service Request, each Responsible Supplier identified in 4.1.3 will receive a DCC Alert containing:

a. The Hash of the Manufacturer Image in the Service Request (to identify the CPL entry)

b. A list of Device IDs to which the Image is being sent

DCC Distribution of the 'Send PPMID Firmware' Service Request

If the checks are successful, the DCC will distribute the Image from the Service Request (having decoded from base64 encoding) to the Communications Hub associated with each of the PPMIDs in the List of Device IDs where the Device ID passed the validation.

SEC Schedule 10 'Communication Hub Technical Specifications' (CHTS) 4.4.4 requires that the receiving Communications Hubs can buffer Images intended for ESME and GSME. The Communication Services Provider (CSP) contracts require Communications Hubs to have the capacity to hold two 750KB Images (to support independent distribution of firmware to one of the ESME and the GSME).

Communications Hub notification of Image availability to the PPMID

Once the Image arrives at the Communications Hub, the Communications Hub will need to:

1. Record OTA Header details

2. Notify the PPMID by sending a message to it/them ('the Communications Hub shall send a Zigbee Smart Energy (ZSE) Image Notify command').

PPMID request for the details of the Image

The PPMID will then, in line with the ZigBee OTA specification, send a message (a 'QueryNextImageRequest' ZSE command containing Manufacturer ID (manufacturer code), model (Image type), current Firmware Version, and optionally hardware version) to ask the Communications Hub if there is an Image that may be suitable for it.

Provision of Image details by the Communication Hub to the PPMID

For the Communications Hub to decide that the Image is suitable for the PPMID, the ZigBee OTA specification details a recommended, default policy to determine its response, specifically to:

'send back a response that indicates the availability of an Image that matches the manufacturer code, Image type, and the highest available file version of that Image on the server. However, the server may choose to upgrade, downgrade, or reinstall clients' Image, as its policy dictates. If client's hardware version is included in the command, the server shall examine the value against the minimum and maximum hardware versions included in the OTA file header'

Note that 'server' in the above refers to the Communications Hub and 'client' refers to the PPMID.

The Communications Hub will send back a 'QueryNextImageResponse' accordingly.

PPMID download and authentication of the Image

The PPMID will then download the Image from the Communications Hub, if one is available for it.

When the PPMID has downloaded the Image, it will check the Manufacturer signature (or equivalent) within it. This confirms the Manufacturer Image is as created by the Manufacturer. The PPMID will then store the Manufacturer Image from within the Image sent, so that it is available for activation . The PPMID will then send a 'UpgradeEndRequest' to the Communications Hub.

Activation of the firmware Image

The Communications Hub will then send a 'UpgradeEndResponse' with the activation date-time set to 0x00000000 for immediate activation in line with the ZigBee specifications. The PPMID will immediately activate the Image.

The PPMID will then create a Device Alert containing its firmware version and send it to the DCC. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

If the Device Alert is not received, the Supplier can send SR11.2 to the DCC. This will result in a Command to the PPMID to respond with its active firmware version. The DCC will forward the Response to the Supplier and update the SMI if the firmware version in the SMI is different. SR11.2 can also be sent at any time by a Responsible Supplier if desired.

Process for updating PPMID Firmware comprised of a single Manufacturer Image

The process described above for processing PPMID firmware updates comprised of a single Manufacturer Image is presented in Figure 1 below.

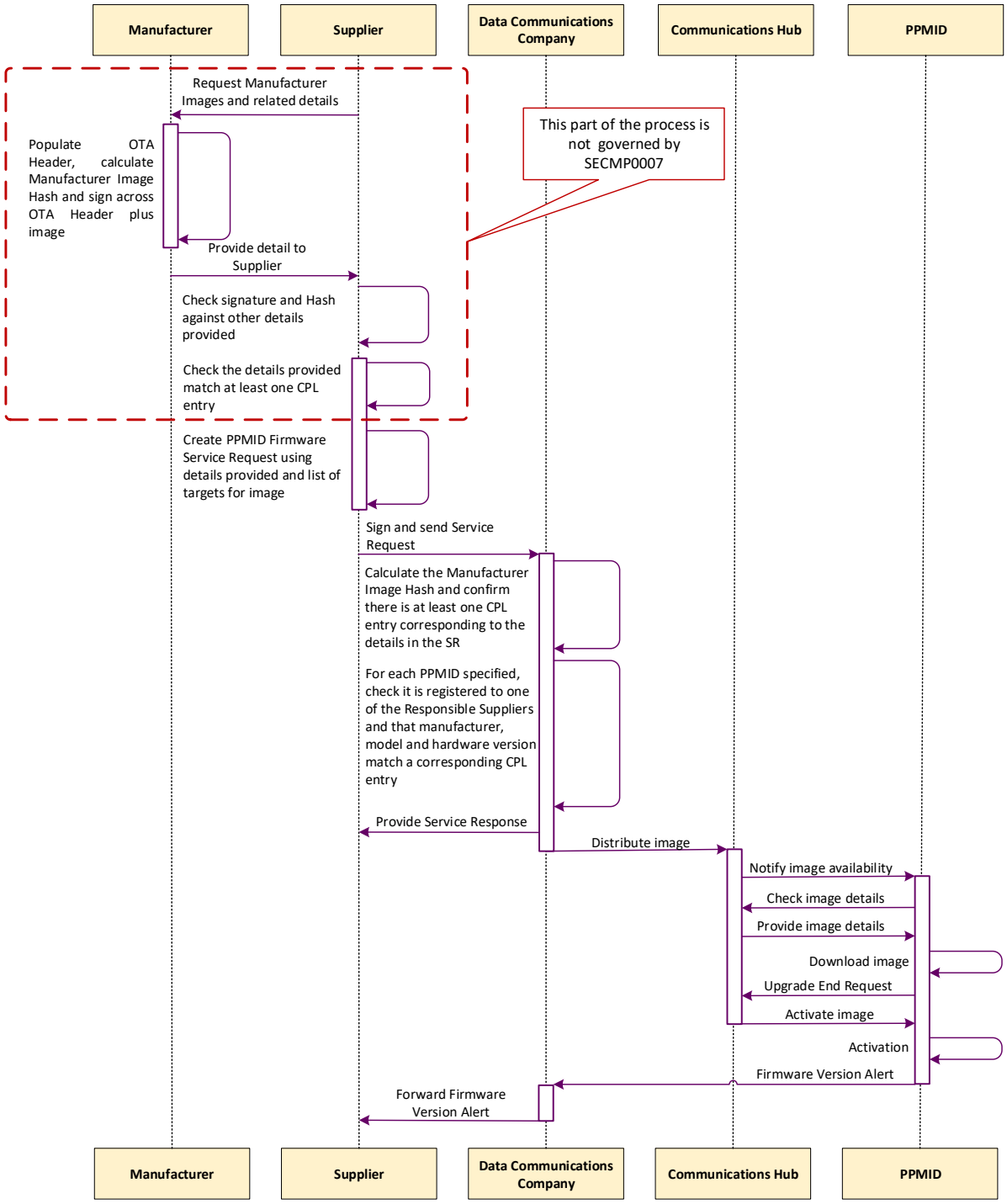


Figure 1 Process for updating a single PPMID Manufacturer Image

2.4.2 Updating PPMID firmware with Multiple Manufacturer Images

This process is for the benefit of Manufacturers and Suppliers, and does not propose any changes to the way in which the DCC manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

A full description of this process is given in Appendix B: Updating PPMID Firmware with Multiple Manufacturer Images on page 59 below.

2.4.3 Sending HCALCS Manufacturer Images

The process for the OTA upgrade of HCALCSs aligns with the current Technical Specifications and GBCS for the Supplier to distribute and activate firmware on the ESME and GSME. This will be accomplished by adding the HCALCS as a target Device Model to the existing Service Reference Variants.

As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

The expectation is that HCALCS firmware is typically below 750KB. However, the existing ESME/GSME OTA firmware upgrade mechanisms contained in the GBCS allow manufacturers to split firmware into multiple OTA Upgrade Images less than or equal to 750KB in size; this method can be employed in case HCALCS firmware exceeds the size of 750KB.

2.5 Non-Functional Requirements

PPMID firmware is expected to be typically less than 750KB in size and updates will occur no more than two times per year. Note that there is no requirement for a Change of Supplier (CoS) action to require a PPMID update.

Device manufacturers have advised that their firmware updates are likely to be no larger than 350KB. However, the customisation of PPMIDs with graphics will increase the firmware size; this may happen going forward and require the mechanism for delivering firmware greater than 750KB. In any case, any single OTA Upgrade Image must be less than or equal to 750KB.

In terms of the numbers of PPMIDS installed and requiring updates, DCC has supplied the following information and assumptions. Overall installation numbers are as follows:

SMETS2	Today	At Scale (End 2024)
PPMIDS	2.4million	17.9million
CHF	2.7million	20.3million
%		88%

In the table above, the ratio of PPMIDS to CHF as of July 2020 (about 88%) has been linearly scaled to an "at scale" number of devices. It should be noted that CSP South and Central accounts for approximately 68% of all installations, based on ITSF forecasts.

For network loading and infrastructure augmentation calculations, there is an assumption that the installed base of PPMIDs should be taken as the updateable base. This is almost certainly an overestimate. SECAS have initiated a Request For Information to try and identify the current position.

A further breakdown of the figures to volumes per minute for an example installed base of 15 million PPMIDS looks like this:

- 15 million PPMID updates over 6 months, with two firmware updates per year
- Even Distribution across each of the 6 months
- Equates to an average of 60 firmware downloads per minute

This assumes the sending of single updates to single devices, therefore excluding any batching of updates, any updates rejected for authentication, and does not include resends of data. In previous discussions there has been a variation of +/-10% over the year, and this figure can be applied to system throughput as well.

Volumes associated with HCALCS firmware is expected to be much smaller and with a very low upgrade frequency. It may be possible that HCALCSs do not need updates at all unless changes to the ZigBee version are required.

Following from the discussion with the Security Sub-Committee (SSC) there are no security concerns with regards to firmware upgrades for PPMID or HCALCS.

2.6 Requirements Summary

Based on the discussions at the Working Group and the Business Requirements as set out in the Solution Design Document, DCC consider the requirements for SECMP0007 to be **STABLE**.

3 Solution Architecture

Over-The-Air (OTA) firmware updates through the DCC Total System are currently supported for the Communications Hub (CH), Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) devices only.

3.1 Solution Overview

This Modification will allow the Service Users to send firmware images for PPMIDs and HCALCS using the DUIS interface. The DSP will process the received request that contains the firmware image and the list of devices, and forward that to the CSPs along with the corresponding Comms Hub identifiers. DSP will make use of the existing Web Service interface at the two CSP SMWAN Gateways to deliver the firmware image to the CSPs. The OTA firmware image processing by CSPs for PPMID differs slightly from that of the other device types (ESME, GSME or HCALCS) as described below, and the DSP will add a new field to the firmware distribution interface such that CSPs will know the device type.

There will be two different firmware image delivery mechanisms used by Comms Hubs:

- A ZigBee Over-The-Air (OTA) delivery mechanism will be used to deliver firmware to PPMIDs. This method introduces the combined distribution and activation of the Manufacturer Image into one single Service Request. This will be a new Non-Critical Service Request created specifically for the PPMID. The Communications Hub is to manage the activation of PPMID firmware. The PPMID itself will manage the notification to the Service User upon activation of the firmware.
- HCALCS will utilise the existing 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. As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 ‘Update Firmware’ and activation via SR11.3 ‘Activate Firmware’, the latter via a Great Britain Companion Specification (GBCS) Critical Command.

The CSPs will deliver the firmware image to the corresponding Comms Hubs and the Comms Hubs will in turn deliver it to the target device within the HAN.

The schematic below shows an end-to-end view of the OTA firmware delivery and the mechanisms used to communicate between different systems. The interfaces and message formats used by DSP to communicate with the other parties or devices remain unchanged. The key change is the introduction of a new firmware distribution mechanism (Zigbee OTA as opposed to a combination of Zigbee OTA and GBCS) between the Comms Hub and the PPMID as shown in the schematic below.

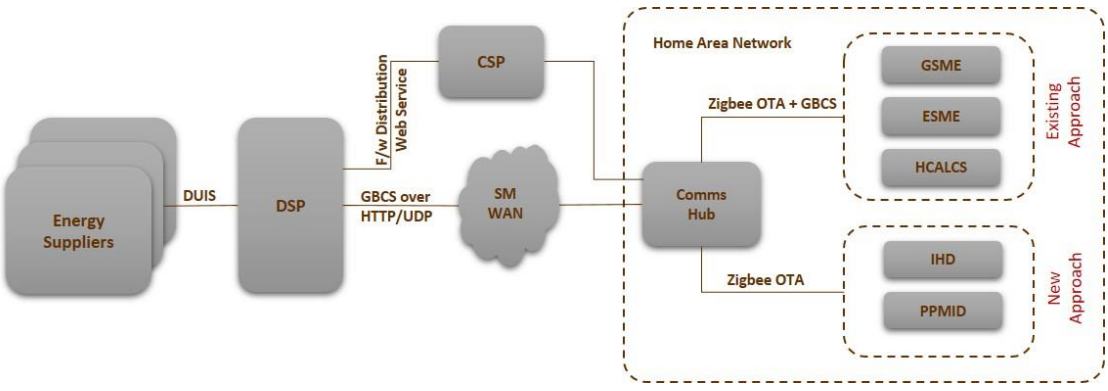


Figure 2 Firmware Delivery Overview

This is a wide-ranging SEC Modification and the impacts across the system actors and components are as follows:

CSP N	H	BIMI	N	CHTS	Y		
CSP S & C	H	GBCS	Y	CH	Y	HCALCS	Y
DSP	H	DUIS, DUGIDS, MMC XML	Y	CPL	Y	PPMID	Y
P & C	H	SMETS	Y	ESME	N		
BT	N	SEC	Y	GSME	N		

Note that SMETS1 devices are not in scope of this Modification, and are covered by a separate DCC programme.

3.2 DSP Solution Overview

The DSP is required to fulfil the following high-level requirements:

- Add support for processing the firmware update requests for PPMID and HCALCS devices within DSP
- Track the progress of the firmware updates and send notifications to the relevant Service Users

The solution is made up of a common component for tracking the firmware distribution progress, and two distinct methods of firmware updating, Zigbee OTA and GBCS Delivery.

The following Service Requests will be enhanced to support the OTA upgrades:

- SR 11.1 ‘Update Firmware’
- SR 11.2 ‘Read Firmware Version’
- SR 11.3 ‘Activate Firmware’

A new Service Request to distribute the firmware images specifically for the PPMIDs, 11.4 Update PPMID Firmware, will be introduced. SRV 11.4 will share its general attributes and validation checks with SRV11.1. Please note that SRV11.4 will be applicable only for SMETS2 PPMIDs.

For HCALCS, the existing Service Requests and the process used for GSME and ESME will be used. These include:

1. Use of the existing SRV 11.1 for distribution of firmware images to HCALCS
2. Use of SRV11.3 for activating the new firmware

The firmware images for both PPMID and HCALCS will be delivered to the CSPs using the existing interfaces.

In the SMETS the HCALCS sections must be updated to reflect the HCALCS capability of receiving and activating new firmware.

3.2.1 CSP Management and CSP SMWAN Gateway

No changes are required within the CSP Management Gateway.

CSP SMWAN Gateway will introduce a new interface for CSPs to notify DSP the status of a firmware image delivery to the Comms Hub.

The existing firmware delivery interface will be updated to include device type as a new attribute. This will help CSPs process the OTA image differently for PPMID device types.

The proposed interface changes are available in the documents attached here.


CR211-Telefonica-SMWAN-Gateway-Ext


CR211-Arqiva-SMWAN-Gateway-Extract

3.2.2 Firmware Distribution Progress Tracking

The DSP will track the progress of the firmware update request at a Device level. This will need to be built as a mechanism common to all device types and the following details will need to be recorded.

Field Name	Notes
Device ID	ID of a Device within the SR 11.1 request
Service Request ID	The Service Request ID
Firmware Version	New firmware version
Processing Status	Indicates the progress of the request (see table below for the status values).
Reason Code	The reason for rejection if the Processing Status indicates a rejection
Last Updated Time	The time at which the latest change in Processing Status was recorded.

Table 2 Firmware Update Tracking

Tracking will allow DSP to block the firmware update request for a device if there is already one in progress. Note there has been a request to change this to a per-Comms Hub basis as described in section 3.2.5 following.

The Service Users will be sent DCC Alerts to notify the different stages of firmware update processing. The input data for these Alerts will be received as notifications from the CSPs or as Device Alerts from the Comms Hubs.

The following diagram illustrates the updates to the firmware distribution flow due to these changes.

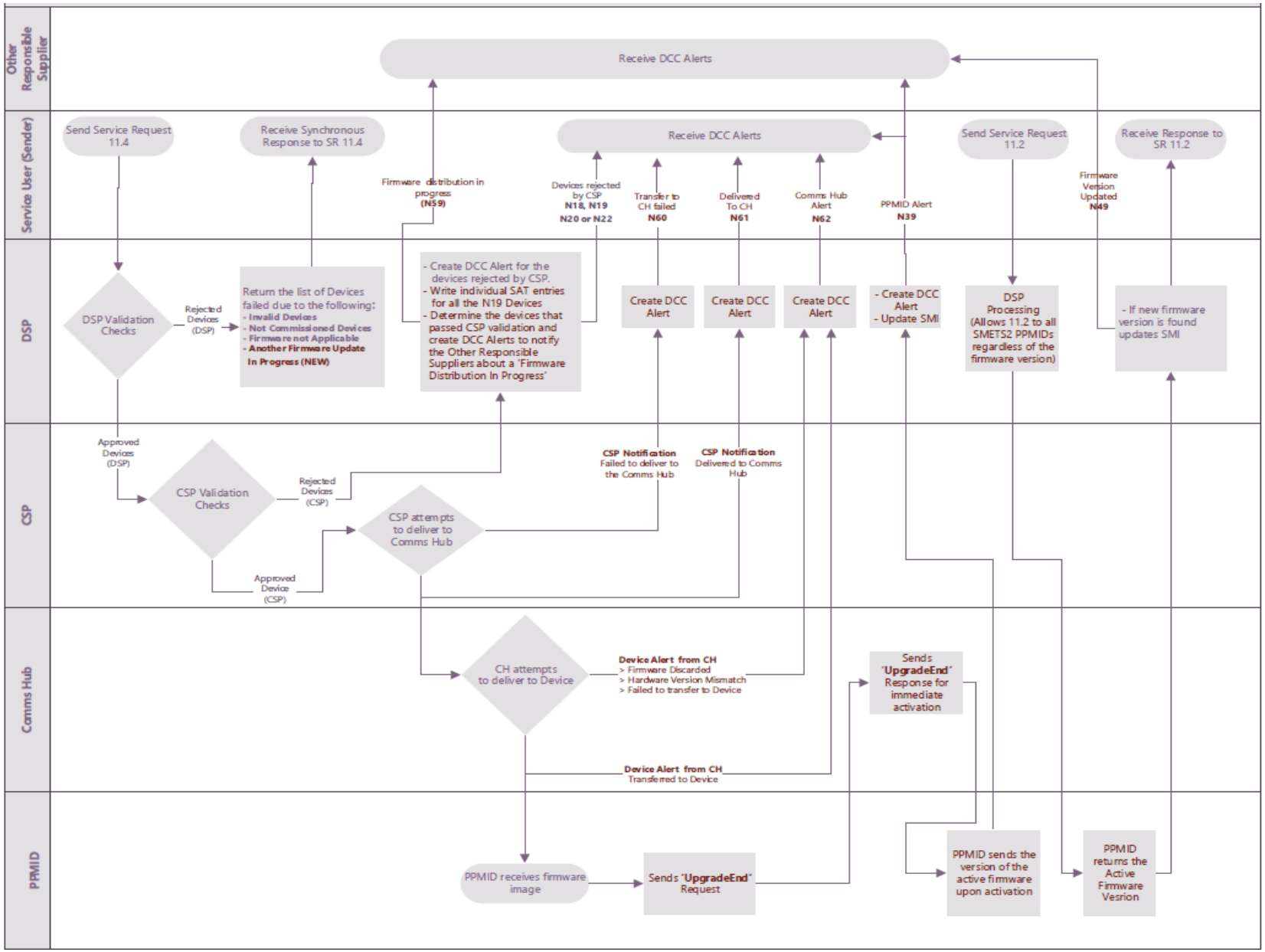


Figure 3: PPMID Firmware Distribution Flow

The first stage of processing by the DSP checks the list of devices included in a Service User request (SR11.1 or 11.4). Devices in the list may be considered as failed as follows:

- Invalid deice
- Not commissioned device
- Firmware not applicable
- Another firmware update in progress

A synchronous response with these device IDs is sent to the Service User that submitted the request.

The DSP then identifies which CSP each device ID is allocated to, and the CSP SM WAN Gateway sends a batched request to the appropriate CSP. The DSP will segregate the PPMIDs based on the region and send them to the relevant CSP using the existing CSP SMWAN Gateway interface to distribute firmware. This interface will be updated to include a new attribute to convey the type of device to the CSPs to help distinguish PPMIDs from the other device types.

The firmware distribution processing statuses maintained by the DSP include associated DCC Alerts as summarised in the table following.

Processing Stage	Processing Step	Processing Status	Notes	Trigger	Outbound Notification Mechanism	Recipients
Processing within DSP	DSP validation checks	REJECTED_BY_DSP	This functionality exists except for the check to see if another firmware update request is in progress for any of the devices.	NA	Synchronous Response	Sender of SR 11.1 or 11.4
Processing within CSP	CSP validation checks failed	REJECTED_BY_CSP	This functionality currently exists.	Notification from CSP	DCC Alerts **N18, N19, N20 or N22**	Sender of SR 11.1 or 11.4
	CSP Validation Checks Successful	APPROVED_ FOR_DISTRIBUTION	Derived by DSP as the inverse of the list of rejected devices. One Alert per Service User.	The above notification from CSP	DCC Alert **N59**	All Responsible Suppliers other than the Sender
	Delivery to Comms Hub Failed	FAILED_CH_TRANSFER	New interface required at CSP SMWAN Gateway to receive this.	Notification from CSP	DCC Alert **N60**	Sender of SR 11.1 or 11.4
	Delivered to Comms Hub	SUCCESSFUL_ CH_TRANSFER		Notification from CSP	DCC Alert **N61**	Sender of SR 11.1 or 11.4
Processing Within HAN	Comms Hub failed to deliver to target Device	FAILED_HAN_ TRANSFER	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 3	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or 11.4
	Delivered to target Device	SUCCESSFUL_ HAN_TRANSFER	Device Alert from Comms Hub with Alert Code 0x8F8A and Transfer Response Code 0	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or 11.4
	Firmware discarded by Comms Hub	HAN_DISCARDED	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 1	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or SR11.4
	Firmware rejected by Comms Hub due to version mismatch of the target hardware	HAN_REJECTED_HW_M ISMATCH	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 2	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or SR11.4
	Device activates the firmware	FIRMWARE_ACTIVATED	Applicable only for PPMIDs. The Alert Code is 0x8F8B.	Device Alert from PPMIDs	DCC Alert **N39**	All Responsible Suppliers
Service Desk Intervention	Device status reset	RESET_BY_DCC	Changed by the DCC Service Desk via the SSMI interface	NA	NA	NA

Table 3: Firmware distribution statues and DCC Alerts

The status values APPROVED_FOR_DISTRIBUTION, SUCCESSFUL_CH_TRANSFER or SUCCESSFUL_HAN_TRANSFER will be considered as 'In Progress' statuses by the tracking mechanism. If DSP receives a firmware update service request (SR11.1 or SR11.4) for a device, which already has another request with an 'In Progress' status, then the new SR will be rejected. A device will be allowed to stay in the 'In Progress' status only for a limited period of 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 and will need to be agreed with DCC.

If there is a need to reset the status of a device manually, the DCC Service Desk will be able to use a new interface provided within the SSMI. This will help reset the status of a device before the tracking timeout expires.

The Service Users will be able to view the last recorded processing status of a device using a SSI screen. Development of the SSI change will be carried out during the design phase.

For the HAN Devices rejected by a CSP due to a Device ID identification failure (DCC Alert N19), individual SAT Log entries will be made.

For the PPMIDs that pass CSP's validation checks, the DCC Alert N59 will be sent to the Responsible Suppliers other than the sender of the SRV 11.4 to notify that a firmware update has been initiated for a given device. DSP derives the list of devices that passed the CSP's validation checks by taking the inverse of the list of devices that fail the validation checks.

In order for DSP to receive notifications from CSP that contain the delivery status of firmware image to the Comms Hub, a new interface will need to be built at the CSP SMWAN Gateway.

Note that a Comms Hub has two slots for firmware upgrades that will also be used for ESME and GSME updates. If several updates are in progress at about the same time then the Comms Hub is expected to prioritise meters upgrades over PPMID upgrades, so a PPMID upgrade may be refused, or an accepted one may be deleted. There will be no retry within CSP or DSP. This situation will be handled by the Comms Hub sending an alert to the DSP as the Access Control Broker, to inform the sender of the firmware update request. It will be the sending supplier's responsibility to re-request the update if required.

