

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 0.5

21 July 2020

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

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

Contents

1. Summary.....	3
2. Issue.....	4
3. Solution	5
4. Impacts	7
5. Costs	11
6. Implementation approach	12
7. Assessment of the proposal	13
Appendix 1: Proposed PPMID OTA firmware process	37
Appendix 2: Proposed HCALCS OTA firmware process	39
Appendix 3: Progression timetable	41
Appendix 4: Glossary	43

This document also has five annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex D** contains the full non-confidential responses received to the first Refinement Consultation.
- **Annex E** contains the full non-confidential responses received to the second Refinement Consultation.

Contact

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

Joe Hehir

020 7770 6874, Joe.hehir@gemserv.com

1. Summary

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

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

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

OTA firmware updates to mandated HAN devices such as In-Home Displays (IHDs), Prepayment Meter Interface Devices (PPMIDs) and HAN Connected Auxiliary Load Control Switches (HCALCSs) and are not specified by the SEC.

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

- **OTA method for PPMIDS**

A ZigBee¹ OTA delivery mechanism will be used to deliver firmware images to PPMIDs. This method introduces the combined distribution and activation of the firmware updates into a single Service Request (SR). The PPMID will manage and distribute the notification to the Service User upon activation of the firmware.

- **OTA method for HCALCSs**

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

This modification will have wide ranging impacts across all SEC Party categories, requiring changes to systems and processes, as well as introducing new capabilities in terms of updating firmware for PPMIDs and HCALCSs. The extent of these impacts has been drawn out through consulting with Smart Energy Code (SEC) Parties and other relevant stakeholders. These impacts are summarised further in this report. The costs and implementation approach are not yet finalised.

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

2. Issue

What are the current arrangements?

Currently, the SEC captures OTA firmware updates via the DCC to the Communications Hub, ESME and GSME only.

Specifications for OTA firmware updates to IHDs, PPMIDs and HCALCSs are not captured anywhere in the SEC.

What is the issue?

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

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

What is the impact this is having?

The lack of an OTA firmware update procedure for mandated HAN Devices requires Suppliers to manage multiple processes and systems for updating firmware (OTA and non-OTA). 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 stack² 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 and therefore impact consumers' access to energy.

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. These risks will result in a negative consumer experience and will add a reputational risk to Suppliers and the Smart Metering Implementation Programme (SMIP). Considering these impacts, the overall benefits argument for smart metering will be lessened.

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

3. Solution

Proposed Solution

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

During industry discussions it was agreed that IHDs would be removed from the scope of this modification. Further information regarding these discussions can be found in Section 7. 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 PPMIDs and the other for HCALCSs. The steps for each process are summarised below, and summary diagrams can be found in Appendices 1 and 2.

PPMID

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

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 OTA firmware method cannot be utilised as this allows Suppliers and Devices to communicate end-to-end.

Once a firmware Image has been developed and gone through the appropriate assurance, the Supplier sends SR 11.4 'Update PPMID Firmware'³. This will contain the firmware Image and the list of Extended Unique Identifiers (EUIs) of the target PPMID to the DCC. This would be a Non-Critical Command (a 'one-to-many' multicast). Furthermore, the new PPMID Service Request will be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME, but counted separately.

In contrast to the ESME/GMSE OTA firmware update procedure, the Service Request will combine both distribution and activation of the firmware within one request. Future dated activation of PPMID Manufacturer Images will not be permitted. Therefore, the Service Request will not contain a field for activation date-time.

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

1. The DCC will distribute the firmware to the Communications Hubs associated with the target Devices.
2. The Device retrieves the new firmware Image from the Communications Hub using ZigBee OTA functionality.
3. Upon successful receipt of the OTA Upgrade Image, the Communications Hub will instruct the PPMID to immediately activate the new Manufacturer Image.

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

4. The Communications Hub will subsequently clear the Image from its memory block.
5. After verification of the firmware, the Device performs the firmware activation.
6. The PPMID will then create a Device Alert containing its firmware version and send it to the DCC.
7. The DCC will update the Smart Metering Inventory (SMI) if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

HCALCS

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

The HCALCS will utilise the existing OTA firmware update procedure used by ESME and GSME. This requires a distinct separation between the distribution and activation of the firmware image. As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

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

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

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

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

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

4. Impacts

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

SEC Parties

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

Supplier Parties

Suppliers are responsible for the procurement, installation and maintenance of SMETS2 Devices in customers' premises. They have a responsibility to ensure Devices are operating 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.

In response to the first Refinement Consultation on this modification, several Supplier Parties advised that this modification would require changes to systems and IT infrastructure, as well as 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 PPMID firmware update is in progress. This could mean that they may have to make minor system changes to facilitate this modification.

Other SEC Parties

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

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

The full responses received from Parties can be found in Annexes D and E.

DCC System

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

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

Data Service Provider

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

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 Services Providers

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

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 AB 'Service Request Processing Document'
- Appendix AD 'DCC User Interface Specification'
- Appendix AF 'Message Mapping Catalogue'

The changes to the SEC required to deliver the Proposed Solution can be found in Annex B.

Consumers

This modification will impact consumers. Being able to update PPMID and HCALCS firmware OTA will mean less chance of Suppliers having to schedule site visits to update these Devices. This would provide more convenience for consumers as they will not be required to set aside time to accommodate these site visits. Furthermore, this modification could indirectly impact consumers trust in the SMIP, as their Devices would be more likely to be operating on the optimal firmware version with Suppliers able to quickly resolve any bugs.

