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.

Paper Reference:	**SECP_75_1312_19**
Action:	**For Decision**

SECMP0007 Modification Report

1. Purpose

SECMP0007 'Firmware updates to IHDs and PPMIDs' is undergoing the Refinement Process. We are carrying out the assessment of the areas requested by the Panel; this paper provides an update on the developments on this proposal. We are recommending that this modification remains in the Refinement Process to resolve the remaining questions. However, we have prepared the draft Modification Report in Appendix A that shows the progress of this modification so far, as well as the detailed discussions that have taken place.

2. Summary of the proposal

What is the issue?

The Smart Metering Implementation Programme (SMIP) technical specifications currently capture Over-The-Air (OTA) firmware updates via the DCC to the Communications Hub, Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) only. Requirements for OTA firmware updates to mandated HAN devices are not captured. This modification seeks to provide the capability to update firmware OTA for In-Home Displays (IHDs), Prepayment Meter Interface Devices (PPMIDs), and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs) via the DCC's infrastructure.

What is the Proposed Solution?

The Proposer has agreed to progress with a combination of two OTA firmware update methods for mandated HAN devices:

OTA method for IHDs and PPMIDS

A ZigBee OTA delivery mechanism will be used to deliver firmware images to IHDs and PPMIDs. This method introduces the combined distribution and activation of the firmware updates into one single Service Request. The existing ESME/GSME method for distribution and activation of firmware cannot be utilised as this allows Suppliers and Devices to communicate end-to-end. As part of IHD/PPMID

OTA firmware method, the Communications Hub is to manage the activation of firmware and the notification to the Service User upon activation.

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. As with ESME and GSME firmware updates, distribution will be carried out via Service Request (SR)11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

3. Next steps

There are several areas of assessment outstanding, meaning we cannot yet fully complete the Modification Report. A draft based on the work so far is attached to this paper for information. We therefore believe that SECMP0007 should remain in the Refinement Process to allow this assessment to be completed.

DCC Impact Assessment

The DCC had advised that it will complete its first version of the Impact Assessment by the end of November 2019. However, we still have not received this. We note that the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC) have both requested to review the assessment, with the SSC also intending to carry out a risk assessment on the completed Impact Assessment response.

Refining the solution

Noting the Panel's request for a minimum viable product, SECAS, the DCC and the Service Providers are working together to identify elements from the solution that could be reduced or removed. We will ask the Working Group on 19 December whether any of these are viable. If any changes are made to the solution, the DCC has advised that it will need to undertake a second Impact Assessment.

Discussions on local updates

The TABASC Chair (who is also the TABASC representative on the SSC) has challenged the Proposer's and the Working Group's proposal to ban local firmware updates following the implementation of this modification. This is on the grounds that not allowing local updates may present unnecessary constraints on industry. The SSC will consider this at its next meeting on 11 December 2019 and the outcomes discussed at an ad-hoc SECMP0007 Working Group meeting on 19 December 2019.

4. Recommendations

The Panel is requested to:

- **NOTE** the update on the progress with SECMP0007; and

- **AGREE** that SECMP0007 should remain in the Refinement Process.

Joe Hehir

SECAS Team

6 December 2019

Attachments:

- **Appendix A:** SECMP0007 Modification Report
    - **Annex A:** SECMP0007 business requirements
    - **Annex B:** DCC Preliminary Assessment
    - **Annex C:** SECMP0007 legal text
    - **Annex D:** First Refinement Consultation responses
    - **Annex E:** Second Refinement Consultation responses

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 0.3

About this document

This document is the Modification Report for SECMP0007 'Firmware updates to IHDs and PPMIDs'. It provides detailed information on the background, issue, solution, costs, impacts and implementation approach. It also summarises the discussions that have been held and the conclusions reached with respect to this Modification Proposal.

Contents

This document also has five annexes:

- **Annex A** contains the business requirements for the proposed solution.
- **Annex B** contains the Data Communications Company (DCC's) full DCC Preliminary Assessment response.
- **Annex C** contains the redlined changes to the SEC required to deliver the proposed solution.
- **Annex D** contains the full non-confidential responses to the first Refinement Consultation.
- **Annex E** contains the full non-confidential responses to the second Refinement Consultation.

1. Summary

The Proposer of this modification seeks to address the lack of capability to update firmware Over-The-Air (OTA) for mandated Home Area Network (HAN) Devices via the DCC's infrastructure. The Smart Metering Implementation Programme (SMIP) technical specifications currently capture OTA firmware updates via the DCC to the Communications Hub, Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) only. Requirements for OTA firmware updates to mandated HAN devices are not captured.

This modification proposes a combination of two OTA firmware update methods for mandated HAN devices:

- **OTA method for IHDs and PPMIDS**

  A ZigBee OTA delivery mechanism will be used to deliver firmware images to In-Home Displays (IHDs) and Pre-Payment Meter Interface Devices (PPMIDs). This method introduces the combined distribution and activation of the firmware updates into one single Service Request.

  As this solution is intended for ZigBee capable Devices only, neither the DCC nor DCC Service Users can communicate directly with an IHD. Furthermore, 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 which do not facilitate OTA updates. Therefore, the existing ESME/GSME method for distribution and activation of firmware cannot be utilised as this allows Suppliers and Devices to communicate end-to-end.

  As part of IHD/PPMID OTA firmware method, the Communications Hub is to manage the activation of firmware and the notification to the Service User upon activation.

- **OTA method for HCALCSs**

  The HAN Connected Auxiliary Load Control Switch (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 Service Request (SR) 11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GB Companion Specification (GBCS) Critical Command.

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 mandated HAN Devices. The extent of these impacts has been drawn out through consulting with Smart Energy Code (SEC) Parties and relevant stakeholders. These impacts are summarised further in this report. The costs and implementation approach are not yet finalised.

2. Background

OTA firmware updates

Currently, the following SMIP Technical Specifications capture OTA firmware updates via the DCC to the Communications Hub, ESME and GSME only:

- SEC Schedule 8 'Great British Companion Specification' (GBCS)
- SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' (SMETS2)
- SEC Schedule 10 'Communications Hub Technical Specification' (CHTS)
- Commercial Product Assurance (CPA) Security Characteristics

Requirements for OTA firmware updates to IHDs, PPMIDs and HCALCSs are not captured in these documents or any others in the SEC.

What is the issue?

For several years, SEC Parties have advocated for the inclusion of an OTA firmware update procedure for mandated HAN Devices. Suppliers agreed that 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; and/or
- Site visits to locally update firmware or to replace/remove Devices.

The lack of an OTA firmware update procedure to mandated HAN Devices requires Suppliers to manage multiple processes and systems for updating firmware (OTA and non-OTA) on all smart metering Devices, with additional costs associated with this. 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. 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.

The Proposer notes that the lack of an OTA firmware update procedure to mandated HAN Devices limits the opportunity to maintain Devices or innovate them in the future. For example, as more and more updates are applied to EMSE/GSME, it becomes more likely the additional features may not be supported by IHDs, PPMIDs and HCALCSs on older firmware versions. Another example can be made with a Change of Tenancy scenario, whereby the previous tenant's consumption data needs to be wiped from their Devices. This could only be made possible to an IHD or PPMID via an OTA update. These risks and others like this will result in a negative consumer experience and will add a reputational risk to Suppliers and the SMIP. Considering these impacts, the overall benefits argument for smart metering will be lessened.

3. Solution

Proposed Solution

The Proposer seeks to amend the SMIP technical specifications and DCC Systems to include the capability to update firmware OTA for IHDs, PPMIDs and HCALCSs. The requirements for the proposed solution will be underpinned by the relevant SEC obligations and SEC Subsidiary Documents.

This modification, developed with extensive industry collaboration, proposes a combination of two OTA firmware update methods: one for IHDs and PPMIDs; the other for HCALCSs. The steps for each method are summarised below, and summary diagrams can be found in Appendices 3 and 4.

IHDs and PPMIDS

Once a firmware Image has been developed and gone through the appropriate assurance, the Supplier sends SR11.4 'Distribute Firmware to PPMID or IHD'. This will contain the firmware Image and the list of Extended Unique Identifiers (EUIs) of the target IHD/PPMID to the DCC. This would be a Non-Critical Command (a 'one-to-many' multicast).

In contrast to the ESME/GMSE OTA firmware update procedure, the Service Request will combine both distribution and activation within one action. Therefore, the Supplier does not need to follow-up with SR11.3 'Activate Firmware' for IHDs and PPMIDs.

Suppliers will also be able to set a future activation date for IHDs and PPMIDs, no more than 30 days from the date the request is sent. This is in line with the Anomaly Detection Threshold (ADT) requirements set by the Security Sub-Committee (SSC). If the Supplier does not specify an activation date, the firmware will be activated immediately.

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:

- The DCC will distribute the firmware to the Communications Hubs associated with the target Devices, with each hub recording the activation date/time for each target Device.
- The Device retrieves the new firmware Image from the Communications Hub using ZigBee OTA functionality.
- The Communications Hub will subsequently clear the Image from its memory block.
- After verification of the firmware, the Device performs the firmware activation.
- Ten minutes after the activation date/time recorded on the Communications Hub, the Communications Hub will query the Device firmware version.
- The Communications Hub will the send an Alert to the DCC with the firmware version which will subsequently be forwarded onto the sending the Supplier.

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. 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 through the introduction of additional Service Reference Variants for the following Service Requests:

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

The reason the HCALCS solution has taken this approach is due it being a load controlling Device and hence it contains Smart Metering Key Infrastructure (SMKI) Certificates. This means that to activate the firmware on the Device, it must be verified against the security credentials held on the Device. In this situation, activation must be carried out via a GBCS Critical Command. This cannot be achieved with the combined distribution/activation approach being utilised by IHDs and PPMIDs.

Implementation

The Proposer seeks to update the SMIP Technical Specifications for each of the three Devices at the same time. However, if phasing is considered more optimal then the order of preference could be with IHDs and PPMIDs in phase 1, followed by HCALCSs in phase 2.

The Proposer notes 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.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex C. This only includes the changes to SEC Schedule 8 ‘GBCS’. The remainder of the legal text will be provided once the DCC have completed its Impact Assessment.

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 as they should be. Therefore, a fit for purpose OTA firmware management process covering all mandated Devices would support Suppliers in delivering their obligation consistently. Further, it is proposed that all local firmware updates will be banned following the implementation of this modification. Therefore, Parties will only be able to carry out firmware updates OTA or by removing and replacing the Device.

In response to the first Refinement Consultation on this modification, several Supplier Parties advised that this modification would impact them in terms of changes to systems and IT infrastructure, as well as 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 greater capability to innovate with mandated HAN Devices.

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 IHD or 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

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

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 DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex B.

Data Service Provider

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

IHDs and PPMIDs

- Communications Service Provider (CSP) Smart Meter Wide Area Network (SM WAN) Gateway and CSP Interfaces;
- Changes to the Self-Service Interface (SSI) to enable the read inventory to include firmware versions ADTs;
- 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; and
- Transform – New GBCS Use case.

HCALCS

- DUGIDS documentation updates for SR11.1, SR11.2 and SR11.3;
- Updates to processing of these Service Requests;
- Support for 'Read Firmware' and 'Activate Firmware' on HCALCSs; and
- Changes to GBCS Use Cases.

Communications Service Provider

The proposed solution has several impacts across the CSP, the components of which are listed below:

IHDs and PPMIDs

- CSP North SM WAN;

- CSP/DSP Interfaces;
- Communications Hub functionality;
- Queuing priorities.

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 AD 'DCC User Interface Specification'
- Appendix AF 'Message Mapping Catalogue'

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, inability to update the firmware on a Device may lead to additional otherwise unnecessary replacement of working Devices.

5. Costs

DCC costs

The estimated DCC implementation costs up to Pre-Integration Testing (PIT) to implement are provided below. These costs are expected to change as the Proposer has opted to seek a solution utilising a combination of the two options provided in the DCC's Preliminary Assessment.

Breakdown of estimated DCC implementation costs (up to PIT)	
Solution Option	**Cost**
Option 1: Original Approach, Zigbee OTA Delivery	£12,300,000
Option 2: Extend Proven OTA Firmware Method for HCALCS	£8,500,000

More information can be found in the DCC Preliminary Assessment response in Annex B.

The costs for Systems Integration Testing (SIT), User Integration Testing (UIT) and implementing to live will be provided as part of the DCC Impact Assessment.

SECAS costs

The estimated Smart Energy Code Administrator and Secretariat (SECAS) implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

This modification will place costs on SEC Parties, the extent of which was investigated as part of the Refinement Consultation.

All SEC Parties who responded advised that they will 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.
- Significant cost for moving to any new version of DUIS, or the device Technical Specifications.

Some respondents also advised that they will 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.
- 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.

6. Implementation approach

Recommended implementation approach

SECAS is proposing an implementation date of:

- **5 November 2020** (November 2020 SEC Release) if a decision to approve is received on or before 5 November 2019.

The Proposer, Working Group members and the DCC agree that the implementation date for this modification must be as soon as possible.

As stated in the Preliminary Assessment response, the DCC requires a six-to-twelve-month lead time between the modification being approved and implementing the proposed solution. This modification has been seen as a candidate for inclusion in the November 2020 SEC Release, should it be approved in sufficient time. However, the DCC has indicated that this may not be possible. SECAS is investigating this further and will advise the Panel on any revised implementation approach following this.

7. Discussions and development

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 its 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 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 controlling load and have a more critical role than IHDs or PPMIDs. It agreed that there were no security concerns with including HCALCSs, adding that there is a greater security risk if HCALCSs are not capable OTA updates. However, it advised that HCALCS firmware must be activated via a GBCS Critical Command, since it is 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 IHDs in the field today are 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 from the solution 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 including IHDs 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.

Conclusions

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

Should PPMIDs be CPA Certified?

The Working Group questioned whether PPMIDs 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

The Working Group discussed the option of using local updates as a backup to OTA updates. The DCC suggested there should be a trust mode in place to update the SMI. Members discussed the option to create governance for this, but it was highlighted that this would involve added costs.

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 Smart Metering Inventory (SMI). This is due to the local update process which does not directly flow through the DCC's validation checks. Therefore, the DCC is unable to track these 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. This 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 wouldn't 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 subsequently update the SMI.

The Working Group raised a security concern with local firmware updates in that they could not be blocked if carried out locally.

Local updates were not considered further until after the DCC had completed its Preliminary Assessment.

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 believes that innovation will be severely curtailed if local updates to firmware is not permitted. It also noted the additional features that are being added to the PPMID and the need for more regular updates to these features. BEIS's recent funding granted to add functionality to the PPMID was noted as an example of this already happening.

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 some amendments to the current solution options for this modification, which would permit the use of local updates.

Proposal 1: Query Next Image Request

geo proposed that the Communications Hub take advantage of the information provided by the IHD/PPMID when requesting if a new Image is available. It suggested the Query Next Image Request is carried out once every 24 hours.

On receiving the command from the Device, the Communications Hub would extract the current firmware version and provide the data to the Head-End-System.

On power-up and after locating the Communications Hub, the Device would query if a new Image is available. Based on the Images currently stored on the Communications Hub, the hub would respond with either:

- No Image available; or
- Information concerning the image available for download by the device.

At the same time, the Communications Hub would record the Device's firmware version contained within the *Query Next Image Request* and send it to the DCC. Upon the DCC receiving the message from the Communications Hub, the SMI would be updated.

geo acknowledged a disadvantage in the 24-hour frequency of this request. The Communications Hub does not know what firmware version the Device is on. Therefore, when the Device carries out the Query Next Image Request, the Communications Hub will have to forward the firmware version of that Device to the DCC, even if it hasn't changed firmware version. The Working Group agreed that if every deployed IHD/PPMID were to carry out the Query Next Image Request every 24 hours, it could lead to an Alert storm for the DCC.

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 original concept the current proposed solution had been based upon. The Communications Hub has been envisaged to transfer firmware information, rather than store it for periods of time. Storing information would require development of additional functionality in the Communications Hub which would increase costs and complexity.

Proposal 2: Firmware Changed Alert

geo also proposed that on completion of a firmware update, 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. However, this would only be applicable to Devices that have the capability of sending Alerts to the DCC, by having the appropriate Device Certificates.

The Working Group advised that it had already rejected this idea due to the need for IHDs/PPMIDs to have to undergo CPA Certification and, in the IHD's case, have the relevant Device Certificates added. This would increase complexity, timescales and costs for SEC Parties.

Making sure authorised Parties can carry out local updates

SECAS explained the current firmware process whereby updates can only be applied by authorised Parties. 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 proposed solutions. It was noted that there is nothing to stop a Party from locally updating a Device with firmware not listed on the CPL. Furthermore, it could also 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.

DCC Assessments

The first Preliminary Assessment

The DCC provided a high-level Preliminary Assessment in May 2017 which provided a cost of between £7.3m and £8.2m to implement the modification. 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. It was also noted that there was limited information on how many IHDs and PPMIDs will be in use upon implementation, if this

modification is to be implemented. It was noted that some Devices may be replaced with applications on consumer devices 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.

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

In reference to Option 2, the Proposer questioned why, if a Device on the HAN is on the CPL, it should need to go through CPA. To go through the CPA procedure would considerably increase the costs on Suppliers to implement the proposed solution. A Device manufacturer agreed and advised that for their organisation, Option 2 could not be explored for IHDs and PPMIDs due to the CPA requirements. The Proposer and the Working Group agreed with this assessment.

The DCC was asked why it had explored Option 2 in the first place, with members noting they felt as though the Working Group's comments had been ignored. The DCC confirmed that it was not its intention to ignore the Working Group and that Option 2 had been explored as it believed it reduced the complexity of the solution and provided the Proposer with an alternative to the original approach.

Questions were also raised with the £12.3 million cost for Option 1 given in the assessment. 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?

Suppliers and Other Parties highlighted that the 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. This was 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 costs for Parties to undergo CPA under Option 2.

The Working Group advised that a breakdown of the costs is 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 them.

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, but it is still a possibility. A Panel member attending the Working Group agreed that this is true but that it does not, nor is it intended to, stop the DCC from estimating the costs as if the modification would be delivered as part of a wider scheduled SEC Release.

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, they 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 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 the IHD in the market.

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

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
2. Extend Proven ESME/GSME OTA Firmware Method for HCALCSs

It is expected that as part of the Modification Process and the Impact Assessment of the modification, the Technical Architecture and Business Architecture Sub-Committee (TABASC) will have a view on the optimal delivery approach for this proposal. That delivery approach could be delivering the two approaches at the same time or via a phased approach as captured above.

How will an IHD/PPMID firmware updated be initiated?

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. Each fulfils the requirement to combine distribution and activation into one command.

The DCC was in favour of using the SR11.1 for IHDs and PPMIDs, rather than creating a new Service Request for these Devices. The DCC believe that using SR11.1 will 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.

SECAS noted that SR11.1 does not already have the functionality to activate firmware. Furthermore, ESME/GSME/HCALCS and IHDs/PPMIDs are each following different procedures for firmware updates. Therefore, if SR11.1 were to be used for IHDs/PPMIDs, the DCC would have to be able to differentiate between these Devices and ESME/GSME/HCALCS firmware. It is for these reasons that SECAS propose 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 provided its view on which Service Request should be used. It noted its requirement for the DCC to be able to differentiate firmware updates to IHDs/PPMIDs from ESME/GSME/HCALCS firmware. This is to enable separate ADT values for IHDs/PPMIDs and ESME/GSME/HCALCS. The SSC therefore agreed with SECAS that a new Service Request for the combined distribution and

activation of IHD/PPMID firmware would 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 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 reference.

A Working Group member noted that the use of SR11.1 could be easier for the DCC to implement as it would only impact 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 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 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.

How far in advance can Users set the activation date?

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.

How will Firmware Images be managed?