A new DCC Alert (N62) will be used for forwarding all the Device Alerts that result from the firmware update processing within a Comms Hub to the Service Users. This will contain a payload with information about any failure messages.

DSP will create SAT log entries for all the Device Alerts. If the Device Alert includes Response Code to indicate a failure, the Response Code will be included in the SAT record. The SAT records for Alerts received from the Comms Hub will contain the Device ID of the relevant device.

Based on the mechanism used by the Comms Hubs to deliver the firmware images to the target devices, the overall solution has been divided into two parts.

3.2.3 Part 1: PPMID Firmware Updates using Zigbee OTA Delivery

The following principles and constraints have been identified for this solution option:

- A Comms Hub needs to be aware of the status of a firmware image download to a HAN device i.e., complete or in progress
- Storage prioritisation for both the Comms Hub and the DSP will be enabled. The DSP will send only one firmware request at a time for a specific device until the Comms Hub indicates the update is complete, and the oldest dated firmware is removed.
- There must be a capability to hold two firmware upgrades in the Comms Hub memory, so there is an ability to queue the upgrades, but there is only one update running at a time

- CHTS changes will be required
- The DSP would reject any request for a firmware upgrade, if there is already one in progress
- There is a requirement for an uplift to any Comms Hub emulator
- Devices remain as Type 2 devices, and communication limited to Zigbee only

A Zigbee OTA delivery mechanism is used for delivering firmware image to a PPMID, the processing of which does not rely on GBCS. The firmware image will be activated automatically after it has been successfully delivered to the PPMID. Therefore, a separate activation request is not needed.

A new Service Request 11.4 Update PPMID Firmware will be introduced to distribute the firmware images specifically for the PPMIDS, and this will enable the DSP to maintain the Anomaly Detection volume thresholds of PPMIDs separate from the other device types. SRV 11.4 will share its general attributes and validation checks with SRV11.1. Note SRV11.4 will be a Non-Critical command and therefore Users aren't obligated to submit ADTs for this. The SSC confirmed this is acceptable as the PPMID devices are not load controlling.

All the Device Alerts from the Comms Hubs will be sent to Service Users as DCC Alerts in relation to the Processing Statuses identified in Table 2. This will help the Service Users to be aware of the progress of the firmware update.

DSP will record the sender's ID of the latest firmware update request (SRV11.4) for the PPMIDs to determine the destination of the DCC Alerts.

Service Users will be able to read the version of the PPMID firmware by using the Service Request 11.2 Read Firmware Version. If the SRV 11.2 is targeted at a PPMID, then the DSP will employ the URP (Unknown Remote Party) pattern to process this. **Note** the correct behaviour relating to 11.2 will only work with PPMIDs where their firmware has been updated using SECMP0007.

If the Response to SRV11.2 contains a version of firmware different to the version in SMI, the SMI will be updated with the new version subject to the rules applicable for the other Devices. Therefore, Service Users could use SRV11.2 also as a vehicle for updating the firmware version of PPMIDs in the SMI.

Summary

- Service Users will be able to use SRV 11.4 to send the firmware update requests for PPMID
- Service Users will receive notifications at different stages of processing across DSP, CSP and the Comms Hubs
- Service Users will be able to use SRV 11.2 to read the firmware version of PPMID as well
- The firmware update mechanism used for PPMID does not require separate activation request as it is activated automatically upon successful distribution

3.2.4 Part 2: HCALCS Firmware Updates using GBCS Commands

The main principles of the alternative approach to implement firmware upgrades is based on a very different approach from the Zigbee OTA delivery.

- This approach treats any device endpoint like an ESME, such that the firmware is pushed to it with credentials
- There is no need for device changes to support keys as HCALCS already have Supplier certificates which can be used to validate security credentials
- There is a requirement to ensure end to end security for the firmware image in the same way as ESMEs
- There is a risk that firmware upgrades could be fired repeatedly at devices with significant impacts on battery life etc. In this case, the required outcome is that the DSP would reject any request for a firmware upgrade, if there is already one in progress
- There is no requirement for any prioritisation of firmware request, which reduces the complexity significantly
- There is no dependency on the ESME device
- CHTS changes will be required to allow the storage of a Firmware update on HCALCS
- GBCS changes are required to support the Read and Activate Firmware Use Case for HCALCS

This option also requires uplift to emulation environments to allow end to end testing of firmware distribution.

The solution to update HCALCS firmware will follow the existing firmware update procedure used for the ESME and GSME. The end-to-end security of the HCALCS will be managed similarly to that of the ESME. The firmware distribution flow for HCALCS is shown following.

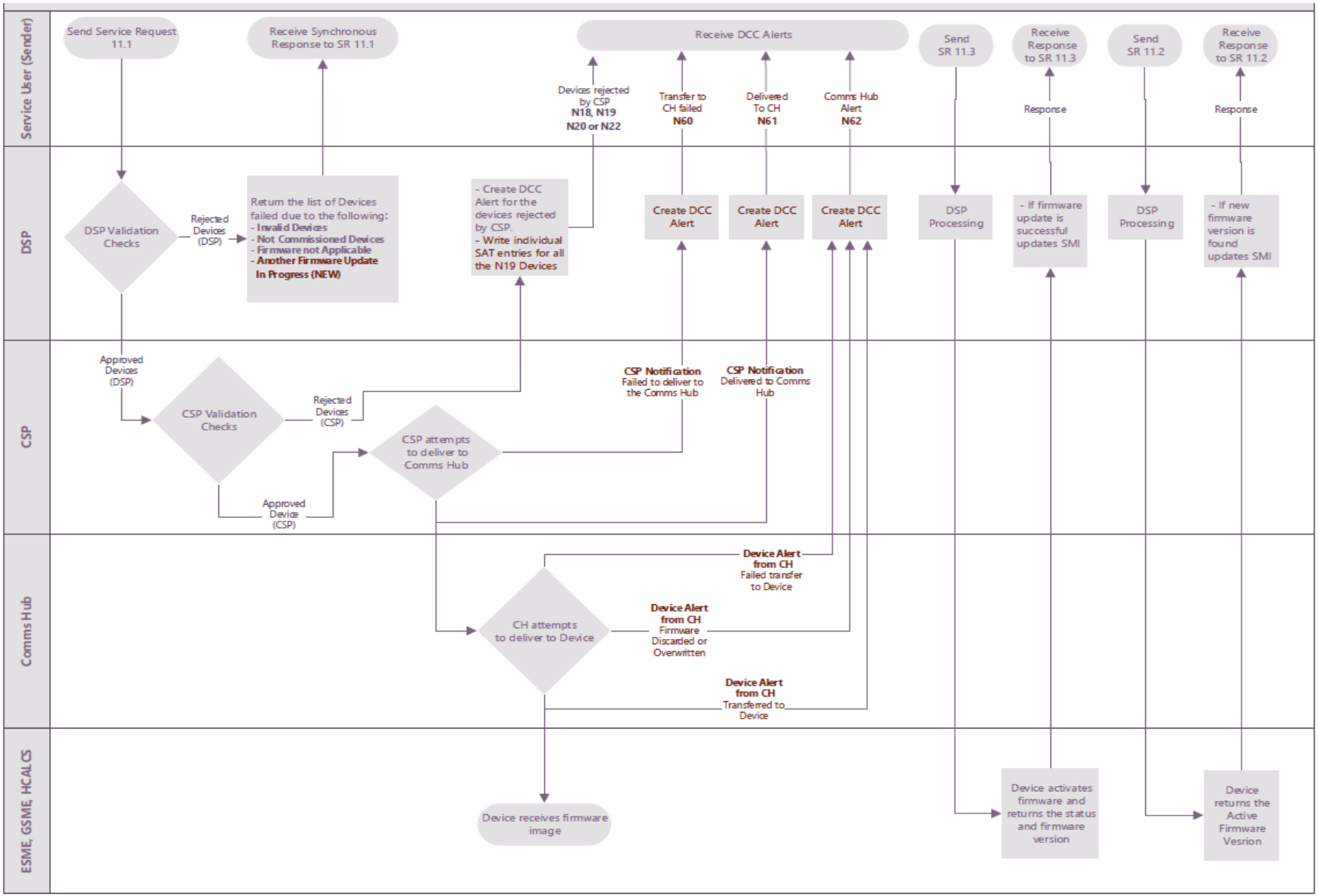


Figure 4: ESME, GSME and HCALCS Firmware Distribution Flow

Service Users will be able to use the following Service Requests for HCALCS firmware updates also.

- SRV 11.1 Update Firmware
- SRV 11.2 Read Firmware Version
- SRV 11.3 Activate Firmware

It is expected that the existing GBCS Use Case for ESME ECS52 (Read Firmware Version) will be implemented for HCALCS and therefore no new Use Case is required. The existing GBCS Use Case CS06 (Activate Firmware) will also need to be extended to HCALCS to support firmware activation.

3.2.5 Control Dependencies on DSP

Controls on firmware Service Requests have been identified as follows.

Note that the DSP implementation of “Firmware Tracking” is a slightly wider scope in that it tracks whether there is a firmware download in progress to the HAN device (i.e. ESME, GSME, PPMID, or HCALCS).

Control 1	Device-Based Control: Recommend a per device check to block any firmware distribution request (ESME / GSME / PPMID / HCALCS) for HAN devices where there is already an update in progress. This will prevent excessive repeated downloads from the CSP to Comms Hub – preventing an “accidental Denial of Service”. Extend the error response on SR11.1/SR11.4 to include an error and a list of devices rejected due to “firmware distribution in progress” to be sent back to the sender of the 11.1 or 11.4. Validation Rule (1) – DSP cannot send another HAN device firmware update to the HAN device until the first update is complete. Return failure code and list of devices Validation Rule (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.
Control 2	Add a CSP “Too Busy” Response to prevent CSP system overload. The proposal is to modify the existing firmware distribution APIs used for all HAN devices (not just for ESME/GSME) to notify the DSP if the CSP is unable to process the firmware upgrade request. The CSP would return a “Busy” (http 503) with a reason code. DSP currently carries out an immediate web service retry and then carries out a retry every hour for 24 hours followed by a timeout A change the DSP to include provision for an http503 (System Busy) response on the firmware distribution API is required and for this to invoke the “long retry” design pattern. Recommendation is that in all cases the "long retry" design pattern is extended to 4 days.
Control 3	CSP and DSP systems SD 4.4.2 / SD 4.4.1 interface change to notify the status of the firmware download over SMWAN, to support both the individual and batch API status notifications.

	Anticipate a high volume of such alert status notifications over the interface and recommendation is for the DSP to implement the batch API option, to potentially minimise the load on both the Telefónica and the DSP systems. The notification interface is included in the DSP changes, but will need an upper limit and other non-functional requirements.

3.3 CSP Impacts

This change enables a firmware upgrade to PPMIDs and HCALCS alongside existing HAN devices i.e. ESME and GSME, using a modified DSP-facing CSP hosted API, the SD4.4.1 (CSP North) or SD4.4.2 (CSP South and Central) Firmware Upgrade API. The firmware images will be subject to firmware validation report generation and communication to the DSP via the existing APIs.

Firmware images will be distributed to Comms Hubs with a priority lower than existing ESME or GSME firmware images such that if an ESME or GSME firmware request is received, they will be prioritised and scheduled for distribution of firmware image ahead of PPMIDS and HCALCS. The image activation instructions for PPMID will be embedded within the firmware image, image activation for HCALCS is separate to the distribute firmware request and follows the existing ESME/GSME firmware service.

The PPMID firmware version is to be read via a new GBCS use case targeting the Communications Hub as defined in GBCS, while the HCALCS firmware version to be read via a change to the existing SR11.2 DUIS command and associated GBCS use case.

Firmware distribution alerts will be sent to understand the device type and transfer success notification will be added. Two new alerts for all HAN device upgrades to indicate success or failure criteria of a firmware download.

This Modification also impacts the CSP Support applications, and will require expansion of environment compute and storage capacity. Whilst the nature of the changes to both the CSP Comms Hubs and support systems are similar, they are broken out and described in the following sections.

3.4 CSP South and Central Solution Overview

CSP South and Central's scope of delivery for this Modification includes the introduction of a new service to support the distribution of firmware images to additional HAN devices, i.e. PPMIDs and HCALCS. The features of this service include the Modification of the existing CS06 meter firmware service and newly introduced service including:

- Introduction of the HAN firmware transfer status alerts from the CSP to the DSP. The business rules with regards to the usage of the new API would be designed in the Design stage, as CSP South and Central anticipates a potential increase to the volume of such SMWAN firmware distribution notification alerts, which will be seen in the DSP hosted API in the SD 4.4.2 SMWAN Gateway interface.

- Confirmation of a failure to transfer a firmware image to the appropriate HAN device.

- Introduction of new service busy alerting to temporarily defer the DSP service request until the CSP platform is able to service the firmware upgrade request.

3.4.1 Impact to CSP South and Central Communication Hubs

The CSP South and Central Comms Hub impacts to deliver this Modification are outlined below.

Change Category	Description of Change
New	Implement new GBCS Use case CS05c Distribute Firmware to PPMID including immediate activation of PPMID as a new command Implement new GBCS Use case CCS08 Firmware Transfer Alert to notify the DSP with the firmware download status alerts in-line with GBCS alert structure (0x8F8A/ 0x8F89) Implement GBCS Use Case CS08 Read PPMID / HCALCS Firmware Version Business Rules in Comms Hub to prioritise GSME over PPMID, HCALCS firmware OTA New alerts relating to error cases relating to Firmware storage prioritisation issues.
Modified	Firmware download status alerts to include HAN device type; GBCS Use Case CS05b Distribute Firmware to include HCALCS in the ESME, GSME device list.

3.4.2 Impact to the Smart m2m Solution Components

The CSP South and Central Smart m2m solution is the core solution component responsible for the scheduling, prioritisation and distribution of the firmware update to the target end HAN devices. The changes proposed in Smart m2m & Networks as part of this Modification include:

SD4.4.2 FirmwareUpgrade API	This is the firmware distribution API is used for all HAN devices not just ESME/GSME. The API specification will be modified to identify the HAN device type in the API request so that CSP South and Central can distinguish between ESME/GSME firmware and PPMID/HCALCs requests to distribute the images and permit the Comms Hub to differentiate and prioritise the images. This interface will also be modified to notify the DSP if Smart m2m is unable to process the firmware upgrade request at the time when the request was received. It is expected that this will be via a HTTP 503 status code however this will be agreed during design.
Modification of existing OTA firmware download alerts	This change requires that Smart m2m process any alerts generated by the Communication Hub with the HAN device “type” corresponding to the firmware image downloaded to the Communication Hub. This change allows CSP South and Central systems & administrators to identify the type of HAN device that a firmware upgrade request was intended for and for use in downstream reporting processes.
Notification of Firmware Download Status to DSP	This new function requires that Smart m2m notifies the DSP of the status of the firmware download to target Communications Hub(s) with a status: • Download Successful • Download Failed • Other • Reason Code (root cause of a failure, for example) Smart m2m will send the notification directly to the DSP using the new notification API hosted by the DSP, via the Access Gateway. This interface will be agreed with the DSP during the design phase.
HAN Device Firmware Upgrade	A new function which, upon receiving an SD4.4.2 firmware update request, will assess service load on Smart m2m. Currently, CSP South and Central has no means by which to protect the CSP South and Central Firmware delivery service. This is covered in section 3.2.5, Control 4 following.

Admission Control	When CSP receives an SD4.4.2 firmware update request, if the Smart m2m cannot accept the DSP request, then Smart m2m will send a synchronous response to the DSP notifying the DSP to defer the firmware upgrade service request until the CSP platform is able to service at a later point in time.
Billing Report	All HAN device firmware upgrades including those to the new HAN devices be represented as separate transactions on the Smart m2m DMM Billing Report i.e. requests to upgrade the Meter and a PPMID device connected to the same CH be represented as separate transactions on the current interface. Additionally, to manage scenarios which could result in such requests showing up as duplicates on a file i.e. same Job Id, same date time etc., add an additional synthetic key (representing a sequence id) to the interface. This is to ensure Netcracker doesn't reject requests against the same Comms Hub under the same Job and the same date-time as duplicates. Additional Billing Report content will include, for each operation: • HAN Device Type • DSP Job ID • Firmware ID
CHF <-> HAN Device Firmware Upgrade Status	This new function provides CSP South and Central Service Management with some visibility of the transfer of HAN device firmware image transfers between the CHF and HAN devices. Also it will provide an indication of the success or failure of the activation of the image on the target HAN device. The Communications Hub will send an alert containing the following HAN device firmware upgrade status to Smart m2m:which will map the alerts received from the Communication Hubs to a corresponding Simple Network Management Protocol (SNMP) trap.
Smart m2m Day 0 & Day 4 Reports	These reports are used by CSP South and Central IT systems to calculate the PM2 performance measures for each HAN Device firmware upgrade request. The reports will identify the device type that the report relates to. This information is required so that the IT systems can identify which target device data needs to be used in the PM2 calculations. Smart m2m will include all Firmware requests which have passed the validation report stage in a SLA Day 0 & Day 4 Report

3.5 CSP North Solution Overview

The Modification will impact the components shaded in the following diagram.

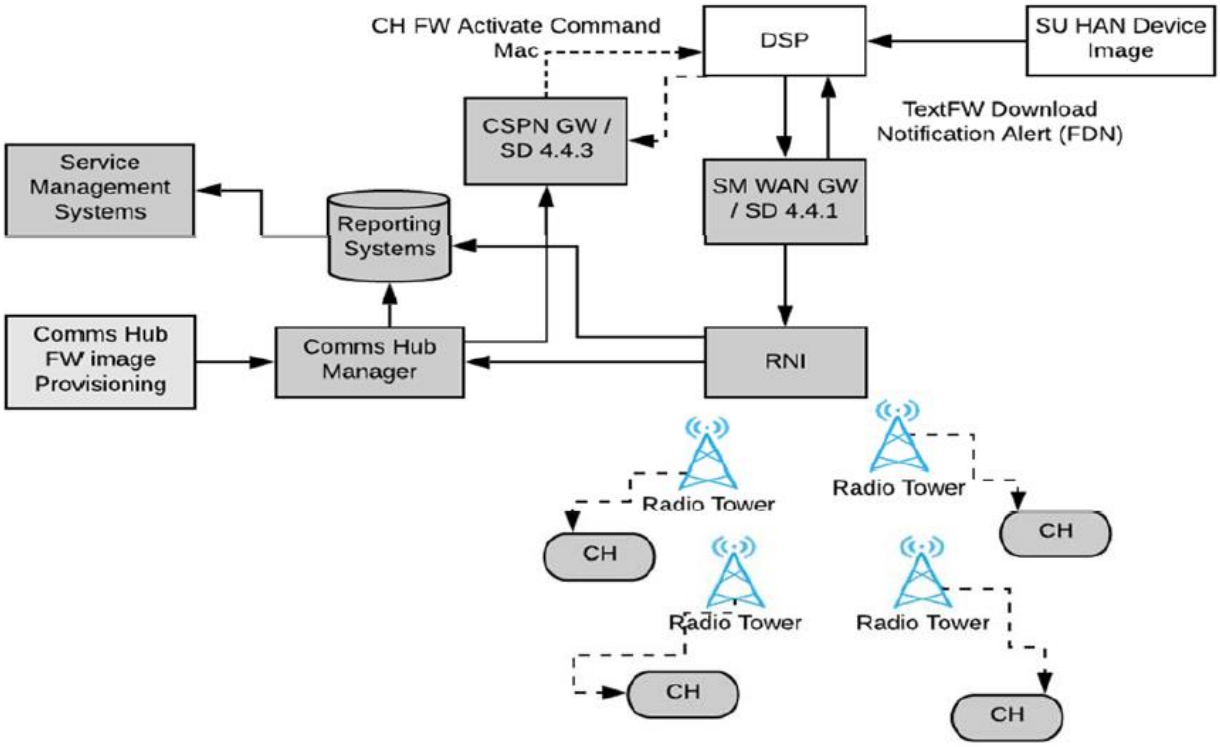


Figure 5: Impacted CSP North Components

Changes specific to the CSP North solution are described following.

3.5.1 Communications Hub Development

Changes to the Communications Hub will be required to:

- support the download of the FW upgrade image to the HCALCS and PPMID and offer it over the HAN
- support the Alerts generated
- update the WAN SDK (Sensus development) with a new API, which will need to be integrated into the Communications Hub
- support the handling of the new API to transfer the new alerts.
- store the update images in the GSME block using the image storage and replacement rules in GBCS. The image will be stored in the GSME memory block for a minimum of 2 (two) weeks before deletion

Alerts

The CHF shall support the generation of new GBCS 8F8A and 8F89 alerts with the option of enhancing the 'Transfer Response Code' or adding 'additional bytes' to the payload defined in GBCS. The exact detail to be agreed during the detailed solution design.

New CHF alerts shall also be generated for the ESME / GSME but not the CHF. The table below provides a breakdown of the image removal triggers and the corresponding GBCS alert code.

Trigger	Action	Alert Code	Transfer Response Code
End device sends an Upgrade End Request with Status of Success	Discard image	8F8A	0 – Success
End device sends a Query Next Image request with a hardware version out of range of the image's min and max hardware versions	Discard image	8F89	2 - hardwareVersionMismatch
Higher priority GSME image received	Discard image	8F89	1 - imageDiscarded
New PPMID/HCALCS image received for the same device model	Abort active download Discard image	8F89	1 - imageDiscarded
End device sends an Upgrade End Request with Status other than Success	Discard image	8F89	3 - fileTransferFailure
End device stopped downloading for 24hrs	Discard image	8F89	3 - fileTransferFailure
End device does not initiate download for 14 days	Discard image	8F89	1 - imageDiscarded

Table 4: Image Removal Triggers and Alerts

3.5.2 SMWAN to SMWAN Gateway Interface

The RNI (Regional Network Interface) is the core server stack that routes traffic from the DSP to the (CSP North) CH. It presents a web services layer to the DSP, to which Service Requests are posted via the relevant API. It also provides the head end control of FWDL jobs and manages routing information for contacting CHs.

There are 4 main impacts to the FlexNet service in the RNI as part of this Modification:

1. FlexNet protocol change to move CHs independently off the FWDL channel when complete.[2]

2. Update to the Distribute Firmware API to handle an additional end point type parameter.

3. New Firmware Delivery Notification in SD4.4.1 to be created and sent to DSP.

[2] While not part of this Modification's objectives, the FlexNet Protocol change has potential future applications for recovery of diagnostic data relating to the HAN, without increasing network bandwidth requirements. This provides potential for much greater insight into the 'last mile' at scale, should it be decided to develop this capability further. This would enable the Service Desk and other support functions to not only provide granular details of the status of the HAN FWDL to their devices but also add such functionality for any other critical services.

4. SDK, FlexNet protocol and RNI changes for logging triage (Service Management) metadata

The CSP North SM WAN Gateway Interface, SD4.4.1, will be impacted by changes required by the DSP.

3.5.3 Access Network – TK Basestation & Network Management System

As a result of increased demand on the network capacity, there will be a requirement to increase the radio channels within the overall CSP North solution from 16 channels to 32 channels. **Note** updated volumetrics information has been provided to all Service Providers to review all infrastructure-based statements.

The Network Management System (NMS) will also change to support the auto tuning of the Communications Hub, which will indicate the conclusion of the FWDL job, instigating a switch to the Communications Hub's normal channel. The Basestations will have to be updated to support the additional radio channels.

3.5.4 Communications Hub Manager

Comms Hub Manager (CHM) is the Device Manager which provides key functions such as providing default credentials to the CH manufacturer by interfacing with BT SMKI, sending CH Install Alerts to DSP, managing CH Firmware download and activation, refreshing credentials following the Install & Commission process, managing credentials during expiry and compromise and getting Unlock command from DSP for returned CH's, including supporting remote CH Diagnostic by Service Users.

This Modification impacts the CHM Console, Middleware and Reporting functions to support the following changes:

- The updated Distribute Firmware API requires an additional end point type mandatory parameter to specify the device type to which FWDL is initiated to, and thus requires changes to CH FWDL capability

- The CHM will provide functionality for Comms Hub Image Provisioning and Activation, support any Comms Hub alerts, and will also provide provisioning of HAN FWDL in test systems.

The CHM – CHF interface will be updated to define the following new messages:

- Alert 1: 0x8F89 - OTA Firmware Image Delivery to HAN Device – Failure (Generic Alert applicable for all HAN Devices)

- Alert 2: 0x8F8A - OTA Firmware Image Delivery to HAN Device – Success (Generic Alert applicable for all HAN Devices)

- Alert 3: 0x8F8B - Firmware Activation PPMID (Applicable for PPMID only)

The Firmware Distribution CH/CHM process flow is as follows.