Other industry Codes

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

Greenhouse gas emissions

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

5. Costs

DCC costs

Implementation 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 DCC implementation costs (up to PIT)	
Activity	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 C.

SECAS costs

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

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

SEC Party costs

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

- The capability to update firmware OTA may increase the number of firmware updates. Consequently, additional resource may be required to manage the due diligence of firmware updates.
- System and process impacts, with significant testing for every combination of the newly upgradeable HAN Devices with all Communications Hubs.
- Significant cost for moving to any new version of DUIS, or the device Technical Specifications.

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

- Parties would experience a dramatic reduction in the risk of a Device irrecoverably failing in the field, which would be a material benefit.
- 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.

The full responses received can be found in Annexes D and E.

6. Implementation approach

Recommended implementation approach

SECAS is recommending a two-part implementation approach:

DSP and CSP South and Central Regions

- **4 November 2021** (November 2021 SEC Release) if a decision to approve is received on or before 5 November 2020.

CSP North Region

- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received on or before 5 November 2020.

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 12-month lead time between the modification being approved and implementing the Proposed Solution.

7. Assessment of the proposal

The development of this Proposal

This Proposal has been time consuming and complex. Below is set out the key areas of concern that have been discussed and the changes that have occurred during the Refinement Process.

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

Which Devices will this modification apply to?

Consumer Access Devices

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

HCALCSs

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

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

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

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

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

IHDs and PPMIDs

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

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

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

After the 2019 Refinement Consultation, a Working Group meeting was held in December 2019 to look at ways to reduce the costs of the solution. The DSP noted that 95% of all deployed displays are PPMIDs. Furthermore, it noted that some of the 5% listed as an IHD, are wrongly listed as an IHD and are in fact a PPMID. The DSP added that IHDs have no firmware version listed in the SMI. Therefore, including them would require development in order to achieve this.

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

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

Conclusion

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

The following record of the discussions include references to IHDs as these were included in the scope of solution at the time.

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

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

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

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

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

geo's proposal to permit local updates

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

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

Geo's Proposals 1: Query Next Image Request		
Process	Advantages	Disadvantages
'Query Next Image Request' command is carried out once every 24 hours by the Device.	24-hour frequency of the process would ensure accuracy of the SMI	At full rollout, all deployed PPMIDs carrying out the 'Query Next Image' could lead to an "Alert Storm".
Upon receipt of the 'Query Next Image Request', the Communications Hub would extract the current firmware		

Geo's Proposals 1: Query Next Image Request		
Process	Advantages	Disadvantages
version and provide the data to the DCC.		
The process would be repeated after completion of a firmware update (OTA or local) and after locating the Communications Hub.		Communications Hub does not know what firmware version the Device is running. Therefore, the Communications Hub will have to forward the firmware version of that Device to the DCC, even if it has not changed firmware version.
Communications Hub would respond with either: - No Image available; or - Information concerning the Image available for download by the Device		To prevent this from happening, it was suggested that the Communications Hub could store the firmware version for the Device. Therefore, it would know on the 'Query Next Image Request' if the Device was reporting a new firmware version and prevent unnecessary Alerts to the DCC. However, SECAS noted this proposal to be a break from the current Proposed Solution; the Communications Hub has been envisaged to transfer firmware information, rather than store it for periods of time. Storing information on the Communications Hub would require additional functionality in the Communications Hub, which would increase costs and complexity.

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

Making sure authorised Parties can carry out local updates

SECAS explained the current firmware process means updates can only be applied by the Responsible Supplier Party. First, the firmware and the Firmware Hash are submitted to the DSP, who validate the Firmware Hash against the CPL. If it is successfully validated, the CSP then sends the

Managed by

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. This could then create a discrepancy between the CPL and the SMI if, following a local update, a Supplier sends SR11.2 'Read Firmware Version'. This would result in the SMI being updated with the correct firmware version, but consequently it would not reflect what is on the CPL.

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

Vote on geo's proposals

The Working Group proceeded to vote on whether to progress geo's proposals as an Alternative Solution under this modification. All Working Group members, other than geo, voted not to take forward these proposals as an Alternative Solution. This was due to the desire not to cause any undue delays to SECMP0007, given that Parties wanted this implemented as soon as possible. However, several members believed that geo had proposed some good ideas and encouraged geo to raise its own Draft Proposal to have its ideas assessed.

SSC consideration of local firmware updates

In November 2019 SECAS advised the Working Group that the SSC had discussed the proposed ban on local firmware updates. The Technical Architecture and Business Architecture Sub-Committee (TABASC) Chair believed that the ban on local updates to IHDs and PPMIDs proposed by this modification may present unnecessary constraints on Parties and other participants in the SMART ecosystem. The TABASC Chair subsequently proposed to the SSC that local firmware updates to IHDs and PPMIDs should not be banned, subject to appropriate security controls.

SECAS noted the main concern with local firmware updates was that the proposed solution would not be able to track local firmware updates. The TABASC Chair proposed two potential options to work around this issue:

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

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

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

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

Subsequently the SSC questioned whether the Working Group had considered triage and refurbishment of IHDs and PPMIDs which would require an alternative (local) means of a firmware. In this respect, the SSC considered that local updates were feasible subject to appropriate security controls.

In December 2019, SECAS recommended to the Working Group that it keep the ban on local updates to prevent any further delay to the modification. It noted that this would not prevent a Draft Proposal from being raised to reinstate local updates.