Firmware Image size

The Working Group noted that HAN Devices have a limited capacity for holding larger firmware Images. A member pointed out that larger Images may slow down the HAN, although typically firmware Images for non-meter Devices can be smaller (in the region of 256-512 kilobytes (KB)). It was agreed firmware Images applied to a HAN Device would be limited to 750KB and that any higher

will require mechanisms in place to support fragmentation. However, there is nothing preventing fragmentation now, as long as the Device is built to support it.

The Working Group asked whether there will be a mechanism to delay the activation of the firmware Image. The DCC advised that there will be an option to specify activation 'date-time' in the Command and that populating this field as 'zero' will activate the Image immediately.

The Working Group questioned setting activation date-time to 'zero' with a fragmented Image when the first part of the Image is sent. 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. The DCC confirmed that both parts of the Image would be activated on the activation 'date-time' specified in the second Command. Manufacturers will provide guidance on how to activate multiple Images within a release note.

Rejected firmware Images

IHDs and PPMIDs

The DCC advised that a provision could be built in to the 'UpgradeEndResponse' Command from the IHD 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 for the HCALCS. SECAS confirmed that the Device would send a corresponding Alert to the appropriate Supplier.

Accepted firmware Images

Once the IHD/PPMID has successfully downloaded the Image, the Communications Hub would read the current firmware version on the Device. The Working Group agreed that this would be 10 minutes after the activation time.

The Communications Hub will then create a Device Alert containing the IHD/PPMID 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.

Failed firmware Images

It was noted that the Communications Hub can only communicate with the 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:

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 an ESME/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.

Failed activation

If the Image is successfully distributed to the Device, but it 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. However, the Communications Hub would not read the new firmware version unless it is told to, increasing the chance of a mismatch between the firmware version on the Device and on the SMI.

Supplier Alerts

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 have processed the Service Request to distribute the Image. The Alert would include a list of specific Device IDs, the Hash of the Image and the activation date-time specified in the Service Request.
2. The second Alert would be sent to all Responsible Suppliers with confirmation of distribution success or failure to the Device.
3. The third Alert would be sent to all Responsible Suppliers confirming the firmware version on the Device, 10 minutes after the activation date-time specified in the Service Request.

Dual Supplier scenarios

Dual Supplier scenarios were noted as having a significant impact. The DCC advised that the benefit of utilising Service Request 11.3 in the proposed solution was that Users would know who the Responsible Supplier for the given meter is. The Working Group advised both options given in the 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. 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 split Supplier scenario, both the Import and Gas Suppliers need to coordinate firmware updates. It is proposed that both Suppliers need to agree to proceed in the event that one Supplier wishes to deploy 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 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.

Communications Hub memory block management

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 and felt that this should be addressed under a separate modification. The Working Group agreed this would be the best course of action.

Device prioritisation

Firmware Images for IHDs, PPMIDs and HCALCSs will be stored in the same memory blocks as ESME and GSME firmware Images. This could lead to a scenario with an ESME or GSME Image arriving whilst both memory blocks are occupied with an IHD, PPMID or HCALCS Image. The Working Group agreed that ESME and GSME updates are of higher priority than IHD, PPMID and HCALCS updates. Therefore, the Image in process will be overwritten by the subsequent ESME/GSME Image.

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

An IHD, PPMID or HCALCS Image could arrives whilst another Image from one these Devices is in process. The Working Group agreed that if the memory blocks are occupied by one of these Devices, the Image on the Communications Hub will be overwritten by the subsequent Image. However, if the Communications Hub has already started the distribution of the Image to the Device, it can only be overwritten by an ESME/GSME Image.

Using one or both memory blocks

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

- Restriction of IHD/PPMID/HCALCS firmware to the ESME block only
- Use of both the 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 propose using both memory blocks on the Communications Hub without distinction. This would reduce the pressure on the WAN and avoid the need to invest in additional WAN capacity.

Suppliers raised concern 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. SECAS advised that the Communications Hub will send Alerts informing the Supplier whether firmware updates have been successfully transferred to the Device and been activated successfully or not. 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 it plans to add functionality to the DSP, flagging when firmware updates are in progress. They could use this information to notify the Service User if there is an update in process, preventing firmware Images from being overwritten.

Pending firmware Images

In relation to the ‘failed firmware Images’ section above, SECAS noted the DCC’s proposal to prevent Images blocking a memory block indefinitely. In this scenario, the Image would in effect be ‘pending’. The DCC proposed a two-day service level agreement (SLA) for which an Image can remain on the Communications Hub 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're eventually overwritten anyway. 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.

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

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.

8. Conclusions

Benefits and drawbacks

The benefits and drawbacks of this modification will be assessed once the impacts of the solution have been confirmed in the Refinement Process.

Proposer's rationale against the General SEC Objectives

Objective (a)[1]

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)[2]

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)[3]

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)[4]

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.

[1] To facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.
[2] 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.
[3] To facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy.
[4] To ensure the protection of Data and the security of Data and Systems in the operation of this Code.

Working Group members' views

The views of the Working Group will be summarised once the impacts of the solution have been confirmed in the Refinement Process.

Sub-Committee views

Views of the SSC

When the full proposed solution is available, the SSC intends to conduct a security risk assessment to confirm that any security risks have been mitigated.

Views of the TABASC

As part of the Refinement Process, the modification was presented to the Technical Architecture and Business Architecture Sub-Committee (TABASC) for consideration. The TABASC questioned the longer-term use of the proposed solution, due to new technology being made available to Consumers in the future (i.e. CADs), noting that new technologies may reduce the usage of IHDs and PPMIDs. The TABASC expressed the importance of the Working Group exploring alternative solutions and suggested that a cost benefit analysis should be a key focus during further refinement.

Appendix 1: 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 Thresholds
BEIS	Department for Business, Energy and Industrial Strategy
CAD	Consumer Access Device
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 Service 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
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
SMS	Smart Metering System
SR	Service Request

Glossary	
Acronym	**Full term**
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
UIT	User Integration Testing
ZCL	Zigbee Cluster Library

Appendix 2: Timeline of events

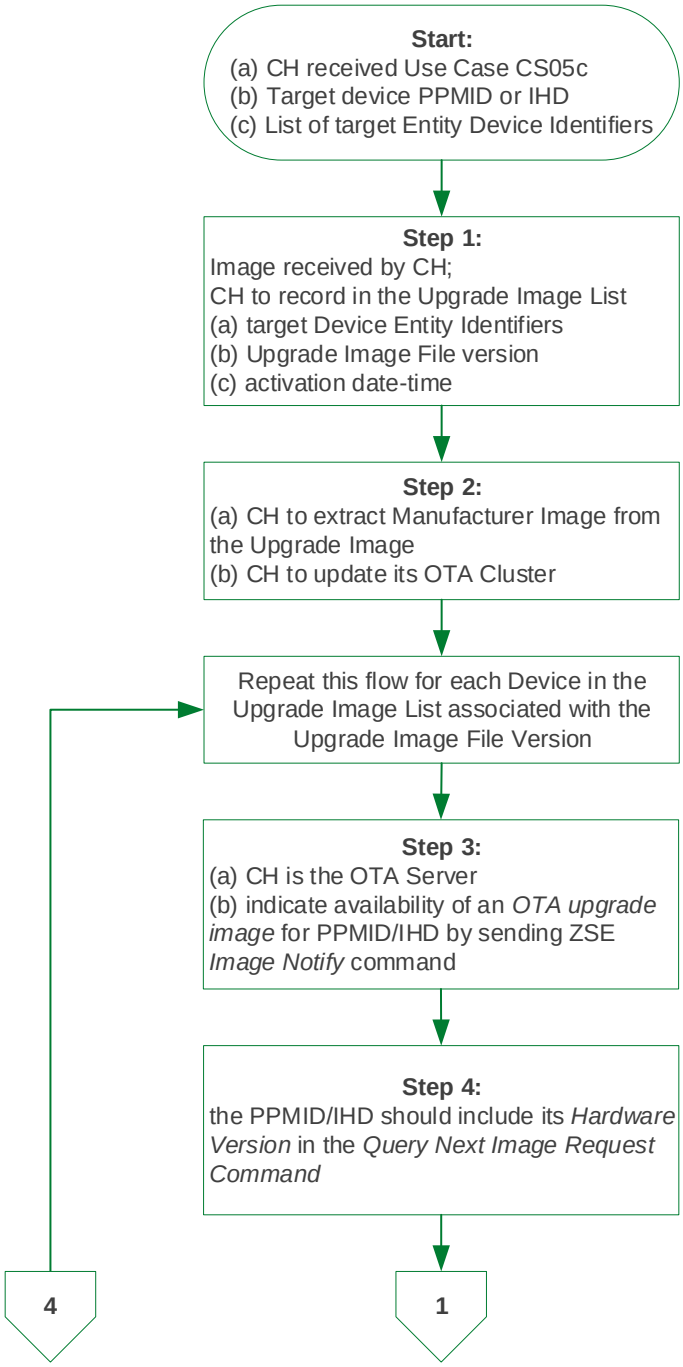
This table summarises the timeline of events that this modification taken.

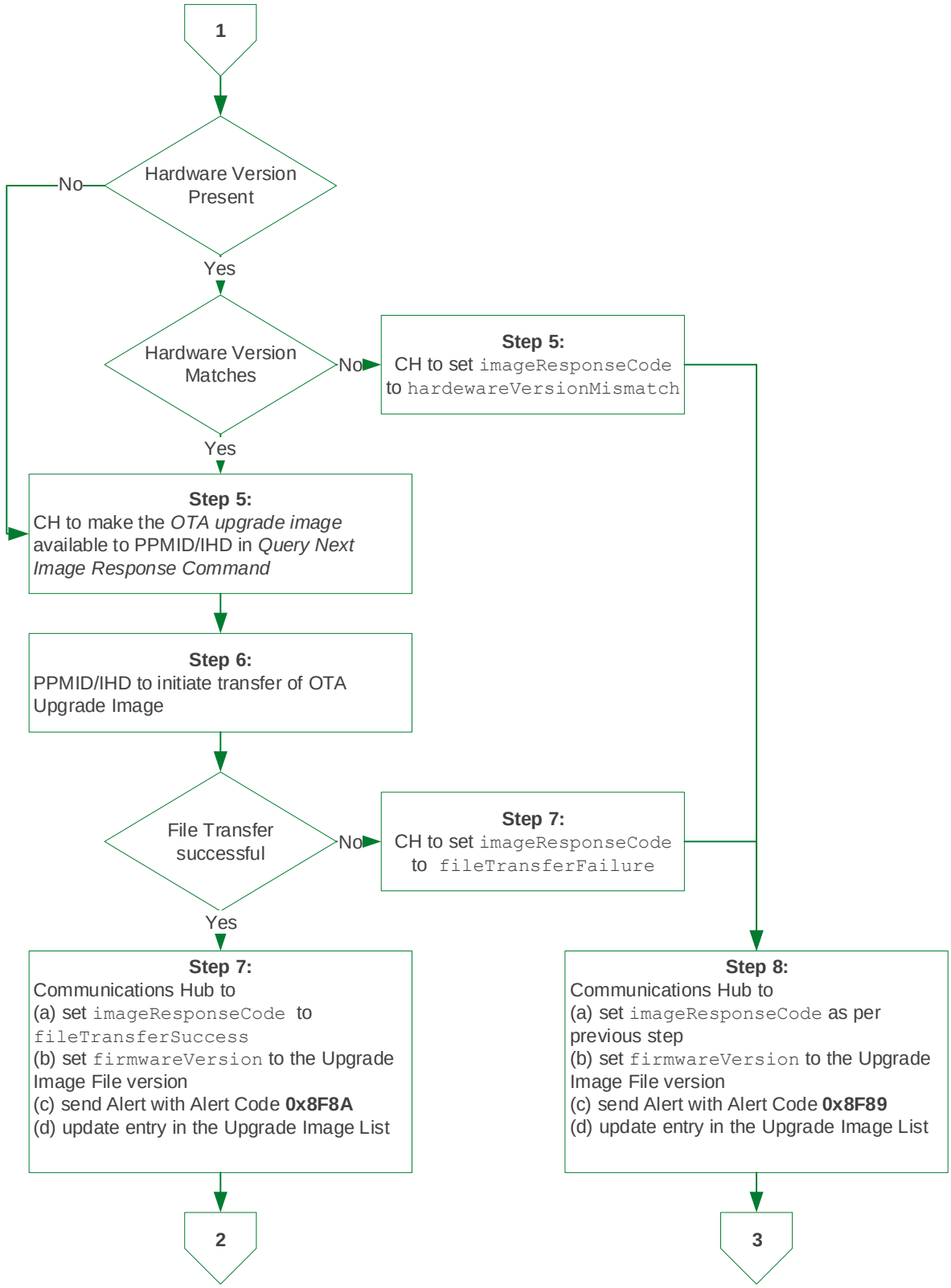
Timeline	
Activity	**Date**
Modification Proposal raised	1 Mar 16
Panel considers Initial Modification Report	11 Mar 16
Initial DCC Preliminary Assessment	10 Jun 16 – 17 May 17
First Refinement Consultation	17 Oct 17 – 8 Nov 17
Firmware industry workshop	29-30 Jun 18
The SSC considers the inclusion of 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
The Proposer[5] raises an amendment to the solution, preferring a different Service Request for combined distribution and activation of PPMID/IHD firmware	15 Oct 19

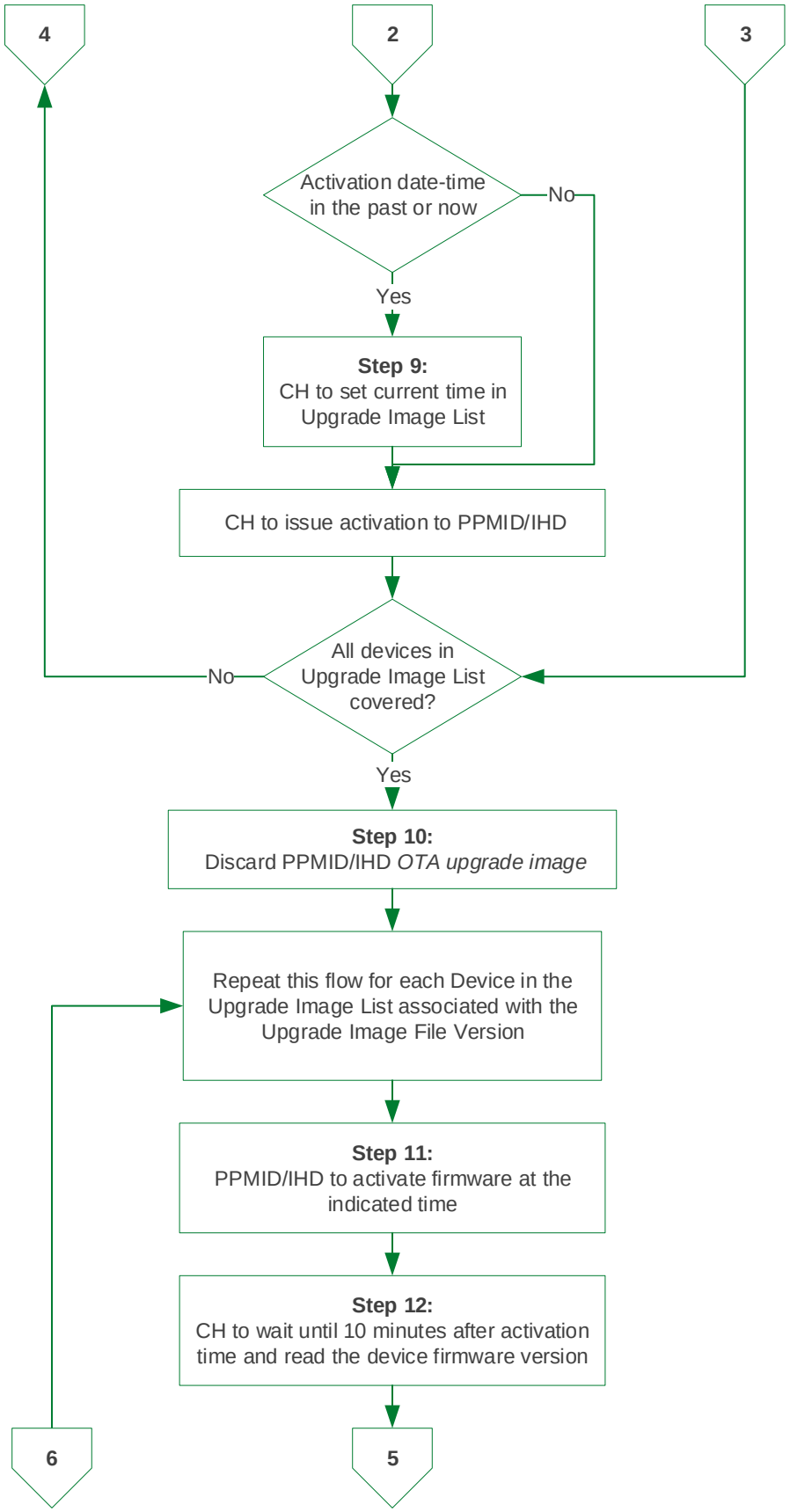
[5] There is also a change in Proposer due to the original named sponsor leaving their organisation.