Step	Event	Process
1	Reception of the Upgrade End Request Command	Communications Hub shall: set transferResponseCode to fileTransferSuccess if the transfer of the Manufacturer Image has completed successfully and process from step 2; and set transferResponseCode to fileTransferFailure if

		the transfer of the Manufacturer Image has failed and process from step 3;
2	[Success] Communications Hub shall create an Alert	Alert with the Alert Code field set to 0x8F8A Set firmwareVersion to the OTA Upgrade Image File version, Include the transferResponseCode from the previous step and process from step 4;
3	[Fail] Communications Hub shall create an Alert	Alert with the Alert Code field set to 0x8F89 Set firmwareVersion to the OTA Upgrade Image File version, Include the transferResponseCode from the previous step and process from step 4;
4	Communications Hub shall send the Alert created in the previous step	CHM to ingest alert 0x8F8A or 0x8F89

Table 5: CHF behaviour and process steps

In the case of the PPMID Firmware Image update, the final step in the process flow includes the PPMID activating the firmware and sending an Alert message with Alert Code 0x8F8B.

3.5.5 Business Support System

The Business Support System (BSS) provides the key functions such as Comms Hub Lifecycle Management that includes Forecast & Ordering, Delivery, Acceptance, Rejection, Installation, Return, Refurbishment and Disposal, maintains Comms Hub Logistical and Operational status, provides Postcode Coverage, supports Performance Measurement & Reporting, and Comms Hub Billing.

This Modification impacts the BSS Integration and Reporting functions to support the following changes and functionalities:

- Updated FW Download and SMWAN Gateway logs to support reporting, analysis and triage activities
- New log for newly supported Alerts to support reporting, analysis and triage activities
- Impact on infrastructure (compute, storage and licensing) due to increased volumes of firmware downloads and Alerts.

4 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0007 on DCC's Services and Interfaces that impact Users and/or Parties. These impact both solution options.

4.1 Technical Specifications

The legal text for all technical specification has been developed as part of the Working Group and SECAS-related activities for this Modification. The intention is that they will be baselined as part of the Modification Refinement process, and released to all parties when this Modification is approved for implementation to commence.

Notes on the applicability of the Zigbee OTA specifications and Smart Metering Technical Specifications are covered in Appendix C: Technical Specifications Changes.

4.1.1 SMETS and CHTS

SMETS and CHTS will be updated as part of this Modification.

Support for the Modifications changes would be mandated through the SMETS for all newly installed PPMIDs, and through the CHTS for installed Communications Hubs. The changes would result in new obligations on the DCC, and Suppliers would be required to demonstrate that they are able to support the sending of the new Service Request and receiving the Service Response and DCC Alerts by way of testing obligations. However, Suppliers would not be required to upgrade Firmware on PPMIDs, unless there were changes to the SEC or a SEC governance mandated upgrade.

4.1.2 DUIS, DUGIDS, MMC, GBCS, CHDS

There will be a new Service Request 11.4 Update PPMID Firmware for the purpose of distributing and activating the firmware image to the PPMIDs.

The existing SRV 11.2 Read Firmware Version will be extended to support PPMID device type.

Unlike the firmware upgrade mechanism for the other device types, there will not be a separate activation SRV for PPMID.

The proposed GBCS changes for this Modification introduces the following GBCS Use Cases:

- CS08 Read PPMID/HCALCS Firmware Version
- CS05c Distribute Firmware to PPMID
- CCS08 Firmware Transfer Alert

The Comms Hubs and PPMIDs will use the following Device Alert Codes to report the firmware distribution statuses.

- Alert 1: 0x8F89 - OTA Firmware Image Delivery to PPMID - Failure
- Alert 2: 0x8F8A - OTA Firmware Image Delivery to PPMID - Success
- Alert 3: 0x8F8B - Firmware Activation PPMID

DUGIDS will need to explain the behaviour of a new DCC Alerts introduced as part of this change. DUGIDS will also need to explain the changes to the behaviour of existing DCC Alerts due to the introduction of PPMID.

The DUIS and MMC schemas will need updates to support the new Service Request.

For the HCALCS solution, DUGIDS documentation will be updated to describe that SRV 11.1, SRV11.2 and SRV 11.3 will be used for HCALCS firmware update. Since this does not involve any changes to the input Service Request format or new GBCS Use Cases, the DUIS and MMC schemas do not require any changes.

The CH2 Communications Hub Detailed Specification (CHDS) will be updated as part of this Modification.

4.1.3 Transform

DSP Transform will need to implement the libraries for the GBCS Use Case CS08 (Read PPMID/HCALCS Firmware Version) and to parse the new Device Alerts.

Configuration updates will be applied to the Transform component to support the GBCS Use Cases for Read Firmware Version and Activate Firmware on HCALCS.

4.1.4 CPL

Implementation of this change will commence with the recording of a firmware hash against a PPMID device.

No change is expected to the structure of the CPL due to this Modification, but the permitted data types and validations may require updates.

4.2 Security

In terms of the DSP, there are no perceived security impacts, and there is no need for additional Penetration Testing or Protective Monitoring specific to this Modification. A penetration test might be required based on any other Modifications or Change Requests that make up a release.

The HCALCS update method would include security related effort for the CSP security certification bodies, to review the design and for full CPA certification.

4.3 Implementation Approach

Within the Smart Meter Implementation Programme (SMIP), the Implementation Approach is referred to as Transition to Operations (TTO).

This change will be implemented as part of a larger release. It is assumed that the activities required for TTO will be minimal following completion of contractual test phases. Some updated service procedures have been implemented and take part in some form of service role playing in advance of go live.

Any required environment uplifts will take place outside of business hours.

4.4 Application Support

The DSP Application Management Support team are responsible for the provision of application level support for the DSP. This Modification provides additional functionality that will be subject to support following its deployment to the Production environment, and it is expected that the added functionality and processing logic to existing SRVs will lead to the raising of additional incidents to cover for OTA firmware upgrades to include PPMIDs and HCALCS. As a result, DSP has made a conservative estimate that the change will result in five medium complexity calls that need to be assimilated, investigated, resolved and monitored per month over the support term.

The DSP team will need to be prepared to support the change from the day it goes into live operation. As such, the team must review the functional solution and its technical implementation. The team must understand any configurable options and develop procedures to support the implantation.

For the CSPs:

- The CSP Service Desks will require coordination for CH Specialists and will need to understand timings and frequency of downloads

- There is a requirement to plan and schedule such that the system can avoid Network conflicts and saturation when trying to push out CH firmware downloads at the same time

Specific **CSP South and Central** Service Management impacts from this Modification include the introduction of:

- New Service User facing functionality that is expected to result in modifications to incident scripts and introduce new incident scenarios that require triage

- New firmware image types whilst retaining the current Communication Hub firmware storage capacity, driving additional new edge cases related to delivering firmware images to HAN devices

Specific **CSP North** Service Management impacts include:

- Updated FW Download and SMWAN Gateway logs from RNI to CSP North support relating to reporting, analysis and triage activities.

- New log for newly supported Alerts from RNI

- Impact on infrastructure (compute, storage and licensing) due to increased volumes of FW downloads and Alerts.

- Modifications to the Incident Management process, Service Desk resourcing and related systems to support additional incidents relating to firmware update failures for PPMID and HCALCS devices. An Additional FTE allowance will be used only in relation to the triage of non-contractor related incidents which occurred as a result of firmware download attempts to PPMID or HCALCS.

- Implementation of monitoring for the new network Service Requests and device alerts.

- Development, integration and assurance activities to include firmware updates to PPMIDs and HCALCSs in monthly Performance Measure reporting. Includes set up and reporting of new exclusions.

4.5 Infrastructure Impact

This Modification does not materially increase processing, data storage or data exchange within the DSP solution. No specific infrastructure requirements or changes have been identified, but there will be an increase in Service Request volumes as a result of this Modification.

The Modification will lead to additional data processing at the DSP. One instance of the new firmware upgrade SR message will trigger a lot more processing effort than typical SRs, since one containing 50,000 device IDs would trigger validation of all of them, the need to generate files, interact with both CSPs and the sending of approximately 100,000 alerts. Assuming the messages are billed appropriately, any additional hardware required would be handled through normal capacity planning processes.

Note that the aggregated impact of many such changes to the DSP solution will ultimately result in a reduction of the available headroom assumed as part of the original DSP agreement. There may be a need to raise a Change Request against the DCC to cover additional compute and storage capabilities to cover this aggregated impact in the future.

For both CSPs, there is a quoted need to increase the capacity, rather the capability of their networks. In both cases, the activity to execute the Production Environment capacity expansion requirement shall be conducted under the business-as usual operational change process, but not before the date that CSP completes the migration of the Production Environment to the technically refreshed platform.

CSP South and Central will provide a quote to provision additional hardware required uplift for the Production Infrastructure in order to meet the firmware upgrade demand once the Modification is Live.

CSP North note the Smart Metering Wide Area radio Access Network (SMWAN) uses dedicated multicast/broadcast radio channels and is technically the same as the mechanism to provide firmware updates to Communications Hubs and ESME/GSME. The use of this mechanism, whilst being efficient, will result in additional traffic to be carried by SMWAN radio channels. This impact assessment includes estimates on the price related to this additional traffic, the additional channels required and the functionality to support these new channels.

Initially, the FWDL system was designed to support small numbers of large multi-cast FWDL Jobs containing upwards of tens of thousands of devices in each Job. Currently, the FWDL system has been expanded from one to three FWDL channels, at ASML cost, to support the usage of Service Users, i.e. a very large numbers of FWDL Jobs containing small numbers of devices, often a single device. *With no change* to Service User behaviour, it is anticipated that further FWDL channels will be required in the system as the numbers of Communication Hubs increase and to support FWDL Jobs introduced by new types of devices.

Note DCC have reviewed this assumption, and will prepare DUIS Guidance notes for changes to procedures for handling all HAN device firmware updates as described in section 4.13 following.

Further information regarding the CSP North infrastructure augmentation is given in Appendix E.

4.6 Non Functional Impacts

DSP does not expect that there will be a material impact on system performance as a result of this change. DSP will validate this with some specific regression tests during the implementation phase.

There will be no change to the system resilience solution as a result of this change.

There will be no change to the Disaster Recovery solution or BCDR procedures as a result of this change.

4.7 Safety Impact

There are indirect but foreseeable systems safety risks associated with the management of device firmware updates. Functional failures could adversely impact communications with a device or render the device inoperable and impact the supply of energy to consumers. Such failures might include:

- device not added to the Central Products List
- device's firmware version not maintained in the Smart Meter Inventory
- failure to validate firmware update request
- firmware is not activated when scheduled
- failure to alert Supplier on failure
- failure of Supplier to re-request update following a delivery failure
- Supplier attempts to update firmware on incompatible device

These types of risk are subject to software Failure Modes, Effects and Criticality Assessment (FMECA) as part of the DSP System Hazard Analysis Report, based on the DSP Use Case level functional design, with any risks to data confidentiality, integrity and availability also addressed by the DSP information security programme.

No new types of hardware infrastructure are required to be procured or installed as a result of this change and, therefore, there is no foreseeable health and safety impact.

4.8 Request Management

The DSP Request Management will implement a mechanism to track the progress of the firmware update process at a Device Level. The DSP will block a firmware update request for a device if there is already one in progress and will return the list of such devices as part of the synchronous response. If the firmware update request for a Device stays in the ‘In Progress’ status longer than a defined duration the Device will be released from tracking so that new requests can be accepted.

The status records held by the firmware update tracking mechanism are expected to be available only for a short-term (up to a week). The housekeeping of these records will be managed by way of configurable parameters.

Request Management needs to amend the processing of all the affected Service Requests and implement the newly introduced Service Request. It also needs to implement the scenarios related to the new Alerts.

Request management needs to validate the firmware image as with existing firmware upgrades (e.g. active according to the CPL and the supplied hash matches the CPL entry) and the list of device IDs (e.g. the sending Service User is the responsible supplier for the device).

Request management will need to look up the appropriate CHF in order to indicate to the CSP to which CHF the request will be directed. For devices which pass validation, Request Management will form a request to send over the new CSP SMWAN Gateway interfaces for the purpose (similar to existing ones), segregated by CSP.

When DSP receives a Device Alert from a PPMID indicating a successful activation of firmware, DSP will update the SMI and notify all the Responsible Suppliers using the DCC Alert N39.

An Electricity Import Supplier (EIS) or Gas Import Supplier (GIS) responsible for the PPMID will be allowed to send a firmware update using the SRV 11.4.

The processing of SRV11.1, SRV11.2 and SRV11.3 will be updated to support HCALCS. The existing validations for the ESME will be applicable for the HCALCS as well. CSP SMWAN Interface documentation will be updated to describe the use of existing ESME/GSME Firmware Update interface for HCALCS.

4.9 Data Management and Data Model

This change does not materially increase processing, data storage or data exchange within the DSP solution, as such, this change on its own does not warrant the procurement of additional infrastructure.

The Data Model will need changes to support the firmware update tracking.

In addition, there is a need to add mappings for the new GBCS Use Cases, for the alerts between the DUIS version and the SRV, and to the GBCS version against the Use Case where applicable.

There will be a new web service interface for SSMI to reset the firmware delivery status of a Device.

Reference data updates will be applied to Data Management related to SRV11.1, SRV11.2, SRV11.3 and SRV11.4.

4.10 Anomaly Detection

No changes are required within the Anomaly Detection component.

Anomaly Detection volume thresholds will need to be applied for SR11.4.

4.11 SSI

SSI will feature a ‘Firmware Update Status’ screen to allow the Service Users to view the last recorded status of a firmware update request against a single device.

SSMI will also feature the ‘Firmware Update Status’ screen, with an additional functionality to reset the status of a device. The data presented in the new SSI/SSMI screens will be applicable to all device types and will be served by the Reporting Database instance and the data synchronisation would take place at an interval of about 15 minutes.

The SSI report RSAT_004 Firmware Activations Service Request Report will be updated to include HCALCS.

4.12 ESI Inventory Extract

No changes are required to Enterprise Systems Interface (ESI).

4.13 SEC Changes and Usage Limitation

Although not directly impacting the Service Providers, DCC have requested that some form of obligation be added to the SEC or in guidance to users to limit the initial take up and general usage of the firmware download channels to "reasonable". While this is not something that has been in place before, it is something that will have a significant impact on additional infrastructure and resources allocated by the Service Providers to firmware downloads. The changes should include:

- DUIS Guidance to Service Users for all firmware downloads that after an initial Service Request that they should wait until they get an alert for a successful or discarded transfer before they resend or send a subsequent SR.

- The Guidance will show that after sending a firmware image, the supplier should wait for an activation alert or failure message from the PPMID before re-sending the image update.

- A managed schedule should be agreed between the DCC and the appropriate parties.

- The guidance should include a statement that firmware updates must be limited to a gap of at least 5 days between attempts.

DCC does not believe Anomaly Detection Thresholds (ADTs) would be an appropriate or valid method of limiting the usage**.**

5 Implementation Timescales

Implementation of this change is assumed to follow a waterfall methodology. For the purposes of this FIA, it is assumed that this change will be implemented alongside other Modifications and change requests.

5.1 Approach

Details of a release plan including all the Service Providers with potentially different release dates and content will be negotiated and evaluated separately, led by DCC. The timelines in the rest of this section are indicative only for each Service Provider, and are based on a standalone Modification release for comparison only.

The **DSP** timeline reflects a start around December 2020 and a subsequent completion in November 2021.

Generic November 2021 Release Phases	**Start**	**End**
DCC confirmation of required November 2021 scope in agreement with SECAS	December 2020	
PIT Phase	January 2021	May 2021
SIT Phase (limited to functional changes only)	June 2021	August 2021
UIT Phase (limited to functional changes only)	September 2021	October 2021
Transition to Operations and Go Live	October 2021	November 2021

Table 6: Potential DSP Release Phases and Dates

Note that the implementation lifecycle is expected to fit into this schedule, but the timescales shown as part of the Price Breakdown run over a shorter elapsed period for the purposes of costing. As additional CRs are applied to the release, timescales are expected to expand to fill the schedule set out above.

In order to achieve this timescale and implement changes alongside other releases such as SMETS1 and the DSP aspect of the Central Switching Programme it may be necessary to align some activities with those programmes of work. Where required, changes will be implemented using feature switches to enable functionality to be only switched on for testing when it is required.

The **CSP South and Central** proposed delivery timeline indicates that after the DCC approval to start project mobilisation, it would take approximately 14 months to exit the PIT phase for this CR, with SIT planned for a duration of 3 months and UIT planned for 2 months. As part of the proposed delivery plan supporting the IA, CSP South and Central anticipates that it would take in total 20 months (approx.) prior to UIT exit as shown in the following plan on a page.

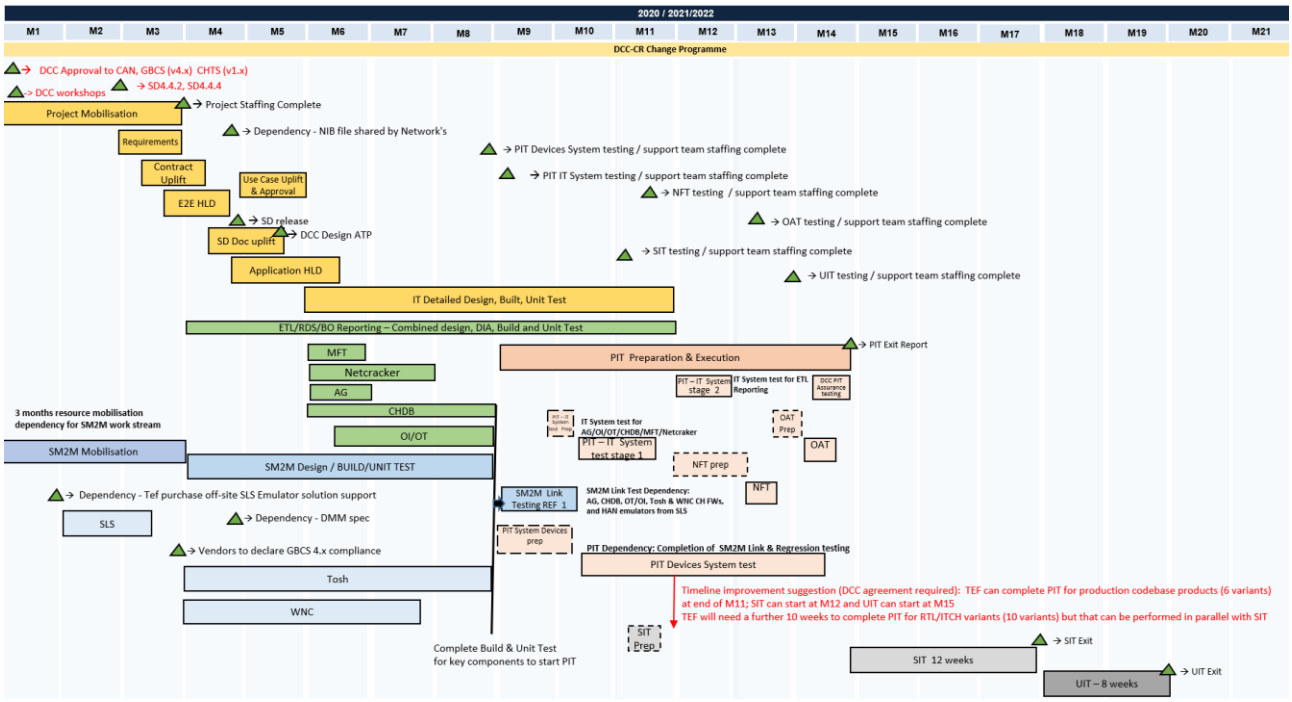


Figure 6: CSP South and Central Indicative Plan

This plan includes the following stages:

- A period of two (2) months to undertake in-depth analysis work to construct technical requirements and high-level design
- A period of three (3) to five (5) months of detailed design across different work streams.
- A period of 5 months to build and unit test Smart m2m changes
- A period of 8-9 months to build & unit test all IT (back office) components
- A period of 1 month required to uplift and link test the PIT B environment for PIT system testing
- A period of 5 month required to deliver the Communications Hub firmware before being made available for PIT testing.
- CSP South and Central PIT testing with the Production codebase Communication Hub variants will take approx.7 weeks while testing with non-Production codebase variants will take approx. 10 weeks to complete. All other phases of PIT i.e. PIT IT System testing and NFT can be executed in parallel and all major defects uncovered during PIT testing can be fixed within the PIT window.
- Around 2 months of Non-Functional Testing which includes performance testing of the new functionality on existing service demand.

Indicative PIT entry and PIT exit, SIT entry and SIT exit dates as shown in the indicative delivery plan.

The **CSP North** proposed delivery timeline indicates that after the DCC approval to start project mobilisation, it would take approximately 14 months to exit the PIT phase for this CR, with SIT planned for a duration of 3 months and UIT planned for 2 months. As part of the proposed delivery plan supporting the IA, CSP South and Central anticipates that it would take in total 20 months (approx.) prior to UIT exit as shown in the following plan on a page.

- A period of two (2) months to undertake in-depth analysis work to construct technical requirements and high-level design

- A period of three (3) to five (5) months of mobilisation, requirement analysis and detailed design across different work streams.
- A period of 3 months to build and unit test the application and consequential Comms Hub firmware changes
- A separate workstream to build and unit test all back office components
- CSP North PIT and SIT will requires two cycles of PIT and two cycles of SIT testing. The combined PIT testing would take approximately 18 weeks to complete, with SIT taking approximately 20 weeks.
- These timelines do not include environment uplift and preparation.

The WAN and Production environment expansion are two separate programmes of work as follows:

- WAN Capacity Expansion Development and Coding, 12.5 months
- WAN Capacity Expansion Deploy, test and go Live, 10 weeks
- Production Environment infrastructure Expansion, 6 months

The **System Integrator** will be responsible for managing and leading the SIT and UIT phases of testing.

6 Testing Considerations

This Full Impact Assessment includes the cost to develop, fully test and deliver this SEC Modification as a standalone change. Costs were submitted by the Service Providers on a per-Application Phase basis, including Development and Build, PIT, SIT, UIT, Implementation (sometimes referred to as TTO), and Application Support.

PIT System testing may, at the discretion of the SP, consist of two cycles of testing of the new functionality delivered by this Modification, plus two cycles of regression testing. A repeat of a subset of PIT System test cases will be conducted for DCC Test Assurance witnessing.

Testing costs for SIT and UIT have been built on the following assumptions:

- Go live in November 2021 (although this will have no impact on costs)
- SIT testing 12 weeks
- UIT testing 8 weeks
- 10 test sets per Comms Hub type. This means 10 for CSP North (5 Single Band CH, 5 Dual Band CH), 20 for CSP South and Central (same split per band, but two meter manufacturers).
- Risk-based regression testing

Note that CSP activities include “Production Uplift” or “environment uplift” which covers the CSPs getting their backend systems up to scratch so that they support the new way of working for SEC MOD 7. As you say the new versions of firmware would be developed but based on experience would be initial cuts and would take a number of iterations before genuine production ready versions can be accepted.

6.1 Pre-Integration Testing (PIT)

For the DSP, System Testing, Performance Testing and the Factory Acceptance Testing (FAT) phase will operate as a single phase of PIT activity with a single drop.

For the CSPs, the Communications Hub change testing will be limited to PIT testing of the new functionality outlined in this Modification as well as PIT regression testing.

Note that DCC are currently leading an initiative to introduce "real" devices in the testing regime, and this is expected to have a positive impact on testing durations and cost.

6.1.1 The CSP South and Central PIT Approach

The CSP South and Central PIT Approach will include:

- Design, build and system test modifications to the CSP South and Central solution to support the delivery of the functionality for the PPMID and HCALCS firmware service within the PIT environment
- Execution of NFT of the uplifted solution in accordance with a defined non-functional test approach. Note this has not been included in the CSP South and Central plan at this stage.
- Provision of a fixed number of ITCH variant Communication Hubs to the meter Test Stub provider to support the meter Test Stub provider develop any meter emulator updates to support PIT testing

Note CSP South and Central indicated that testing with real devices in PIT is currently out of scope, as well as any uplift or use of NXP based emulator in PIT.

Due to the DUIS changes as part of this Modification, existing Test Stubs would be uplifted for to be able to PIT test the firmware upgrade to PPMIDS and HCALCS. PIT device testing will validate using the Test Stubs with added capability to test firmware OTA over the HAN to PPMIDS and HCALCS.

Updated versions of the wired ITCH variant Communication Hubs will be provided to the Test Stub provider for use in developing and testing the uplifted Test Stub as follows.

	Changes
Modified	Modification to test stubs to support new GBCS alert definition; Modification to the test stubs to include the additional attributes including additional value in the enumeration for error code; Modification to the PIT test stubs required to validate the new API developed regarding the status of the firmware download status notifications over SMWAN to the DSP.