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

Conclusion

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

DCC Assessments

The first Preliminary Assessment

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

The Proposer and the Working Group raised questions in relation to the business case of the modification and the high cost to complete a DCC Impact Assessment. They also noted that there was limited information on how many IHDs and PPMIDs will be in use at the time of implementation. It was noted that some physical Devices may be replaced with applications on consumer devices such as phones or those connected via Wi-Fi.

Whilst noting that there are assumptions and non-functional requirements outlined in the Preliminary Assessment that require clarification and development, the Proposer and the Working Group agreed that a Refinement Consultation would be the best method to assess the next steps. A Refinement Consultation was subsequently issued from 17 October 2017 to 8 November 2017 to clarify these areas. These responses were used to inform a second Preliminary Assessment.

The second Preliminary Assessment

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

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

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

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

Questions were also raised around the £12.3 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 for the change?

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

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

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

What did the Proposer agree to take forward?

Partly due to the high costs as well as the complexity of the proposed solution, the Working Group agreed that in order to progress the modification, 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 second Refinement Consultation would seek this information from Parties. The Working Group acknowledged that the removal of IHDs from the proposal could further reduce the role of IHDs in the market.

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

As a result, the Working Group agreed to progress with a combination of the two solutions:

1. Original Approach, Zigbee OTA Delivery for IHDs and PPMIDs

Note: this solution now only includes PPMIDs. As noted above, IHDs were later removed from the scope of this modification.

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

How will a PPMID firmware update be initiated?

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

SECAS's and the DCC's views

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

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

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

SECAS proposed adding a new Service Request, specifically designed for the combined distribution and activation of IHD/PPMID firmware. This would prevent any risk of issues with amending SR11.1 which already works for ESME/GSME. It would also create a clear distinction for the DCC and the Service User as to which Device type is contained in each Service Request.

The SSC noted its requirement for the DCC to be able to differentiate firmware updates to IHDs/PPMIDs from ESME/GSME/HCALCS firmware. This would be essential to enable separate ADT values for IHDs/PPMIDs and ESME/GSME/HCALCS. This would enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs. The SSC therefore agreed that a new Service Request for the combined distribution and activation of IHD/PPMID firmware would better achieve this. However, it was not against SR11.1 from being used, as long as it could also achieve separate Anomaly Detection for each Device type.

Working Group discussions

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

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

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

A Working Group member preferred the use of SR11.1 for PPMIDs/IHDs, noting that it would simply be extending its scope to additional Devices. They didn't see the benefit in creating a new Service Request for what is the same job as SR11.1. Furthermore, the Party already has operational

processes in place that are based upon the use of SR11.1. However, the Party did note that either way, they will have to make changes to their interface with the DCC.

It was noted that evidence is needed for SR11.1 being able suffice the SSC's statement. This is that the DCC must be able to differentiate between Device types, as well as be able to apply different ADT values to each Device type.

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

Conclusion

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

Activation date-time of PPMID firmware

Enabling future activation date-time

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

SECAS proposed a six-month limit on future dating firmware updates, in line with the proposal under [SECMPO024 'Enduring Approach to Communication Hub Firmware Management'](#). However, the SSC advised this is too long and the limit must be set to no more than 30 days. This is in order to match existing ADT volume regime as ESME/GSME.

Immediate activation only

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

This requirement was subsequently discussed at the December 2019 Working Group meeting where the decision was made to remove IHDs from the scope of this modification. The DCC proposed that firmware updates to IHDs, PPMIDs and HCALCSs be limited to immediate activation only. This would significantly reduce costs in defining test cases and test execution. It added that with future activation, as the activation date goes further into the future there is an increased risk of firmware Image corruption.

The TABASC Chair advised that they did not see any considerable benefit in Suppliers being able to future activate their firmware updates. Two Device manufacturers advised that they saw a benefit in being able to future activate firmware, in that it would allow Suppliers to synchronise their firmware updates, especially when there are major updates to the Technical Specifications which they must

upgrade to. However, both manufacturers agreed that this benefit does not warrant any considerable increased costs or implementation timescales on the solution.

Conclusion

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

How will Firmware Images be managed?

Firmware Image size

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

Communications HubTS section 4.4.4 requires that the receiving Communications Hubs can buffer Images intended for ESME and GSME. The CSP contracts require Communications Hubs to have the capacity to hold two 750KB Images (to support independent distribution of firmware to one of the ESME and the GSME). The Working Group acknowledged this obligation and agreed that OTA Upgrade Images⁴ must be less than or equal to 750KB. Firmware larger than 750KB would be split into single Images less than or equal to 750KB in size. Members agreed there is nothing preventing fragmentation of firmware now, if the Device is built to support it.

Handing firmware⁵ larger than 750KB

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

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

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

It added that the process does not propose any changes to the way in which the DCC currently manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up

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

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

of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

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

Conclusion

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

Activation of fragmented Images

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

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

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

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

Rejected firmware Images

PPMIDs

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

HCALCS

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

Failed firmware Images

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

Switched off Devices leads to two possible scenarios:

1. Failed distribution

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

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

2. Failed activation

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

Dual Supplier scenarios

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

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

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

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

At the December 2019 Working Group meeting, SECAS sought a decision from the Working Group on how to handle dual Supplier scenarios for PPMIDs. SECAS recommended that only the Lead

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

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

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

Conclusion

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

Managing Alerts

What Alerts will Suppliers receive?