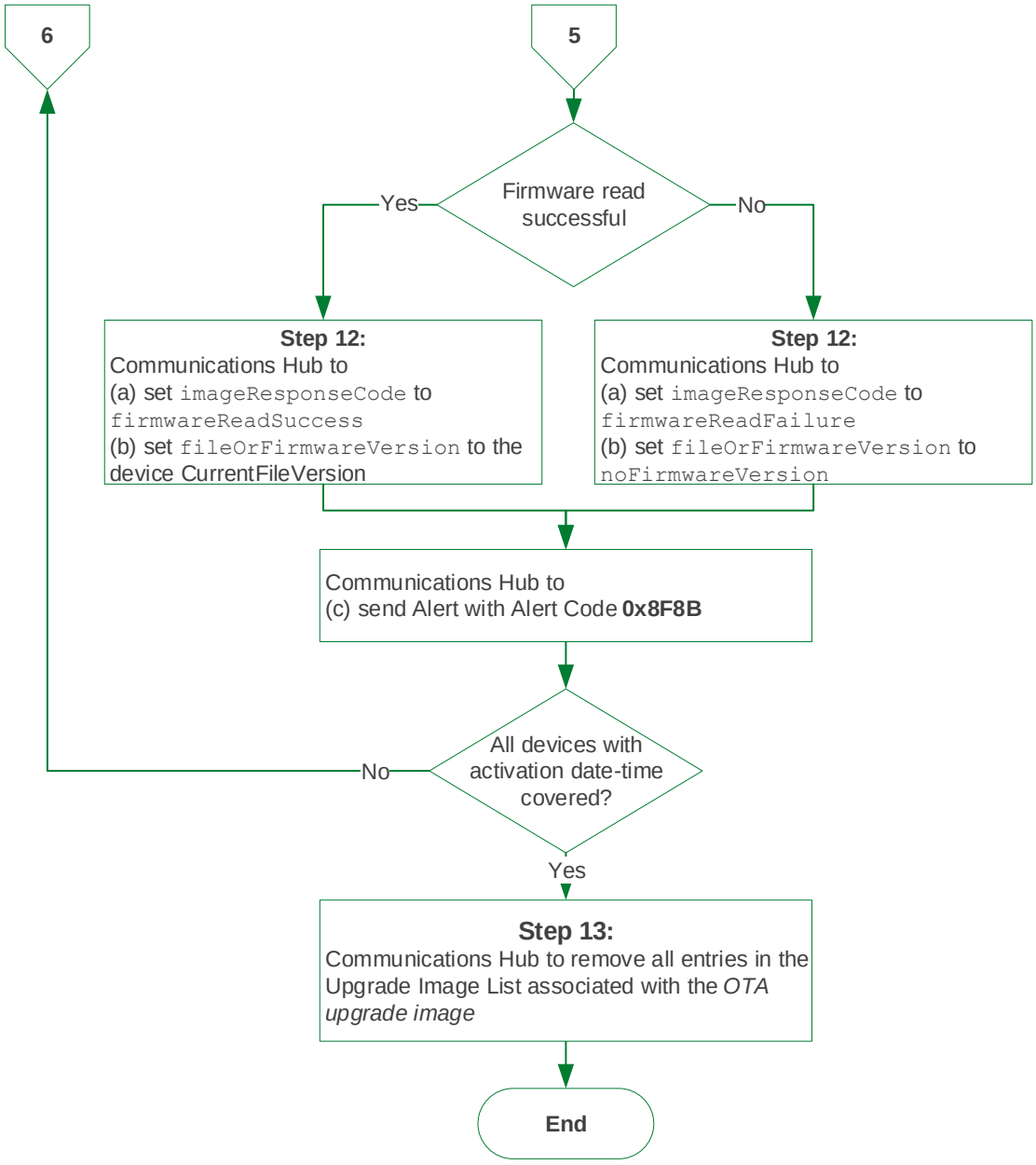
Timeline	
Activity	**Date**
The Working Group discuss the outstanding questions on the solution • **Outcome**: The DCC is to proceed with its Impact Assessment as-is • **Outcome**: The DCC is to ask its Service Providers to provide cost impacts on the use of different Service Requests as well as the use of memory blocks on the Communications Hub	6 Nov 19

Appendix 3: IHD and PPMID OTA firmware process

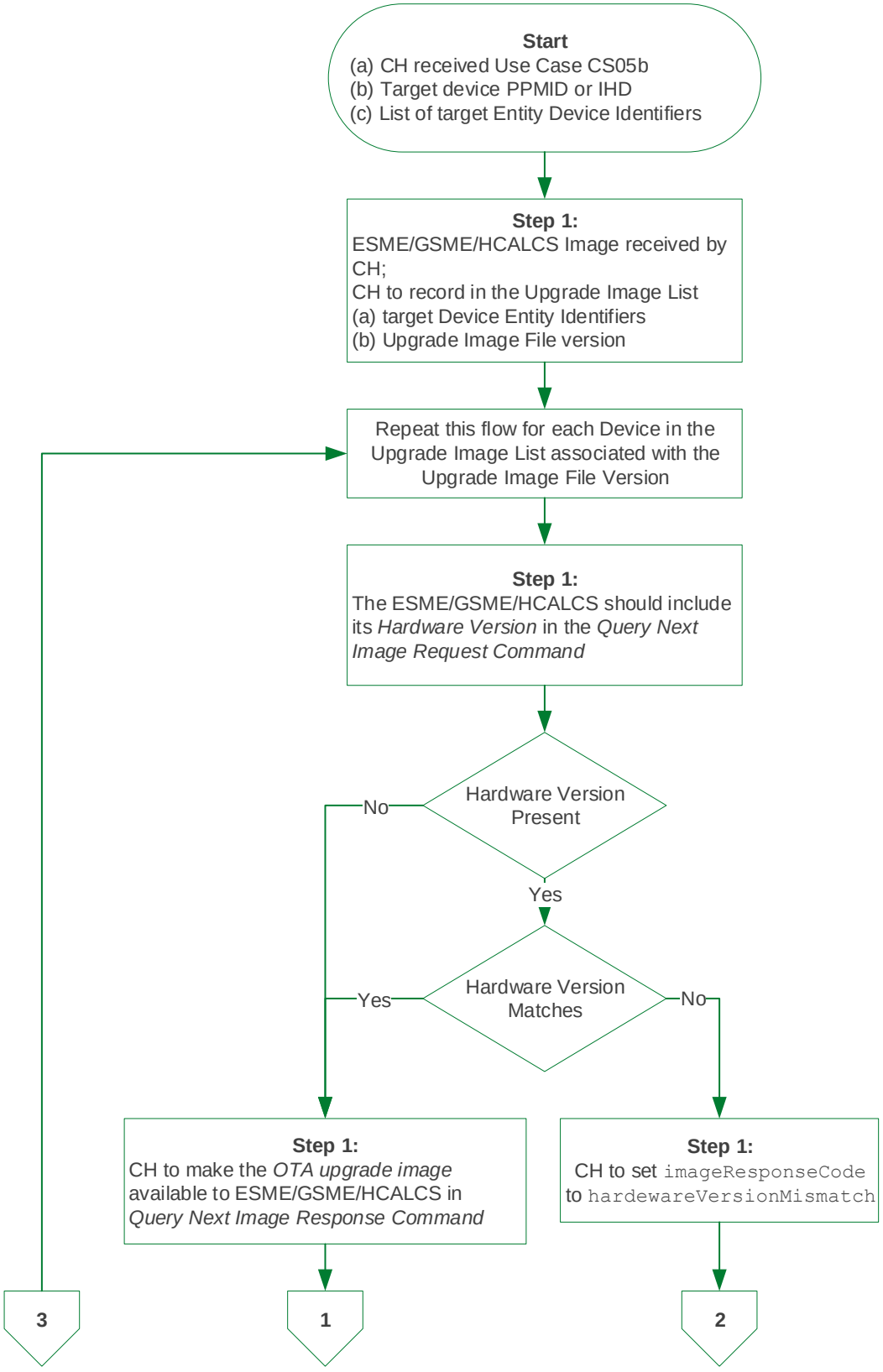


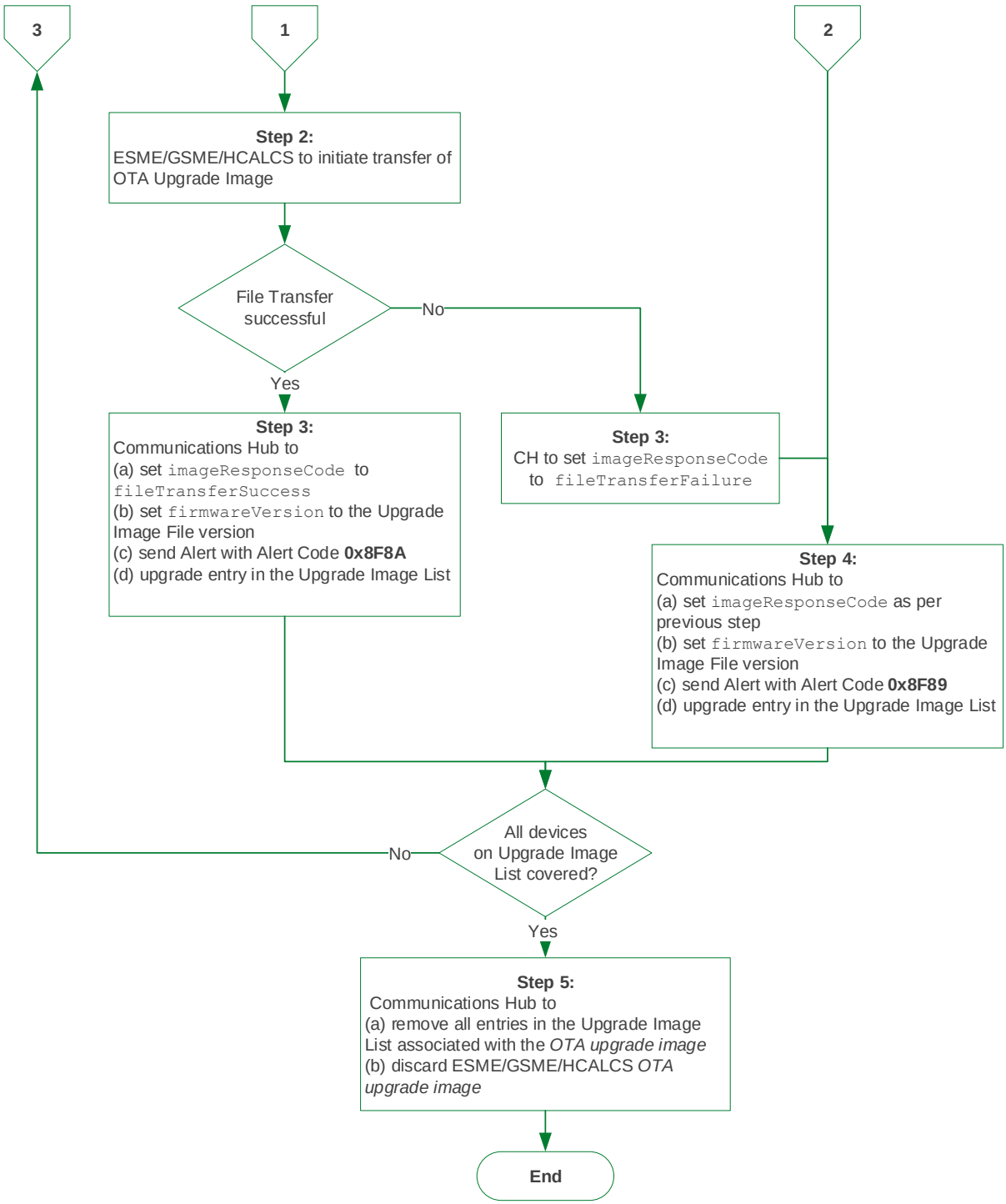

1
Hardware Version Present
No
Yes
Hardware Version Matches
No
Yes
Step 5:
CH to set imageResponseCode to hardewareVersionMismatch
Step 5:
CH to make the OTA upgrade image available to PPMID/IHD in Query Next Image Response Command
Step 6:
PPMID/IHD to initiate transfer of OTA Upgrade Image
File Transfer successful
No
Yes
Step 7:
CH to set imageResponseCode to fileTransferFailure
Step 7:
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) update entry in the Upgrade Image List
Step 8:
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) update entry in the Upgrade Image List
2
3


4
2
3
Activation date-time in the past or now
No
Yes
Step 9:
CH to set current time in Upgrade Image List
CH to issue activation to PPMID/IHD
All devices in Upgrade Image List covered?
No
Yes
Step 10:
Discard PPMID/IHD OTA upgrade image
Repeat this flow for each Device in the Upgrade Image List associated with the Upgrade Image File Version
Step 11:
PPMID/IHD to activate firmware at the indicated time
Step 12:
CH to wait until 10 minutes after activation time and read the device firmware version
6
5


6
5
Firmware read successful
Yes
No
Step 12:
Communications Hub to
(a) set imageResponseCode to firmwareReadSuccess
(b) set fileOrFirmwareVersion to the device CurrentFileVersion
Step 12:
Communications Hub to
(a) set imageResponseCode to firmwareReadFailure
(b) set fileOrFirmwareVersion to noFirmwareVersion
Communications Hub to
(c) send Alert with Alert Code 0x8F8B
All devices with activation date-time covered?
No
Yes
Step 13:
Communications Hub to remove all entries in the Upgrade Image List associated with the OTA upgrade image
End

Appendix 4: 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

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

Joe Hehir

020 7770 6874

joe.hehir@gemserv.com

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

sec.change@gemserv.com

SECMP0007 'Firmware updates to IHDs and PPMIDs'

Annex A

Business requirements – version 1.1

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 Commination's Company (DCC) and Sub-Committees. It also provides the considerations and assumptions for each business requirement with respect to this Modification Proposal.

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 IHDs, PPMIDs and HCALCSs to be added to the CPL
2	Suppliers to send firmware updates to IHDs, PPMIDs and HCALCS
3	The DCC to notify all Responsible Suppliers at certain stages of the associated processing of firmware updates
4	The DCC and Responsible Suppliers to check the latest firmware version on IHDs, 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 affected Device
7	Additional Communications Hub functionality to support the distribution of firmware Images to IHDs, PPMIDs and HCALCSs
8	Firmware update support capability will need to be mandated on IHDs and PPMIDs installed after this modification is implemented
9	Local firmware updates will be banned following the implementation of this modification

2. Considerations and assumptions

2.1 Scope of the modification

The scope of this modification currently covers In-Home Displays (IHDs), Pre-Payment Meter Interface Devices (PPMIDs) and HAN Connected Auxiliary Load Control Switches (HCALCSs).

2.2 Firmware update approach for IHDs, PPMIDs and HCALCSs

The Proposer has agreed to progress with a combination of the two solutions given in the DCC's Preliminary Assessment. It is expected that IHDs and PPMIDs will receive firmware updates Over-The-Air (OTA) via Zigbee, and that HCALCSs will receive firmware updates OTA via Great Britain Companion Specification (GBCS) Critical Commands.

2.3 Non- Functional Requirements

Firmware update Images for IHDs and PPMIDs are expected to be typically less than 750KB in size and would occur infrequently e.g. once per year. The customisation of IHDs and PPMIDs with graphics will increase the firmware size, this may happen going forward and require the mechanism for firmware sizes greater than 750KB.

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

2.4 Manufacturer Image Hashes associated with IHDs, PPMIDs and HCALCSs will be added to the CPL

In order 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 IHD, PPMID or HCALCS communicates using ZigBee.

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

2.5 Communications Hub memory considerations

No additional buffer space on the Communications Hub is being proposed. The same buffer space as for Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) Images will be used for storing IHD / PPMID / HCALCS Images. IHD / PPMID / HCALCS Images can be overwritten by ESME or GSME Images if one arrives whilst a IHD / PPMID / HCALCS one is in process, and there is insufficient buffer space. If another IHD / PPMID / HCALCS Image arrives whilst a IHD / PPMID / HCALCS one is in process and there is insufficient space or it is for the same Device Model, the newly arrived one will overwrite the one in process.

3. Sending IHD and PPMID Manufacturer Images that are less than or more than 750KB

This section outlines how the process will work for IHDs and PPMIDs if Manufacturer Images are less than 750KB, as well as how firmware updates can be achieved where Images are 750KB or greater in size. HCALCSs are covered in Sending HCALCS Manufacturer Images below.

3.1 Sending a Manufacturer Image less than 750KB to an IHD or PPMID

This section details the steps that will need to be taken to update the firmware on an IHD or PPMID. It is assumed that a Manufacturer provides a Manufacturer Image to the Supplier, the Image is a single Image less than 750KB in size, and a new CPL entry has been created.

Sending a Manufacturer Image to an IHD or PPMID will require a new non-critical Service Request 'Send IHD / PPMID Firmware'.

3.1.1 Supplier preparations

Before sending a new Service Request to the DCC to 'Send IHD / PPMID Firmware', the Supplier will be required to follow similar steps as in the case of sending an 'Update Firmware' Service Request to the DCC is respect of 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.

3.1.2 Supplier creation of a 'Send IHD / PPMID Firmware' Service Request

Having obtained the information and upon the above checks being successful, the Supplier will create a 'Send IHD / 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 || activation date-time

   Note: activation date-time will include an option for an 'activate now' value (e.g. zero)

2. List of Device IDs

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

3.1.3 The DCC checks on the 'Send IHD / PPMID Firmware' Service Request

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

1. Check whether the Manufacturer Image contained within the Service Request is less than 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 an IHD or PPMID;
   b. From the 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.

3.1.4 DCC response to the 'Send IHD / 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 IHD / PPMID Firmware' Service Request:

1. Upon the DCC receipt of the 'Send IHD / 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 3.2.3 (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 IHD / PPMID Firmware' Service Request, each Responsible Supplier identified in 3.2.3 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; and
    c. The activation date-time specified in the Service Request.

3.1.5 DCC Distribution of the 'Send IHD / 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 IHDs / PPMIDs in the List of Device IDs where the Device ID passed the validation.

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

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

3.1.7 IHD / PPMID request for the details of the Image

The IHD / 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.

3.1.8 Provision of Image details by the Communication Hub to the IHD / PPMID

For the Communications Hub to decide that the Image is suitable for the IHD / 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 IHD / PPMID.

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

3.1.9 IHD / PPMID download and authentication of the Image

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

When the IHD / 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 IHD / PPMID will then store the Manufacturer Image from within the Image sent, so that it is available for activation[1]. The IHD / PPMID will then send a 'UpgradeEndRequest' to the Communications Hub.

The Communications Hub will then send a 'UpgradeEndResponse' with activation date-time in it. The Communications Hub will set a 'reminder' for activation time (or current time, when activation time is zero) plus [X] minutes, and record IHD / PPMID Device ID against that reminder (there can be multiple IHDs / PPMIDs of the same type on the HAN, so the Communications Hub will need to remember which one this reminder relates to).

The IHD / PPMID will wait for activation time (or begin activation now if activation time is zero). It will need to check time against the Communications Hub if it has no clock of its own. (Note the Smart Metering Equipment Technical Specification (SMETS) does not require a clock on either IHDs or PPMIDs.) The IHD / PPMID will then activate the Manufacturer Image, changing Firmware Version if successful.

The Communications Hub will wait to activation time (or current time, when activation time is zero) plus [X] minutes and read the OTA cluster's Firmware Version attribute from the IHD / PPMID. The Communications Hub will then create a Device Alert containing the IHDs / PPMID's 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 Responsible Suppliers recorded to receive the Alert.

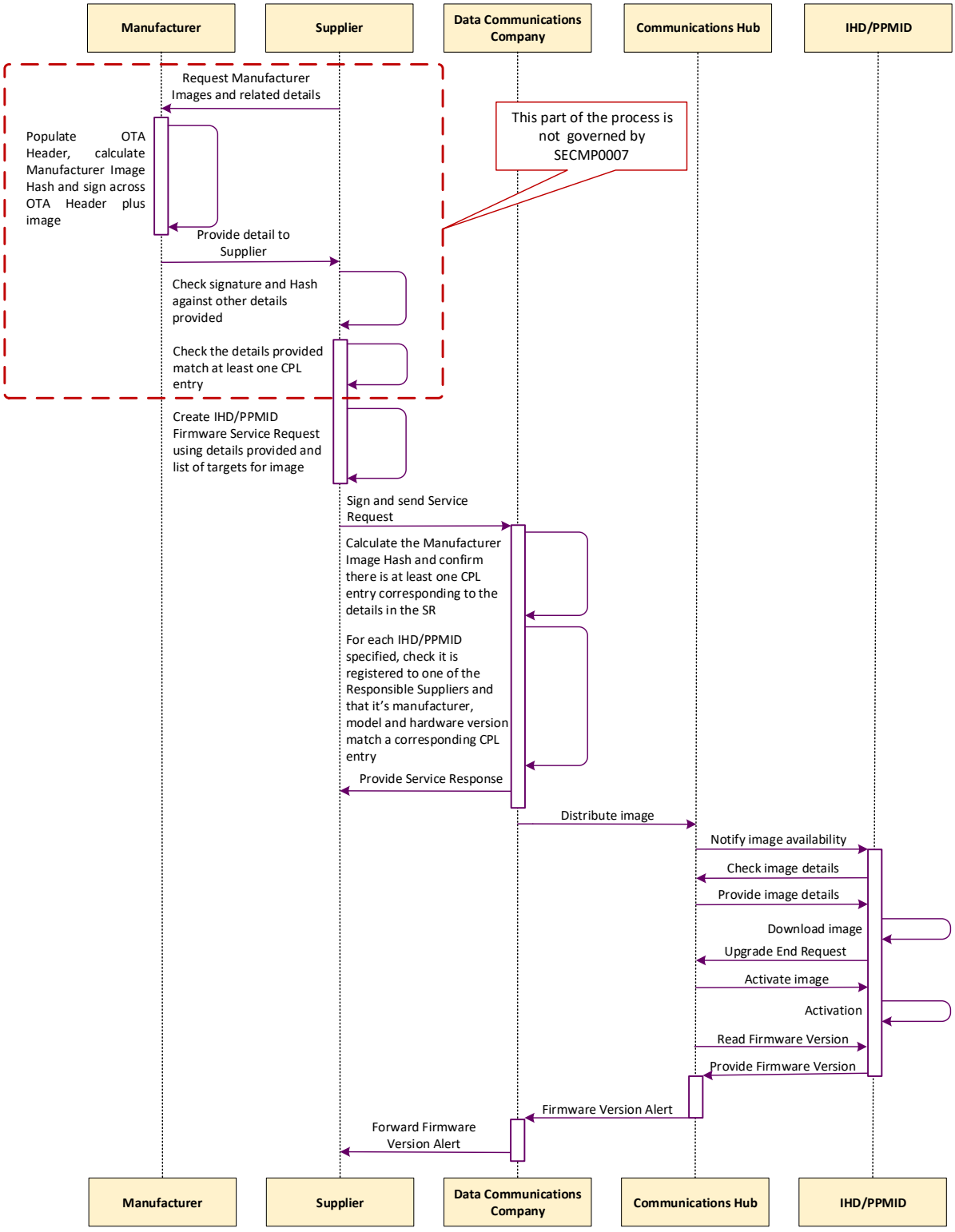
If this Device Alert is not received the Supplier can send a 'Read IHD / PPMID Device Model via the CH' Service Request to the DCC. This will result in a Command to the Communications Hub to read the OTA Cluster's Firmware Version, manufacturer etc. from the IHD / PPMID. The Communications Hub will send a Response containing these details to the DCC, the DCC will then update the SMI and forward the Response to all Responsible Suppliers.