The following System Test activities are required for PIT:

- Modification to existing test scripts to support updates to functionality within the CSP solution
- To support assurance of the new functionality within the PIT environment
- Regression testing of existing System Test scripts
- Documentation of the testing artefacts as per the existing PIT approach

The system test activities described in the following table:

Use Case	Title	Activity	Description
UC4.01	Meter firmware distribution.	Test Script Uplift & Regression	Updated functionality test case to include the new functionality being introduced as part of this CR and also confirm that meter firmware operation has not been impacted by software changes to the Communications Hub
UC4.02	Communications Hub firmware distribution and activation.	Test Script Regression	Test case to confirm that CH firmware operation has not been impacted by software changes to the Communications Hub
UC8.01	Input Billing Data (Auto)	Test script regression	Test to prove the Netcracker Billing interface for firmware downloads being extended to additional HAN devices.
UC8.0	Create DCC Bills and Invoices	Test script regression	Test to validate the Netcracker Billing process and validation of invoices generated as part of tests.

UC12.08	Test Messages	Test script regression	Regression of the test case to confirm that the test message processing has not been impacted by software changes to the Communications Hub
UC13.01	GBCS commands, responses and alerts	Test script uplift and regression	Regression of the test case to confirm that the test message processing has not been impacted by software changes to the Communications Hub
UC13.05	Power Alerts	Test script regression	Regression of test case to confirm that power outage alert transmission and processing has not been impacted by software changes to the Communications Hub.
UC14.01	Smart m2m DMM management	Test script regression	Regression of test case to confirm that device management and monitoring firmware operation has not been impacted by software changes to the Communications Hub.
UC14.02	DSP Diagnostics.	Test script regression	Regression of test case to confirm that device management and monitoring firmware operation has not been impacted by software changes to the Communications Hub.
UC23.01	Communications Hub Installation	Test script regression	Regression of test case to confirm that installation and CSP commissioning and processing has not been impacted by software changes to the Communications Hub.

Table 7: CSP South and Central System Test Activities

A defined non-functional test cycle on the functionality in this Modification will include:

- Testing approach and scope
- testing may occur during the Release PIT timeframe however this is not on the critical path for exit from PIT;
- Test volumes will reflect a scaled view of service demand with some consideration for new functionality within this demand

6.1.2 CSP North PIT Approach

It is assumed that all testing in PIT will be performed with meter emulators and real PPMIDs and HCALCS and that both CH variants (SBCH and DBCH) will be tested in a near parallel approach.

The upgraded applications RNI, CHM and BSS will be regression tested prior to commencing CH testing. NMS and TK testing will be performed separately, treated as a maintenance release (environment A path first).

CH firmware changes will be verified primarily in two variants, SBCH and DBCH, and the full regression test suite will be shared between both CH firmware variants, with regression targeted on modified firmware sections.

The PIT Test Approach will be to test DBCH and SBCH in near parallel when execution commences and DBCH –F will be verified following DBCH completion, as per the Plan on a Page above.

The PIT Test Team will perform Targeted regression in DBCH – F, SBCH ITCH, DBCH ITCH, W-ITCH firmware and in the CHM application, and the Test Team will verify all changes for the Modification in the CH FW, RNI, BSS and CHM firmware in parallel.

Note that CSP North will implement a multi-phase PIT testing approach, essentially with a cycle sequence of PIT -> SIT -> PIT > SIT, because of the large number of defects that are not detected in PIT that only become apparent in SIT. This clearly has a significant impact on testing costs and durations.

Also it should be noted that CSP North currently only has the capability to execute two sets of Comms Hub firmware PIT testing in parallel. If PIT testing of other changes are not complete, and this capability is not increased, before the Modification release is received from their supplier, this Modification's SBCH PIT testing may have to be prioritised over DBCH PIT testing.

6.2 System Integration Testing (SIT)

CSP test lab support will be required to permit the System Integrator (SI) to execute the SI regression test pack for System Integration Testing. The same support will provide triage and defect resolution activities during any SI managed integrated testing.

6.2.1 DSP System Integration Testing

Tests described in this section are specific to this change and independent of any release-based testing.

New scenarios and scripts will be created as follows:

Firmware update for PPMID	Create new scenario and script for new SRV11.4 – Update PPMID Firmware (which should be very similar to the existing SRV 11.1 scenarios and scripts). The scenario and script will include the relevant DCC Alerts indicating the progress of the firmware through the different stages of distribution, update and activation processing, including N59, N61, N62 and N39. This SRV will share its general attributes and validation checks with SRV11.1. The firmware will be distributed OTA and the PPMID will activate the firmware update. Update the SRV11.2 existing scenario and scripts to include support for Firmware Reads and Updates for PPMID.
Firmware update for HCALCS	Will follow the existing procedure currently used for ESME and GSME: • Update existing SRV11.1 scenario and script to include the relevant DCC Alerts indicating the progress of the firmware through the different

	stages of distribution and update processing. DCC Alerts include N59, N61 and N62. • Update existing scenarios and scripts for the following SRVs to include support for Firmware Updates for HCALCS: o SRV 11.1 Update Firmware; o SRV 11.2 Read Firmware Version; o SRV 11.3 Activate Firmware. • Update scenario and script for SSI Report RSAT 004 Firmware Activation Report to include HCALCS.
Negative Scenarios of SRV11.1 for HCALCS and for SRV11.4 for PPMID Firmware	Four existing negative DCC Alert Test Scenarios and scripts to be updated to include PPMID and HCALCS devices for the following DCC Alerts: N18, N19, N20 and N22. SAT entry for N19 defines entry for each rejected device. • Three new negative DCC Alert scenarios and scripts to be created and executed for N49, N50 and N51 covering PPMIDs and HCALCS when executing SRV11.2. • New Negative scenario for Hash on CPL for PPMID and HCALCS to verify if Firmware Update can be applied or not.
Applicable to ESME, GSME, HCALCS and PPMID	Two new negative DCC Alert scenarios and scripts to be created for the following new DCC Alerts to be tested for ESME, GSME, HCALCS and PPMID: o N60: Delivery to Comms Hub failed o N62: Failed to deliver firmware image to device o N62: Firmware image rejected/overwritten at Comms Hub Creation of one new negative scenario and script for ESME, GSME, CHF, HCALCS and PPMID where another Firmware Update is in progress. New scenario and SSI script for users to access a 'Firmware Update Status' screen to allow the Service Users to view the last recorded status of a firmware update request against a single device. New scenario and SSMI script for users to access a 'Firmware Update Status' screen, to view the last recorded status of a firmware update with additional functionality to reset the firmware status of a device. An update to the Business Scenario for Change of Mode and Firmware: o Additional Alerts to be added o Additional scenario for PPMIDs o Update to Interaction diagram required

SIT Execution Approach	The SIT execution approach will be: 1. Validation performed by CSPs and within HAN with DCC Alert Codes generated will be tested against all three CHFs including SBCH and DBCH 2. The validation performed by DSP with DCC Alert Codes generated to be tested against a single CHF 3. The Firmware Update, Read and Activation of Firmware updates for PPMID will be tested against all three CHFs including SBCH and DBCH 4. The Firmware Update, Read and Activation for HCALCS will be performed against all three CHFs including SBCH and DBCH
SIT Execution	**Happy Path Test Execution** Execute SRV 11.4 and SRV11.2; Update and Read Firmware for PPMID, verifying DCC Alert Codes N59, N61, N62 and N39 through the three CHFs; Execute SRV11.1, SRV11.2 and SRV11.3 Update and Read Firmware for ESME, GSME and HCALCS through the three CHFs, verifying DCC Alerts N59, N61 and N62. Verify users can access new SSI and SSMI screens “Firmware Status Update” to query the status of firmware updates and reset firmware status. Generate SSI Report RSAT 004 Firmware Activation Report to verify HCALCS are included. **Negative Scenarios Test Execution** Negative DCC Alert Codes N49, N50 and N51 to be executed for PPMID and HCALCS are validated by DSP. Only to be executed against single CHF (SRV11.2). The three DCC Alert Codes will be spread across the three CHFs. Negative DCC Alert Codes N18, N19, N20 and N22 are validated by CSPs therefore, tested for PPMID and HCALCS against all three CHFs. Negative DCC Alert Codes N60 and N62 are validated by CSP/HAN area therefore, to be tested for ESME, GSME, HCALCS and PPMID against all three CHFs; Negative validation tests for ESME, GSME, CHF, HCALCS and PPMID where another Firmware Update is in progress (spread across the three CHFs) Negative test for hash on CPL. Verify the hash for PPMID and HCALCS to determine if firmware update can be applied

6.2.2 CSP South and Central SIT

There will be provision of an agreed amount of CSP test lab support including:

- Support the SI for the testing of scenarios within SIT

- Support the SI for the installation of the provided meter equipment within the CSP Test Lab to support the testing with physical devices.

- Provide 20 existing SIT Communication Hub sets (10 Toshiba, 10 WNC) during the SIT execution period for a period of 12 weeks; CSP South and Central will re-allocate its existing SIT Communication Hub (20) to support the SIT. Charges do include the required associated equipment (debug boards, ZigBee sniffers).

CSP South and Central assumes that the following devices will be made available by the DCC-L for testing in SIT:

- 2.4GHz and sub-GHz ESME and GSME compatible with a specified version of GBCS

- PPMID and HCALCS devices operating on 2.4GHz and sub-GHz from two separate manufacturers with firmware revisions comparable to those available in Production at the time of SIT entry

- PPMID and HCALCS devices operating on 2.4GHz and sub-GHz from two separate manufacturers with compliance to a specified version of GBCS

- DCC provided device emulators for that operate as a specified version of GBCS compliant PPMID and HCALCS devices on 2.4GHz and sub-GHz

  CSP South and Central will support the SI during System Integration Testing (SIT) including defect triage and resolution Including the following System Test activities:

  - Modification to the existing test scripts to support updates to the functionality within the CSP solution

  - Device set-up

  - Execution of the tests with support from the DSP

  - Test execution monitoring as required

  - Collection of logs

6.2.3 CSP North SIT

PIT and SIT will be performed using Debug and Non-debug CH variants.

Other activities are essentially the same as those for CSP South and Central.

6.2.4 User Integration Testing (UIT)

UIT will comprise the preparation and execution stages for the relevant UIT environment, and will take place following completion of PIT and SIT.

The overall UIT project window is scheduled to run for approximately eight calendar weeks and will cover three separate testing elements:

- Firmware Tracking (2 weeks)
- PPMID Firmware Updates using Zigbee OTA Delivery (3 weeks)
- HCALCS Firmware Updates using the GBCS Commands (3 weeks)

Real ESME, GSME, and PPMID devices will be used. HCALCS emulators will be used.

Specific UIT test activities will include the following:

- Planning and preparation of the tests
- Testing of the OTA process for ESME and GMSE devices on meter sets covering all three CHF manufacturers, both single and dual band, to ensure that tracking of the firmware process is working as expected in the UIT environment
- Testing of both the OTA process for PPMID and separately HCALCS devices on meter sets covering all three CHF manufacturers, both SBCH and DBCH, to ensure:
    - Tracking of the firmware process is working as expected in UIT
    - Firmware is updated on the devices and device alerts are received
    - DSP returns details of the firmware for the applicable device in response to SR8.2
    - (PPMID only) The CHF returns the current firmware version of the PPMID in response to SR11.2 when sent to the applicable device
- Preparing, presenting and agreeing a test completion report on the testing results
- Providing a summary of defects raised during testing

6.2.5 Support for Integration Testing

DSP Effort will be required from the Implementation and Triage teams to support the additional testing. This consists of issue investigation, resolution and deployments to the environments.

7 Service Operation and Transition

This section contains information about the transition to a live environment.

7.1 PPMID Numbers and Functionality at Go Live

Once implemented this Modification will ensure that a PPMID-related SR11.2 would send the firmware activation 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. However, no existing devices could support this functionality, namely the redirected firmware alert, until after a successful PPMID firmware update had been applied by this Modification, because until then, existing devices do not send any Firmware Activation Alerts today and they would need a SECMP0007 driven firmware update in order to do that.

If an existing, deployed PPMID supports the standard Zigbee OTA process today then there's no reason why the (new) Comms Hub can't use the Zigbee OTA process to get the new firmware onto the PPMID.

Note that SECAS have issued a Request for Information to get an idea of the number of Transition to Operations (TTO) Approach

CSP South and Central will provide costs and durations to deploy the CSP changes in Production.

CSP North costs have been provided. Note the switch of the Communication Hub manufacturing line to the new firmware version shall be decided under business-as-usual process.

8 Costs and Charges

8.1 Application Development and Support Costs

This section indicates the total quote for each application development stage for this modification. Note these costs assume a standalone release of just this SEC Modification without any other Modifications or Change Requests, which may not be truly reflective of what the test costs or programme duration might look like. A calculation of those costs will be carried out when the contents of the future Release is determined through a "Grouping CR" also referred to as a "Release CR".

£ (million)	Design and Build	PIT	SIT	UIT	TTO	App. Support	SP Total
Phase Total	9.4m	4.2m	3.8m	1.6m	0.7m	1.1m	20.8m

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC. This phase also includes regression testing across all Comms Hub products
Systems Integration Testing (SIT)	The PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution. The System Integrator is responsible for leading this phase with the SPs offering testing support services.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change. The DCC is responsible for leading this phase with the SPs offering testing support services.
Implementation to Live (TTO)	The solution is implemented into production environments and ready for use by Users as part of a live service.
Application Support	Any costs associated with supporting the new functionality.

8.2 Impact on Contracts and Schedules

Schedules will require modification for the Service Providees to reflect the changes under this Modification. The contract schedules will be updated as part of a CAN which combines schedules updates from other relevant Modifications

8.2.1 DSP

Expected contract schedules to be amended include:

- Schedule 2.1 – Review to determine whether updates are required as a result of the new functional requirements outlined within this Full Impact Assessment
- Schedule 6.1 - Inclusion of three new milestones referencing completion of PIT,SIT and go live for this change
- Schedule 7.1 – Update to include a payment against the Schedule 6.1 milestones and the Operational charge uplift

There will be no updates to SLAs as a result of this change.

8.2.2 CSP South and Central

CSP South and Central has asked for Introduction of the new Service exemptions in the PM2 Category 1 Firmware Payload Service Measure. **DCC** are reviewing this and all the following requests.

- Review SMWAN transaction billing approach with the DCC, due to the potential increase in the number of SMWAN transactions. The billing process will aim to reduce the complexity and operational cost whilst permitting a charge for increased SMWAN transactions.
- Review of the PM2 Category 1 Firmware Payload success rate including:
    - Revision to the PM2 Target Service Level and Minimum Service Level
    - Introduction of the relief on the application of Service Credits and associated escalation mechanisms for the early period of implementation
    - Extension to the current 4-day Distribute Firmware window. DCC do not believe this should be adopted.

8.2.3 CSP North

CSP North has indicated the following changes:

- Schedule 2.1 – to reflect additional requirements related to the delivery of new firmware image types
- Schedule 2.2 - Modification to the existing PM2 Category 1 Firmware Payload Service Measure
- Schedule 3 - to include the DCC responsibilities i.e. to monitor and confirm that minimum PPMID endpoints i.e. 2.5M PPMID firmware requests has been achieved in Production, ensure that there are process controls in place in the upstream DCC

systems i.e. service request throttling, manage backlog /pent up demand in a controlled manner, availability of physical devices in SIT.

- Schedule 6.1 – to include delivery Milestones in relation to this CR
- Schedule 7.1 – to reflect any payments under this Change Request and to include payment milestones
- Schedule 11 – to reflect an uplift to the CH specifications
- Schedule 12 – to reflect the uplifted technical specification versions (such as GBCS and CHTS)

Note The DCC is reviewing the above changes and charges.

Appendix A: Glossary

The table below provides definitions of the acronyms and terms used in this document.

ACB	Access Control Broker	ITCH	Instrumented Test Comms Hub
API	Application Programming Interface	ITSF	Intention to Submit Final Tender
BEIS	Department for Business, Energy & Industrial Strategy	Manufacturer image	a full firmware Image or one part of a firmware Image as defined in the GBCS.
BSS	Business Support System	MMC	Message Mapping Catalogue
CAN	Contract Amendment Note	NFT	Non-Functional Testing
CH, Comms Hub	Communications Hub	NMS	Network Management System
CHDS	CH2 Communications Hub Detailed Specification	OTA	Over The Air
CHF	Comms Hub Function	OTA Upgrade Image	the concatenation of the OTA Header and the Upgrade Image that is equal to or less than 750KB. This is defined in GBCS and DUIS
CHTS	Communication Hubs Technical Specification	PIA	Preliminary Impact Assessment
CHM	Comms Hub Manager	PIT	Pre-Integration Testing
CoS	Change of Supplier	PM2	Performance Measurement 2
CPA	Commercial Product Assurance	PPMID	PrePayment Meter user Interface Device
CPL	Central Products List	RNI	Regional Network Interface
CR, CRP	Change Request, BEIS Change Request	ROM	Rough Order of Magnitude
CSP	Communication Service Provider	SAT	Service Audit Trail
CSP N, CSP S&C	CSP North, CSP South and Central	SEC	Smart Energy Code
DCC	Data Communications Company	SECAS	Smart Energy Code Administrator and Secretariat
DSP	Data Service Provider	SI	System Integrator
DUGIDS	DCC User Gateway Interface Design Specification	SIT	Systems Integration Testing
DUIS	DCC User Interface Specification	SMETS	Smart Metering Equipment Technical Specification
DSMS	DCC Service Management System	SMI	Smart Metering Inventory
DUGIDS	DCC User Gateway Interface Design Specification	SMIP	Smart Meter Implementation Programme
EIS	Electricity Import Supplier	SMKI	Smart Meter Key Infrastructure
ES	Electricity Supplier	SMWAN	Smart Meter Wide Area Network
ESI	Enterprise Systems Interface	SNMP	Simple Network Management

			Protocol
ESME	Electricity Smart Metering Equipment	SP	Service Provider
FAT	[DSP] Factory Acceptance Testing	SR	Service Request
FIA	Full Impact Assessment	SRV	Service Request Variant
firmware	A package of firmware which can be made up of a single or several Manufacturer Images. This term will NOT be capitalised.	SSC	Security Sub-Committee
FWDL	firmware download (delivery)	SSMI	Self Service Management Interface
GBCS	Great Britain Companion Specification	SSI	Self Service Inventory
GFI	GBCS Integration Test for Industry	TK	Transceiver Kit (CSP North)
GPF	Gas Proxy Function	TSIRS	Technical Specification Issue Resolution Sub-Group
GS	Gas Supplier	TTO	Transition to Operations
GSME	Gas Smart Metering Equipment	UIT	User Integration Testing
HAN	Home Area Network	Upgrade Image	The Manufacturer Image concatenated with additional information as defined in the GBCS.
HCALCS	HAN Connected Auxiliary Load Control Switch	WAN	Wide Area Network
IHD	In Home Display	W-ITCH	Wireless ITCH
		ZSE	Zigbee Smart Energy

Appendix B: Updating PPMID Firmware with Multiple Manufacturer Images

The process set out in this section is for the benefit of Manufacturers and Suppliers. This process does not propose any changes to the way in which the DCC currently manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

The expectation is that PPMID firmware is typically below 750KB. However, it may be possible for PPMID firmware to exceed this in the future. This section illustrates how to activate firmware comprised of multiple OTA Upgrade Images that are less than or equal 750KB in size.

The operating firmware version in this example is 0x10, which is reflected in the CPL entry example in Table 8 below.

A PPMID is to be updated to firmware version 0x20. This requires two Images to be sent to the PPMID, to provide all the changed firmware/configuration data required for firmware version 0x20.

The Manufacturer has split this upgrade data into two Images:

- Image 0x15: this contains the first part of the upgrade data and contains Manufacturer instructions for the PPMID to only store this first part on activation
- Image 0x20: this contains the second part of the upgrade data and contains Manufacturer instructions for the PPMID to check that Image 0x15 has already been activated. Activating this Image causes the functionality of the PPMID to be upgraded to firmware version 0x20.

The new CPL entry will look like this.

Manufacturer identifier	Model identifier	Hardware version	Hardware version revision	Firmware version	Hash
FF: FE	AA:BB	01	01	00:00:00:10	(Hash of Image 10)
FF: FE	AA:BB	01	01	00:00:00:15	(Hash of Image 15)
FF: FE	AA:BB	01	01	00:00:00:20	(Hash of Image 20)

Table 8: Example New CPL Entry for firmware comprised of multiple Manufacturer Images

To upgrade firmware for a PPMID, the Supplier will follow the following process:

1. Having undertaken the necessary checks, the Supplier will create a ‘Send PPMID Firmware’ Service Request to distribute Image 0x15.

2. The DCC will distribute Image 0x15 to the Communications Hub and the PPMID will download the Image. The PPMID will then send a Device Alert containing its firmware version. Note that this value will still be 0x10 (in line with the Technical Specification Issue Resolution Sub-Group (TSIRS) decision). Therefore, the Device Alert will only indicate delivery of the Image. It will NOT indicate that the PPMID has successfully validated the Image. The DCC will update the SMI if

the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

3. On receipt of the Device Alert from the DCC containing the PPMID's firmware version, the sending Supplier will send Image 0x20. If this Device Alert was not received the Supplier can only resend Image 0x15 (since the TSIRS decision means, there is no mechanisms to discover if the PPMID had that Image).

4. The DCC will distribute Image 0x20 to the Communications Hub. When the PPMID has downloaded the Image, the PPMID will send a Device Alert containing its firmware version. Note that this value will, if activation was successful, now be 0x20 (in line with the TSIRS decision). Therefore, this Device Alert will indicate delivery of the Image and that the PPMID successfully activated the Image. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

5. The Supplier can only resend Image 0x20 if this Device Alert is not received. However, the Supplier should verify this first by sending SR11.2 to the PPMID. The DCC will then update the SMI if the firmware version has changed and forward the Device Response for SR11.2 to the Supplier.

The result is that the PPMID (excluding where the OTA firmware upgrade process cannot be completed e.g. where there is no Wider Area Network (WAN) connectivity), will be operating firmware version 0x20.

The above process is explained in detail in Figure 7 and Figure 8, Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2 (parts 1 and 2 respectively) below.