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

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

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

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

modification. However, the majority of the Working Group agreed that these Alerts were beneficial to have now and noted the limited impact these Alerts would have on development and testing.

Conclusion

The Working Group agreed to keep the original proposed Alerts.

Firmware activation Alert mechanism

Initial approach

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

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

New approach

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

Upon successful firmware activation, instead of the Communications Hub managing the Alert for successful activation, the PPMID would send this Alert directly to the Supplier. The Alert would be directed to the ACB on the Device. The ACB, using registration data, would then validate that the Supplier the Alert is addressed to is the Supplier for the Device.

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

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

A Device manufacturer noted that the TABASC Chair's proposal would only apply to future updates. No existing Devices could support this until after a successful update had been applied. The Working Group agreed that manufacturers needed to ensure that the first OTA firmware update to already deployed PPMIDs following the implementation of SECMP0007 needed to include the functionality

implemented by this modification. If this initial OTA firmware update were to fail, the sending Supplier will not receive an Alert confirming this as the Device will not have the capability to do so.

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

Conclusion

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

Communications Hub considerations

Memory block management

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

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

The DCC currently use dedicated memory blocks on the Communications Hub for ESME and GSME firmware. It advised that using both blocks will require changes to the Communications Hub design to build in the required logic to prioritise both ESME and GSME firmware, as well as distribute firmware to the available blocks. The CSP would be required to test all the possible combinations of firmware on the Communications Hub. Noting this, the DCC advised that the use of both blocks would increase implementation timescales as well as costs. Considering these impacts, the DCC proposed that IHD/PPMID/HCALCS firmware should be restricted to the ESME block only.

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

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

- GSME firmware is likely to be updated once per year; and
- Each GSME update will take no longer than two weeks to complete.

Using these estimates, the GSME block on the Communications Hub is likely to be free for 50 weeks (96%) of the year. It is for these points that SECAS proposed using both memory blocks on the Communications Hub without distinction. This would reduce the pressure on the WAN and avoid the need to invest in additional WAN capacity.

Suppliers raised concerns with the use of both memory blocks as it would not be possible to distinguish which block each firmware Image is on. Therefore, they would not know if the Image has been overwritten or not. Noting this, the Working Group agreed that using both memory blocks on the

Communications Hub could make it harder for Suppliers to manage their firmware updates. However, SECAS advised that Supplier Alerts will be generated, advising whether firmware updates have been successfully downloaded and activated. At any point in time, SR11.2 'Read Firmware Version' can be utilised in order to read the firmware version for the Device.

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

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

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

Members repeated their preference for use of a single block, making it easier for Suppliers to orchestrate firmware updates. SECAS noted the increased risk of Image overwrites with the use of a single block. Parties accepted this risk and still preferred the use of a single block.

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

Conclusion

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

Additional memory space

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

Conclusion

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

Device prioritisation

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

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

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

Pending firmware Images

Initial solution

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

The Working Group was not in favour of this requirement and noted that this is not how the SMETS1 firmware update procedure works. In SMETS1, the Image will sit on the Communications Hub until it has failed, been activated or is overwritten with another Image. Working Group members advised that it is common for IHDs and PPMIDs to be switched off for long periods of time, in some cases up to six months or more. It also questioned the benefit of clearing the memory blocks if they are eventually overwritten. The Working Group agreed that it is up to Suppliers to manage their firmware and to plan updates in a logical order to prevent this from happening. Therefore, if a customer has their PPMID switched off during a firmware update, the Image will still be available on the Communications Hub for download and activation once the Device is switched back on, unless it has been overwritten.

Limitations and proposed workaround

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

SECAS and the DCC proposed that when the firmware update is sent to the Communications Hub, it would initially be stored in the flash memory for up to a week. If the Image has not been sent to the

PPMID after one week, it would be moved to the Communications Hub Random Access Memory (RAM). The image would remain in the RAM until the Communications Hub reboots or until it is overwritten. In both cases the Communications Hub would generate an Alert that the image has been discarded.

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

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

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

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

Second workaround and agreed approach

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

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

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

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

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

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

Conclusion

The Image shall remain on the Communications Hub for no longer than two weeks, after which it will be discarded.

Note, this approach will be reviewed by the Working Group at its next meeting.

Logging of updates

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

SECAS highlighted this at the December 2019 Working Group meeting. The DCC advised that neither of the CSPs currently carry out such logging and that the requirement would subsequently increase costs in development and testing.

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

Conclusion

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

Forecasting the size and frequency of firmware updates

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

- How many Devices there will be at full deployment
- The frequency of updates to these Devices per year
- The average size of each firmware update

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

A member noted that there are very few HCALCSs, if any, deployed so it is hard to estimate how many there will be at full deployment. However, the Working Group agreed that the DCC should take a ratio-based approach to identify how many PPMIDs there will be at full deployment as the DCC hold the current deployment data. Furthermore, the ratio of deployed Communication Hubs to PPMIDs is unlikely to change so could this be used to estimate future numbers.

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

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

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 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.