3.1.10 Process for updating an IHD / PPMID Firmware – Image less than 750KB

The process described above for processing IHD / PPMID firmware updates for Images less than 750KB is presented in Figure 1 Process for updating an IHD / PPMID Firmware – Image less than 750KB below.

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

Figure 1 *Process for updating an IHD / PPMID Firmware – Image less than 750KB*



3.2 Sending a Manufacturer Image 750KB or greater to an IHD / PPMID

The expectation is that Manufacturer Images are typically below 750KB. It may be possible for Manufacturer Images to become larger in size; this section illustrates how activating Images that are 750KB or more in size can be achieved. The operating Firmware Version in this example is 0x10, which is reflected in the CPL entry example in Table 1 below.

An IHD / PPMID is to be updated to Firmware Version 0x20. This requires two Images are to be sent to the IHD / PPMID, to provide all of the changed Firmware / configuration data required for Firmware Version 0x20.

The Manufacturer has split this upgrade data in to two Images:

- **Image 0x15**: this contains the first part of the upgrade data and contains Manufacturer instructions for the IHD / 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 IHD / 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 Manufacturer Image Greater than 750KB

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 an IHD / PPMID, the Supplier will follow the following process:

1. Having undertaken the necessary checks, the Supplier will create a 'Send IHD / PPMID Firmware' Service Request to distribute Image 0x15 and set the activation date-time as zero (i.e. 'activate now'). Note that when the Image needs to be split into two Images or more, the activation date-time should not be in the future, as explained below.
2. The DCC will distribute Image 0x15 to the Communications Hub. When the IHD / PPMID has downloaded the Image, the Communications Hub will start a timer for now plus [X] minutes. When that time has passed, the Communications Hub will read Firmware Version from the IHD / PPMID and send a Device Alert containing that value. 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 IHD / PPMID has successfully validated the Image.
3. On receipt of the Device Alert from the DCC containing the IHD's / 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 IHD / PPMID had that Image).

4. The DCC will distribute Image 0x20 to the Communications Hub. When the IHD / PPMID has downloaded the Image, the Communications Hub will start a timer for activation time plus [X] minutes. When that time has passed, the Communications Hub will read Firmware Version from the IHD / PPMID and send a Device Alert containing that value. 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.
5. If this Device Alert is not received the Supplier can only resend Image 0x20.

The result is that the IHD / PPMID (excluding where the 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 illustrative process is explained in detail in Figure 2 and Figure 3: Process for upgrading an IHD / PPMID Firmware – Image more than 750KB, Part 2 (parts 1 and 2 respectively) below.

Figure 2: *Process for upgrading an IHD / PPMID Firmware – Image more than 750KB, Part 1*

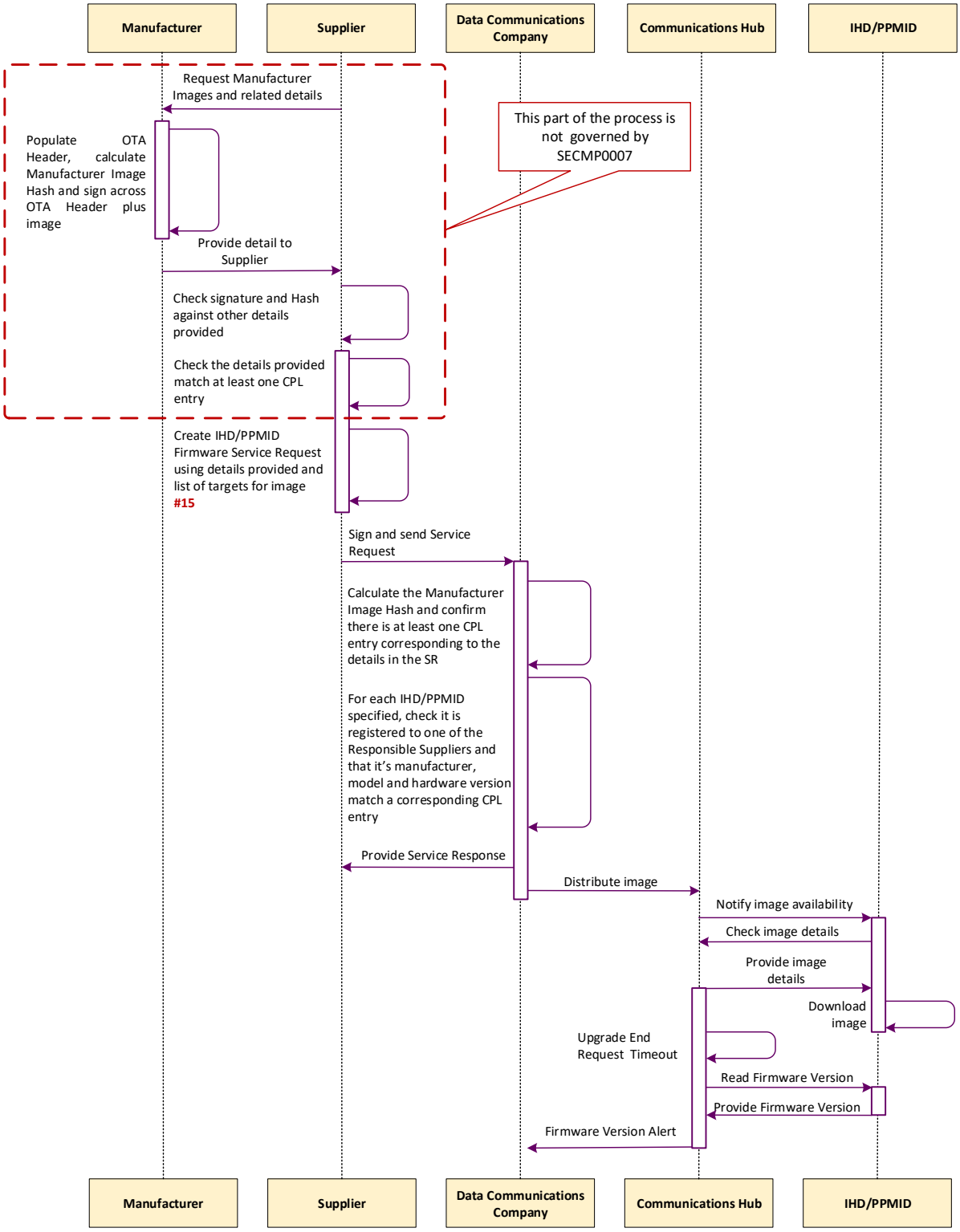
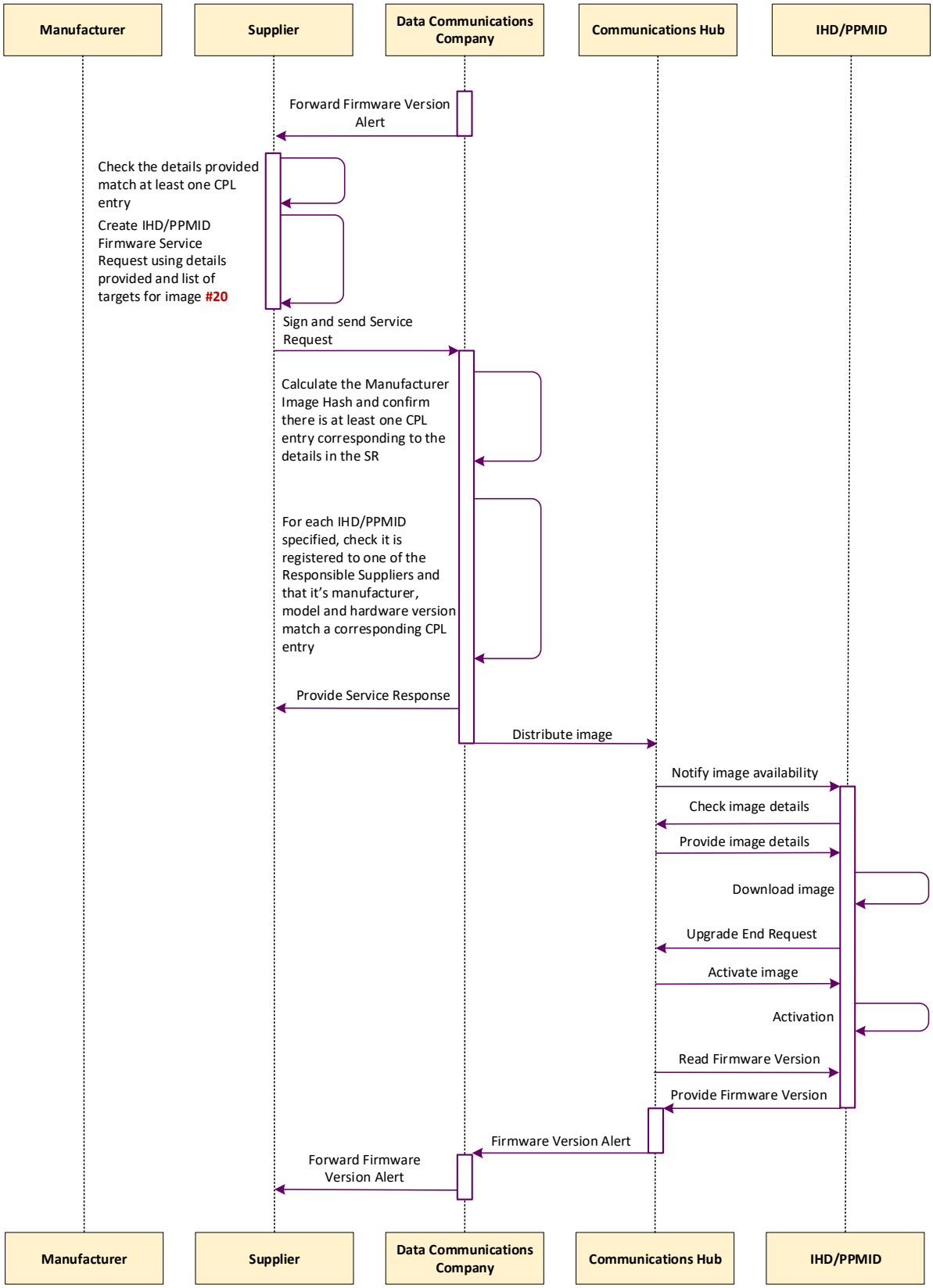


Figure 3: *Process for upgrading an IHD / PPMID Firmware – Image more than 750KB, Part 2*



4. Sending HCALCS Manufacturer Images

The process for the OTA upgrade of HCALCSs aligns with the current Smart Metering Implementation Programme (SMIP) technical specifications for the Supplier to distribute and activate firmware on the ESME and GSME via an OTA update; this will be accomplished through the introduction of additional Service Reference Variants for the existing Service Requests.

The expectation is that Manufacturer Images for HCALCSs are typically below 750KB. The existing OTA firmware upgrade mechanisms contained in GBCS allow manufacturers to split firmware upgrades into several parts; this method can be employed in case HCALCS firmware Images exceed the size of 750KB.

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

- SR 11.1 ‘Update Firmware’;
- SR 11.1 ‘Read Firmware Version’; and
- SR 11.3 ‘Activate Firmware’.

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

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

5. Glossary

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

Glossary	
Acronym	**Full term**
CH	Communications Hub
CHF	Communication Hub Function
CHTS	Communication Hub Technical Specification
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
PKI	Public Key Infrastructure
PPMID	Pre-Payment Meter Interface Device
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specification
SSC	Security Sub-Committee

SEC Modification Proposal, SECMP0007, DCC CR 211

Firmware Updates to IHDs, PPMIDs and HCALCS[1]

Updated Requirements and Preliminary Impact Assessment (PIA)

Version:	**1.0**
Date:	**19th July, 2019**
Author:	**DCC**
Classification:	**DCC PUBLIC**

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

Data Communications Company

Contents

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
27/03/2019	0.1	Compilation from Service Providers, based on new Solution Design including two options and requested changes
11/04/2019	0.3	Internal DCC Review
23/04/2019	0.60	Further review with Service Providers, SECAS, small revisions
19/07/2019	1.00	Requirements and Scope updated to match Working Group and Change Board decision to proceed.

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	SECMP0007 CR211 - Firmware Updates PIA - Requirements v0.51	DCC	25/02/2019

References are shown in this format, [1]

1.3 Terminology

Note the terms "Device" and "HAN Devices" are used interchangeably with the phrases "IHD / PPMID / HCALCS" and "IHD, PPMID, and HCALCS" in this document.

2 Introduction

2.1 Document Information

The Proposer for this Modification is Mark Pitchford of npower.

An Early Impact Assessment was requested of DCC on 10th June 2016. The Preliminary Impact Assessment was requested of DCC in July 2018, after updated requirements were issued by SECAS.

A full review of the PIA was carried out based on the expiry of the original design and cost estimates in the original PIA. That version of the PIA (0.60) submitted in April 2018, includes a full listing of the requirements and two options for a solution approach; the first option was covered in the previously issued PIA, but a new approach for implementing firmware upgrades 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.

Note that the Risks, Assumptions, Issues, and Dependencies section were reviewed in the older documents and contains many updates considered by the Working Group and Proposer that should help and influence the Service Providers in producing a Full Impact Assessment (FIA). The additional section for Clarifications was also reviewed and feedback provided as well.

2.2 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 IHDs and HCALCS via the DCC, and for PPMID and IHDs and HCALCS 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 and IHD devices in the field that will require firmware upgrades, and this number will have increased by the time this Modification is implemented.

2.3 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 can be summarised as follows.

1.	In Home Displays (IHDs) to be added to the Certified Product List (CPL).
2.	Manufacturer Image Hashes associated with IHDs, Pre-Payment Metering Interface Devices (PPMIDs) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs) to be added to the CPL.
3.	Suppliers to send firmware updates to IHDs, PPMIDs and HCALCS.

4.	The DCC to notify all Responsible Suppliers at certain stages of the associated processing of firmware updates.
5.	The DCC and Responsible Suppliers to check the latest firmware version on IHDs, PPMIDs and HCALCS.
6.	Rules around sharing capacity and buffering on the Communication Hub (CH).
7.	SRs supporting the maintenance of the Smart Metering Inventory (SMI) to be revised.
8.	Additional CH functionality.
9.	Firmware update support capability will need to be mandated on IHDs and PPMIDs installed after this modification is implemented.
10.	Local firmware updates will be banned following the implementation of this modification.

Support for the above changes would be mandated through the SMETS for all newly installed IHDs / 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 or IHDs, unless there were changes to the SEC or a SEC governance mandated upgrade.

2.4 Detailed Requirements and Business Processes for Firmware Upgrades

A detailed breakdown of the requirements and potential business process solutions for each requirement follows.

2.4.1 Requirement 1- IHD's will be added to the CPL

To support firmware management, IHDs will need to be captured in the CPL. IHDs will need to be subject to the following conditions:

1. The provision of the required values of attributes of the Product to the Panel (e.g. Manufacturer ID, hardware version, firmware version) – an example CPL published on behalf of the SEC Panel specifies the format and contents of each of the attributes required in a CPL entry.

2. The provision of the ZigBee Assurance Certificate to the Panel.

The process for adding an IHD to the CPL will be the same as that for Pre-Payment Metering Interface Devices (PPMIDs). The SEC does not constrain who supplies this information to the Panel. For the purposes of illustrating the processes of adding an IHD and PPMID to the CPL, the following assumptions are made:

1. The Manufacturer is a member of the ZigBee Alliance and the required Manufacturer ID has been issued accordingly

2. The organisation undertaking the ZigBee testing is referred to as a “Test Lab”

3. The organisation notifying the SEC Panel of a Product’s details and assurance certificates is the Manufacturer

The resulting steps for adding an IHD and PPMID to the CPL are as detailed following.

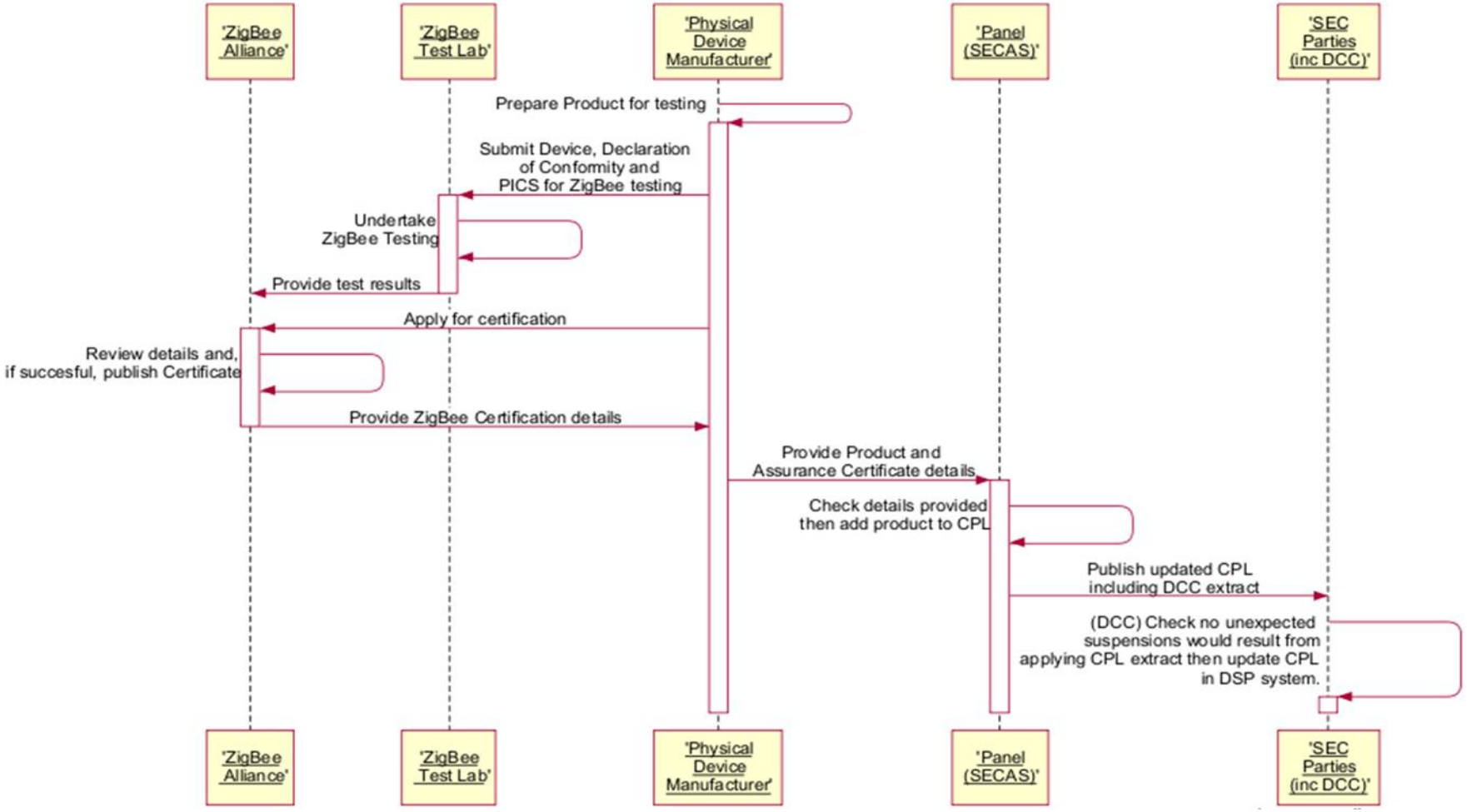


Figure 1 Process for adding an IHD or PPMID to the CPL

Below is an illustrative CPL entry that will be created by the above process. It uses sample data for the hardware, model and manufacturer. It assumes the factory installed firmware is version 10. In summary that example entry is:

Manufacturer Identifier	Model identifier	Hardware Version	Hardware version revision	Firmware version	Hash
FF:FE	AA:BB	01	01	00:00:00:10	(Hash value)

Table 1: Example of a New CPL Entry

2.4.2 Requirement 2- Manufacturer Image Hashes

In order for a Manufacturer Image to be added to the 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 SEC Panel that the firmware update does not affect how the IHD, PPMID or HCALCS communicates using ZigBee. If there is an impact on how the IHD, PPMID or HCALCS communicates using ZigBee which 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
- 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, HCALCS must comply with the Commercial Product Assurance (CPA) Security Characteristics as per the Smart Metering Equipment Technical Specification (SMETS). Changes to the HCALCS firmware may require either the inclusion of the new firmware version in the existing CPA certificate or a new CPA certificate. For HCALCS this CPA certificate must be submitted to the Panel when adding a new firmware version to the CPL.