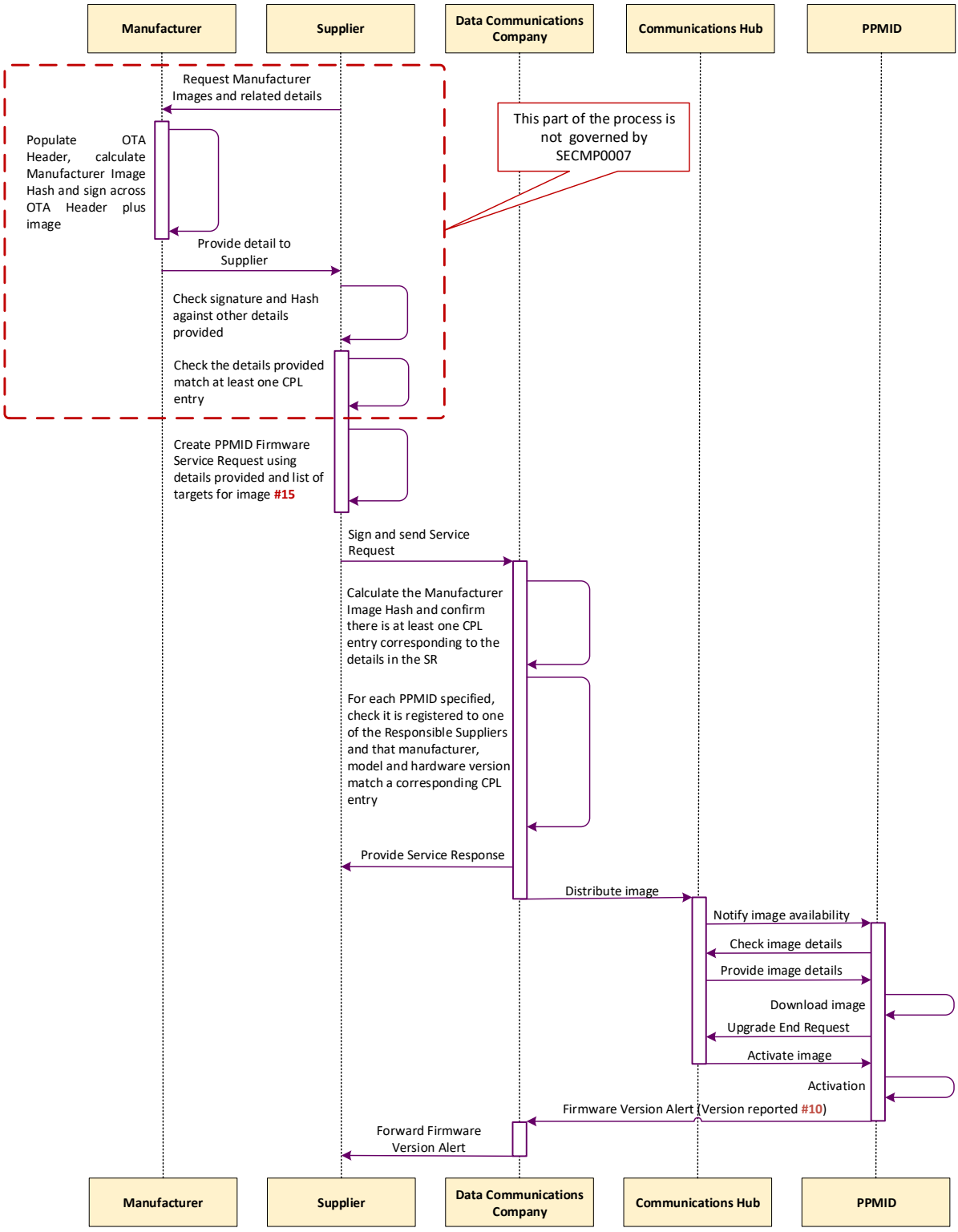


Figure 7: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 1

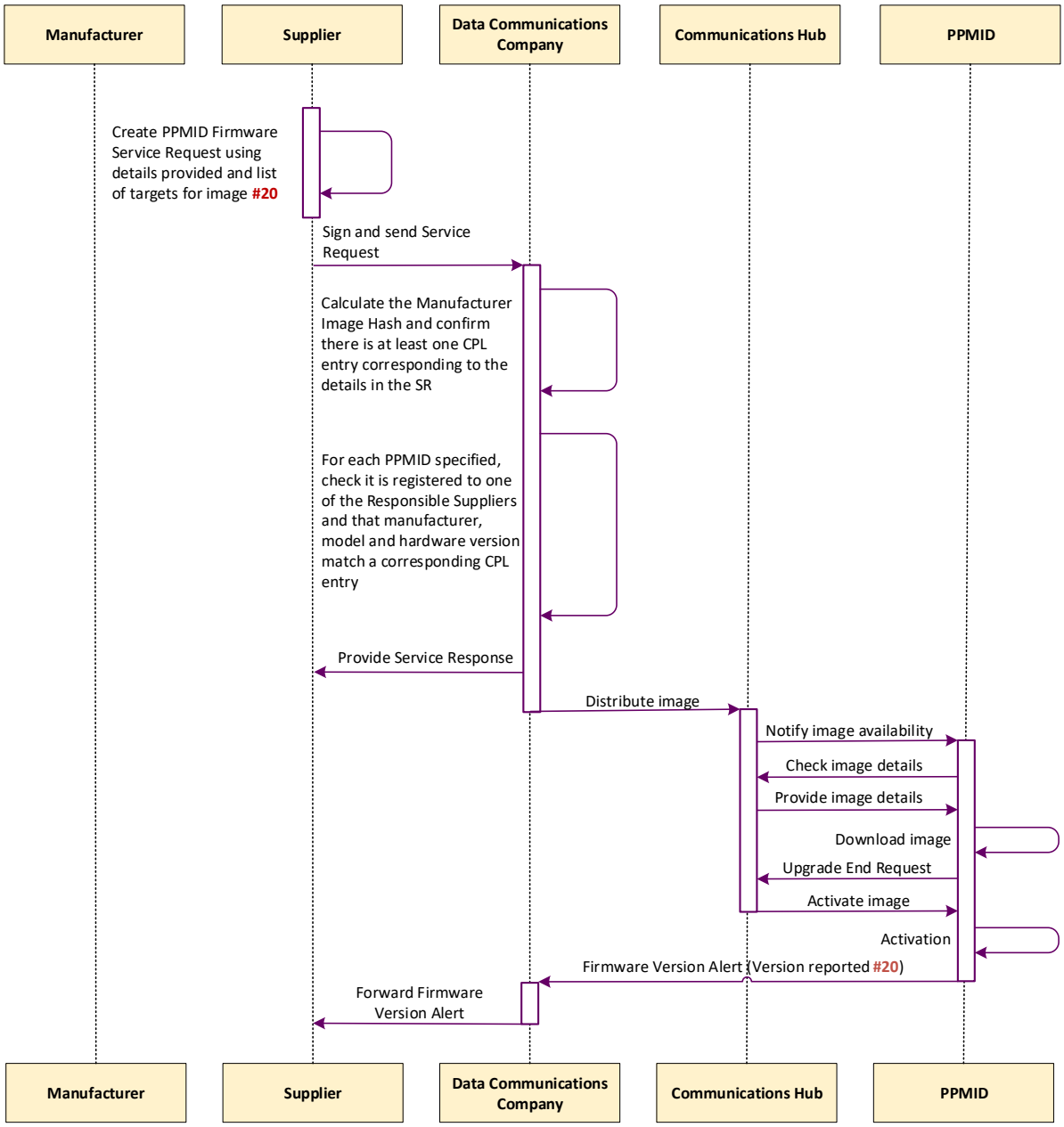


Figure 8: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2

Appendix C: Technical Specifications Changes

In the case of PPMID firmware updates, the GBCS, SMETS and CHTS technical specifications, as noted in section 4.1, mandate the use of ZigBee specifications but do not repeat the details of the ZigBee specifications. There are a few exceptions where functionality differs from the ZigBee specification. The manufacturer specific ZigBee implementation may differ between chipset vendors and device manufacturers and this must be considered by manufacturers when designing devices based on the ZigBee specifications.

With regards to the ZigBee OTA specifications GBCS doesn't deviate from the ZigBee standard except for the activation command where for ESME and GSME no activation is allowed by the server (CH) and for PPMID and HCALCS only immediate activation by the server (CH) is allowed.

The ZigBee OTA specifications allow for different timings e.g. for clients (PPMID) to send the Upgrade End Request and the server (CH) must be able to handle these different timings and the possibly different content of the Upgrade End Request. The ZigBee OTA specifications are clear about the communication between the server (CH) and the client (device). To be on the safe side only mandated attributes and commands should be relied upon; optional commands and attributes may or may not work and this needs to be addressed in the server firmware.

Currently the CH must be able to handle the OTA upgrade for different ESME makes and models and up to four ESMEs in parallel. The OTA upgrade to the PPMID and HCALCS follows the exact same set of specifications at the ZigBee level as the ESME OTA upgrade with the exception of the activation at the end of a successful transfer (see above).

Appendix D: Design Decisions

This section contains design decisions agreed by the DCC and Working Group during the development of this SEC modification.

July 2018, First Preliminary Assessment sent to Working Group, scope extended to HCALCS

February 2019, DCC and Service Provider review of requirements with two solutions proposed:

1. Original Approach, No GBCS Changes

2. Extend Proven OTA Firmware Method; create a type 1 IHD and extending PPMID's, HCALCS, and the new type 1 IHD to support firmware distribution in a manner that would be similar to ESME firmware distribution and activation

July 2019, Working Group agrees to two solutions:

Option 1; for PPMIDs and IHDs, ZigBee Over-The-Air (OTA) delivery mechanism

Option 2; for HCALCS, OTA firmware update procedure used by Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME)

Expense of adding PPMIDs and IHDs to CPL was cited as a major cost, and the reason for not using Option 2 for PPMIDs and IHDs.

September 2019, DCC and SP Design Review 1

Rather than use new DUIS Service Requests 11.4 Download Firmware and 11.5 Read Firmware specifically for PPMIDs and IHDs, SPs recommended extending SR11.1 to support SMETS2 PPMIDs and IHDs.

New API to the CSPs for Distribute Firmware to PPMID/IHDs. Although the Modification suggested a new API from DSP to CSP for distribution of Firmware to PPMID or IHD, SPs can see no reason why a new API is required. The content to be sent between DSP and CSP is exactly the same as the current API for ESME/GSME firmware and therefore it is proposed that the existing DSP -> CSP API is used. To ensure that Service Users get feedback of the firmware download to the Comms Hubs, there needs to be a notification from the CSP's central systems back to the DSP through a custom API, with settings of Success and Fail. This notification will then trigger a new DCC Alert to be sent to the Service User informing them of the status of the download to the Comms Hub. It is suggested that this notification should apply to all firmware download activities, not just PPMID/IHD but also ESME, GSME, and HCALCS. This is more than current SECMP0007 scope, but would help users.

Notifications of delivery to PPMID/IHD: In order to track delivery of Firmware from the Comms Hub to the PPMID/IHD, further notifications are needed from the Comms Hub. 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 CHF.

Map SR11.2 to new GBCS Use Case with new GBCS Use Case required for the CHF, allowing Service Users to be able to read the firmware version with a Service Request.

HCALCS to 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. Assume the ESME buffer gets overwritten so there is no need for an additional buffer.

September 2019, DCC and SP Design Review 2

Activate Firmware Date and Time: In cases where the PPMID or IHD updates are sent to the Comms Hub, the activation date and time isn't set as currently SR11.1 doesn't contain the date and time of when a firmware activation is required. Suggestion is that rather than updating 11.1 with a date and time value, we assume the firmware implementation should be immediate. We noted that storing updates which would be activated at a later date or time would take up both network and Comms Hub capacity, and potentially would add risk to the stored image. SPs suggested removing option completely to reduce testing, SSC mandated that the maximum delay for activation will be 30 days.

Business Rules for Firmware Updates on Comms Hub Storage:

- If the firmware is downloaded, then the images should be offered to all related ESMEs on the SM HAN.
- If some of the ESMEs on the SM HAN are still updating, then the ESME buffer space must not be overwritten until all downloads are complete.

DSP will add functionality for validation of the firmware image, tracking of progress including the notification of a valid download to the Comms Hub, and to reject any potential downloads when an update is already in place. As Service Users don't have visibility of the firmware management, there is a proposal to make this functionality available for all types of device. This is based on discussions with the DAB. The CSP systems would have this information in a report, and there would be an added call in the DSP to retrieve the relevant information. Tracking and other pieces are included in SECMP0007.

Firmware scheduling and rules for rejection if a pre-existing download is still active:

- If a CSP receives a firmware request for an end device (i.e. ESME, HCALC, PPMID/IHD) that targets a Comms Hub, where a prior firmware download request has already been received and is being actioned within the SLA window, then the CSP can reject the second firmware request, and it will not count as a failure from a Service Measure perspective. It will be deemed an allowable exception. Feedback from SECAS: "Existing Firmware Update functionality uses the Extended Unique Identifier (EUI) to identify the individual target device, updates to the PPMID/EUI use the same concept; in this context “offering” the image to all related ESMEs doesn’t seem to fit in." However, if the CSP can complete the download for the first image and still complete the second download within the four day SLA period, then it should be allowed to schedule it.
- If the firmware download is rejected, the CSP should send a Firmware Download Delivery alert, with the status code set to an error code indicating that an existing download was

already in place. The view of the working group was that ESME and GSME firmware updates have priority, to the extent that it is allowed to purge a PPMID/IHD update from the CH memory. Such a mechanism is desirable since PPMID/IHD may be removed by the consumer at any time (even when the transfer from the CH to the PPMID/IHD has been started) and pending upgrade images could block the memory in the CH.

The transfer of ESME and GSME images to the CH has been estimated to take about half a day. The transfer of the image from the CH to an ESME should be reasonably fast to free up the memory in the CH to support PPMID/IHD/HCALCS images in a short time; the GSME image will remain much longer in the CH memory and may take at least one day to transfer over the HAN

October 2019, requirement for new SR 11.4 relating to PPMIDs:

The Security Sub-Committee (SSC) have stated that Service Requests to update firmware for PPMIDs must be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME. However, PPMIDs must be counted and reported separately to enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs.

The SSC also stated that Service Requests to update firmware for HCALCS should be subject to the same ADT procedures as ESME and GSME since similar risks to the supply of energy apply to HCALCS.

December 2019, streamlining review with Working Group, Service Providers, and BEIS results in reduced scope.

1. In-Home Displays (IHDs): remove IHDs from scope
2. Local firmware updates: allow local firmware updates to PPMIDs only
3. Communications Hub memory block rules: restrict PPMID and HCALCS firmware Images to GSME block of Comms Hub
4. Comms Hub SLA: remove the requirement for a two-day SLA for an Image to stay on the Comms Hub. The Image will remain until it is overwritten
5. Comms Hub logging of updates: remove the requirement for the Comms Hub to log the progress of up to 15 Devices in the Upgrade Image list
6. Firmware updates over 750KB: 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.
7. Future-dated Update Activation: limit firmware updates to immediate activation only.
8. Service Request for PPMID firmware updates: new SR to distribute and activate PPMID firmware, to facilitate separate Anomaly Detection Thresholds (ADTs) required for PPMIDs.
9. Alerts and notifications remain unchanged
10. Dual Supplier Scenarios: in a dual Supplier scenario, both Responsible Suppliers shall be able carry out firmware updates to PPMIDs and HCALCS
11. The PPMID generates the success/failure Alert to the DCC. This removes the following Communications Hub requirements:
    - to record the activation date-time plus [X] minutes
    - to subsequently read the firmware version on the Device

June 2020, GBCS Change to reflect new requirements:

> The Communications Hub shall make the GSME image available for fourteen (14) days and, after this period, replace the GSME image with an image for the PPMID / HCALCS, if one becomes available. If the transfer of a GSME image to the GSME is in process, the Communications Hub shall only replace this GSME image with an image for the PPMID / HCALCS once the GSME image transfer has completed.
>
> The Communications Hub shall make the PPMID / HCALCS image available for fourteen (14) days unless a new PPMID / HCALCS / GSME image is available.
>
> If a PPMID / HCALCS / GSME Upgrade Image is discarded or replaced prior to having been successfully transported over the HAN, the Communications Hub shall send an Alert for each target Device Entity Identifier associated with the Upgrade Image File with the Alert Code 0x8F89 as specified in Section 11.7 by setting firmwareVersion to the Upgrade Image File version and transferResponseCode to imageDiscarded.

Note 1: there is no requirement specifying the time for the new image to live on Comms Hub in the GBCS legal drafting.

Note 2: This is a divergence from the design proposal previously discussed with DCC. Analysis of the previous design proposal has highlighted a constraint with the way memory protection is implemented that means the use of RAM as an alternative storage area for OTA images is no longer considered a viable option.

Appendix E: CSP North Hardware Augmentation Details

The capacity of the CSP North firmware download solution is very high. Each base station transceiver kit (TK) currently supports 3 FWDL channels that together will support 3 FWDL jobs running concurrently. There are approximately 1,350 macro TKs in the radio network, each supporting 3 FWDL channels. The system will accept up to 400 FWDL Jobs simultaneously, each of which can contain 10k devices and be spread across a large number of TKs in the network. The success of the FWDL process in a large capacity network is dependent upon the efficient creation of large FWDL jobs in relatively small geographic areas that then utilise only a small number of TKs and subsequently a small number of FWDL channel resources at the TKs. Currently there is almost no management of FWDL jobs by Service Users and as a result there have been occasions where the system has become overloaded and FWDL jobs have either been rejected by the system or timed out due to lack of channel resources at a TK.

The system is currently set up with 3 FWDL channels per TK, which can be increased to 6. Six FWDL channels per TK is the current system maximum, without further extensive changes being made to the system operation.

This channel expansion is currently available to provide more FWDL capacity as Communications Hub numbers increase and assuming Service Users continue to submit FWDL jobs with limited management processes in place. However, there is a limit to the FWDL system capacity available and at it has been stated by CSP North that some FWDL management process is required in order to support the FWDL requirements to all devices, once numbers scale to multiple millions of Communications Hubs. For example, several Service Users have been submitting large numbers of FWDL jobs containing only a single device to be upgraded. Whilst this is sometimes unavoidable, it should be done by exception and not as standard practice.

The proposal within this Modification is to increase the FWDL channels to the maximum of 6 per TK in order to support the additional FWDL jobs that will be generated for the additional HAN devices. All FWDL jobs to any device type will be transmitted on these FWDL channels and therefore it should be noted that jobs to PPMIDS and HCALCS will potentially use FWDL capacity that would otherwise have been available as spare capacity for CH, ESME and GSME FWDL jobs. Therefore, it is important to also note that in the longer term, in order to support the additional FWDL capacity, a process must be put in place that allows Service Users to manage FWDL job in a more efficient manner. Without a change in Service User behaviour in creating FWDL jobs, there will potentially be some capacity bottlenecks in the FWDL system as Comms Hub numbers scale to multiple millions.

There are three significant changes required to support the FWDL channel expansion:

- New FWDL radio channels allocated to base stations to support additional traffic from new devices

- Modification to functionality within the Network Management System (NMS) CH tuning process to allow for dynamic automated updates to the Communications Hub default embedded channel tables to allow all Communications Hubs to be able to operate on newly defined FWDL channels.

- Modification to the Transceiver Kit (TK) firmware to increase the number of radio channels that the TK is programmed to transmit on from 16 to a new upper limit of 32 channels.

New Radio Channels required to support Firmware Downloads to HAN Devices

The number of dedicated broadcast radio channels allocated to support FWDL Jobs at each macro TK (radio cell) shall be increased by 3 new channels from 3 to 6. After this upgrade, each TK will be able to support firmware upgrades to devices that are contained in 6 separate FWDL Jobs simultaneously. The process to upgrade all Production Environment Base Station Transceiver Kits (TK) with the new channel plan requires a period of up to 4 weeks, as each individual base station must be upgraded individually in a serial process.

The current FWDL Broadcast channels support all FW upgrades to ESME, GSME and Communications Hubs (CH). The FWDL Jobs to upgrade CHs use only a very small proportion of the available FWDL channel resource because these jobs can be managed in large groups very efficiently by ASML.

The majority of the current available FWDL channel resource is allocated to FWDL jobs for ESME and GSME. These FWDL Jobs are created by the Service Users and tend to be many Jobs daily, typically containing small numbers of devices. It is the expectation that this type of usage of the FWDL system will continue once HAN devices are included until a process for optimisation of FWDL Job management is agreed with Service Users. The estimates for the numbers of PPMIDs and HCALCS to be included in the sizing for this CR leads to an expectation that the number of device upgrades and subsequently the number of FWDL Jobs submitted to the system will approximately double compared to the original system design. **Note these and the following estimates have been reviewed and further estimates are expected.**

Increasing the number of FWDL channels per TK from the current 3 to the system maximum of 6 will provide a 100% increase in FWDL capacity providing the maximum FWDL capacity at each TK.

Once 6 FWDL channels are available at each TK, they will be available to all FWDL Jobs irrespective of device type and therefore the system will be more resilient to large peaks in FWDL Job numbers issued by Service Users across all device types.

4.1.3.4. NMS functionality

The Communications Hub contains a default channel table, which details the frequencies of all channels being used in the current channel plan including all FWDL and GBCS Messaging channels, plus the three uplink control channels L2Ack, RTS and CH Alert.

When 3 additional FWDL channels are introduced into the system at each TK, Communications Hubs will need to be informed of the frequencies of these new FWDL channels in order to be able to operate on them as part of the FWDL OTA process. This will be done by means of a new automated process within the NMS, which will send messages to the Communications Hubs informing them of the new FWDL channels. This updating of the CH channel table can currently be done manually but a new automated process will be required in the NMS to update Communications Hubs on a larger scale.

Transceiver Kit (TK) transmit channels

Transceivers at each base station are required to transmit on multiple channels and currently are set up to be able to transmit on up to 16 different channels. Within the current channel plan, TKs may transmit on:

- Admin channel
- 1-4 Primary messaging channels
- 3 FWDL channels
- Time Sync messages on up 11 secondary channels

When these additional FWDL channels are introduced into the system, an expansion in functionality will be required to enable the TKs to transmit on an increased number of channels.

This new functionality requires a change request to Sensus on several aspects of the TK functionality.

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'

Annex F

First Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the first SECMP0007 Refinement Consultation.

Question 1: Will your organisation be impacted due the implementation of this modification?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	The implementation of this modification will result in changes to: • IT infrastructure; • Operational Processes; and • Contractual arrangements In addition, there may be impacts to any such Devices installed prior to the implementation date should the ban for Local Updates be applied to non-upgradable Device. This however is unclear to us from the Modification and we would welcome clarity around this point.
EDF Energy	Large Supplier	Yes	As an Energy Supplier we would be impacted in 2 ways: • We would need to ensure that the relevant devices that we procure and install are able to meet the revised Technical Specifications that would be implemented as a result of this Modification. However we understand that while many of the current IHDs/PPMIDs are being built with a firmware upgrade capability, it is just that this cannot be accessed via DCC services and so is 'switched off'. • We would need to make changes to our systems and processes to manage firmware across the extended range of devices. This would include changes to our interfaces with the DCC systems in order to deploy firmware to the extended range of devices, as well as changes to processes to track and manage firmware versions. We would hope that we would be able to align the processes for managing firmware in the new devices with those that we use for other devices, and specifically meters, wherever possible.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Npower	Large Supplier	Yes	Yes, this provides a positive impact as it increases control of customer facing devices and reduces operating cost risks. Given the maturity of the SMETS and GBCS specifications, it also provides mitigation for firmware management risks.
Scottish Power	Large Supplier	Yes	The implementation of this proposal would have both positive and negative impacts on our business: i.e. it may be beneficial to have the facility to upgrade IHD / PPMID firmware using the OTA process, but we would need to implement costly new service request functionality in our IT solution. Implementation would also be an unwelcome distraction from our other rollout activities.
SSE Energy Supply	Large Supplier	Yes	Implementation of this modification will have an impact upon systems and processes within our organisation.
Utilita	Large Supplier	Yes	The ability to update IHD/PPMID firmware may reduce the number of site visits we are required to perform to fix/replace faulty devices. This also means that overall fault resolution time may be brought down. We would always prefer a scenario where we can fix an issue remotely, as opposed to going through the timely and disruptive process of organising and fulfilling a site visit. The modification would also fundamentally change how we view our IHDs/PPMIDs that are in the field. The ability to update firmware remotely means that we could theoretically innovate in this area and improve the experience for the customer through introduction of new features. There is likely to be minimal impact on our BAU activities.
SSE Networks	Network Party	Yes	The working group has assessed that Electricity Distributor parties will not be impacted by this modification. Whilst this may be true of the specific functionality proposed it is inevitable that overall system performance may be affected which in turn will impact SSEN.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			It may be possible that DCC to SSEN services will be impacted by new functionality delivered by this change. These may be in terms of our ability to communicate with a meter whilst an IHD or PPMID firmware upgrade is in progress. The solution does not yet seem sufficiently developed to enable us to understand the impact of this change on the service that will be delivered to SSEN. We expect the final design of this modification to deliver a solution that has little or no impact on the level of service delivered to SSEN. SSEN may need to make minor system changes to facilitate this modification. It is possible that this modification will create issues associated with the management of data capacity on the DCC's systems. Given that users are "blind" to system component capacity constraint we require further information from the modification working group regarding how capacity and any potential conflicts/ user priorities will be managed. We will inevitably incur increased DCC charges (see Q2).
Chameleon Technology	Other Party	Yes	Our products will be expected to implement the OTA features described in this modification. We will also be expected to continue to support deployed products with firmware updates as appropriate after deployment.
TMA Data Management	Other Party	Yes	There might be some minor system changes required.

Question 2: Will your organisation incur any costs due to the implementation of this modification?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	The implementation of this modification will incur costs; such costs are not quantifiable until more is known with regard to a) the solution proposed here, and b) the management process adopted by Industry for Firmware changes, specifically in CoS situations.
EDF Energy	Large Supplier	Yes	We would definitely incur costs as a result of the changes detailed in our response to Question 1 but at this stage is not possible to give any indication as to what those costs would be. It is likely that any changes required to devices and/or the DCC systems as a result of this Modification would form part of a wider release which would include other changes – providing costs that are specific to this Modification as if it were to be implemented in isolation from other changes would be very difficult and would provide unrealistic costs. On that note, we believe that the DCC's costs are probably not realistic on that same basis, and are far higher than they would actually be if this Modification were to be implemented as part of a wider package of changes.
Npower	Large Supplier	Yes	Yes, circa £500k. this will involve changes to our DCC gateway, asset management and front end-systems, as well as testing/assurance activities.
Scottish Power	Large Supplier	Yes	As indicated in our response to Q1, we would expect the costs impacts from implementing the SECMP0007 solution in our IT systems to be of a material nature.
SSE Energy Supply	Large Supplier	Yes	Following implementation, we will be able to run OTA which will result in costs for us, but for every device that we are able to OTA rather than replace, we will avoid disruption or adverse consumer experience and reduce the costs of issuing replacement devices.

Question 2			
Respondent	**Category**	**Response**	**Rationale**
Utilita	Large Supplier	No	(Excluding our share of the cost of the modification) We believe that there would be no substantial direct costs to our organisation. There may be some relatively small costs to test new functionality/train staff to utilise said functionality. These costs would likely be accounted for as BAU costs. We believe most of the risk lies with the asset owners (MAPs), but this depends on each Suppliers' contractual arrangement with their MAP.
SSE Networks	Network Party	Yes	SSEN may incur costs associated with a need to make some minor changes to its systems. SSEN do not have sufficient information at this time to determine whether this change will result in specific additional DCC charges. Should SEC parties in future be required to pay charges for individual service requests then it is possible that further additional costs will be incurred. There are potential situations associated with this modification where capacity constraint means SSEN service requests will fail leading to a need to re-issue a command. This will lead to an increase in internal administration costs and may in future be subject to individual service request charging. As a SEC party SSEN will incur higher DCC charges for functionality that will not improve our ability to deliver benefit to our customers.
Chameleon Technology	Other Party	Yes	The extra functionality requires more code space and storage space in our products, increasing the unit cost. The extra development time required to implement and test the features will also add cost. These extra costs have to be taken in the context that there is a significant benefit to having the capability to update assets once deployed. It is not expected that there would is likely to be an increase in the price of assets on a like for like basis.