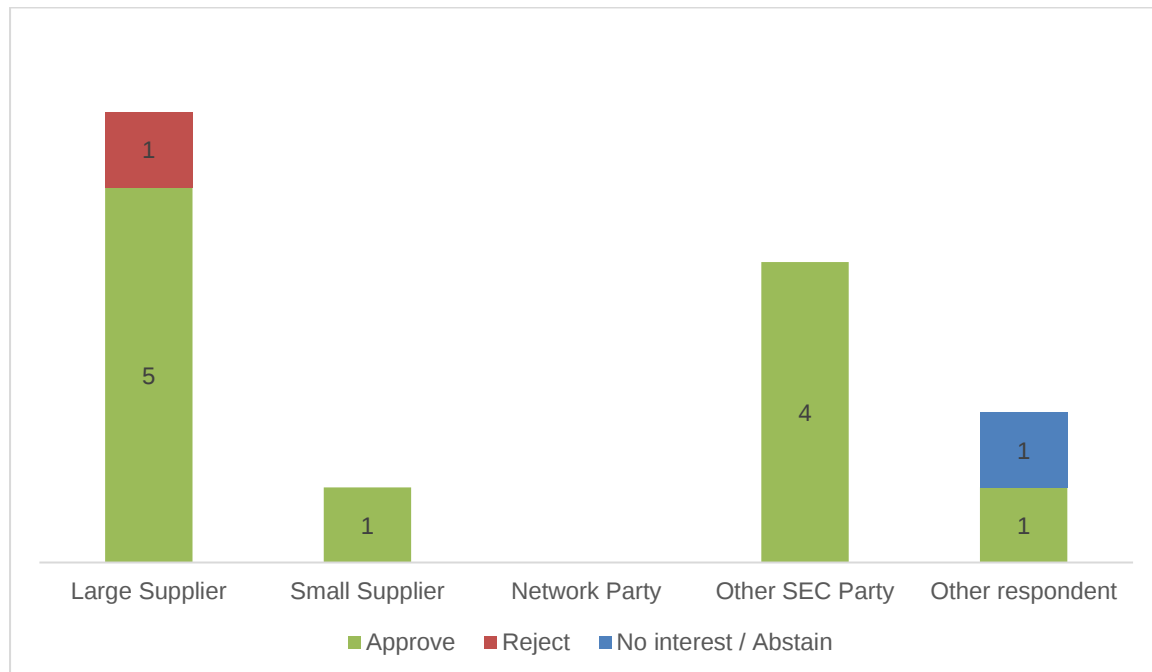
The Working Group agreed the liability for physical damage should lie with the sender of the Image but questioned how a Supplier would know who the sender was. The DCC advised that it would keep this in its audit trail. However, there are constraints on the information that can be shared. The Working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

Support for Change

Refinement Consultation responses

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



Ten respondents agreed with the solution put forward by this modification, noting that it would prevent unnecessary site visits and limit the risk of stranded Devices. These respondents also agreed with the different approaches for PPMIDs and HCALCSs. Two of the supportive respondents raised points in their responses. One advised that although it agreed with the solution, it was concerned the costs noted in the DCC's Preliminary Assessment. Another advised that the solution needs to be compatible with existing Devices. It added that this is necessary to maximise the benefits to be gained from making this change and minimise the number of Devices that would remain exposed to the risk of stranding.

One respondent did not agree with the solution put forward. This was due to the ban on local firmware, which has since been removed. It added that it disagreed with one of the assumed benefits of the solution; providing a more reliable and an up to date SMI. It added that its experience with the current firmware ESME/GSME firmware solution, which the HCALCS proposed solution relies on, is that it is not reliable. The respondent also raised concern with the longer-term use of the solution. It believed that it could be undermined by new technology.

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

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

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

The full responses received can be found in Annex E.

Working Group attendees

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

The SSC

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

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

Views against the General SEC Objectives

Proposer's views

Objective (a)⁶

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

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

Objective (c)⁷

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

Objective (d)⁸

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

Objective (f)⁹

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

Industry views

Ten respondents to the 2019 Refinement Consultation agreed that this modification would benefit at least one of the SEC Objectives, with all ten in unanimous agreement that it would benefit Objective (a). They noted reasons such as increased interoperability of PPMIDs and the avoidance of unnecessary costs in replacing these Devices.