The process for adding a Manufacturer Image to the CPL is detailed in Figure 2 below.

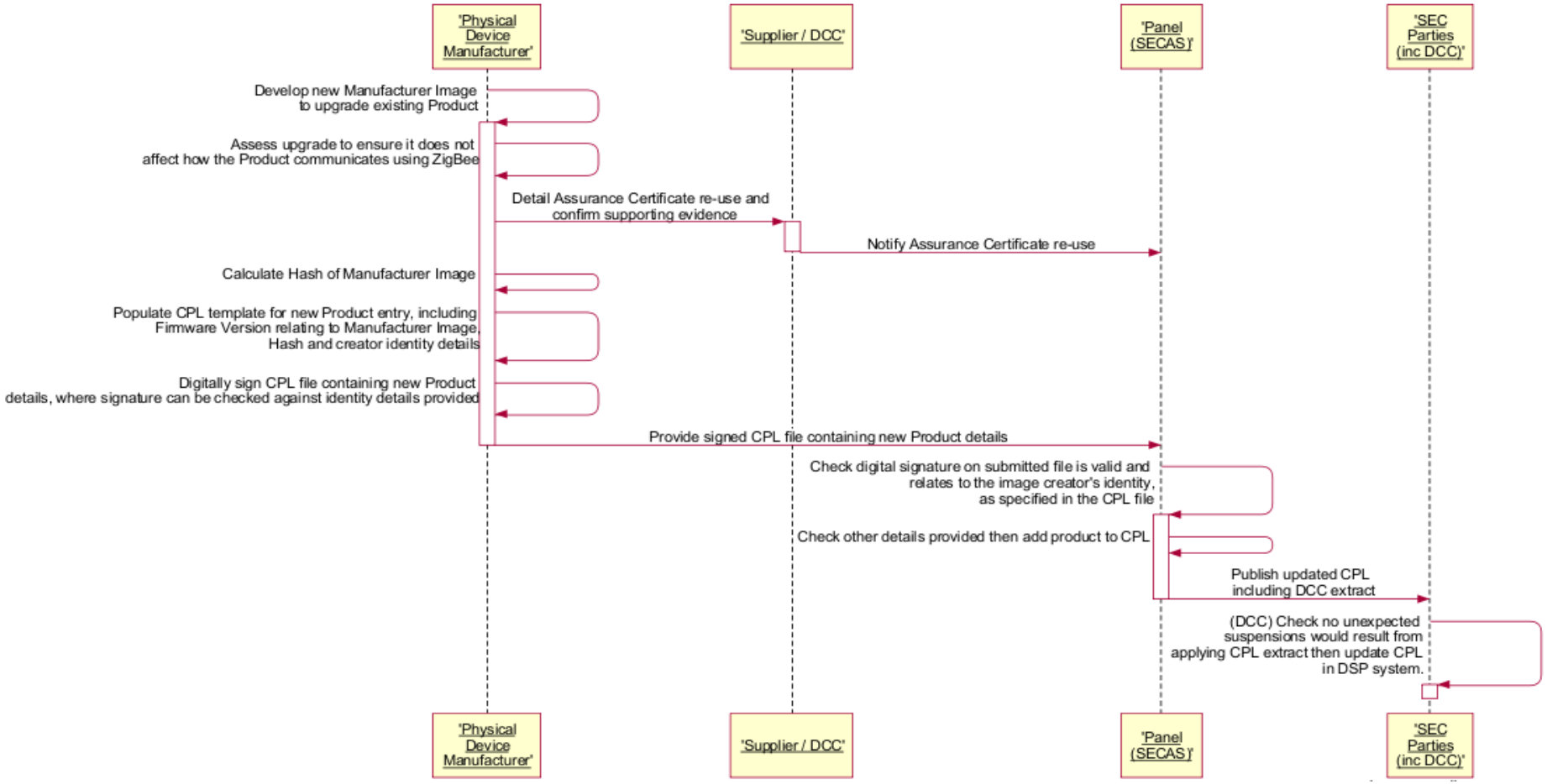


Figure 2: Process for adding a Manufacturer Image to the CPL

.

2.4.3 Requirement 3- Sending Manufacturer Images

There should be no limitation on the size of the manufacturer's firmware change, and this should be treated as an "Image" sent to the appropriate device. The expectation is that Manufacturer Images are typically below 750 KiloBytes (KB), in particular for HCALCS, but it may be possible for Manufacturer Images to become larger in size.

The following sections outline the processes required for Manufacturer Images that are either less than 750KB, or 750KB and greater in size.

Sending a Manufacturer Image less than 750KB to an IHD or PPMID

This section details the steps that will need to be taken to update the firmware on an IHD, PPMID, or HCALCS, where the image is a single image less than 750KB in size, and a new CPL entry has been created. A sequence diagram summarising the steps is shown in Figure 3 on page 14 following.

Sending a Manufacturer Image to an IHD / PPMID / HCALCS will require a new non-critical Service Request 'Send IHD / PPMID / HCALCS Firmware'.

Supplier Preparations

Before sending a new Service Request to the DCC to 'Send PPMID / IHD / HCALCS Firmware', the Supplier will be required to follow similar steps as in the case of sending an 'Update Firmware' Service Request to the DCC in respect of a Meter:

1.	Obtain the following information	The Manufacturer Image An Over the Air (OTA) Header, which should include: i. Manufacturer ID ii. Model to which it can be applied iii. Firmware Version in the image iv. Minimum and maximum hardware version to which it can be applied v. A Hash of the Manufacturer Image
2	Undertake the following checks on that information	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) Check the Manufacturer Image is associated with one or more Device Models on the CPL. The check should include i. The Hash is recorded on the CPL against one or more entries ii. The OTA Header Manufacturer ID, model and Firmware Version fields match identically with one of the entries identified at step (i)

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

Supplier creation of a 'Send IHD / PPMID / HCALCS Firmware' Service Request

Having obtained the information and upon the above checks being successful, the Supplier will create a 'Send IHD / PPMID / HCALCS Firmware' Service Request. The Service Request (SR) 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 || activation date-time Note: activation date-time will include an option for an 'activate now' value (e.g. 0)
2	List of Device IDs	Up to 50,000 IHD / PPMID / HCALCS can be listed within the SR.

DSP Checks the 'Send IHD / PPMID / HCALCS Firmware' SR

On receipt of the 'Send IHD / PPMID / HCALCS Firmware' Service Request, the DSP will follow the following steps:

1. Check whether the Manufacturer Image contained within the SR is less than 750KB in size
2. Calculate the Hash of the Manufacturer Image contained within the SR
3. Check whether the Hash the DCC has calculated is on the CPL, and identify CPL entries with that Hash
4. For each Device ID in the SR:
   a. Check the Device is an IHD, PPMID or HCALCS
   b. From the 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
   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. In case the Device is an HCALCS, only the Import Supplier will be recorded as Responsible Supplier. This temporary record will be used to populate the DCC Alerts at the next step.

DCC Response to the 'Send IHD / PPMID Firmware' Service Request

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

1. Upon the DCC receipt of the 'Send IHD / PPMID / HCALCS Firmware' SR, the requesting Supplier will receive a Service Response. If some of the Device IDs in the SR failed any of the checks at step 4a, 4b, 4c, and 4d 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 IHD / PPMID / HCALCS Firmware' SR, each Responsible Supplier identified in 4d will receive a DCC Alert containing:
    a. The Hash of the Manufacturer Image in the SR (to identify the CPL entry)
    b. A list of Device IDs to which the image is being sent
    c. The activation date-time specified in the SR

Distribution of the 'Send IHD / PPMID / HCALCS Firmware' Service Request

If the checks are successful, the DSP will distribute the Image from the SR (having decoded from base64 encoding) to the CH associated with each of the IHDs / PPMIDs / HCALCS in List of Device IDs where the Device ID passed the validation.

The Communication Hub Technical Specification (CHTS) section 4.4.4 requires that the receiving CHs can buffer Images intended for Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME). The Communication Service Provider (CSP) contracts require CHs to have the capacity to hold two 750KB images (to support independent distribution of firmware to the GSME and one of the ESME).

No additional buffer space on the CH is being proposed. The same buffer space for ESME and GSME images will be used for storing IHD / PPMID / HCALCS images. IHD / PPMID / HCALCS images can be overwritten by ESME or GSME images if one arrives whilst an IHD / PPMID / HCALCS one is in process, and there is insufficient buffer space. If another IHD / PPMID / HCALCS image arrives whilst an IHD / PPMID / HCACLS one is in process and there is insufficient space or it is for the same Device Model, the newly arrived one will overwrite the one in process.

Communication Hub notification of image availability to the IHD / PPMID / HCALCS

Once the image arrives at the CH, the CH will need to:

1. Record OTA Header details and activation date-time
2. Notify the device(s) by sending a message to it/them ('the CH shall send a Zigbee Smart Energy (ZSE) Image Notify command').

IHD / PPMID / HCALCS request for Image Details

The IHD / PPMID / HCACLS 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 CH if there is an image that may be suitable for it. The Great Britain Companion Specification (GBCS) will mandate the hardware version to avoid wasted downloads over the Home Area Network (HAN).

Provision of Image Details by the Comms Hub to the IHD / PPMID / HCALCS

For the Comms Hub to decide that the Image is suitable for the IHD / PPMID / HCALCS, 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 [in this case, the Comms Hub] 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 IHD / PPMID / HCALCS.

The CH will send back a 'QueryNextImageResponse' accordingly.

IHD / PPMID / HCALCS Download and Authentication of the Image

The IHD / PPMID / HCALCS will then download the image from the CH, if one is available. When the IHD / PPMID / HCALCS 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 IHD / PPMID / HCALCS will then store the Manufacturer Image from within the image sent, so that it is available for activation . The IHD / PPMID / HCALCS will then send a 'UpgradeEndRequest' to the CH.

The CH will then send a 'UpgradeEndResponse' with activation date-time in it. The CH will set a 'reminder' for activation time (or current time, when activation time is zero) plus [X] minutes, and record IHD / PPMID / HCACLS Device ID against that reminder (there can be multiple IHDs / PPMIDs / HCALCS of the same type on the HAN, so the CH will need to remember which one this reminder relates to).

The device will wait for activation time (or begin activation now if activation time is zero). It will need to check time against the CH if it has no clock of its own. (Note the Smart Metering Equipment Technical Specification (SMETS) does not require a clock on the device the device will then activate the Manufacturer Image, changing Firmware Version if successful.

The CH will wait to activation time (or current time, when activation time is zero) plus [X] minutes and read the OTA cluster's Firmware Version attribute from the IHD / PPMID / HCALCS. The CH will then create a Device Alert containing the IHD's / PPMID's /HCALCS' 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 Responsible Suppliers recorded to receive the Alert.

If this Device Alert is not received the Supplier can send a 'Read IHD / PPMID / HCALCS Device Model via the CH' SR to the DCC. This will result in a Command to the CH to read the OTA Cluster's Firmware Version, manufacturer etc. from the IHD / PPMID / HCALCS. The CH will send a Response containing these details to the DCC, the DCC will then update the SMI and forward the Response to all Responsible Suppliers.

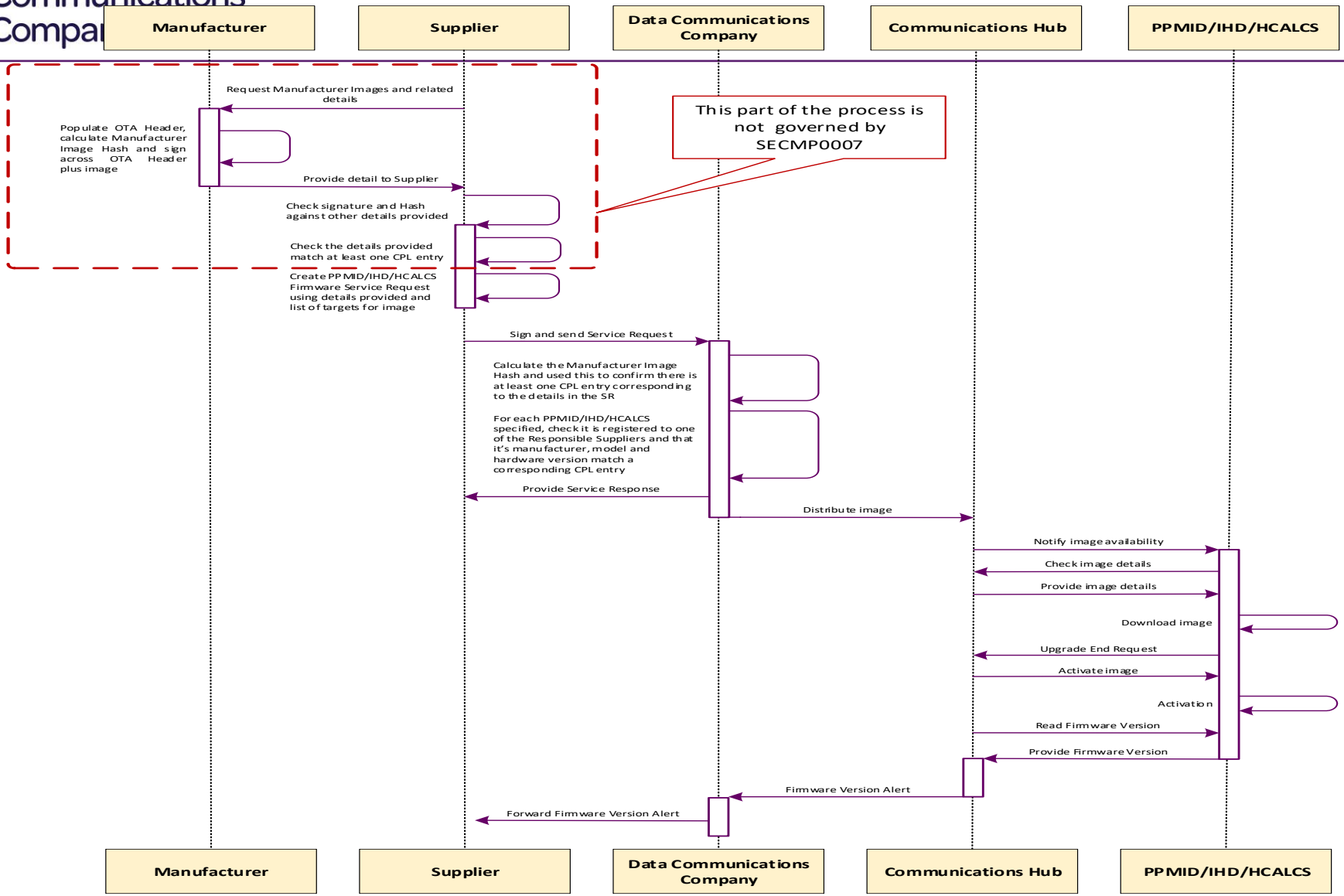


Figure 3: Process for updating an IHD's / PPMID's / HCALCS' Firmware – Image less than 750KB

Sending a Manufacturer Image 750KB or Greater

This section illustrates how activating images that are 750KB or more in size might be achieved. In the illustration following, the operating Firmware Version is 0x10, which is reflected in the CPL entry example in Table 2 below.

In this example, an IHD / PPMID / HCALCS image is to be updated to Firmware Version 0x20. This requires two images to be sent to the device, to provide all of the changed Firmware / configuration data required for Firmware Version 0x20.

The Manufacturer has split this upgrade data in to two images:

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

The New CPL entry looks like the following.

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 2: Example New CPL Entry for Manufacturer Image Greater than 750KB

To upgrade the Firmware of PPMID/IHD/HCALCS, the Supplier will follow the following process. The illustrative process is shown in Figure 4 on page 17.

1. Having undertaken the necessary checks, the Supplier will create a ‘Send IHD / PPMID / HCALCS Firmware’ SR to distribute Image 0x15 and set the activation date-time as zero (i.e. ‘activate now’). Note that when the image needs to be split into two images or more, the activation date-time should not be in the future, as explained below.

2. The DCC will distribute Image 0x15 to the CH. When the device has downloaded the image, the CH will start a timer for now plus [X] minutes. When that time has passed, the CH will read Firmware Version from the IHD / PPMID /HCALCS and send a Device Alert containing that value. Note that this value will still be 0x10 (in line with the Technical Specification Issue Resolution Sub-Group (TSIR) decision). Therefore, the Device Alert will only indicate delivery of the image. It will NOT indicate that the IHD / PPMID / HCALCS has successfully validated the image.

3. On receipt of the Device Alert from the DCC containing the device’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 TSIR's decision means there is no mechanisms to discover if the IHD / PPMID / HCALCS had that image).

4. The DCC will distribute Image 0x20 to the CH. When the device has downloaded the image, the CH will start a timer for activation time plus [X] minutes. When that time has passed, the CH will read Firmware Version from the device and send a Device Alert

containing that value. Note that this value will, if activation was successful, now be 0x20 (in line with the TSIR's decision). Therefore, this Device Alert will indicate delivery of the image and that the IHD / PPMID / HCALCS successfully activated the image.