Question 2			
Respondent	**Category**	**Response**	**Rationale**
TMA Data Management	Other Party	Yes	The cost associated would be very low.

Question 3: Please provide any views or rationale on whether the benefits of the change, outweigh the costs associated with assessing and implementing it. Noting:

questions raised in relation to how many IHDs and PPMIDs will be in use when this modification is implemented; and this will be implemented (if approved) no earlier than Spring 2019.

Question 3		
Respondent	**Category**	**Comments**
E.ON	Large Supplier	We do not understand how the costs proposed have been reached and would welcome a detailed explanation of how DCC arrived at such costs. In addition, the value of this modification is likely to be consumer driven and the use of these Devices across time has not yet been established at Industry. However, it is believed likely that the use of PPMIDs and AIHDs are likely to continue since their use is purpose-driven. At the present time we do not believe that there is sufficient information to inform such a consideration with regard to this modification. We would note however, that we fully support the progression of this modification and the benefits it will bestow upon Industry.
EDF Energy	Large Supplier	We believe that the benefits of this change are likely to outweigh the costs, but we recognise that further detailed analysis needs to be undertaken to determine whether this is the case. As noted in the response to Question 2 we do not believe that the estimated costs that have been provided by DCC are reasonable or realistic, especially as they are based on this being made as a standalone change. Assessing whether this change should be progressed on the basis of these costs is not appropriate. We believe that not being able to upgrade the firmware on additional devices, and especially on PPMIDs and potentially HCALCSs creates a significant risk in relation to those devices. We note that HCALCSs are not currently within the scope of this Modification but many of the risks that this change is looking to address would apply equally to those devices.

Question 3		
Respondent	**Category**	**Comments**
		It should also be noted that in many if not most cases Suppliers are deploying devices that deliver IHD and PPMID functionality within the same device, which for DCC purposes would be registered as a PPMID on the DCC's Inventory. It is not clear how many devices that are purely IHDs will actually be installed – this would need to be understood further. Where it is not possible to upgrade the firmware on a device there is a risk that device may no longer be able to perform its mandated function, or it may not be possible to upgrade that device to include additional functionality which may be required to support the consumer. In the absence of an ability to fix or upgrade a device via a firmware update devices will need to be replaced, which invoices unnecessary cost to consumers, especially should that replacement require a site visit. This is less likely to be the case for IHDs which have limited maintenance requirements, but as noted above in many or most cases Suppliers will be deploying PPMIDs rather than IHDs, with the anticipation that these devices will be more permanent than IHDs – especially where the customer is in prepayment mode. Suppliers will have an ongoing obligation to keep these devices operational that extends beyond the 12 month minimum for IHDs. As noted previously we understand that many of the current IHDs/PPMIDs are being built with a firmware upgrade capability, it is just that this cannot be accessed via DCC services and so is 'switched off'. This would mean that these devices which are provided before 2019 might be capable of receiving a firmware upgrade even if this change is not approved until 2019 – depending on whether this functionality needs to be 'switched on' – if so and this is not possible then these devices would remain incapable Of receiving a firmware update even if the DCC functionality is introduced in 2019 While some of the risks that would cause a device to be replaced might be able to be mitigated through other actions (such as pre-deployment testing) there will always be a residual risk that devices will be stranded and will need to be replaced. We believe that the working group should undertake further analysis which considers what device types are actually being rolled out by Suppliers, what the risks associated with those devices are, and how they might be mitigated. The level of residual risk once these mitigating actions have

Question 3		
Respondent	**Category**	**Comments**
		been taken will indicate whether the costs of progressing this Modification will outweigh the costs – our initial view is that this is likely to be the case.
Npower	Large Supplier	We believe the benefits far outweigh the costs. If we assume that at circa £20 a unit for a PPMID and that by early 2019 we would be a ¼ of the way through the rollout and therefore ¾ of the PPMID population could be upgraded and that ½ the PPMIDs suffer an issue that could be fixed by an OTA firmware upgrade then 54m meters = 27m installed PPMIDS x ¾ x ½ = 10.125m potential PPMIDS that may need an upgrade. If we had to replace those PPMIDS then the benefits would become £202.5m! Also, if a visit is required to replace any of these PPMIDs then the benefits become even greater.
Scottish Power	Large Supplier	The implementation of SECMP0007 is not now expected until Spring 2019 at the earliest; by which time a significant proportion of households can already be expected to have IHD / PPMID units or equivalent deployed. We are concerned, therefore, that the benefits of being able to deliver OTA firmware to these devices are significantly reduced, as this late delivery would mean site visits are not avoided in the interim. Moreover, if the implementation of SECMP0007 was to be pushed out towards 2020, it is likely that only a minimal number of units would ever require this OTA facility during the Relevant Period outlined in the supply licence. In our view, the proposed 2019 implementation date is a consequence of the DCC being unable to divert resources away from its main implementation programme and onto SEC Mods. In our view, then, delaying a decision on SECMP0007 at this time would have no material impact on its subsequent delivery, should we later decide to proceed. We would, therefore, suggest placing this Mod on hold until, say, the second half of 2018, when it could be revisited and a final decision made. We believe, this would require the Proposer to Withdraw the Mod, as the Suspension process only appears to be available to the Panel in very limited circumstances that do not apply in this case.

Question 3		
Respondent	**Category**	**Comments**
SSE Energy Supply	Large Supplier	-
Utilita	Large Supplier	-
SSE Networks	Network Party	There will be no benefit to SSEN from this proposed change. We have no information regarding whether benefits will outweigh the high cost of this change.
Chameleon Technology	Other Party	The ability to OTA update an IHD/PPMID after deployment will provide significant net benefit, by allowing bug-fixes, feature enhancements and security improvements to be applied, rather than needing to recover/replace with new units. The sooner that this change can be implemented the sooner the benefit can be felt. However, once the details are finalised we expect that compatible products may be able to be deployed before the implementation date (subject to suitable testing) on the expectation that the update capability will be able to be used later on. It is key to get the details finalised and the modification introduced at the earliest opportunity in order to realise the maximum benefit from the modification.
TMA Data Management	Other Party	Providing the astronomical cost put forward by the DCC (7.4 to 8.2 Million), no amount of benefit will outweigh that. We find ourselves in a position to reject a change we would otherwise support. This is a major gap in the original design that is unlikely to be addressed given the prohibitive cost put forward by the DCC.

Question 4: If you are a Supplier Party, please provide examples of when you are likely to need to update firmware on IHDs and/or PPMIDs, and how often you expect to do so when this modification is implemented (earliest Spring 2019).

Question 4		
Respondent	**Category**	**Comments**
E.ON	Large Supplier	Based on today's landscape and our experience of SMETS1s, we believe that a minimum of two firmware updates per annum would be required to these Devices.
EDF Energy	Large Supplier	Based on our experience of our SMETS1 IHDS (which are capable of processing firmware updates) the key drivers for updating firmware on these devices is: • To address inaccuracy and defect propagation on devices to ensure they remain compliant with Supplier licence obligations related to these devices. • To resolve any identified risks or vulnerabilities to the HAN from IHDs or PPMIDs. • To deliver functional enhancements that improve the consumer experience and support the delivery of the consumer benefits associated with the smart metering rollout. It is almost impossible to take a view as to how frequently we might need to undertake firmware updates for any of these reasons after 2019 but our experience of our SMETS1 devices is that we have needed to undertake relatively frequent updates. While some of the root causes of this might be addressed and the number of updates reduced, it is unlikely that the need to upgrade devices can be eliminated entirely.
Npower	Large Supplier	Device defects including security Specification level defects including security Interoperability issues New application functionality

Question 4		
Respondent	**Category**	**Comments**
		New service functionality
Scottish Power	Large Supplier	Firmware upgrades would most likely be needed in the event that a corresponding upgrade to other Devices (e.g. Comms. Hub or ESME / GSME) led to a loss of IHD/ PPMID functionality. An indication of such incidence would be a function of testing.
SSE Energy Supply	Large Supplier	-
Utilita	Large Supplier	See Q3.
SSE Networks	Network Party	N/A
Chameleon Technology	Other Party	N/A
TMA Data Management	Other Party	N/A

Question 5: Please provide your organisations views on:

responsibilities for Suppliers that send firmware images to rectify any interoperability issues that may occur; and liabilities for damaged Devices because of firmware updates; and

responsibilities for ensuring that damaged Devices are un-joined and decommissioned, and new devices are whitelisted, joined and commissioned.

Question 5		
Respondent	**Category**	**Comments**
E.ON	Large Supplier	We believe that there is a fundamental requirement to resolve such issues at Industry, but we believe that this needs to be done in a single space and to be made applicable to all Devices requiring Firmware Updates. We would highlight that this modification can be accepted on a good faith basis with regard to the requirement to have a Firmware Management Process.
EDF Energy	Large Supplier	Where a device is 'shared' by multiple Suppliers it should be possible for either of those Suppliers to send updated firmware to that device – the concept of a 'lead' or 'responsible' Supplier would not be appropriate. Where a Supplier sends a firmware update that means a device ceases to work of deliver the functionality required by the other Supplier then it is reasonable to expect that Supplier to be responsible for rectifying that issue, and where required replacing that device. The actions undertaken by one Supplier in deploying firmware should never leave the consumer in a worse position than they were before that update was undertaken.
Npower	Large Supplier	Given suitable levels of assurance from device manufacturer that the firmware has been thoroughly tested and suppliers own assurance processes that they may choose to carry out, then these risks can be minimised anyway. Npower does not think you can lay responsibility on one party in a shared HAN situation for interoperability where the Installing Supplier is no longer a Responsible Supplier, especially when dealing with firmware upgrades as it may be a particular device that is causing an interoperability issue and may be

Question 5		
Respondent	**Category**	**Comments**
		due to a device that hasn't been upgraded. Suppliers have a shared responsibility for the HAN and that should endure. We would expect some level of collaboration between parties in this scenario. Where the installing supplier is the responsible supplier then they should perform the firmware update. Where devices are damaged then responsibility for decommissioning (if possible) the old device and commissioning the new device can only be with the Responsible Supplier or the upgrading party for a shared device.
Scottish Power	Large Supplier	As a supplier committed to delivering an excellent customer experience, we would expect to resolve any issues with IHDs/PMIDs in our customers' premises; though we realise it might not be to the customer's convenience if a site visit is required. Given that alternatives to IHDs and PPMIDs are likely to emerge (e.g. as a feature of a product), a better customer experience might be delivered by providing access to such alternatives, and might also serve to obviate the need for such site visits.
SSE Energy Supply	Large Supplier	We believe that the Responsible Supplier should rectify any interoperability issues and ensure that damaged Devices are exchanged, following the relevant processes. In terms of damaged devices, it is our view that it would be the responsibility of the Responsible Supplier to rectify these situations as and when they become aware. That being said, the answers for the question on liabilities may depend upon the scenario, such as if they were the installing or gaining supplier, and each supplier's commercial arrangements. A particular concern around this is that it could be difficult to determine what has happened at a dual supplier site that has been damaged. This is a complex matter that we believe should be further assessed by the Working Group based upon the consultation responses, and take into consideration the existing SEC provisions for liabilities.
Utilita	Large Supplier	We agree that the Supplier responsible for the damage should be responsible for the replacement. We do not believe that any new obligations should be introduced with regards to joining and commissioning of new Devices. Existing obligations (supply licence conditions) relating to supply and maintenance of an IHD should remain. Provision of a PPMID should remain optional.

Question 5		
Respondent	**Category**	**Comments**
		Firmware upgrades which result in damaging either device should be dealt with using existing obligations and whatever the Supplier believes to be in the best interest of the consumer. We cannot foresee a situation where a firmware upgrade would inadvertently result in a faulty Device which we not then subsequently replace, as this would obviously be in the best interests of the impacted customer(s).
SSE Networks	Network Party	N/A
Chameleon Technology	Other Party	In this topic what must be borne in mind is that at present until this modification is introduced then there is no practical means to address issues in the field with these assets should these occur. It is expected that issues were introduced as a consequence of an update then the update mechanism would have to be used again in order to correct matters.
TMA Data Management	Other Party	N/A

Question 6: Having considered the potential impacts and costs to your organisation, as well as the cost to deliver the modification, do you agree that SECMP0007 should continue to be progressed?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	We believe this modification ought to progress.
EDF Energy	Large Supplier	Yes	We believe that SECMP0007 should continue to be progressed as we do not believe that evidence has been presented that would indicate that the costs of this change (which we believe are too high) outweigh the benefits. The working group should continue to refine this change to see how costs could be minimised. They should also conduct a more detailed analysis, supported by device manufacturers to understand what risks could arise in relation to maintenance these devices, what other mitigating actions could be taken to address these risks (and their associated costs) and what residual risk remains. This risk analysis should be undertaken on a collective basis rather than by individual parties.
Npower	Large Supplier	Yes	Yes, we believe the benefits far outweigh any costs.
Scottish Power	Large Supplier	No	We do not think SECMP0007 should continue, as the cost of implementation and the late delivery of the solution might well far outweigh any benefits. We also think that less costly, but equally effective, solutions are likely to emerge in the interim, which could be made available to customers in such circumstances.
SSE Energy Supply	Large Supplier	Yes	We do believe this should be progressed but we have significant concerns around interoperability that we believe should be discussed by the workgroup before progression. We recognise that this will require an effort across industry to identify potential issues, but on the basis of mitigating risks, this change is an appropriate capability to develop.

Question 6			
Respondent	**Category**	**Response**	**Rationale**
Utilita	Large Supplier	Yes	We do believe that this modification should be progressed, however we note that the costs seem high. This modification is in the interest of the customer and would also facilitate further innovation by facilitating future IHD/PPMID related modifications. However, it is very hard to evaluate whether this is a justifiable move from an economic standpoint. It is hard to predict whether other innovations will make IHDs/PPMIDs redundant soon. We remain uncertain of how much customers will use their IHDs, especially when considering certain prepayment demographics. Innovations in the payment space may also drastically reduce the usage of PPMIDs. Total costs (£7.3 million - £8.2 million. Rising to £10 million) seem high given that service requests already exist for ESME/GSME firmware upgrades. As DCC do not have any involvement in the creation of the firmware images, we struggle to see how adapting these messages for IHD/PPMIDs could cost up to £10million. We would like to request that the DCC to provide a full and transparent break down of costs before it progressed for voting to Change Board.
SSE Networks	Network Party	Abstain	SSEN will not derive any benefit from this change. We are therefore not able to provide a view regarding whether this modification proposal should progress.
Chameleon Technology	Other Party	Yes	This is a significant benefit that should definitely continue to be progressed.
TMA Data Management	Other Party	No	As mentioned in response to question 3, we are forced to reject the change despite the fact that it would be very beneficial. It is not the first time, we were in favour of SECMP004 and 008 but due to the cost put forward by the DCC, were left with no option but reject them.

Question 7: Do you have any other comments on the solution?

Including any impacts not identified by the Working Group as set out in the consultation document, any alternative solutions, and/or any other comments/questions that you would like the Working Group to consider?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	The diagram provided for the proposed Firmware update process for Images of 750kb or above, does not seem to match the text provided for the process: the text gives that the first Image (0x15) will "set the activation date-time as zero (i.e. 'active now')."", but the diagram does not contain the associated "Activation" step in the Device column. We would be grateful if the diagram could be update in order that this step being visible.
EDF Energy	Large Supplier	Yes	If this Modification is not progressed Suppliers are likely to seek alternative solutions to maintaining devices – one example would be deploying firmware updates to these devices via an internet connection (which is not precluded by SMETS). Any such solution would not be guaranteed to be interoperable and would not be subject to the security controls that the DCC provides. The DCC systems were always intended to be flexible to enable additional devices to be connected and additional services associated with those devices to be supported. The estimated costs provide by DCC indicate that this flexibility does not exist, and that development of their systems to support the emerging smart energy system is likely to have a very high cost. We are concerned that the costs of this and other modifications are likely to make evolution of the DCC systems cost prohibitive, and to drive Suppliers and other industry parties to seek alternative communication solutions that undermine the case for having a DCC. We note that HCALCSs are not currently within the scope of this Modification but it is not clear why this is the case. These devices are likely to be prone to some of the same issues

Question 7			
Respondent	**Category**	**Response**	**Rationale**
			as IHDs and PPMIDs; they are also permanent devices that need to be maintained over the whole life of the metering system. Consideration should be given to including these devices within the scope of this Modification.
Npower	Large Supplier	No	-
Scottish Power	Large Supplier	No	-
SSE Energy Supply	Large Supplier	Yes	-
Utilita	Large Supplier	Yes	We believe that this should have been part of the fundamental design. The infrastructure should allow for this, given that we are supposed to be providing a "smart" experience to consumers. Needing to visit a property to update software on a Device seems like the opposite of a smart experience. If this modification is not implemented, we note that Suppliers deploying IHDs will be at a disadvantage compared to those who may be able to provide a richer experience via wifi enabled devices. Those deploying wifi enabled devices are still likely to be at an advantage, regardless, given the speed of the DCC network.
SSE Networks	Network Party	Yes	SSEN seek further information regarding how this modification will impact the ongoing capacity management process and its ability to deliver an E2E solution including the Communication Hubs potential constraints. SSEN remain concerned regarding the high costs associated with changes to central systems to deliver modifications. The scale of cost associated with system changes will inevitably lead to many modifications "failing" and stifle innovation. Failure to innovate will ultimately lead to reduced benefits realisation and poorer customer service.
Chameleon Technology	Other Party	Yes	A solution that used the OTA capability as described in the ZigBee specification (with no added requirements) would be the simplest to implement and deploy from our point of view

Question 7			
Respondent	**Category**	**Response**	**Rationale**
			and would be our preferred solution. At the cost of slight increase in comms hub complexity, a less bespoke solution can be provided on the IHD/PPMID devices.
TMA Data Management	Other Party	No	-

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'

Annex G

Second Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the second SECMP0007 Refinement Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	Yes	We support the functionality provided by the solution put forward, subject to suppliers providing reassurance that excluding an IHD solution will not significantly affect their service provision for a significant number of consumers.
Shell Energy Retail	Large Supplier	No	The Modification report concludes that CADs were excluded from scope. However, it is not clear that consideration of the solution scope for OTA firmware updates included combined PPMID/CAD units, where the upgrade path to both PPMID and CAD firmware via the internet is a working and viable solution. Although such an upgrade path is not 'local', the rationale for banning local firmware updates as a result of this modification could be assessed as including upgrading firmware via the CAD capability. We would welcome clarity on this point and trust that the intention of banning 'local' upgrades does not remove upgrading via CAD in a combined PPMID/CAD unit.. The timescales to successfully implement the proposed solution once this SEC Mod is approved mean that suppliers could be actively using the CAD route as the firmware upgrade path. We also note that excluding the CAD upgrade path increases the risk of unsuccessful firmware upgrades using the proposed route (via the Comms Hub), with all traffic being sent over a congested and (at the moment, and possibly enduring?) unreliable delivery method, to the shared limited buffer space on the Comms Hub. We expect that work to make this solution 'fit for purpose' will be many years in the making, across Comms Hub variants and CSP regions. Exclusively placing more volume on this single approach, by banning a viable and working OTA firmware management process using CADs is misplaced.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			One of the assumed benefits of the proposed solution is that it provides for reliable and up to date information of the firmware versions held in the SMI. Our experience is that this aspect of the current firmware solution, which the proposed solution relies on, is not reliable, and due to process issues, result in device firmware that has been upgraded via OTA but has not been updated in SMI, which still holds the 'old' firmware version. It has been necessary to run SR11.2 (Read Firmware Version) to validate the device firmware version and update SMI accordingly. We believe that it could be acceptable to require Suppliers to ensure that SMI has been updated following a firmware upgrade (if not already a SEC requirement) by always running SR11.2 as a matter of process, with this obligation applying regardless of upgrade mechanism (for example, via the Comms Hub, as proposed, or via the CAD, as currently). We would ask that the proposal is considered by Alt HAN Co and their vendors to assess the impact on supporting this additional firmware upgrade traffic across its developing solutions and HAN-extending devices, for a more complete impact assessment. We think that more weight should be given to the TABASC view that longer-term use of the proposed solution would be undermined by new technology, and recognised in a cost benefit assessment to inform whether this modification can still be justified.
SMS Plc	Other SEC Party	Yes	SMS agrees with the implementation of this solution
DCC	Other respondent	-	We do not have an opinion on this, as we are directed by the Working Group
Chameleon Technology	Other SEC Party	Yes	The proposed solution will allow future PPMID/HCALCS devices to be kept up to date with security/functionality improvement after deployment. It will also allow a significant percentage of devices that have already been installed to gain the same benefits.
Npower	Large Supplier	Yes	We are supportive of this modification and we believe it's the right thing to do. We

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			are concerned at the level of DCC costs involved with the investment of this modification
TMA Data Management Ltd	Other SEC Party	Yes	-
E.ON	Large Supplier	Yes – providing the below is met	Agree that the Zigbee OTA route is needed for SMETS2 PPMIDs, and HCALCs to be via GBCS Critical Commands. SMETS2 IHDs can be discarded if the cost savings are worthwhile in doing so. The ability to OTA SMETS1 IHDs post Enrolment and Adoption must be unaffected, and suppliers must still be able to roll out a firmware update OTA once enrolled and adopted and SECMP0007 is implemented. DCC must provide clarity on this.
Scottish Power	Large Supplier	Yes	The solution will allow the PPMID functionality to be updated without need for a site visit and replacement of older units. In particular, if a gap in functionality is found for prepayment customers such upgrades may prove necessary. The solution in terms of CH notifying the PPMID of the availability of the image and activation on download means that all existing units in the field will be upgradable. The units we have installed have this capability built in, though it has not been tested as yet. De-scoping the IHD from the OTA process means a simplification in the DSP changes, with a potential cost saving and reduced delivery risk. The IHD is not currently in CPL and has reduced validation in the DCC inventory, so not requiring this "fix" reduces complexity.
SSE	Large Supplier	Yes	We require the ability to upgrade firmware OTA on the devices referenced (PPMIDs/HCALCS), to minimise the potential of stranded assets or the need to visit the site locally for resolution activity, with resulting impacts on the consumer. We have raised points for clarification in response to Question 10.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			In our response to Question 6, we set out our view that there needs to be further investigation undertaken by the working group to understand the proportion of installed devices that may or may not be capable of firmware upgrades.
EDF	Large Supplier	Yes	We agree that the proposed solution seems appropriate. It is our understanding that some existing installed devices, and specifically some PPMIDs, have the capability within that device to accept and process a firmware upgrade; however the ability to send such a firmware update is not present in the DCC systems. Device manufacturers need to be engaged in the detail of this solution in order to ensure that the proposed solution will be compatible with their existing devices, and would therefore enable devices installed before this SEC Modification is made to be upgraded once the Modification has come into effect. This is necessary to maximise the benefits to be gained from making this change, and minimise the number of devices that would remain exposed to the risk of stranding. If this is not done then every PPMID or HCALC installed before this change comes into effect is exposed to a significant risk of being stranded should the version of SMETS they are compliant with have a Maintenance Validity Period (MVP) end date set. We note that BEIS have recently consulted on designating an end date for SMETS2v2 that would impact PPMIDs and HCALCs compliant with that version of the Technical Specifications. BEIS have decided not to implement the proposal to implement that MVP at this time specifically as a result of the concerns about the impact on the compliance of PPMIDs and HCALCs.
Smartest Energy Ltd	Small Supplier	Yes	The proposed solution will allow all affected parties to allow their customers better manage their energy usage by using the most-up-to-date versions of their devices. This could also see the development between Supplier and Meter Manufacturer's when discussing possible triage solutions (should issues present themselves).

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Green Energy Options Limited	Other SEC Party	Yes	1. geo strongly supports the introduction of a DCC firmware upgrade process for HAN connected devices. This is for three principle reasons (there are others too): a. IHD/PPMIDs have always been valuable consumer engagement devices and the ability to upgrade these to apply enhanced feature sets over time is a sensible way of getting additional value out of the asset being provided as part of the mandate. b. There are several reasons why IHD/PPMIDs could become stranded assets if enhancements to meter/CH firmware are made of which the IHD/PPMID is unaware, both at a ZigBee cluster level and also with respect to (currently unforeseen) security patches. c. The alternative to OTA upgrades to HAN devices is either to send a field operative to each site (clearly very expensive) or a return to base for reprogramming (which has a low level of success through logistical complexity and consumer inertia).