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

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

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

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

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

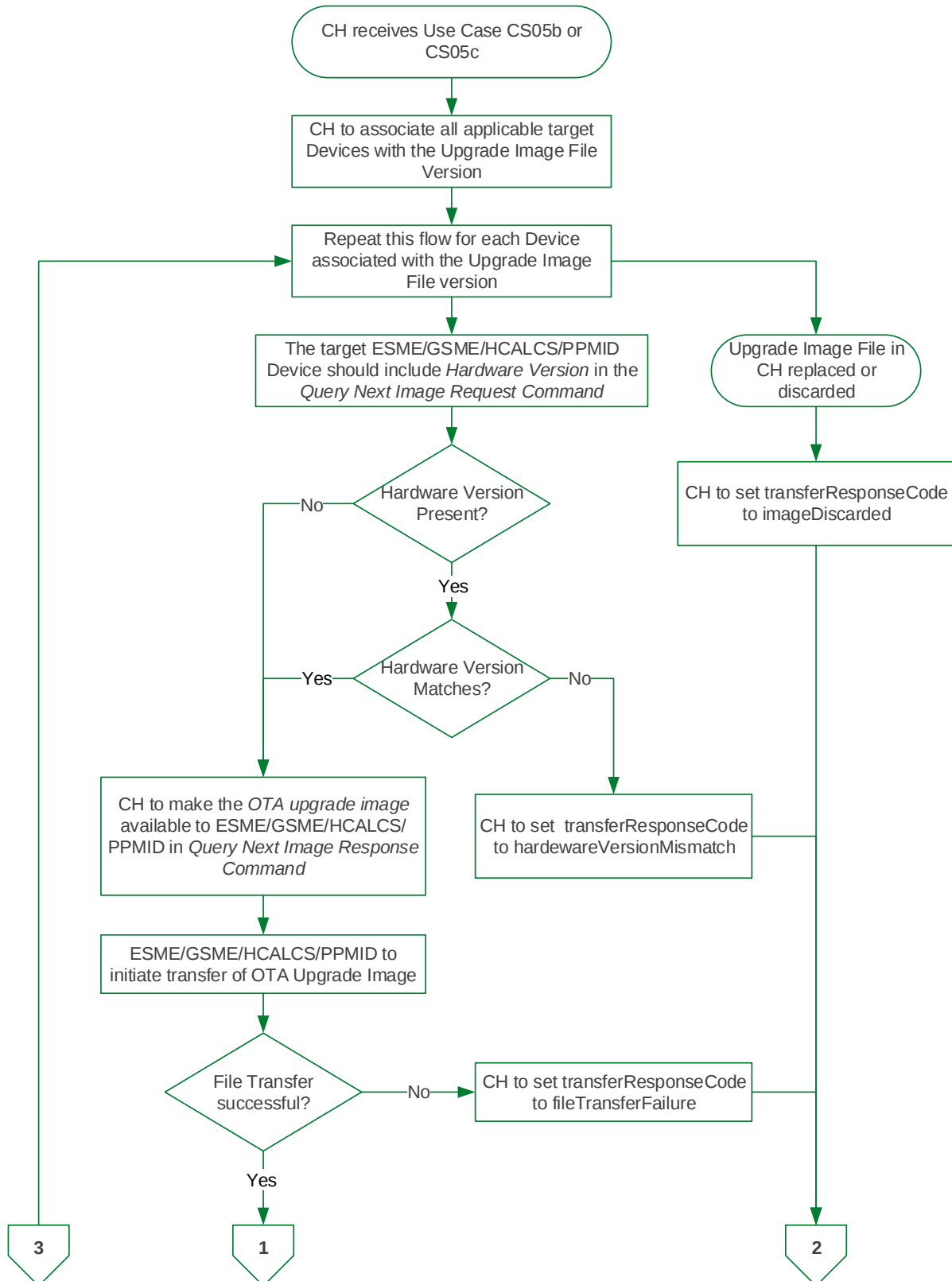
⁸ To facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy.

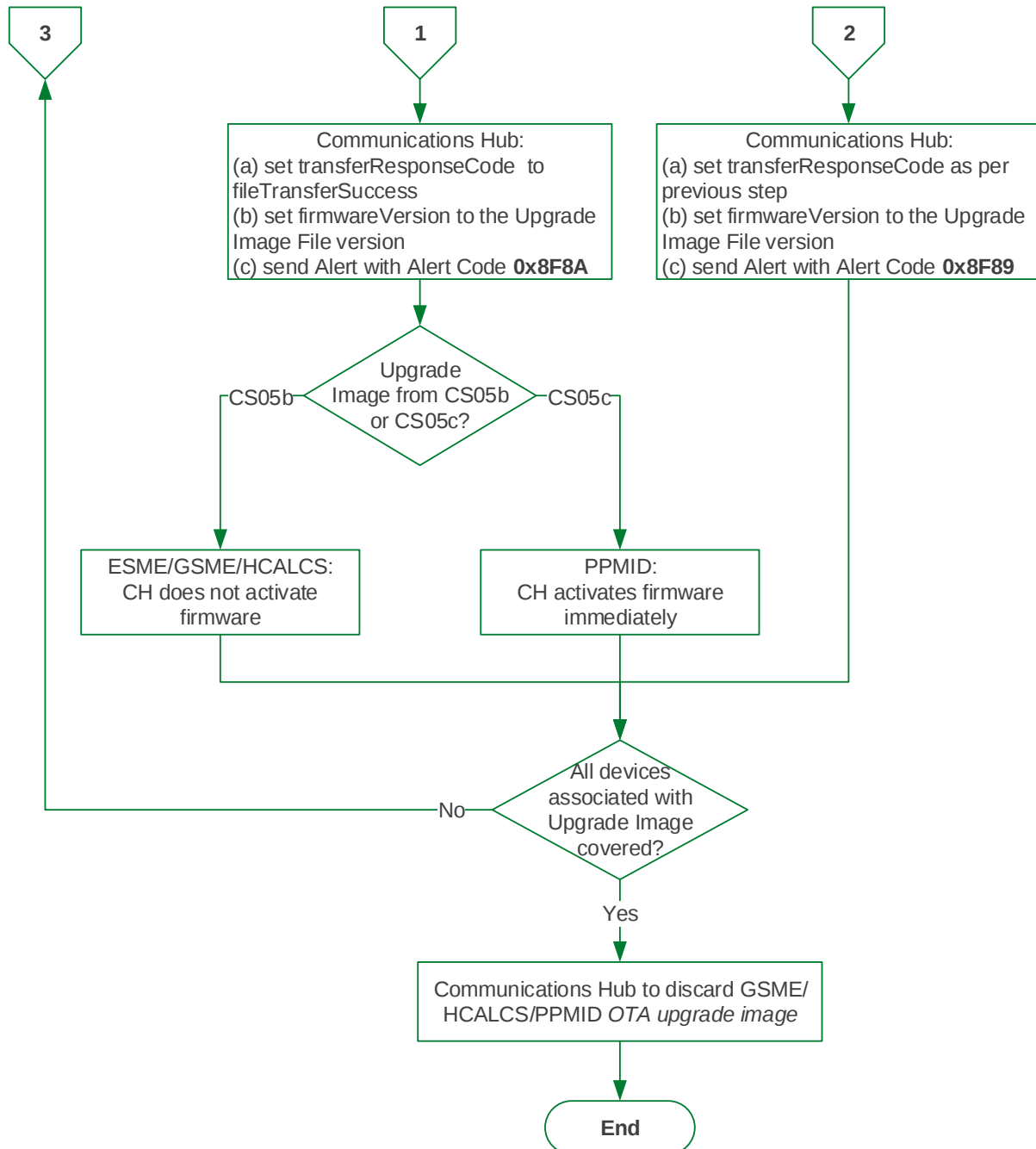
⁹ To ensure the protection of Data and the security of Data and Systems in the operation of this Code.