5. If this Device Alert is not received, the Supplier can only resend Image 0x20.

The result is that the device will be operating Firmware Version 0x20, except where the Firmware upgrade process cannot be completed, such as where there is no Wide Area Network (WAN) connectivity,

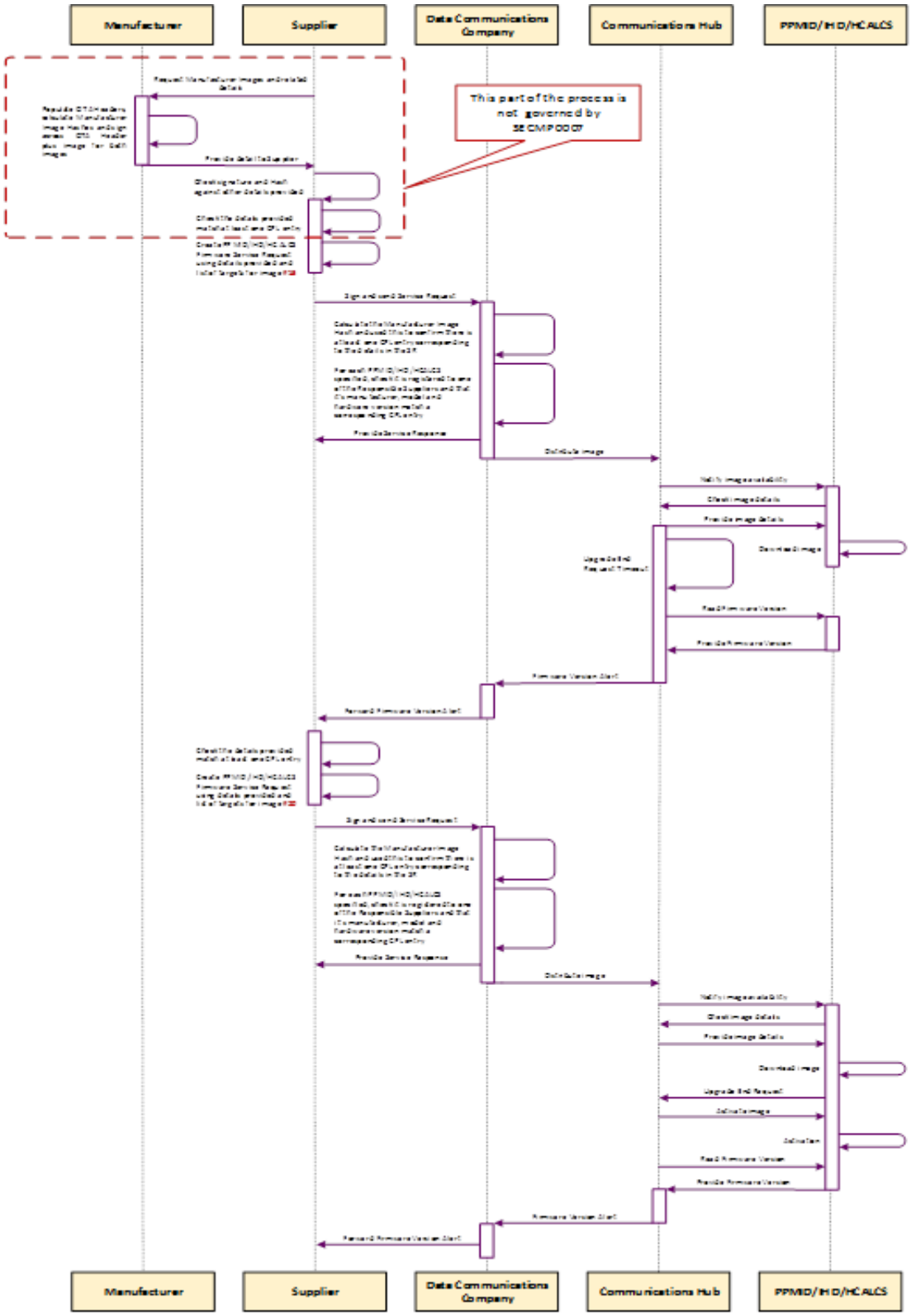


Figure 4: Process for upgrading an IHD's / PPMID's / HCALCS' Firmware – image more than 750KB

Non-Functional Requirements for Firmware Upgrades

Firmware upgrade images for devices are expected to be typically less than 750KB in size and would occur infrequently e.g. once per year. The customization of IHDs or PPMIDs

with graphics will increase the firmware size, this may happen going forward and require the mechanism for firmware sizes greater than 750 KB.

HCALCS are expected to have a much smaller firmware size and with a very low upgrade frequency. It may be possible that HCALCS 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 IHD / PPMID / HCALCS.

2.4.4 Changes to Existing Business Processes

Implementing the above requirements will have impacts on the existing business processes as noted below.

CPL Removal and SMI status, including Suspension

The changes defined above will mean that IHDs are on the CPL and therefore can be removed from it. This means that IHDs will need to be 'suspended' on the SMI. In turn, this means they will need to have an SMI status, whose values will need to be defined. Specifically, how the previous steps change IHD status (e.g. Update HAN Device Log) affects this status.

This will also constrain which Firmware updates can be sent to IHDs / PPMIDs / HCALCS (e.g. they cannot be sent if the CPL entry related to them is marked 'removed'). This will affect SEC obligations on DCC Users and Suppliers in terms of which SRs can be sent to IHDs / PPMIDs / HCALCS in which circumstances.

Consumers are currently able to operate 'suspended' PPMIDs. If this Modification Proposal is implemented, Consumers will be able to operate 'suspended' IHDs.

2.4.5 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 Overview, Option 1 – Original Approach, Zigbee OTA Delivery

Based on a review carried out by DCC and the key Service Providers in February 2019, two potential solution options were identified.

The first option is the one originally defined in the Solution Design provided by SECAS [Document 1].. Notes that since the SEC Modification was issued, Service Users have not deployed any significant volume of ZigBee only capable devices and instead a large majority of IHDs deployed are actually PPMID devices.

This option involves a mechanism to deliver the firmware images to the PPMID and IHD HAN devices, using Zigbee OTA delivery, the processing of which differs from that of other Devices. This mechanism requires new GBCS use cases to read device firmware. As this solution is intended for ZigBee capable devices only, the solution cannot communicate directly with the Service User and cannot re-use the existing capability for distribution and activation of HAN device firmware. As part of this option:

- The Comms Hub is to manage the activation of firmware
- The Comms Hub is to manage the notification to the Service User upon activation

A new DCC Only Service Request will be provided for the Service Users to send the firmware image to DCC Data Systems. DCC Data Systems will perform the necessary validations and forward the firmware image to the relevant Comms Hub by using an interface provided by the CSPs dedicated for firmware image delivery. The Comms Hubs will need to be updated to handle the delivery of the firmware images to the target Devices utilising the Zigbee OTA capabilities.

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

ARQ	H	BIMI	M	CHTS	Y		
TEF	H	GBCS	Y	CH	Y	HCALCS	N
CGI	H	DUIS, DUGIDS, MMC XML	Y	CPL	Y	PPMID	Y
P & C	H	SMETS	Y	ESME	N	IHD	Y
BT	N	SEC	Y	GSME	N		

A conceptual architecture view of the solution is shown following.

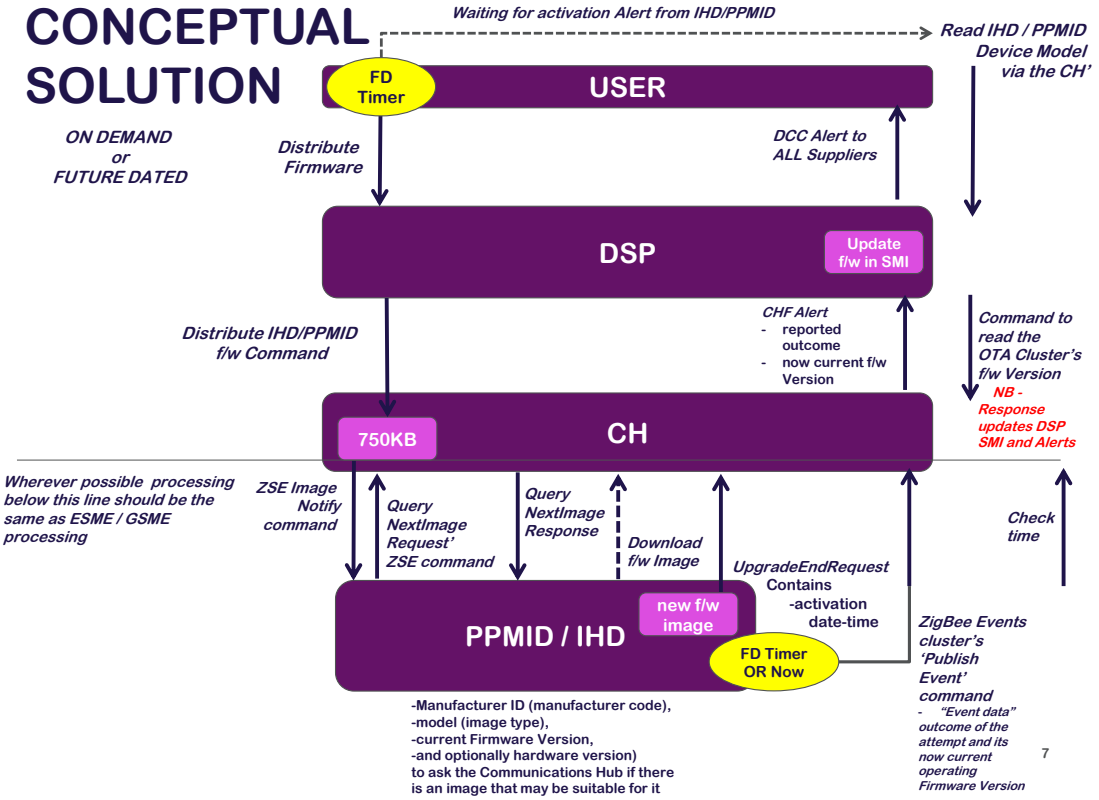


Figure 5: Solution Option 1 Conceptual Architecture

3.1 Approach Principles and Constraints

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 need to be enabled. In a proposed change to DSP functionality described in Assumption MP07-AT-1 below, the DSP will send only one firmware request at a time until the Comms Hub indicates the update is complete, and the oldest dated firmware is removed
- There must be a capability for 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

3.2 DCC Total System Impact

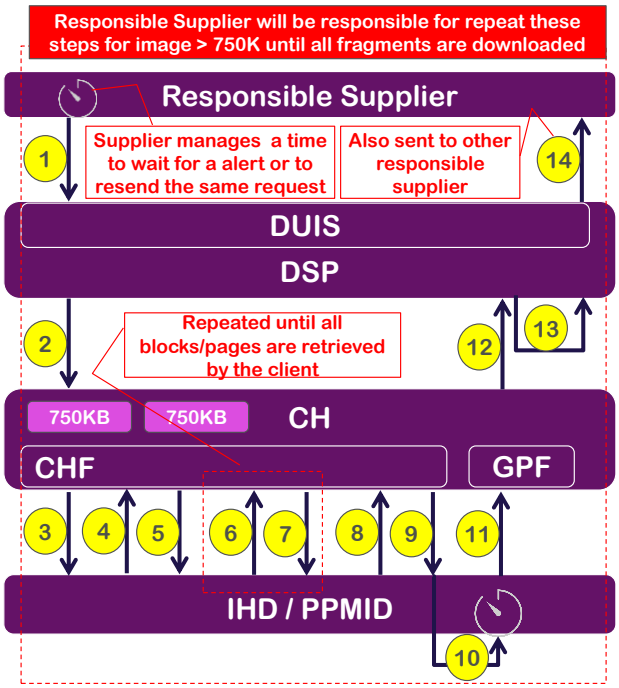
Analysis of the above requirements and consequential changes suggests that support would be mandated through the SMETS for all installed IHDs and PPMIDs, and through the CHTS for newly installed Communications Hubs. The changes would result in new obligations on the DCC, and Service Providers would be required to demonstrate that they are able to support the sending of a 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, unless there were changes to the SEC or a SEC governance mandated upgrade.

System	Component	Detail
DSP	CSP SMWAN Gateway and CSP Interfaces	New interfaces (one per CSP) required for sending a firmware image and a list of validated device IDs to the CSP, and for each device the associated CHF to which the request should be directed. There should be a mechanism to enable the CSP to reject device IDs if necessary (e.g. if they do not recognise a Comms Hub device ID), in a similar way to existing firmware updates.
	Self Service Interface	The SSI read inventory screen needs to be able handle an IHD firmware version, SSI Reports RSMI_001 and RSMI_002 will be updated to enable firmware versions to be reported for IHDs. The following SRs will be updated: • 12.2 Device Pre-notification • 8.4 Update Inventory • 8.2 Read Inventory
	Anomaly detection	Anomaly detection volume thresholds will apply to the new Service Requests and will be mandatory for a new SR11.4, even though it is not a critical request; it is assumed to be similar to SR11.1 in this respect.
	Energy Service Interface Inventory Extract	The Energy Service Interface (ESI) inventory extract for the Device table needs to be able contain a firmware version for an IHD.
	DUGIDS, DUIS SRs, and MMC, Alerts and Messages	Two new Service Requests will be introduced for Service Users to manage the firmware updates: SRV 11.4 – for suppliers to send the firmware; SRV 11.5 – for suppliers to read the firmware version. Unlike existing firmware upgrades there will not be a separate activation SRV. New Alerts will be introduced to handle the following scenarios: • Device image successfully downloaded • Device image successfully activated (or stored an image greater than 750KB and is not the last fragment) Given that PPMIDs, IHDs, and HCALCS may communicate with both GSME and ESME, both Import Supplier(s) and the Gas Supplier associated with the Communications Hub will be notified at the following stages of processing when:

		• the DSP has successfully processed a Service Request for an image's distribution • the device has attempted to activate new firmware (or attempted to store a part of a firmware that is greater than 750KB). New DCC Alert types are required to: • indicate failure by a Comms Hub to deliver a firmware image • notify successful firmware activation • report the Devices rejected by CSPs Changes to SR8.4 Update Inventory, SR8.2 Read Inventory and SR12.2 Pre-Notification.
	CPL	No changes to the structure of the CPL. Updates to CPL interface specification and to the processing of incoming CPL files.
	Transform	New GBCS Use case for CHF to read Firmware Version from device.
	Queuing	Implementation of a mechanism in the DSP solution to manage the queuing priorities of firmware distribution, to prioritise the ESME/GSME firmware distribution over other devices.
CSP	SM WAN (Network)	Within the CSP North SM WAN, Firmware upgrades are supported on dedicated broadcast Firmware download channels within each radio cell. To support this Modification, additional loading will be placed on the Firmware download channels. In the FIA there will be an action to understand the viability to support what this Modification requires, given the current capacity. Further capacity analysis to estimate the scale of any new requirements and any SLA impacts.
	Interfaces	Modification to the CSP/DSP SD4.4.2 interface to include a new API to provide firmware for IHD and PPMID devices. This is required to distinguish between ESME/GSME images and images for ZigBee only capable devices
	Comms Hub	Uplift the Communication Hubs to support the new commands to download firmware to devices in line with GBCS guidelines, over the SM WAN
	Comms Hub	Add support to Communications Hub to make system aware that a command or download is a completed action
	Solution	Modifications on CSP solution to support the new commands, data model variables and reports required to implement the download of firmware to the devices;
	Comms Hub	The Comms Hub will need to support the prioritisation of images, the reading of device model details and storage for additional Alerts, Commands, and Responses
All Service Providers	Support Systems	Uplift of billing and reporting systems/components to incorporate the additional SR transaction charges. The SM WAN transaction billing approach may need to change as a result of this Modification.

	Support Systems	Support for additional alerts, commands, and responses.

3.3 Impact on System Integration and Interfaces



No	Description
1	Call DUIS SR – Upgrade Firmware with Activation Date (must be 'Now' if fragmented image and not the last fragment)
2	Send corresponding GBCS command to CH (CSP Systems not shown to aid clarity)
3	OTA: Notify Image
4	OTA: Query Next Image Request
5	OTA: Query Next Image Response
6	OTA: Image Block/Page Request
7	OTA: Image Block/Page Response
8	OTA: Upgrade End Request
9	OTA: Upgrade End Response (includes activation date) If Image > 750, the activation date will always be 'now' except for the last fragment
10	Activate Firmware (If fragmented image and not last fragment, it will just be stored)
11	Event : Publish Event (Firmware Upgraded or Firmware Downloaded based on last fragment or not)
12	Forward Event
13	Update SMI If event = 'Firmware Upgraded' and not 'Firmware Downloaded'
14	DUIS Alert to Supplier and other Responsible Supplier

One new interface per CSP will be built for sending a firmware image and a list of validated device IDs of PPMIDs, HCALCS or IHDs to the CSP, and for each device the associated CHF to which the request should be directed. There should be a mechanism to enable the CSP to reject device IDs if necessary (for example if they do not recognise a Comms Hub device ID), in a similar way to existing firmware updates.

3.4 Data Management

Data Management requires changes to enable the IHDs to have firmware versions mapped to a GBCS version.

In addition, there is a need to add mappings for the new DUIS SRVs, for the alerts between DUIS version and the SRV, and to the GBCS version against the use case where applicable.

3.5 Infrastructure

The Modification will lead to additional data processing. 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 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.

4 Solution Option 2 –Extend Proven OTA Firmware Method for HCALCS

The imperative for Option 2 is to extend the existing OTA firmware update procedure to the mandated HAN devices. This approach support firmware distribution in a manner that would be similar to ESME and GSME firmware distribution and activation using GBCS critical commands.

For this Option, impacts across the system actors and components are as follows:

ARQ	H	BIMI	N	CHTS	N		
TEF	H	GBCS	N	CPL	N,	HCALCS	Y
CGI	H	DUIS. DUGIDS, MMC XML	Y	CH	Y	PPMID	N
P & C	H	SMETS	Y	ESME	N	IHD	N
BT	N	SEC	Y	GSME	N		

4.1 Approach Principles and Constraints

The main principles of the alternative approach to implement firmware upgrades is based on a very different approach from Option 1, described in section 3 above:

- This approach treats any device endpoint like an ESME, such that the firmware is pushed to it with credentials.
- This approach may require modification to the ESME firmware distribution approach in that the user may be required to plug a battery powered device into the mains supply before transferring and activating an image as well as handling exceptions generated by a loss of power during firmware distribution and activation.
- There will need to be device changes to support keys.
- There is a requirement to ensure end to end security for the firmware image.
- 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. This approach will use separate functionality as described in Assumption MP07-AT-2.
- There is no dependency on the ESME device.
- CHTS changes will be required.

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

4.2 Comparison of Option 1 and 2 System Impacts

Both options would require development by manufacturers under the direction of Service Users and would likely not be supported by any HAN devices that have been deployed to date.

The second option uses proven technologies and protocol implementation, relatively limited DCC change, and limited SIT testing costs based on a modified testing approach. There would be changes to Technical Specifications, costs for CPA, and a major concern that no such devices exist, but the request from the Working Group is to progress with Option 2 for HCALCS.

The following table summarises the impacted components for each of the options.

Component	Option 1	Option 2
CPL	No changes to the CPL structure. Updates to CPL interface specification and to the processing of incoming CPL files.	Updates to CPL interface specification and to the processing of incoming CPL files.
DUGIDS, DUIS and MMC	Changes to DUIS and MMC XML schemas. New SRV 11.4 for Service Users to send firmware images. New SRV 11.5 for Service Users to read the firmware version from a Device. New DCC Alert types • to indicate failure by a comms hub to deliver a firmware image; • to notify successful firmware activation; and • to report the Devices rejected by CSPs. Changes to SR8.4 Update Inventory, SR8.2 Read Inventory and SR12.2 Pre-Notification.	DUGIDS documentation updates for SR11.1, SR11.2 and SR11.3. Changes to DUIS or MMC XML schema to support the Type1 IHDs. Changes to SR8.2, SR8.3, SR8.4 and SR12.2
Request Management	Processing new Service Requests, new validation checks, handling scenarios of the new DCC Alerts etc.	Updates to processing of SR11.1, SR11.2 and SR11.3. Changes to SR8.4 Update Inventory, SR8.2 Read Inventory, 8.3 Decommission Device and SR12.2 Pre-Notification.
Data Management	No changes	Reference data updates to support new Type1 IHD.
Transform	New GBCS Use case for CHF to read Firmware Version from PPMID/HCALCS/IHD.	Support for Read Firmware and Activate Firmware on HCALCS.

		Changes to GBCS Use Cases.
CSP SMWAN Gateway	New interfaces (one per CSP) required for sending a firmware image and a list of validated device IDs of PPMIDs, HCALCS or IHDs to the CSP, and for each device the associated CHF to which the request should be directed.	No changes.
SSI	Add support for IHD in the Read Inventory screen. Updates to SSI Reports RSMI_001 & RSMI_002 to enable firmware versions to be reported for IHDs.	
Anomaly Detection	Anomaly detection volume thresholds will apply to the new Service Requests and will be mandatory for SR11.4.	No changes.
ESI Inventory Extract	Include firmware version of the IHD in the ESI inventory extract for the Device table.	

5 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 are expected to impact both whichever solution option is selected.

5.1 Security

The solution presented in this PIA will require a security review, particularly in relation to the solution options that require introduction of a new Device Type and the aspect of key management it necessitates. The costs within this PIA assume that the functionality does not require a specific security solution such as physical or logical separation from other parts of DCC Data System (in the same way as SMKI Recovery and Change of Supplier is separated) and does not require any separation of duty for the purposes of operational support.