Question 2: Will there be any impact on your organisation to implement SECMP0007?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	No	Implementation of the modification will not impact Citizens Advice. However, delay to implementation and a continued lack of capability to carry out OTA firmware updates to mandated HAN Devices creates risk that Devices which are not currently OTA upgradable may lose their functionality. The impact on consumer engagement with their smart meters, capability to top-up a PPMID and manage load will cause detriment to consumers. Depending on the scale of the impact, Citizens Advice Consumer Service is likely to have increased correspondence with consumers about these issues.
Shell Energy Retail	Large Supplier	Yes	Development of new adaptor process orchestration, testing and operational monitoring and exception management procedures.
SMS Plc	Other SEC Party	Yes	Commercial contracts with IHD/PPMID manufactures will need amending. Mainly around delivery of releases, level of testing and assurance.
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	No	Subject to some details laid out in the response to Question 8, the proposed solution is already being used within our devices – the proposal extends support for this to the rest of the system.
Npower	Large Supplier	Yes	-
TMA Data Management Ltd	Other SEC Party	Yes	There might be some system changes required, expected to be small.
E.ON	Large Supplier	Yes	The implementation of this modification will result in changes to:

Question 2			
Respondent	**Category**	**Response**	**Rationale**
			• IT infrastructure to deliver the additional SRs required; • Operational Processes that can be modified to benefit from this capability; It must be highlighted that while the ban on local upgrades to PPMIDs will come into effect once SECMP0007 is implemented, the capability to do so will still exist within the assets that are already deployed, unless a new firmware image to disable local OTA is developed by manufacturers and deployed. Whilst this capability may still be there, E.ON will not be intending to use it once SECMP0007 is implemented.
Scottish Power	Large Supplier	Yes	As PPMIDs cannot currently be upgraded by OTA, the functionality is not part of our backend IT solution. We will therefore need to design, build and test the change in our system. If the cost of implementing the Modification is as high the PA indicates it might be, it will require careful budgetary planning. Moreover, we would highlight that we are still to be advised of other potentially high cost 2020 SEC Modifications, which may also impact our financial planning.
SSE	Large Supplier	Yes	Implementation of this modification will have an impact upon systems and processes within our organisation. There will be a need for significant testing for every combination of newly upgradeable HAN Devices with all Comms Hubs.
EDF	Large Supplier	Yes	We will be impacted should SECMP0007 be approved for implementation. It is, however, very difficult to isolate and identify the impacts of making any one change as these changes will be made as part of a wider change to the Technical Specifications. We will incur a significant cost for moving to any new version of DUIS, or the device Technical Specifications – the specific impacts associated with individual changes within those new versions is incredibly difficulty to identify.

Question 2			
Respondent	**Category**	**Response**	**Rationale**
			Any new version of the Technical Specifications will have the following impacts, amongst others: • Engaging with device manufacturers to procure devices compliant with the revised versions of the Technical Specifications • Testing of existing devices that are deemed compatible with the revised versions of the Technical Specifications • Testing of the new devices to ensure they are compliant • Operational transition from installation of the previous version of devices to the new version • Design build and test changes to our internal systems to comply with the new version of DUIS • Regression testing of the new version of DUIS against current. • E2E testing of the new version of the DUIS in the DCC UIT environment • Transition to the new version of DUIS • Post-implementation support for the new version of DUIS
Smartest Energy Ltd	Small Supplier	Yes	• Refinement of current internal Firmware Upgrade process • DCC forecasts to be amended to reflect Firmware Upgrade SRs more regularly and not according to when is the most cost affective time to do so
Green Energy Options Limited	Other SEC Party	Yes	The degree of implementation effort required will depend on the technical solution adopted, specifically how firmware update notifications are notified and how larger image sizes are handled. This should be subject to discussion at a working group meeting.

Question 3: Will there be any impact on your organisation with the exclusion of In-Home Displays from the proposed solution?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	Yes	Consumers that will not receive OTA firmware updates to IHD's need to be provided with an alternative solution. Depending the number of consumers affected and the form of alternatives available, consumer trust in the rollout could be affected.
Shell Energy Retail	Large Supplier	No	We fit PPMIDs
SMS Plc	Other SEC Party	Yes	If a batch of IHD's with old firmware is in stock, Suppliers will choose the latest. If there is no ability to upgrade firmware once installed – we could be in a position of having significant obsolete stock and a potential gap in the Supply Chain and subsequent roll out. This logic applies for industry change cut over too
DCC	Other respondent	Yes	We believe that DCC are required to support
Chameleon Technology	Other SEC Party	Yes	There will be no impact on future devices. However, IHDs that have already been installed that are technically capable of supporting this solution (from a device point of view) will be unable to be updated, leaving them unable to be supported through security/capability upgrades.
Npower	Large Supplier	No	-
TMA Data Management Ltd	Other SEC Party	No	The impact is likely to be the same with the IHD excluded or included.
E.ON	Large Supplier	No – providing SMETS1 IHDs remain	All E.ON SMETS2 customers will be benefit from this capability.

Question 3			
Respondent	**Category**	**Response**	**Rationale**
		unaffected from this proposal	DCC need to provide explicit confirmation that this proposal will not affect SMETS1 IHDs that have been enrolled and adopted into their systems, and the ability to OTA these SMETS1 IHDs remains.
Scottish Power	Large Supplier	Yes	Although most such Devices that we install are PPMID capable, we cannot guarantee that the same can be said for the Devices we gain. Nevertheless, we support the designed solution.
SSE	Large Supplier	Yes	We have assessed this to be a limited impact as we have low volumes in our estate of IHD-only devices, these will need to be managed separately with a different method. We are unable to independently quantify the potential impacts and projected volumes where we may gain a customer who uses an IHD. However, we believe this scenario could be effectively managed by offering a consumer a PPMID.
EDF	Large Supplier	No	We would not be impacted by the exclusion of In-Home Displays from the proposed solution. We, in common with a number of other Suppliers, are rolling out PPMIDs rather than IHDs. While these devices meet the licence obligations relating to IHDs, they are designated in the DCC systems as PPMIDs. In general we would regard the stranding risk associated with IHDs as being much lower. As Type 2 devices the security risk associated with IHDs is very low, and they are less likely to be impacted by any mandatory upgrade to resolve a security vulnerability. Supplier licence obligations also only require the IHD to be compliant with the relevant version of the Technical Specifications for 12 months after it has been provided. PPMIDs and HCALCS are Type 1 devices, and Supplier are obliged to ensure they remain compliant with a valid version of the Technical Specifications for the whole of the time they are installed. They also have 'active' functionality that has the potential to change over time, unlike IHDs which are 'passive' devices'. The likelihood of such devices needing to be

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			upgraded is far higher, and the risk of stranding them if this is not possible is exponentially greater than for IHDs.
Smartest Energy Ltd	Small Supplier	Yes	We are a supplier that does not off Pre-Payment services as a method of payment. This means that we will only be offering customers IHD's.
Green Energy Options Limited	Other SEC Party	No	-

Question 4: Will your organisation incur any costs in implementing SECMP0007?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	No	As discussed, there are risks associated with delay to a solution for Citizens Advice and for consumers.
Shell Energy Retail	Large Supplier	Yes	SWAG Capex £300K; Opex £75K
SMS Plc	Other SEC Party	Yes	Resource – managing the due diligence of a higher frequency of change to IHD firmware. Logic being that if an IHD manufacture has the ability o change remotely and fix a vulnerability/issue of increase or improve functionality. They will do so, and more often.
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	Yes	As we have already implemented the proposed solution, our extra costs will be minimal, covering only the additional end-to-end testing that comes from having the rest of the system support the capability. While we would not achieve any direct cost savings, we would experience a dramatic reduction in the risk of our product irrecoverably failing in the field (either through fault of our own or due to changes to the rest of the deployed equipment), which would be a material benefit.
Npower	Large Supplier	Yes	We will incur significant costs, if this modification was implemented and we would require further analysis of the costs. We will also incur our own internal costs as well as the DCC costs.
TMA Data Management Ltd	Other SEC Party	Yes	Likely to be low cost.

Question 4			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes	E.ON are likely to incur costs due to changes stated in Question 1, these are hard to quantify until we know exactly what modifications to our infrastructure is required. E.ON will benefit from this because there is the reduced risk of unnecessary cost, because fixes to PPMIDs can be applied remotely without the need for a physical visit to the property for exchange.
Scottish Power	Large Supplier	Yes	Our implementation costs are subject to a detailed impact assessment to be carried out internally if/once this Modification is approved; however, we fully expect to save on costs of site visits and PPMID replacements by its implementation, and would note that, conversely, these would translate to cost impacts if the proposal was not implemented. Nevertheless, at this relatively nascent stage it is not possible to identify the likely extent of costs or savings as these will only become clear once a reasonable canon of empirical knowledge has built up. At this stage it is also very difficult to assess the impact that alternative smart technologies could have: e.g. smartphone apps may be preferred to a static IHD.
SSE	Large Supplier	Yes	As per our response to Question 2, there will be costs associated with System and process impacts, with significant testing for every combination of the newly upgradeable HAN Devices (PPMIDs/HCALCS) with all Comms Hubs. The extent of the costs to be incurred is difficult to ascertain until we receive the confirmed proposed solution. There could be ongoing costs where we offer a customer a PPMID to replace their SMETS2 IHD. This would be dependent on factors, that cannot be independently quantified, such as the IHD volumes deployed and potential churn.
EDF	Large Supplier	Yes	As noted in our response to Question 2 it is very difficult to isolate and identify the impacts of making any one change as it will be made as part of a wider set of changes to the

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			Technical Specifications. We will incur a significant cost for moving to any new version of DUIS, or the device Technical Specifications – the specific costs associated with individual changes within those new versions is incredibly difficulty to identify.
Smartest Energy Ltd	Small Supplier	-	-
Green Energy Options Limited	Other SEC Party	Yes	-

Question 5: Do you believe that SECMP0007 would better facilitate the General SEC Objectives?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	Yes	This modification is critical to efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises (A). It is a method of facilitating energy consumers' management of their use of electricity and gas through the provision of appropriate information via smart metering systems (C). It will also facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy (E).
Shell Energy Retail	Large Supplier	No	Objective (a) cost effectiveness is finely balanced, and in our opinion is negative, given the costs; timescales to implement the fit for purpose solution; the volume of PPMIDs installed (with CAD capability) that will already be installed and using an alternative firmware upgrade path; and the unquantified HCALCS volumes, timing of availability of devices and the extent of actual usage of intended use cases.
SMS Plc	Other SEC Party	Yes	-
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	Yes	This solution allows key parts of smart metering infrastructure to be kept up to date without the need for a costly replacement. This will enhance the security of the system, and provide better assistance to the Energy Consumer in the management of their energy.
Npower	Large Supplier	Yes	We believe that should this modification be implemented it would better facilitate SEC objectives a, c, d and f as outlined within the modification report

Question 5			
Respondent	**Category**	**Response**	**Rationale**
TMA Data Management Ltd	Other SEC Party	Yes	-
E.ON	Large Supplier	Yes	We believe SECMP0007 facilitates the General SEC Objectives in line with the proposer; Objective A Enables PPMIDs to be operational and interoperable with the ever-developing meter firmware for the long term within Smart Metering Systems. Objective C Maintains the ability for the device to display information that Consumers can use to manage their use of electricity and gas. Objective D Industry aligned process for updating firmware on PPMIDs, in line with the processes for ESMEs and GSMEs. Objective F It can patch any security vulnerabilities that arise in PPMIDs in a quicker, more manageable fashion to current processes where this OTA is not available. This is also fundamental for the delivery of SECMP0056 to already deployed assets.
Scottish Power	Large Supplier	Yes	We agree that Objectives A & C will be better facilitated by implementation of SECMP007.
SSE	Large Supplier	Yes	Objective (a): We agree that SECMP0007 will better facilitate this SEC Objective as the proposed solution will provide an efficient and effective process for updating firmware on the PPMID and HCALCS. This will support the ongoing operation and interoperability of these devices and would avoid unnecessary cost expenditure relating to their replacement.

Question 5			
Respondent	**Category**	**Response**	**Rationale**
			Objective (c): We agree that SECMP0007 will better facilitate this SEC Objective as the modification would allow consumers to better manage their energy usage by having sustainable most-up-to-date Devices that provides them with energy related information. Objective (d): We believe that this proposal is neutral in terms of facilitating effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy. Objective (f): We believe that this proposal is neutral in terms of better facilitating the protection of Data and the security of Data and Systems in the operation of this Code.
EDF	Large Supplier	Yes	We strongly support this Modification and believe that it better facilitates General SEC Objectives (a), (c), (d) and (f) for the reasons detailed in the Modification Report.
Smartest Energy Ltd	Small Supplier	Yes	This modification better facilitates: Objective (a) – suppliers will/can avoid unnecessary costs replacing devices Objective (c) – having the most up-to-date software will help end users continue to better manage their energy
Green Energy Options Limited	Other SEC Party	Yes	The modification meets objectives a) c) d) and f) of the SEC objectives as noted in the consultation document. We would also wish to emphasise: • that there are as yet unresolved elements of IHD/PPMID functionality that will provide a better customer experience if a firmware upgrade is provided, for example, the treatment of import/export and local generation. This can be confusing to the user at present yet could be resolved in the future with an OTA upgrade. • Device manufacturers have been encouraged by government to use the smart meter infrastructure for additional services. Many will need to be supported by

Question 5			
Respondent	**Category**	**Response**	**Rationale**
			upgrades, particularly when DSR becomes a viable markets in the near future. The smart metering system will be branded as obsolete if it cannot support upgrades to more advanced HAN devices in the future.

Question 6: Noting the costs and benefits of this modification, do you believe SECMP0007 should be approved?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	Subject to value for money being established for the modification.	We are concerned by the costs being quoted by the DCC do not offer value for money following the 'SEC Mod and BEIS Mandated Change Review'. However, the modification represents important functionality that represents significant value to consumers and needs to be approved promptly.
Shell Energy Retail	Large Supplier	No	As previous rationale
SMS Plc	Other SEC Party	Yes	Benefits of the change will in turn out-weigh costs associated.
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	Yes	SECMP0007 should be approved as the costs to the industry as a whole to maintain the system through device replacement are prohibitively high compared to the costs to implement OTA capability.
Npower	Large Supplier	Not at this time	
TMA Data Management Ltd	Other SEC Party	No	The DCC costs estimated at 7.3 to 8.2 M make it difficult to see that SECMP0007 will actually deliver benefits to the Industry.

Question 6			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Yes – providing clarity on the impacts of SMETS1 meet our concerns below	We believe this modification should be progressed providing that SMETS1 IHDs that will be enrolled and adopted into the DCC systems, and the ability to OTA these SMETS1 IHDs is still available.
Scottish Power	Large Supplier	Yes	Although the costs uncovered by the Preliminary Assessment are very high, we still believe these to be outweighed by the significant benefits of SECMP007. Nevertheless, we cannot yet quantify these benefits with any real accuracy. Therefore, noting the costs of SECMP007 in the context of a range of current proposals, we would caution that a degree of pragmatism is going to be needed in prioritising which, if any, of the current crop of modifications to implement.
SSE	Large Supplier	Yes	We are supportive of the intent of this Modification and the ability for Suppliers to upgrade firmware on HAN Devices. We believe there does need to be a solution to upgrade PPMIDs and HCALCS. However, we believe the working group should undertake further investigation to understand the existing capability and planned development of PPMIDs and the future capability of HCALCS. For those devices that currently do not have upgrade capability, we would need to understand the timescales where Device Manufacturers would be developing their products to meet the required capability to OTA upgrade. Given the high volume that would be deployed before these become commercially available, there needs to be further analysis to understand the proportion of devices across Industry that would or would not be capable of being upgraded.

Question 6			
Respondent	**Category**	**Response**	**Rationale**
			Given the indicative costs of this modification, we would support and welcome a rigorous approach to Cost Benefit Analysis. We recommend that the working group engages with Device Manufacturers to gain an understanding of the existing/future capability and determine volumes that could be deployed over the timeline leading up to the implementation of this modification.
EDF	Large Supplier	Yes	We strongly agree that this Modification should be approved, and implemented at the earliest possible opportunity. The volumes of devices, and especially PPMIDs, that are being installed means that the stranding risk associated with such devices is very significant, and will only increase as the rollout accelerates. We have already seen proposals from BEIS to end the MVP for the current version of SMETS which would make the PPMIDs that have been provided to date non-compliant, and in need of replacement. Assuming an average cost of £15 to £25 for a PPMID, the cost of replacing a million of these devices (which we believe is a conservative estimate) is going to be £15million to £25million, easily outweighing the costs of making this change. That in itself is a conservative estimate, and does not take into account additional costs associated with returning and replacing devices, or site visits to provide and install the replacement devices. While we believe that there is a strong business case for making this change, we would still like to see the costs that have been estimated by the DCC reduce significantly. We struggle to see how the DCC costs for implementing this change could be in the region of £10million, this needs to be reduced as far as possible and unnecessary cost eliminated. Should this change not be progressed, it is likely that alternative 'unofficial' routes might be sought to enable devices to be upgraded and avoid the stranding risk; for example through an internet connection to the device. Such an outcome would create numerous problems in regard to the ability to manage firmware upgrades, and understand what version of

Question 6			
Respondent	**Category**	**Response**	**Rationale**
			firmware a device is compliant with. Such solutions would also not be interoperable, and only accessible to the Supplier that originally provided the device.
Smartest Energy Ltd	Small Supplier	Yes	Even though the DCC costs are consistently high, it should still be approved as this modification will have the same process for all parties that will be affected across the industry. The change will also prevent SmartApp providers charging suppliers to upload a new Firmware Image when the firmware image is provided to suppliers free of charge.
Green Energy Options Limited	Other SEC Party	Yes	-

Question 7: How long from the point of approval would your organisation need to implement SECMP0007?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	-	-
Shell Energy Retail	Large Supplier	12-15 months	Design, development, and testing in line with other smart metering product roadmap priorities, and third party adaptor release cycle, subject to DCC alignment and provision of solution in UIT-A environment (our timescales assume early availability) recognising DCC's cited 6-12 month lead time.
SMS Plc	Other SEC Party	In line with change, given notice of <2 months	-
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	0	Our products already support the proposed solution.
Npower	Large Supplier	6 months minimum	-
TMA Data Management Ltd	Other SEC Party	4 to 6 months	-
E.ON	Large Supplier	<6 months from SEC Mod approval. But	Minor changes would be required for our IT infrastructure to implement this proposal once it is delivered by the DCC.

Question 7			
Respondent	**Category**	**Response**	**Rationale**
		to be phased with DCC delivery for testing.	Procedural changes can be developed once approved and delivered in line with DCC delivery. Capability will need to be tested internally before we deploy this for our live customers.
Scottish Power	Large Supplier	1 year	There are a significant number of changes on going at the present time, such as the R2 transition and SMETS1 Enrolment and Adoption. Moreover, the 2020 Mod drops promise further changes that may also impact our systems; though as they are still going through the refinement process we do not yet have a full view of these. Given such levels of change, each competing for the same valuable resources, we do not anticipate changes being fully tested and implemented within a short lead time.
SSE	Large Supplier	At least 12 months lead time	Difficult to ascertain until we get the exact proposal; we would need at least 12 months to undertake the required changes to System and process impacts and the testing for every combination of the newly upgradeable HAN Devices with all Comms Hubs.
EDF	Large Supplier	12 months (although this could potentially be 6)	The amount of lead time required largely depends on the amount of change required to devices to support the new functionality. As noted in our response to Question 1 we understand that many existing devices are already capable of supporting firmware upgrades. If this is the case and existing devices are capable of being made compliant with the revised Technical Specifications then this would reduce the lead time required for our implementation.
Smartest Energy Ltd	Small Supplier	N/A	This will be dependant on the new number of SRs introduced and what impact these may have on forecasts.
Green Energy Options Limited	Other SEC Party	3 months	-

Question 8: Do you agree with the proposed implementation approach?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
Citizens Advice	Other respondent	-	As outlined in question 6.
Shell Energy Retail	Large Supplier	Yes	If business case can be justified and agreed before 5 Nov 2019
SMS Plc	Other SEC Party	Yes	Date for implementation as part of the release is agreed as long as no other elements of the release have the potential to cause negative impact. Testing of this would be beneficial.
DCC	Other respondent	-	-
Chameleon Technology	Other SEC Party	Yes (with comments)	The solution (from the point of view of our PPMID devices) uses the widely understood and tested ZigBee standard, which is expected to support existing and future devices. However, there is some lack of clarity over how the success of the upgrade is communicated back to the comms hub. The "Proposed Solution" states that after a timeout the comms hub reads back the version. The DCC response sometimes describes a mechanism whereby the PPMID publishes an event using a (presently unsupported) extra ZigBee mechanism and sometimes refers to the comms hub reading back the version. We would support either option, with a preference for the comms hub polling the device rather than the device implementing a new ZigBee cluster, on the understanding that the extra ZigBee mechanism could only be used by a device that had successfully received a firmware upgrade. In the case of a pre-existing device, it would be unable to be able to support this mechanism to report failures to update. In the case where the DCC-described mechanism of publishing events is used, the proposal does not detail the payload of the event – the earlier this can be specified, the sooner affected devices can support the change (even in advance of the capability being supported within the system as a whole).

Question 8			
Respondent	**Category**	**Response**	**Rationale**
			The PIA contains the text “The Great Britain Companion Specification (GBCS) will mandate the hardware version to avoid wasted downloads over the Home Area Network (HAN).” This should remain as an optional feature, to ensure already-installed devices see as much benefit from this as possible, if they have not implemented an optional feature in expectation of this modification.
Npower	Large Supplier	Yes	-
TMA Data Management Ltd	Other SEC Party	Yes	-
E.ON	Large Supplier	No	This needs to be delivered before November 2020. PAYG is likely to see increased volumes be deployed across the industry from Q4 2019, this will likely bring with it challenges and potential firmware/security issues with PPMID devices that we can’t yet see in testing. SECMP0007 needs to be delivered sooner to help industry deliver PAYG to its customers as smoothly as possible, and this capability is needed ASAP to ensure that customer faith in smart can be maintained because bugs with PPMID firmware can be deployed OTA without the need to inconvenience the customer with a site visit, just like meter firmware.
Scottish Power	Large Supplier	Yes	SECMP007 has been under discussion and refinement for a number of years now and we have reached a point where there is a compromise between cost, complexity and the need to deliver the solution quickly. We therefore believe it should be taken forward to full Impact Assessment as soon as possible.
SSE	Large Supplier	Yes	We agree with the proposed implementation approach. As per our response to Question 6, there needs to be further analysis to understand the implications to the PPMIDs volumes

Question 8			
Respondent	**Category**	**Response**	**Rationale**
			deployed, and their capability, in conjunction with the timeline to meet any implementation date.
EDF	Large Supplier	Yes	We agree with the proposed implementation approach. We also agree with the Proposer, Working Group members and the DCC that the implementation date for this Modification must be as soon as possible
Smartest Energy Ltd	Small Supplier	Yes	As this modification may potentially not affect us, the recommended implementation approach is fine.
Green Energy Options Limited	Other SEC Party	No	• We cannot support the prohibition of local upgrade and we very strongly wish to represent that this is NOT implemented. The only reason for preventing local upgrade would appear to be the reporting of firmware version which is triggered by the CH after the download of a new firmware image. We believe there are other ways to notify the Supplier of firmware version that can be resolved in a working group meeting to get round this. Our principle objections to this proposal are: a. The industry is being encouraged to make more of the HAN provided by the smart metering programme to add more functionality to households. This applies to combined PPMID/CAD devices as well as other feature sets over and above the mandate for an IHD. It is quite probable that these feature sets could rely on real time data and/or real time commands and that the devices require timed (and possibly rapid) upgrade. This may not be available from the Supplier controlling the SMS and may be required faster than the DCC SLA allows for. b. Some images for advanced functionality beyond mandated PPMID may be larger than the size the CH can handle c. There will be a cost associated with DCC services which need not be incurred with a local upgrade path.

Question 8			
Respondent	**Category**	**Response**	**Rationale**
			d. It is very likely that devices which support non mandated or CAD services will churn from Supplier to Supplier. In such circumstances the new Supplier may not be able to support an upgrade or may have no incentive to do so with any sense of urgency leading to customer frustration and likely stranded assets. This would bring unacceptable negative publicity to the smart metering programme and potentially loss of functionality that a consumer may be paying for if an upgrade becomes essential. • It is our view that local upgrade MUST be permissible in addition to OTA upgrade via the comms hub.

Question 9: How will the exclusion of In-Home-Displays impact consumers?