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

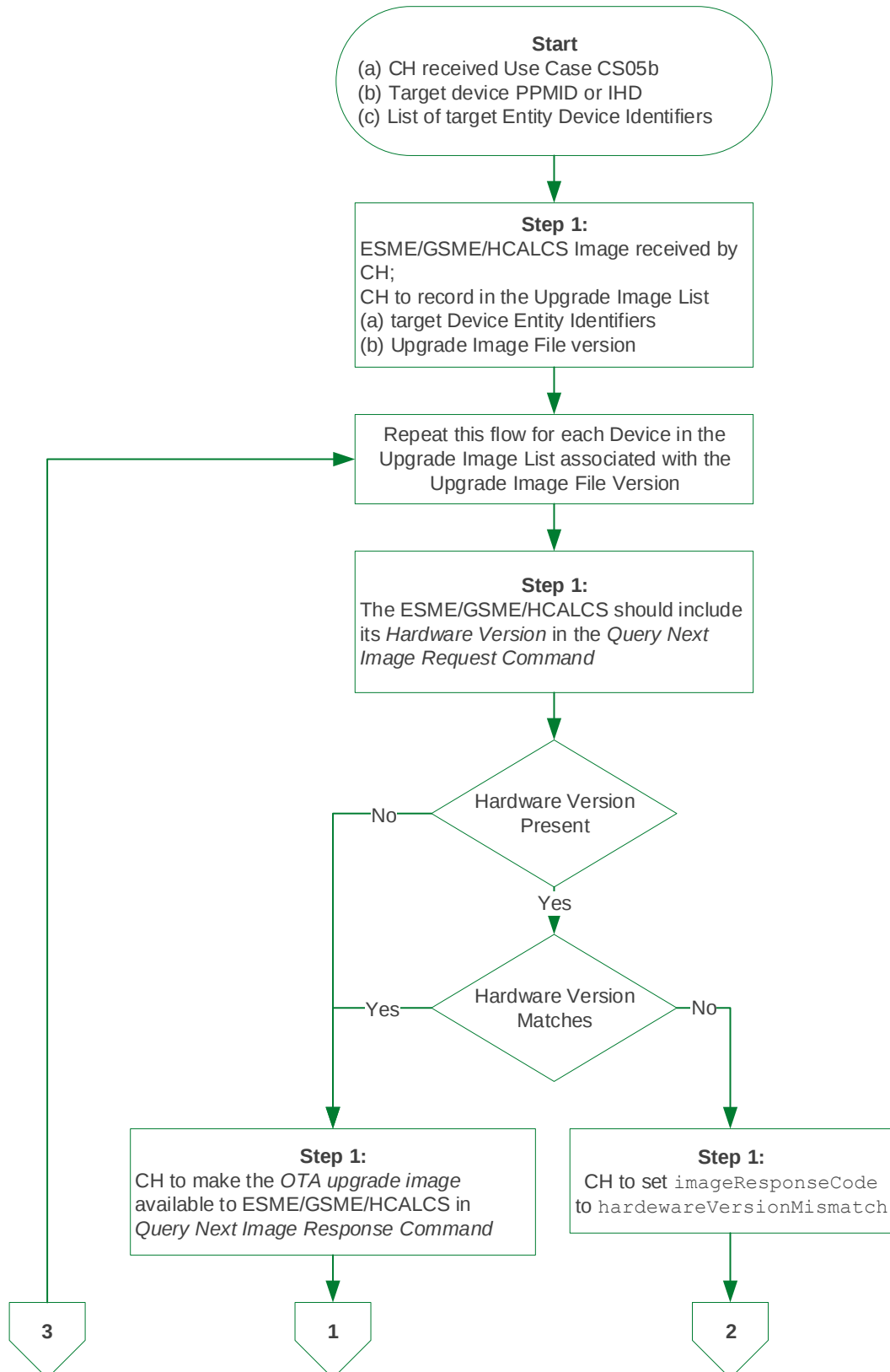
One respondent did not believe this modification would benefit any SEC Objectives. It specifically noted this against Objective (a), advising that the cost effectiveness of this modification is finely balanced and in its opinion negative. It noted the costs of the modification and the implementation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