The solution must allow for maintenance of any existing product certification such that the product certification can be reasonably extended to include the functionality in this Modification.

Further discussion is required in respect of the security solution prior to progressing to Full Impact Assessment. Solution Option 2 would include security related effort for device manufacturers.

5.2 Release Approach

Following discussion, this PIA response is based on the possible delivery of SECMP0007 alongside other similar SEC Modification changes as part of a larger release. The finalising and timing of the release will be considered as part of the FIA, but is referenced as the November 2020 release at this time.

5.3 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.

5.4 Application Support

On the basis that updates to configuration will be charged under separate Operational Change Requests, it is not expected that there will be any change to ongoing levels of support as a result of the change. There will need to be some updates to service procedures in advance of the new solution being deployed to the Production system.

Logging and ad-hoc retrieval of HAN firmware transfer history where available should be implemented.

There will be a need to support the generation, processing and storage of CH triggered alerts in relation to progress of transfer of firmware across the HAN for both CSPs. CSP South and

Central has identified the need for this capability due to the expected increase of firmware distribution activities and the expected associated increase in firmware storage contention within the Communication Hub.

5.5 DCC Service Management System (DSMS) Impact

No specific DSMS requirements or changes have been identified for either of the options at this stage.

Two further items will be included in the FIA:

- The CSP Service Desk will require coordination for CH Specialists and will need to understand timings and frequency of downloads
- An requirement to plan and schedule such that the system can avoid Network conflicts and saturation when trying to push out CH firmware downloads at specific same time

5.6 Infrastructure Impact

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.

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 Modification to cover additional compute and storage capabilities to cover this aggregated impact in the future.

5.7 Volumetrics

Around 25 million devices are expected to be made firmware updatable as a result of this change. Firm volumetric estimates have not been supplied but as an illustration: if all of them were to have their firmware updated once per year in batches of 10,000, that will result in 2500 Service Requests per year and associated Alerts.

5.8 Safety Impact

DSP will perform a safety risk assessment of the functional design and will update the DSP Safety and Environment Case deliverables accordingly. These items are updated and re-issued for each major DSP release (at least once annually).

5.9 Billing, Reporting and Performance Measures

For both Solution options, the FIA for each Service Provider's reporting solutions will require in-depth analysis to ascertain the impact on Performance Measurement 2 (PM2).

The Category 1 Firmware Payload Service Measure target service level may be impacted by the volumes, and therefore the CSPs expect to review this PM target service level to counteract any risk of meeting PM2; There may be a need to expand the scope of the PM to include the delivery of IHD, PPMID and HCALC firmware, and potentially to include an additional service reporting exemption where a CSP is unable to deliver firmware due to an in-progress delivery of firmware

Potentially an additional service reporting exemption where firmware image data integrity issues are identified may be needed.

At this stage we are assuming that the firmware requests are not to be included in the PM2 measurement/calculation, with no associated costs, but the SPs will need to evaluate the impact and timings for these Firmware downloads. Any changes to the reporting will require design, build, and test.

As noted above, a review is required of whether the CSP's SM WAN transaction billing approach needs to change as a result of this Modification. The current SM WAN transaction charging approach defined in schedule 7.1 does not permit Telefónica to charge for any transactions where transaction charges are within band 2 and that this Modification will further increase the number of transactions expected such that Telefónica will be unable to charge for band 2 transaction. CSP South and Central therefore expects to renegotiate the SM WAN transaction billing approach during the FIA process to something that reduces the complexity and operational cost whilst permitting charges for increased service usage.

5.10 Contract Schedules

Schedules will require modification for both the Central and South CSP regions to reflect the changes necessitated under this Modification. The contract schedules will be updated as part of a CAN which combines schedules updates from other relevant Modifications.

Expected contract schedules to be amended include:

- 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 7.1 – to reflect any payments under this Change Request and to reflect any additional service requests to be billed;
- Schedule 11 – to reflect an uplift to the CH specifications;
- Schedule 12 – to reflect the uplifted technical specification versions (such as GBCS and CHTS).

6 Implementation Timescales

Implementation of this change is assumed to follow a waterfall methodology. It is assumed that this change will be implemented as part of the November 2020 release alongside other change requests. This change will take of the order of six months to achieve PIT Complete status, which includes design, development and system testing. The need for some more complex Systems and User Integration testing means that the release will take 12 months to implement. However this duration will be confirmed as part of the FIA.

6.1 Testing and Acceptance

This change includes the standard test phases as documented in schedule 6.2 and standard exit criteria will apply:

It should be noted that this Modification applies to a large number of devices already in the field, such that testing can be against devices rather than emulators in a large number of cases. The addition of HCALCS to the scope of this solution will have a material impact on testing the firmware update functionality,

The SPs will need to plan for PIT testing which will be performed against stubbed HAN devices, assumed to be developed and supplied by the meter suppliers, as part of their Workstream testing. Further modification of Test Stubs to support the testing of this Modification across the CSP solution within the PIT environment.

Testing against actual devices will be performed in SIT but is not included in the following estimates at this time. If SIT testing for this modification is interleaved with other SIT testing, there will be an opportunity to save testing effort - there will be a dependency on the device manufacturer providing timely updates to their HAN devices.

Further savings could be made if the timings of the device releases are managed carefully so that one Test Engineer can test all the device types/models with no downtime. Similarly, PIT and SIT regression testing effort can be performed once per release. If a future release contains multiple Modifications, the regression testing can be performed once per release rather than once per Modification.

7 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The ROM shown here describes indicative costs to implement the functional requirements as assumed now. The price is presented as a +/-15% range and is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result the final offer price may result in a variation outside of the indicative range.

7.1 Design, Build, and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification.

Implementation Costs							
Solution Option	**Design**	**Build**	**Pre-Integration Testing**	**System Integration Testing**	**User Testing**	**Implement to Live**	**Total**
Option 1	*£12,300,000*			*Not included*	*Not included*	*Not included*	**£12.3m**
Option 2A	*£8,500,000*			*Not included*	*Not included*	*Not included*	**£8.5m**

Supplementary Information	
Implementation cost assumptions	*A. Costs are exclusive of VAT and any applicable finance charges* *B. Majority of the costs above represent labour costs.* *C. Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers with specific exclusions of costs as identified above. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* *D. Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design 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.* • *Pre-integration Testing: Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.*

	• *System Integration Testing (SIT): All Service Providers' PIT-complete solutions are brought together and tested as DCC's Total Solution, ensuring all Service Provider solutions align and operate as an end to end solution.* • *User Integration Testing (UIT): Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.* • *Implementation to Live Costs: The solution is implemented into Production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

The fixed price cost for a Full Impact Assessment is **£187,703**, and is expected to be completed in 60 days.

8 Risks, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

8.1 Risks

Ref.	Area	Description	Impact
MP07-RD01	HCALCS	Is the addition of HCALCS to the scope warranted in terms of the business case? How likely are we to need HCALCS firmware updates? It should be noted if issues with HCALCS firmware occurs, the only way to resolve these is via exchange of the HCALCS. This mandates an installer attending the site; inclusion of the HCALCS in SECMP0007 mitigates these costs	H Accepted, HCALCS is warranted for the business case. They must be OTA upgradeable
MP07-RA02	General	Any changes to the scope or interpretation of the items in scope will require re-assessment	M Accepted
MP07-RD03	Non Functional Requirements	Without a detailed provision of Non Functional Requirements (NFR), particularly relating to expected frequency and extent of firmware upgrades, it will be difficult to assess network and other infrastructure requirements.	M SECAS advise that the business requirements document notes that firmware updates for IHDs and PPMIDs are expected to be aprox once a year. HCALCS may be once per year, potentially even less frequent.
MP07-RD04	Non Functional Requirements	Without a detailed provision of Non Functional Requirements (NFR), particularly relating to monthly volumes will be difficult to assess PM2 implications.	M SECAS advise that the business requirements document notes that firmware updates for IHDs and PPMIDs are

			expected to be aprox once a year. HCALCS may be once per year, potentially even less frequent.
MP07-RD05	CSP North	In the event that allocating 5 additional channels is not possible due to conflicting demands on bandwidth in the CSP North solution, there is a further risk that CSP North will need to install additional masts and base stations to support the need for additional bandwidth. Note there is a suggestion that updates can be time-multiplexed on a single physical change.	M Noted. However, solution via CR1047 will address this as noted in MP07-AT-11.
MP07-RT01	Technical Specifications	The technical specifications (including GBCS, SMETS and CHTS) associated with the functionality described in this Modification have not been developed, nor have the change resolution proposal (CRP) that would normally be developed to specify new functionality in the technical specifications. As a result, there is a risk that the design effort and duration required to deliver this Modification will increase. Telefónica would expect to review this Impact Assessment following review of the technical specifications should there be a material difference between the information provided to date and the technical specifications. One approach would be to arrange for the formal documentation of the modifications to the technical specifications via CRP / IRP prior to the completion of the Impact Assessment of this Modification	M Accepted
MP07-RT02		There is a risk that due to there not being any clear, granular NFRs for firmware delivery within this Change Request, Telefónica will need to revise the PM2 target service level as part of this Change Request. Telefónica will review the viability of maintaining the current PM2 target service level as part of the Impact Assessment. Note that the NFRs provided as part of this Change Request are: - based on an assessment of usage prior to deployment in live; - defined at an annual granularity. This is not a sufficient granularity to determine system capacity. Wider discussions have been taking place with DCC demand management regarding the existing	Noted

		demand planning and providing hourly breakdowns on key service requests which would include firmware delivery. - have not been provided by Service Users as part of a demand forecasting exercise.	
MP07-RT03		There is a risk that increasing the number of devices that can receive firmware images on the HAN via the Communication Hub may result in image storage contention on the Comms Hub and therefore limit Telefónica's ability to meet PM2 in relation to firmware distribution without either overwriting firmware images before they have transferred. Telefónica expects to mitigate this risk by introducing a service reporting exemption for PM2 where the Communication Hub cannot download the firmware image within the PM2 timeframe due to storage contention.	Accepted – Solution via CR1047 should partially address this as noted in MP07-AT-11.
MP07-RT11	DCC-L	There is a risk that extending firmware upgrades to HAN devices that are distributed amongst consumer premises and directly interacted with consumers may result in additional failure modes through consumer manipulation of devices (e.g. removing the power supply). IHDs must be mains powered, so this is most likely a risk for PPMIDs. From a Telefónica perspective, this may result in an increase in the number of tickets regarding HAN communication failure. Telefónica cannot accept liability for indirect or consequential losses which arise in respect of this risk.	Accepted
MP07-RT12	DCC-L	There is a risk that DCC's overall timeframe for the June 2020 release is not viable given the current Change Request approach of considering each Change Request in isolation rather than as a single delivery. Telefónica recommend that the DCC-L attempt to mitigate this risk via the following points prior to any request to start the Impact assessment process: - confirm the scope of the solution; - progress with a single Impact Assessment containing only the confirmed scope for the June 2020 release; - provide a single list of all solution related and test related clarifications; - confirm the expected Change approval timeframes; - confirm the expected PIT exit timeframes.	Noted – SECAS confirm the scope of this modifications includes IHDs, PPMIDs and HCALCS.
MP07-RT13	DCC-L	There is a risk that the timeframe for the delivery of this Modification and that of DCC CR1047	Accepted

		(assumed to be delivered via as part of a maintenance release) in accordance with the DCC defined Firmware Management Policy will overlap. If this is the case, this may add significant complexity to the delivery of this Modification and potentially affect delivery timeframes.	
MP07-RT14	DCC-L	There is a risk that the PIT approach for this Modification may change as there have been no requirements on Testing aspects as to how the solution is to be assured during the PIT timeframe. Assumptions on both the PIT approach and firmware merging approach have been made below.	Accepted
MP07-RS20	Option 2A	PPMID devices can have multiple suppliers, which implies there is a need to support two sets of supplier certificate trust anchors as well as two sets of device certificates This adds the obligation for IHD manufacturers to pre-load Supplier or ACB certificates. In the case of preloaded ACB certifcates it needs establishing how the second supplier can load their certificates.	Rejected as Option 2A only applies to HCALCS. IHDs and PPMIDs will be following Option 1. SECAS note that the Proposer and the Working Group opted to utilise option 1 specifically for IHDs and PPMIDs. Option 2 would have required IHDs and PPMIDs to go through CPA which the Working Group were against due to the time and effort this would take. This will be noted in the Modification Report.

8.2 Assumptions

It is likely that further assumptions will be established as part of the FIA.

Ref.	Area	Description	Accept
MP07-D01	Option 1	It is assumed that the DSP will keep track	Accepted,

		of which individual PPMIDs, HCALCS and IHDs have upgradeable firmware and block firmware upgrade requests to older devices which cannot support upgrades. GBCS version information will be used for IHDs where it is available, however the DSP does not currently record firmware version for IHDs and in such cases the IHD will be assumed to have non-upgradeable firmware. For any cases where IHDs are already in the inventory, before the DSP release, are later-model devices which do have upgradeable firmware, suppliers would be able to use SR8.4 Update Inventory to change the inventory firmware version of the IHD, which would be permitted in such cases.	Any updatable Devices will need to be added to the CPL; this is a clear inidiciation to Suppliers as to which Devices can be targeted.
MP07-D02	Option 1	If a CPL update removes validity for an IHD firmware version, IHDs using it cannot be suspended since IHDs do not have device status. The effect of the CPL removing validity would be that new pre-notifications or firmware upgrades for that firmware version would be blocked, but devices already using it would not be affected.	Accepted
MP07-D03	Option 1	The expectation is that within the Comms Hub the implementation will use the ESI of the GPF. We assume that it is the CSPs' responsibility to verify that this will work even if there is no gas meter on the HAN, or the device is not joined to the GPF, and that there is no requirement for the DSP to check whether the device is joined to the GPF.	Noted, but this doesn't make sense. SECAS believe it would make more sense to use the Communications Hub Function. There is no requirement for the DSP to check whether a Device is joined to a Gas Proxy Function.
MP07-D04	Option 1	Although not identified in the requirements above, we understand that it is expected that a single physical device may contain PPMID, IHD and CAD functionality, with a single device ID. It is assumed that in this case the device model would be identified on the CPL as a PPMID, and correspondingly an individual device would be pre-notified as a PPMID. The inventory would store a record of the device as a PPMID and would have no record of the existence of the IHD or CAD functionality of the device. Any firmware update would be	Accepted

		just to the PPMID, again with no separate identification of the IHD.	
MP07-D05	Option 1	It is assumed that no change is required to CPL processing to handle firmware updates which are split across two or more images. Each will have a separate CPL entry with a unique firmware version ID and hash for that fragment, and there will be no identification in the CPL or the DSP database that the firmware versions are components of a multi-part firmware version.	Accepted
MP07-D06	Option 1	The CPL will contain no more than one entry for a firmware version. If a firmware version is compatible with more than one GBCS version it will be reported in the CPL for only one of them. This seems to contradict current CPL rules where some meters are associated with two GBCS versions.	Noted. Although this isn't in the scope of this modification, but SECAS think it should be able to follow current standard process as noted here.
MP07-D07	Option 1	Currently hand-held devices are pre-notified as IHDs. However this will not work if a CPL-compliant IHD firmware version is required in the pre-notification message. A revised approach to managing hand-held devices may be needed as a result of this change. This is not currently included in the scope of this assessment.	Accepted – Although not necessarily in the scope of this modification, SECAS ask DCC to consider listing Hand-Held Terminals as a Device.
MP07-D08	Option 1	The original requirements of Option 1 state that there will be an alert which indicates "IHD / PPMID image successfully downloaded". It is assumed that this refers only to successful download of an intermediate part of a multi-part firmware download, and that for a future-dated update there will be no device alert until the trigger date is reached and the update is activated.	Accepted
MP07-D09	Option 1	Although not identified in the requirements above, we assume from workshops that there will need to be a device alert from the comms hub to the ACB if delivery of a firmware image from the comms hub to the target PPMID, HCALCS or IHD has failed, for example because the firmware image was deleted due to a higher-priority firmware image for another device.	Accepted
MP07-D10	Option 1	Where delivery of a firmware image has failed and the comms hub sends a device	Accepted

		alert to the ACB, there will be no attempt by the CSP or DSP to retry delivery. It will be the supplier's responsibility to re-request delivery.	
MP07-D11	Option 1	Anomaly detection volume thresholds will apply to the new service requests and will be mandatory for SR11.4 (in a similar way to SR11.1).	Accepted
MP07-D12	Option 1	The DSP will not manage the state of in flight requests, for example if an ES and a GS send firmware updates for the same device at about the same time, the DSP is not required to prevent that situation and will simply forward valid requests as they are sent.	Accepted
MP07-D13	Option 1	The new DCC Alert which is to be sent to suppliers when firmware for a PPMID or IHD is successfully activated or downloaded will go to all interested suppliers. In the case where it indicates successful download of part of a multi-part firmware update, the SECAS information appears to suggest that the firmware successfully downloaded will not be identified in the device alert which is sent (as only the currently active version will be sent). This means that if two suppliers are trying to upgrade firmware for the same IHD or PPMID at about the same time, the DCC Alert will not enable the suppliers to determine that it might not be their own firmware image which was successfully downloaded.	Accepted as will be covered by SECMP0024
MP07-D14	Option 2A and 2B	The Modification notes that Option 2A and Option 2B may require the consumers to plug a battery powered device into the mains supply before transferring and activating the firmware image. The firmware update process will need to handle exceptions generated by a loss of power during firmware distribution and activation. The PIA assumes that this will be handled outside of the DSP solution.	Accepted, only applies to the PPMID
MP07-D15	Option 2A and 2B	It is assumed that the proposal for the Access Control Broker (ACB) to add Supplier certificate information to commands sent to PPMIDs will be acceptable from a security perspective	Accepted. SSC agreed with option 1 which does not require to add ACB certificates to the devices. Option 2A for HCALCS needs

			to reviewed by SSC.
MP07-D16	Non Functional Requirements	For volumetric calculations, assume two firmware upgrades per device per year	Rejected, Solution Design states one per device per year
MP07-A24	CSP North Volume	It is assumed that 5 channels of additional Spectrum are required to support Firmware downloads of devices. The network has been sized for the current expectation of traffic volumes and will be reviewed during IA stage. We will require confirmation of the number of Firmware downloads if a FIA is requested.	Rejected – As noted under MP07-AT-11, CR1047 limits the number of firmware updates and therefore does not require additional channels.
MP07-A25	Priority	A new priority will be configured in the CSP networks that would prioritize ESMEs and GSMEs over IHDs, PPMIDs, and HCALCS.	Accepted
MP07-A26	CSP Operations	No new Service Levels or Performance Measures will be required.	Accepted, there is no new service level required relating to SRs. In any case this would be between the DCC and the CSPs.
MP07-A27	Comms Hub	Assumed no impact to CH Memory. If CH Memory is impacted CSPs will need to investigate alternative approaches such as Image Compression and/or the management of ESME, GSME, PPMID, HCALCS, and IHD firmware downloads to avoid concurrent images. These alternatives are not included in the RoM or IA production cost.	Accepted
MP07-A28	Service Management	Assume that no additional Incident Management will be required to support these Firmware downloads. Should the chosen solution create the need for additional incidents then an assessment of resource levels would need to be undertaken as part of the IA.	Accepted, this should be standard Incident Management.
MP07-AT-3	Firmware Image	Any firmware images that are deployed as part of functionality within this Change Request will match the current ESME / GSME firmware image sizes	Accepted