Question 9		
Respondent	**Category**	**Response and rationale**
Citizens Advice	Other respondent	We are not in position to take a stance on this question but refer to our answer to Question 2. We are likely to only support the exclusion of IHDs if the proportion of consumers affected will be very minimal. If this approach is approved we would encourage an industry agreed approach to address those consumers who are affected. This will help consumers to understand the process.
Shell Energy Retail	Large Supplier	Suspect limited as majority of Customers will expect, and industry innovations may drive, the use of new engagement and energy insight technologies, reducing the use and reliance on IHDs.
SMS Plc	Other SEC Party	-
DCC	Other respondent	-
Chameleon Technology	Other SEC Party	A small set of consumers with IHDs that are not also PPMIDs will be unable to receive security updates or functionality fixes which could potentially render their display unusable.
Npower	Large Supplier	No impact for our consumers
TMA Data Management Ltd	Other SEC Party	N/A
E.ON	Large Supplier	There will be no impact to E.ON's SMETS2 customers because our assets are PPMIDs. The savings of excluding SMETS2 IHDs need to be made known, so industry can decide if the values are worthwhile for exclusion. DCC needs to provide explicit clarity that SMETS1 IHDs that have been Enrolled and Adopted into the DCC should not be affected by the implementation of SECMP0007, and that suppliers will be able to OTA SMETS1 IHDs once enrolment and adoption has occurred, and SECMP0007 has been implemented.

Question 9		
Respondent	**Category**	**Response and rationale**
Scottish Power	Large Supplier	We note that the relevant supplier is only obliged to replace a faulty IHD if it is within its 12-month guarantee, leaving some potential for standalone IHDs to lose their functionality if the firmware cannot be remotely upgraded. We therefore believe a focus on PPMID OTA to be an acceptable compromise between cost and delivery timescale.
SSE	Large Supplier	We note the impacts set out in the modification report and agree these could result in impact to consumers. However, we believe that the impact to consumers can be mitigated by the offering of PPMIDs. We would be interested to understand the overall volumetric, where SMETS2 IHDs have been or will continue to be offered by suppliers, as this would impact the extent of the cost of this mitigation across Industry.
EDF	Large Supplier	As detailed in our response to Question 3 we do not believe that the exclusion of In-Home-Displays from the solution will have an impact on consumers.
Smartest Energy Ltd	Small Supplier	-
Green Energy Options Limited	Other SEC Party	In the SMETS2 environment, the exclusion of IHDs should not impact customers for any geo device. If the proposal for this modification is that OTA to HAN devices is unavailable on adopted SMETS1 devices, then this means any SMETS1 HAN device effectively becomes stranded. In our view this is unlikely to cause any consumer issue.

Question 10: Please provide any further comments you may have

Question 10		
Respondent	**Category**	**Comments**
Citizens Advice	Other respondent	-
Shell Energy Retail	Large Supplier	None.
SMS Plc	Other SEC Party	1. Will the implementation of this change be completed in a phased approach and testing completed after each stage to ensure there are no issues or will this be a big bang approach. 2. Will workaround be put in place in event change does not go to plan and how will it be rolled back? 3. After implementation - The document provides many details on how on firmware will be able to be uploaded to the devices, how will these patches etc be rolled back in the event of any issues – can this please be confirmed and has this been considered
DCC	Other respondent	-
Chameleon Technology	Other SEC Party	There are small but significant implementation details that need to be addressed (see comments to Question 8). However, these should not slow the progress of this modification. It is significant that any solution that is selected is supported by as many existing devices as possible, and decisions should include consideration of this.
Npower	Large Supplier	N/A
TMA Data Management Ltd	Other SEC Party	-
E.ON	Large Supplier	Every potential cost saving measure should be explored by the DCC to test and deliver the agreed approach, in line with other SECMPs that are currently being reviewed for delivery.

Question 10		
Respondent	**Category**	**Comments**
		A detailed breakdown of the costs for this SECMP should be made available from the DCC as these costs are excessive from initial assessments and beliefs.
Scottish Power	Large Supplier	We believe that the industry should be provided with a detailed justification of the high PA costs, as well as a route to challenge them at the Impact Assessment stage. There are questions of whether the Full Cost approach may be inflating the actual delivery cost, as overall the costs to the programme may be reduced materially if a number of such Modifications were to be bundled into a single drop.
SSE	Large Supplier	We note in the Risks/Assumptions (RD05) that DCC lists that there is concern CSP North may not be able to increase the amount of available radio channels for firmware download. We have separately been made aware, via the SMD+WAN Forum, that there are significant issues with existing OTAs using CSP North's infrastructure, which may require further investment from CSP North to meet its existing obligations. One of the proposals put forward to remedy this already includes extending the amount of available radio channels for firmware download. We expect this to have been resolved and implemented ahead of any implementation of this modification. Regarding the solution proposed in this consultation, we have a few points where we request clarification. These may impact the implementation of the proposed solution. We have extracted the relevant text (with reference) and this is included in italics with our points for clarification following that text. **Modification Report: Section 2 Background – What is the issue?** *"There is also a risk that Devices which are not currently OTA upgradable may lose their ability to communicate on the HAN if there is a ZigBee stack upgrade that needs to be applied to address, for instance, a security related issue."* As per our response to question 6, can this risk be quantified regarding the volume of PPMIDs that are not capable of being OTA upgraded?

Question 10		
Respondent	**Category**	**Comments**
		a) Those already installed; b) Those that will be installed until this Modification is implemented. What action(s) are being taken to manage and mitigate this risk? **Modification Report: Section 7 Discussions and development - Dual Supplier scenarios** *"DCC's second Preliminary Assessment would allow for either of the Responsible Suppliers, as according to the DSP's registration data, to submit the relevant Service Requests. The DCC will be required to notify all Responsible Suppliers at different stages of the Service Request processing."* We note from the Modification Report that dual Supplier requirements developed under "SECMP0024 Enduring Approach to Communication Hub Firmware Management" will apply to this modification. We have some queries on the proposed solution for this modification regarding definition of Responsible Suppliers and what they can do – noting variance between requirements for PPMID and HCALCS. How and where are dependencies between different SEC modifications being managed, to ensure that development and implementation is aligned?
EDF	Large Supplier	As noted above we strongly support this Modification and believe that the benefits outweigh the costs, although the costs do need to be reduced further. As we have noted the nature of changes to the Technical Specifications means that it is very difficult to accurately capture the impacts and costs associated with any individual change. This then makes any accurate cost/benefit analysis difficult. While we believe that SEC Parties are likely to take the same view as us and support this Modification, we need to ensure that we are able to present information to Ofgem, who will make the final decision, that strongly supports the progression of this Modification. In the absence of an accurate view of the costs, it will be challenging to put together a Modification Report that makes the benefits of making this change (and the risks associated with not making it) clear to Ofgem to support their decision

Question 10		
Respondent	**Category**	**Comments**
		making. We cannot afford for this change to be delayed, or worse rejected, because the benefits have not been made clear to Ofgem.
Smartest Energy Ltd	Small Supplier	Although we agree with Modification, we strongly believe **ALL** variations of IHD's should be included
Green Energy Options Limited	Other SEC Party	There are several issues about the upgrade process, the implementation of fragmented images and the reporting of firmware updates that require detailed discussion and agreement before the proposal will work acceptably for all PPMID devices. There is no reason why this cannot be achieved, but it will require full working group attendance to make sure it suits all parties' product sets.

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'

Annex H

Request for Information responses

About this document

This document contains the full non-confidential collated responses received to the SECMP0007 Request for Information.

Question 1: How many times would you expect to update the PPMIDs in your estate each year?

Question 1		
Respondent	**Category**	**Response and rationale**
OVO Energy	Large Supplier	The update of our PPMIDs in our estate is driven directly by the roadmaps of the Device Manufacturers. Their view has already been provided in that they do not plan to make more than 2 per annum. The issue we DO need to call out is that we have found the deployment of the new firmware has had to be managed in several batches, of significant sizes, over a relatively short period of time. This has had a success rate of about 60% first time upgrade and the remaining 40% have required continual attempts over time.
Chameleon Technology	Other SEC Party	As a manufacturer, it would be up to our customers how often to update the PPMIDs. However, we would expect to make updates for our products available twice a year for the first year after a product has been released, and then once per year for the following three years. This reflects the need for newer products to receive more support earlier in their lifetime – later updates would typically be to coincide with new features introduced with new versions of SMETS.
E (Gas and Electricity) Limited	Small Supplier	It is our expectation that the PPMIDs would need to be updated twice per year. This an estimate at present due to the small number of SMETS2 meter sets with PPMIDs. It is expected that the update would be completed in one batch.
SMS PLC	Other SEC Party	As we aren't the Energy supplier, we wouldn't control the schedules to update PPMID firmware. However, we would expect the firmware updates around twice a year and would typically expect suppliers to update them in a single batch following successful testing and small pilot.
E.ON	Large Supplier	Our forecast can only be based on what we know right now, combined with an estimation for the future. However, we expect that a security, interoperability, compliance or bug fix may be required once per year.

Question 1		
Respondent	**Category**	**Response and rationale**
		The expectation is that updates would be spread throughout the year, unless there is a specific security incident or compliance issue called out by the SSC.
Bulb Energy	Large Supplier	Bulb might expect to upgrade a PPMID firmware a minimum of twice in the first year after the PPMID's installation and then on an annual basis after the first to fourth year. Bulb would anticipate PPMID firmware upgrades would not be required after four years.
EDF	Large Supplier	Our expectation, based on the agreements with our device providers, is that we would have two maintenance releases for the PPMIDs in our estate per year. These releases would be intended to improve performance; support additional features introduced by the SEC change process (like CoT event detection) and resolve outstanding defects. Our assumption is that the PPMID specifications will remain broadly stable over time and that there will be no more than one new version each year comprising of relatively minor changes. Making multiple significant changes to PPMID functionality would require an additional number of updates to be sent.

Question 2: From your experience, how long do the PPMIDs you roll-out remain successfully connected to the Home Area Network (HAN)?

Question 2		
Respondent	**Category**	**Response and rationale**
OVO Energy	Large Supplier	Unfortunately, we have no visibility of a device 'falling off' the HAN until we actively attempt to communicate with it. The DCC, and SMiP, solution has not provided us the tool, including alerts, to do this any other way. It would require a constant 'ping' to establish what is connected and not a reason why it has been removed due to many reasons.
Chameleon Technology	Other SEC Party	Our understanding is that the vast majority of PPMID devices remain connected to the HAN once successfully installed. This is particularly true where the device is used as a tool for customer engagement alongside novel offerings, rather than as a box to tick as part of the smart metering mandate.
E (Gas and Electricity) Limited	Small Supplier	Our expectation is that the PPMIDs remain successfully connected to the HAN for at least 3 months. Again, period of time is estimated due to the small number of live meter sets however, it has impacted on a very small number of customers.
SMS PLC	Other SEC Party	We don't have access to data to answer this question although we generally see PPMID issues turn into full set replacements due to lack of fault-finding capabilities by engineers on-site
E.ON	Large Supplier	A request to the DCC TOC would provide statistics for industry-wide last comms to end-devices.
Bulb Energy	Large Supplier	Bulb's experience since 2018 indicates that PPMID connectivity on the HAN is reliable, save for consumer behaviour that might impact HAN connectivity eg. moving the PPMID too far from the ESME and CH.
EDF	Large Supplier	We do not currently proactively monitor PPMID connectivity and do not know how many PPMIDs are still switched on at the customer's premises. In theory it would be possible to obtain this information as a one-off exercise by sending a command to each PPMID we are aware of. That would take some time to set up as a one off bulk run and may incur some costs, but it could be done if required.

Question 2		
Respondent	**Category**	**Response and rationale**
		We have anecdotal evidence from the feedback we get from customer enquiries which suggests that for PAYG customers; engagement in PPMID use is quite strong for obvious reasons. For credit customers (where the PPMID is operating in the role of an IHD) we would tend to agree that it seems that, after the initial curiosity of having a PPMID, customer interest does wane over time. There is then a normal range of engagement from those that look at it regularly and tell us whenever there is a problem, to those that leave it on but don't really look at it, to those that have turned it off and never turned it on again and have put it in drawer. At a guess we would think only up to 50% of credit customers (probably less) use their PPMID. Historically suppliers (including EDF) have not necessarily offered PAYG products for SMETS1 meters, and the rollout of smart PAYG has been behind that of credit functionality. Previous experience around the connectivity of these devices may not be that instructive as we would expect the value of the PPMID to consumers to increase as a result of the increased penetration of smart PAYG products. Regarding our experience of OTAs to SMETS1 devices, the PPMID/IHD was always the last device in the SMETS1 OTA sequence and we never put out comms to customers in advance to ask them to turn them on to receive the update (which was noted at the Working Group meeting on 28/7/20). So, although we sent down the firmware upgrades to the PPMID/IHD we never really knew how many were turned on at the time, and even for those that were we only had confirmation that the firmware was successfully sent to the device but not that it actually was successfully applied to the device.

Question 3: Will your organisation incur any costs and/or realise any cost savings in implementing SECMP0007?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	Any solution that requires a new version of DUIS, and changes to the technical specifications, impacts us directly and there will be costs. We'd expect these changes to be implemented in at DCC Release so would be applicable to all the changes being made and not just these in isolation. The savings will be made in us not needing to physically replace devices due to them being out of date or correcting issues such as those faced in the North with the Alert storms. At this stage we have had little cause to re-issue devices out for firmware related issues and, as such, have an ever-growing portfolio of different combinations – over 35 – holding different devices on different Firmware versions. We have the details of all versions if required. This is unsustainable and cannot continue. The approx. cost of a PPMID is about £20 per device. Based on our portfolio and an issue / improvement / SEC Change comes in requiring the firmware to be upgraded, based on this being applicable to even 10% of our estate, equates to £1.1 million. Another example is, of our predominant device provider, we have 6 different firmware versions on the same model. To get them all up to the latest version, we would need to replace just under 50% of the devices, based on our portfolio would equate to £4.5 million… If, in the worst possible situation, we needed to upgrade just those on that model, would equate to £10 million. On just that model. In the period of 01/08/19 to 31/07/20, we sent out over 16,000 replacement devices. This equates to £320K in a year.

Question 3			
Respondent	**Category**	**Response**	**Rationale**
Chameleon Technology	Other SEC Party	Yes	As we have already implemented the proposed solution, our extra costs will be minimal. These mainly consist of the additional end-to-end testing that comes from having the rest of the system support the capability and Zigbee test house costs associated with the additional cluster; existing products/software already included this as part when verified at the test house. While we would not achieve any direct cost savings, we would experience a dramatic reduction in the risk of our product irrecoverably failing in the field (either through fault of our own or due to changes to the rest of the deployed equipment), which would be a material benefit. The cost of any action necessary by the industry to deal with in field units would be large as it would be a remedy cost per unit multiplied by the field population. The remedy cost per unit would include replacement unit costs, potential recovery costs and re-supply costs.
E (Gas and Electricity) Limited	Small Supplier	Yes	We will realise cost savings due to a reduction of engineer visits to customer homes in order to update PPMIDs. It is our expectation that the number of visits would reduce by around 10%. There is likely to be a cost to update our systems to allow for the service requests to be sent to the PPMIDs in addition to the current devices enabled. At this time, it is not possible for us to estimate the costs involved.
SMS PLC	Other SEC Party	Yes	SMS would incur additional costs due to following 3 points • We would need to add the facility for collating and distributing PPMID firmware to our partners • Would add complexity and additional testing into our SMETS2 Firmware Management service

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			• Agreements with PPMID manufacturers would need to be changed form a 1-time purchase to include a support model
E.ON	Large Supplier	Yes	There would be IT costs for providing the implementation, but as this should be similar to the existing implementation of firmware updates to meters, then the costs are not expected to be excessive. Cost savings realisation would be significant if we needed to go out to site and replace assets because of a firmware issue, or a compatibility issue with legacy PPMID firmware and either new Meter or new Comms Hub firmware. The costs would consist of:
Bulb Energy	Large Supplier	Yes	The PPMID is the part of the smart meter system that most visible and important to the customer, so Bulb would hope to realise reduced costs from a) a reduction in replacement PPMIDs where we have no ability at present to deliver a firmware improvement that could rectify the issue observed and b) a reduction in customer queries and contact related to observed PPMID issues. PPMID firmware upgrades will allow us to maintain and resolve known issues on the device (similar to meter firmware), whereas at present there may be no alternative but to replace the customer's PPMID at our own cost. Bulb would anticipate some minimal increased operational costs to manage the firmware of its PPMID estate.
EDF	Large Supplier	Yes	In terms of costs, we would not expect to incur significant additional cost as a result of this change. Our PPMID devices are already capable of processing firmware upgrades - it is just that the DCC is not able to send them. We do not expect to have to amend our device specifications as a result of SECMP0007. The main cost we would incur would be upgrading out back end systems to the new version of DUIS required to support the new/amended SRs required. We incur a pretty much fixed cost for each DUIS release, and

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			will they generally occur once a year. The incremental cost of each change within that new release of DUIS is minimal, especially in this case as this is broadly using the existing SRs that are used to send firmware updates to other devices. In order to try and get an accurate cost associated with delivering this specific change we would need to engage our service providers, we have not taken this step as we incur additional costs by doing so. Regarding operational costs resulting from SECMP0007, we have an established and quite fixed cost due to the need to resource for both the complexity of the SMETS2 firmware deployment processes, and the volume of new firmware releases by manufacturers requiring OTA activity. The operational cost impact for additional PPMID OTA activity would be marginal as in reality we would essentially be re-using existing processes and systems. The main benefit of SECMP0007 is going to come as a result of reducing the risk of PPMIDs becoming unusable, and being stranded as a result. In many cases, and especially where the PPMID is installed in premises where the meter is in prepayment mode, this will result in the PPMID needing to be replaced. … so the costs associated with this replacement can escalate quite quickly where an issue affects a large number of these devices. This cost is much higher if the PPMID needs to be provided in person by an installer and connected as part of a site visit. In most cases we are able to send out a PPMID by post and connect it remotely. Based on the volumes of such devices that are installed it would actually require a relatively low percentage of them to need to be replaced to get to a benefit equivalent to the costs that DCC are quoting to make the changes to their systems. Given the functionality of the PPMID, the type of issue that is most likely to arise is a security issue or vulnerability that would require all devices of a specific model or version to need to be disconnected from the HAN in order to protect the wider smart metering system. While it is relatively easy to quantify the impact of such a widespread issue arising, it is hard to know how likely it is that

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			such an issue, one that would require PPMIDs to be disconnected or suspended, would occur. It might be that the devices that were 'stranded' did not have to be replaced in all cases - where the PPMID is only operating as an IHD (i.e. for a credit customer) suppliers are only obliged to maintain the device for a year after providing it to the customer. However many suppliers would choose to provide a replacement device free of charge, and if they don't the benefits to be gained by consumers from having an IHD (as set out in the BEIS Impact Assessment for smart metering) would no longer be gained. The other key benefit of being able to upgrade firmware on PPMIDs is to resolve interoperability issues. Smart metering is a complex landscape with a variety of device types and device manufacturers all needing to work together. As much testing as you might do before you start to rollout devices, it is hard to identify all issues, and impossible to test devices with every possible combination of equipment that might be found in a customer's home. SMDA has found at least one issue where a PPMID and a meter have issues communicating with each other, but when either is paired with another manufacturer's device they both work fine. In this case both manufacturers could be construed as aligning to the technical specifications, but with a slightly different interpretation. These devices are already out in production. If the device that is 'at fault' is the PPMID is would be best to resolve that device, rather than having to apply a fix to the meter to make it work with the PPMID. The other benefit that exists for SECMP0007 but is hard to quantify is enabling customers that already have these devices to benefit from new or additional functionality that might be delivered through firmware. By not enabling devices to be updated through firmware you are saying that customers with installed devices can't benefit from any new functions or

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			capabilities unless they receive a new device – which would result in additional costs to either the customer or their supplier.

Question 4: Please provide any further comments you may have

Question 4		
Respondent	**Category**	**Comments**
OVO Energy	Large Supplier	Details of all our devices and versions is available if required but would be subject to commercial sensitivities so is not for sharing.
Chameleon Technology	Other SEC Party	The ability to keep all parts of a system updated is becoming a steadily increasing priority, as recognised in the DCMS Code of Conduct for IoT devices. Adopting SECMP0007 will ensure that the most customer-visible part of the smart meter roll out is able to receive updates, allowing it to stay secure and relevant throughout the lifetime of the system. Without this there is a risk to the industry that the device that is key to customer engagement could undergo enforced obsolescence due to some unforeseen issue in the future – whether that be a system security issue, or a change in user behaviour requiring new features. Trying to work around system or PPMID issues when the PPMID cannot be updated can lead to greater costs being incurred in the industry (utilities and DCC) than otherwise would be the case for resolving an issue and may not in some cases be possible.
E (Gas and Electricity) Limited	Small Supplier	E (Gas and Electricity) Ltd are in favour of this change.
SMS PLC	Other SEC Party	The industry will require some level of assurance that updating PPMID firmware will not cause issues with multiple different HAN combinations, including older Meter and Comms Hub firmware
E.ON	Large Supplier	In all the Working Groups attended by E.ON, there is a general consensus that this SEC Mod is definitely something the industry needs and should implement. In terms of the customer journey, OTA firmware updating is a much better prospect than a Meter Technician visit as it improves customer perception of the SMART program. In the future, HAN stability fixes could be provided with the functionality provided by SEC Mod 0007.

Question 4		
Respondent	**Category**	**Comments**
		The reduced environmental impact should also be noted in this SEC Mod (Savings on Landfill, CO2 from vehicles for customer visits etc).
Bulb Energy	Large Supplier	To support this modification, Bulb would like to see a simple process for obtaining firmware images between various PPMID manufacturers, which reduces commercial and operational complexity, so as to prevent a recurrence of the challenges faced by suppliers to obtain images necessary to deploy upgrades to SMETS2 devices in their estate.
EDF	Large Supplier	We have one comment on the legal text. The alert code for PPMID firmware activation is/should be 0x8F8B; however it is quoted as 0x88B in the draft DUIS changes

PPMID - Firmware Distribution Flow – DCC Data Systems

Other Responsible Supplier

Receive DCC Alerts

Service User (Sender)

Send Service Request 11.4

Receive Synchronous Response to SR 11.4

Firmware distribution in progress **(N59)**

Receive DCC Alerts

Devices rejected by CSP **N18, N19 N20 or N22**

Transfer to CH failed **N60**

Delivered To CH **N61**

Comms Hub Alert **N62**

PPMID Alert **N39**

Send Service Request 11.2

Firmware Version Updated **N49**

Receive Response to SR 11.2

DSP

DSP Validation Checks

Rejected Devices (DSP)

Return the list of Devices failed due to the following:
- **Invalid Devices**
- **Not Commissioned Devices**
- **Firmware not Applicable**
- **Another Firmware Update In Progress (NEW)**

- Create DCC Alert for the devices rejected by CSP.
- Write individual SAT entries for all the N19 Devices
- Determine the devices that passed CSP validation and create DCC Alerts to notify the Other Responsible Suppliers about a 'Firmware Distribution In Progress'

Create DCC Alert

Create DCC Alert

Create DCC Alert

- Create DCC Alert
- Update SMI

DSP Processing (Allows 11.2 to all SMETS2 PPMIDs regardless of the firmware version)

- If new firmware version is found updates SMI

CSP

Approved Devices (DSP)

CSP Validation Checks

Rejected Devices (CSP)

CSP Notification Failed to deliver to the Comms Hub

CSP Notification Delivered to Comms Hub

CSP attempts to deliver to Comms Hub

Approved Device (CSP)

Comms Hub

Device Alert from CH Failed transfer to Device

CH attempts to deliver to Device

Device Alert from CH Firmware Discarded or Overwritten

Sends **'UpgradeEnd'** Response for immediate activation

Device Alert from CH Transferred to Device

PPMID

PPMID receives firmware image

Sends **'UpgradeEnd'** Request

PPMID sends the version of the active firmware upon activation

PPMID returns the Active Firmware Vesrion

ESME, GSME, HCALCS - Firmware Distribution Flow – DCC Data Systems

Service User (Sender)

Send Service Request 11.1

Receive Synchronous Response to SR 11.1

Receive DCC Alerts

Devices rejected by CSP **N18, N19 N20 or N22**

Transfer to CH failed **N60**

Delivered To CH **N61**

Comms Hub Alert **N62**

Send SR 11.3

Receive Response to SR 11.3

Response

Send SR 11.2

Receive Response to SR 11.2

Response

DSP

DSP Validation Checks

Rejected Devices (DSP)

Return the list of Devices failed due to the following:
- **Invalid Devices**
- **Not Commissioned Devices**
- **Firmware not Applicable**
- **Another Firmware Update In Progress (NEW)**

- Create DCC Alert for the devices rejected by CSP.
- Write individual SAT entries for all the N19 Devices

Create DCC Alert

Create DCC Alert

Create DCC Alert

DSP Processing

- If firmware update is successful updates SMI

DSP Processing

- If new firmware version is found updates SMI

CSP

Approved Devices (DSP)

CSP Validation Checks

Rejected Devices (CSP)

CSP attempts to deliver to Comms Hub

CSP Notification Failed to deliver to the Comms Hub

CSP Notification Delivered to Comms Hub

Approved Device (CSP)

Comms Hub

Device Alert from CH Failed transfer to Device

CH attempts to deliver to Device

Device Alert from CH Firmware Discarded or Overwritten

Device Alert from CH Transferred to Device

ESME, GSME, HCALCS

Device receives firmware image

Device activates firmware and returns the status and firmware version

Device returns the Active Firmware Vesrion