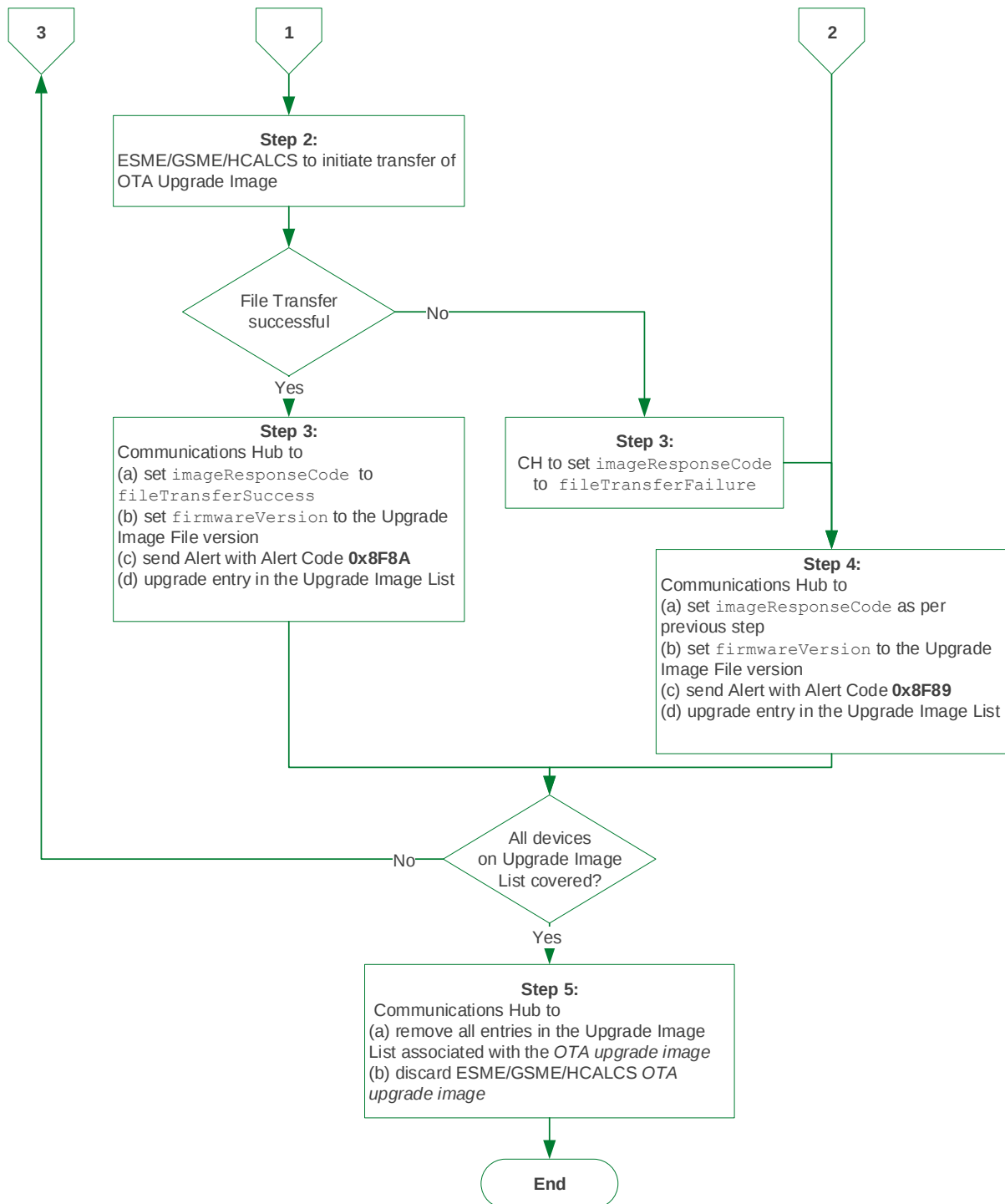
Appendix 1: Proposed PPMID OTA firmware process





Appendix 2: Proposed HCALCS OTA firmware process





Appendix 3: Progression timetable

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

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

Timeline	
Activity	Date
The Proposer ¹¹ raises an amendment to the solution, preferring a different Service Request for combined distribution and activation of PPMID/IHD firmware	15 Oct 19
The Working Group discuss the outstanding questions on the solution Outcome: The DCC is to proceed with its Impact Assessment as-is Outcome: The DCC is to ask its Service Providers to provide cost impacts on the use of different Service Requests as well as the use of memory blocks on the Communications Hub	6 Nov 19
SEC Panel ask for the solution to be streamlined in order to provide a Minimum Viable Product	15 Nov 19
SECAS, the DCC and its Service Providers discuss potential options that could be used to streamline the solution	28 Nov 19
The Working Group discuss options to streamline the solution Outcome: Several elements of the solution are removed Outcome: In light of the changes made, the TABASC Chair proposes a change to the approach for the PPMID	19 Dec 19
Agreement reached with all PPMID manufacturers to progress the TABASC Chair's proposed PPMID method	22 Jan 20
New business requirements are agreed with the DCC and its Service Providers are instructed to proceed with the Impact Assessment	6 Feb 20
SECAS are awaiting the return of the DCC Impact Assessment	ongoing

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

Appendix 4: Glossary

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

Glossary	
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 Services Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
EUA	Energy and Utilities Alliance
EUI	Extended Unique Identifier
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
IDTS	Industry Draft Technical Specification
IHD	In-Home Display
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch
MMC	Message Mapping Catalogue
OTA	Over-The-Air
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
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
XML	Extensible Markup Language
ZCL	Zigbee Cluster Library