MP07-AT-4	Service Reporting	CSPs assume the following for service reporting of the functionality associated with this Modification: - To be included within the existing PM2 Service Measure - Telefónica may review and amend the PM2 target service measure as required - A period, the duration of which to be defined, of monitoring service performance after the introduction of this Modification into the Live environment during which there will be a let on the PM2 target DCC is supportive of new PM2 service reporting exemption(s).	Accepted. SECAS note they are not asking for any changes in service reporting.
MP07-AT-5	Specifications	Assume that the scope of the PIT Approach uplift required to support this Modification is limited to changes that are required to assure the specifications as noted above and do not introduce any additional scope including but not limited to: - Distribution of firmware using new service request to updated PIT emulator - Distribution of multiple firmware jobs in succession using both existing and new service requests - Confirmation of correct billing behaviour - Confirmation of correct service reporting and service reporting exemption behaviour - Potential introduction of multiple testing phases to consider reporting as a separate phase to all other aspects to occur after formal PIT exit / SIT entry	Accepted
MP07-AT-6	Changing Specifications	Assume that when the associated TSG specifications and / or CRPs / IRPs to support specification change for this Modification are defined such that there will be no material changes from the documentation referenced above.	Accepted
MP07-AT-7	DUIS Version	Assume that the DUIS schema version used for the CSP management interface will not be required to increment because of this Modification. If this is not the case, then there will be additional effort to load the updated DUIS	Rejected – Likely to be changes to DUIS Schema but SECAS are not aware of any changes to the

		schema into Telefónica systems and to regression test this functionality in PIT.	CSP management interface.
MP07-AT-8	Firmware Change	Assume that the firmware changes to support the delivery of this Modification will be managed as part of a DCC release operating in parallel with the maintenance release process.	Accepted, SECMP0007 will be implemented in a Scheduled SEC Release along with other modifications. Firmware changes will be managed in that SEC Release.
MP07-AT-9	Specifications	Assume that modifications to the GBCS, SMETS, and CHTS specifications will be based on a baseline in place and established by the time this Modification is implemented.	Accepted, SECMP0007 will be implemented in a Scheduled SEC Release along with other modifications. Firmware changes will be managed in that SEC Release.
MP07-AT-10	Emulator Devices	Meter emulator functionality modification to support this Modification is required for PPMID OTA when connected via a meter (rather than direct to the CH). Note that the meter emulator used in the Telefónica PIT environment does not currently emulate interactions with an IHD. If the Working Group believe that IHD testing beyond that detailed in this Modification is required, then this needs to be flagged and added to the scope prior to the FIA creation.	Accepted but SECAS do not believe meter emulator changes are required.
MP07-AT-11	Firmware Image Validation	Assume that the cryptographic validation required by the CSP solution for device images is the same as that currently in place for meter firmware, namely hash integrity checks only	Accepted, the crypotographic specification will follow the OTA requirements in GBCS. Manufactureres are free to add addiotnal cryptographic security inside the firmware Image.
MP07-AT-12	Firmware Storage Prioritisation	Assume that HAN device firmware storage prioritisation rules for implementation in the Comms Hub specifically regarding	Accepted. If no firmware upgrade is in

		overwriting stored images on the Comms Hub with a new SMWAN download will be limited to rules of the following complexity: 1. Existing firmware image has been stored on CH for a maximum defined duration and is eligible to be overwritten; 2. No HAN device has attempted to retrieve the original firmware image or any parts of the firmware image following download across the SMWAN; 3. There is currently no firmware image transfer across the HAN in progress; 4. Use of the force replace flag to override firmware storage, except in case 3, when force override will occur after HAN image transfer is complete; 5. Storage of new ESME / GSME firmware will overwrite CH stored IHD / PPMID / HCALC images, except in case 3 where HAN image transfer needs to complete before overwriting.	place the a new SM WAN download can be started (subject to a reasonable timeout for devices on the HAN to react
MP07-AT-13	CSP Queuing and Prioritising	Assume that the DSP will implement a firmware service request prioritisation approach as follows: - Firmware SRs will be throttled such that there is only one firmware service request per active Communication Hub in progress within the CSP. - Progress in determining whether a Comms Hub has an in-progress firmware SR. This will be measured by the monitoring from the point at which a firmware service request is received for a specified Comms Hub until a GBCS defined alert associated with receiving a firmware image is sent from the HAN and received by the DSP. - The DSP will implement a per Communication Hub timeout for a period that will be agreed with the CSPs to override any throttling by the DSP. It should be noted that a DCC Change Request has been raised to allow DSP to deploy a capability that will serve to throttle and queue firmware distribution SRs to the CSP by limiting Service Requests sent by Service Users such that only one firmware distribution activity is in progress per CH at any point in time.	Accepted, CR1047 will address this.

MP07-AT-14	Service Request Management	Assume that Service Request compatibility across HAN devices including the Communications Hub introduced by this Modification will be managed by an upstream system / party (e.g. DSP / Service User) such that Service Requests to deploy HAN device firmware for HAN devices that do not support this type of operation and not sent to the CSP	Accepted, this should be carried out via the CPL and the SMI as the two of these define what Devices are eligible for firmware updates.
MP07-AT-15	Device	The CHF created Device as described in the Requirements above, is a GBCS defined alert sent from the CHF to the DSP directly over the SMWAN.	Accepted – Note: This will also be a Response to the DSP as well as an Alert.
MP07-AT-16	Testing	Assume that later phases of testing will from a testing perspective include the following as a minimum prior to any Go Live of the functionality delivered in this Modification: - System Integration Testing; - User Integration Testing; - Operational Acceptance Testing; - Business Acceptance Testing - Security Testing	Accepted
MP07-AT-17	Firmware Images	Assume that the DSP solution will be updated to validate the structure and integrity of the firmware images supported as part of this Modification	Accepted, but needs to be verified by DSP. SECAS believe this will be closely aligned to the OTA requirements set out in GBCS. Only the Hash integrity check will be carried out.
MP07-AT-14	Firmware Images	Firmware image sizes will not exceed 750Kb and will be prevented from transmission to Telefónica's solution by the DSP should they exceed this. This contradicts the requirements and should be investigated. The suggestion is that larger images must be supported.	Rejected as its possible for PPMID firmware Images to exceed 750Kb, as noted in the SECMP0007

			business requirements.
MP07-AT-21	PIT	Confirm expectations regarding the PIT Test approach for this Modification in relation to the scenarios and variants to be used in PIT testing. It is assumed the current PIT test approach as used for the testing of maintenance releases of Firmware will be sufficient for the testing of this Modification.	Accepted
MP07-AT-22	CSP Queuing and Prioritisation	CSP provision of support for queuing and prioritising specific types of firmware distribution over other types. It is assumed the DSP will deploy a capability that will serve to throttle firmware distribution SRs to the CSP by limiting Service Requests sent by Service Users such that only one firmware distribution activity is in progress per CH at any point in time.	Accepted, this relates to CR1047.
MP07-AD-30	Comms Hub Device	Assume there is no option to upgrade memory on the Comms Hub.	Accepted
MP07-AD-31	Split Ownership	In the cases of split ownership of devices, the SEC indicates that either party should be allowed to upgrade the firmware. The DSP will carry out an access control test, and if a response is directed from a responsible supplier, the upgrade shall be allowed.	Accepted

8.3 Issues

None at this time.

Ref.	Description	Mitigate?

8.4 Dependencies

Ref.	Org	Dependency	Impact	Accept
MP07-DD1	GBCS	There is a dependency on provisioning of two new GBCS use cases for Option 1. This has a high impact on the timescales.	Timescales and Cost	Accepted, the use case will recycle aspects of the update firmware request for meters.
MP07-AD2	GBCS	CH development is currently based on the GBCS 2.0 Draft 5. At the time of writing	GBCS Version for Baseline	Appected but the GBCS version will be defined at the

		this is the latest version of GBCS as per the Agreement. However, GBCS 3.2 Is planned to be released in November 2019.		time of development.
MP07-DT-1	DCC-L	CSPs have a dependency on the DSP sharing a version of any updated interface specification during the early design stages such that CSPs can review and incorporate the specification into system designs	Telefónica will not be able to complete design activities in alignment with any provided delivery plan	Accepted
MP07-DT-2	TEF	Telefónica has a dependency on the implementation of the next major release of Telefónica's Smart m2m solution to support the deployment of this Modification whilst maintaining the existing service obligations as the solution continues to be deployed. Should the timeframes for the deployment of the next Smart m2m (Telefonica application) version make the delivery of this Modification to support a June 2020 Go Live not feasible, Telefónica will review the feasibility of delivering this Modification without the Smart m2m release.	Telefónica assume that DCC-L will be amenable to a temporary let to a number of Service Measures (to be determined during the FIA process) where it is required to meet the timeframes of this Modification.	Accepted
MP07-DT-3	DCC-L	Telefónica has a dependency on the DCC-L providing technical specifications or CRPs/IRPs related to any additional GBCS functionality related to this Modification prior to agreement of the Impact Assessment associated with this Modification.	Telefónica will produce an impact assessment based on the material provided however this may include (1) additional planned delivery time to review and assess specifications and (2) retaining additional contingency related.	Accepted
MP07-DT-4	DCC-L	Telefónica have a dependency on DCC-L arranging for uplifted specifications (which may include GBCS, SMETS , and CHTS) to be added within the following documentation prior to Telefónica deploying any	Firmware versions compliant with the GBCS version associated with this Mod cannot be submitted to the CPL if the CPL template does not support the specific GBCS version and	Accepted

		Production firmware variants under this Modification attempting into the Production environment: - CPL template - SEC schedule 11 installation and maintenance validity periods Noting that the concepts that are introduced in SEC schedule 11 have not currently been incorporated within Telefónica's CSP contract	therefore cannot be pre-notified or OTA'd onto installed Comms Hubs If the SEC schedule 11 has not been updated, then the DCC will be non-SEC compliant should Telefónica deploy any Communication Hubs operating a firmware version associated with this Modification in the Production environment.	
MP07-DT-5	DCC-L	Approval of Telefónica's Impact Assessment for DCC CR1013	Telefónica will be unable to support the reduced step upgrade approach introduced within CR1013	Accepted
MP07-DT-6	DCC-L	Development of the key principles relating to the following areas during the FIA: - CSP/DSP interface - CH storage prioritisation rules	TBD	CSP/DSP interface: Accepted but this is between DCC and their Service Providers. CH storage prioritisation rules: Accepted, rules outlined in the business requirements. ESME and GSME will take priority over any other Device updates.
MP07-DD-8	DSP and DCC	A separate DCC Change Request has been raised to allow DSP to deploy a capability that will serve to throttle and queue firmware distribution SRs to the CSP by limiting Service Requests sent by Service Users such that only one firmware distribution activity is in progress per CH at any point in time.	This will be required to implement Solution Option 2.	Accepted and will be implemented under CR1047.

8.5 Clarifications

The following clarifications have been requested. which may require Telefónica to review the fixed price for the Impact Assessment and the ROM cost for the future activity contemplated as part of the Impact Assessment. These clarifications must be provided, considered and where relevant incorporated prior to the issue of an Impact Assessment Approval Notice in relation to this Modification, in the following areas noted in the table below:

Ref	Area	Clarification	Impact	Status
C_2	Specification	Provide the technical rules on firmware storage prioritisation within the Communication Hub	Needs to be provided for a complete and more accurate FIA	Noted, the business requirements need to be expanded to include this. SECAS assume this will not impact the cost for the solution to this modification.
C_3	Requirements	Confirm the functional requirements on the DSP in limiting multiple requests through to CSP systems per CH	Telefónica assume the DSP behaviour is as noted in dpendency MP07-DD-8 above.	Accepted, CR1047 will address this.
C_4	Firmware approach	DCC-L to confirm expectations regarding how Communication Hub firmware is to be developed and tested for this Modification in relation to firmware developed as part of the firmware maintenance policy.	TBD	Accepted, but this is not material to this modification. DCC will also deliver a planned test strategy before the Impact Assessment has begun.

C_5	Firmware approach	DCC-L to confirm expectations for how any firmware developed as part of this Modification and delivered as part of a programme release will incorporate any modifications that have been delivered via maintenance releases	Telefónica assume that: Code deployed into PIT for this Modification will be branched off a version of firmware that is delivered via the Firmware Management Process; Defects identified in Prod during PIT will not prevent PIT exit or SIT entry if the fixes are not in the codebase used in PIT. Telefónica expect a SIT test cycle will be used to assure this (outside of the scope of this Modification); The Communication Hub firmware used to exit PIT will be a merge with whatever version of FMP code production candidate if Telefónica unilaterally view this to be reasonable and possible to merge in the timeframes for testing within the PIT window; PIT exit and SIT entry criteria will not use FMP / OAB criteria and in particular defect masks will relate only to the functional change in the scope of the Modification; PIT exit and SIT entry is driven only by the production codebase maturity and does not consider not RTL / ITCH variants; Regression test will include all test products.	Accepted and SECAS note that this modification will likely be implemented in a scheduled SEC Release. DCC will also deliver a planned test strategy before the Impact Assessment has begun.

C_6	Requirements	DCC-L to confirm how delivery of OTA firmware images to IHD/PPMID/HCALC devices will operate on a Sub GHz HAN, with particular reference to treatment of the OTA during limited and critical duty cycle scenarios.	Telefónica assume that OTA will be suspended during any period when the Sub GHz HAN is in limited or critical duty cycle mode.	Accepted The firmware upgrade to IHD/PPMID/HCALCS must respect the Sub-GHZ rules for the HAN pted.
C_7	Firmware Image Size	We understand that the Firmware Image Size for an ESME is anything up to 750KB, and a GSME is slightly smaller. Are figures available for the HAN devices?	Working on assumption that these images would not exceed 750KB would simplify workings significantly.	Rejected. Note the CSPs will only see fragments not exceeding 750Kb in size. These frgaments will be handled independent from each other from the CSPs perspective. SECAS state that current ESME and GSME firmware image size may exceed 750 kB; where this is the case the firmware is broken into multiple segments which are treated indepently and are listed individually on CPL. The Suppliers must send the individual segments in the required order and the meter's duty to reassemble the full firmware image from the segments. The same process must be followed by SECMP0007

C_8	Comms Hub Memory	Is extra memory required such that an ESME or GSME download is not interrupted during downloads?	Device specifications might be impacted.	Rejected. SECAS suggestion xMSE updates always take priority over IHD/PPMD/HCALCS updates at any time. If necessary the IHD/PPMI/HCALCS update can be be purged from the CH memory However, DSP prioritisation and queuing should eleiminate this concern

Appendix A: Glossary

The table below provides definitions of the acronyms and terms used in this document.

ACB	Access Control Broker	HCALCS	HAN Connected Auxiliary Load Control Switch
API	Application Programming Interface	IHD	In Home Display
CAN	Contract Amendment Note	OAB	Operational Acceptance Board
CH, Comms Hub	Communications Hub	OTA	Over The Air
CHF	Comms Hub Function		
CHTS	Communication Hubs Technical Specification	MMC	Message Mapping Catalogue
CoS	Change of Supplier	PIA	Preliminary Impact Assessment
CPA	Commercial Product Assurance	PIT	Pre-Integration Testing
CPL	Certified Products List	PM2	Performance Measurement 2
CR, CRP	Change Request, BEIS Change Request	PPMID	PrePayment Meter user Interface Device
CSP	Communication Service Provider	ROM	Rough Order of Magnitude
DCC	Data Communications Company	SEC	Smart Energy Code
DSP	Data Service Provider	SIT	Systems Integration Testing
DUGIDS	DCC User Gateway Interface Design Specification	SMETS	Smart Metering Equipment Technical Specification
DUIS	DCC User Interface Specification	SMI	Smart Metering Inventory
DSMS	DCC Service Management System	SMIP	Smart Meter Implementation Programme
ES	Electricity Supplier	SMKI	Smart Meter Key Infrastructure
ESI	Energy Service Interface	SMWAN	Smart Meter Wide Area Network
ESME	Electricity Smart Metering Equipment	SP	Service Provider
FIA	Full Impact Assessment	SR	Service Request
GBCS	Great Britian Companion Specification	SRV	Service Request Variant
GFI	GBCS Integration Test for Industry	SSC	Security Sub-Committee
GPF	Gas Proxy Function	SSI	Self Service Inventory
GS	Gas Supplier	TSIR	Technical Specification Issue Resolution Sub-Group
GSME	Gas Smart Metering Equipment	UIT	User Integration Testing
HAN	Home Area Network	WAN	Wide Air Network

Appendix B:System Impacts, Requirement Traceability Matrix

At the highest level, the changes to the DCC Total System for Option 1 mapped to the specific requirements would be as follows:

1.	In Home Displays (IHDs) to be added to the Certified Product List (CPL).	IHD to be added to CPL This will mean a change to the CPL interface spec and to the processing of incoming CPL files. Hash for both the images to be added to CPL Enable a firmware hash to be recorded for a PPMID. Currently hash is treated as optional in CPL data, and there is no specified behaviour to prevent a hash being provided for a PPMID, but none are expected. No change is expected to the structure of the CPL, only to the permitted data types and validation
2.	Manufacturer Image Hashes associated with IHDs, PPMIDs and HCALCS to be added to the CPL.	To guard against corruption of images and needless distribution of corrupt images, Manufacturer Image Hashes associated with device CPL entries would be added to the CPL. The hash checking would then be undertaken by the Supplier and DCC as part of Service Request generation and processing. ZigBee Assurance Certificates, SMETS/GBCS versions and contact details would need to be provided to the Panel, along with IHD Device Model details in line with the DUIS.
3.	Suppliers to send firmware updates to IHDs, PPMIDs and HCALCS.	SMI to be updated to maintain firmware version for PPMID, IHD, and HCALCS. The following SRs will be impacted: - Device Pre-notification - Update Inventory - Read Inventory
4.	The DCC to notify all Responsible Suppliers at certain stages of the associated processing of firmware updates.	New DUIS request(s) required that enable Responsible Suppliers to upgrade Firmware. Will also contain activation date and time – no separate DUIS request for activation. New DUIS Alerts to notify all responsible suppliers when: - IHD / PPMID / HCALCS image successfully downloaded

		- IHD / PPMID / HCALCS image successfully activated. Given that the devices may communicate with both GSME and ESME, both Import Supplier(s) and the Gas Supplier Associated with the Communications Hub would be able to update a PPMID, IHD or HCALCS Firmware, and be notified at key stages of processing. All Suppliers would be notified at the following stages of processing: a) When the DCC has successfully processed a Service Request for an image's distribution; and b) When the IHD / PPMID / HCALCS has attempted to activate new firmware (or attempted to store a part of a firmware that is greater than 750KB).
5.	The DCC and Responsible Suppliers to check the latest firmware version on IHDs, PPMIDs and HCALCS.	See impacts related to Requirement 3 To enable this, a new 'Read IHD / PPMID HCALCS Device Model' via the CH' Service Request would be needed (provisionally numbered 11.5). This would result in a Command to the CHF. On receipt, the CHF would query the device and create a Response containing the values provided by the device (or error values if no response is received from the device after [30] seconds)
6.	Rules around sharing capacity and buffering on the Comms Hub.	Rules around sharing capacity on the Communications Hub and buffering would need to be introduced: this is because the proposal is that there would not be additional buffer capacity on Communications Hubs to store PPMID and IHD images
7.	SRs supporting the maintenance of the Smart Metering Inventory (SMI) to be revised.	Service Requests supporting the maintenance of the SMI would need to be revised: The SEC Device Model (including Firmware Version) for IHDs would need to be maintained on the SMI. Three Service Requests supporting the maintenance of the SMI (1. Device Pre-notification, 2. Update Inventory, 3. Read Inventory) would be affected by the adding and updating of related PPMID, IHD and HCALCS information on the SMI
8.	Additional CH functionality.	Support image prioritisation, the activation date-time mechanism, the reading of Device

		Model details from PPMIDs, with corresponding support for additional Alerts, Commands and Responses.
9.	Firmware update support capability will need to be mandated on IHDs, PPMIDs and HCALCS installed after this modification is implemented.	Correspondingly, the GBCS would mandate ZigBee OTA cluster support on PPMIDs and IHDs. Note that, by definition, already installed Devices cannot be required to support this change, since there is no required mechanism to update them.
10.	Local firmware updates will be banned following the implementation of this modification.	No impact

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 D

Working Group Consultation responses

About this document

This document contains the full non-confidential collated responses received to the SECMP0007 Working Group 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 E

Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the 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.