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'

Business requirements – version 1.31

About this document

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

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

Version history

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

Definitions

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

1. Business requirements

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

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

2. Summary of OTA firmware solutions

2.1 Updating PPMID firmware

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

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

2.2 Updating HCALCS firmware

The HCALCS will utilise the existing OTA firmware update procedure used by Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME). This requires a distinct separation between the distribution and activation of the firmware. As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 ‘Update Firmware’ and activation via SR11.3 ‘Activate Firmware’, the latter via a Great Britain Companion Specification (GBCS) Critical Command.

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

3. Considerations and assumptions

3.1 Scope of the modification

This Modification Proposal will only apply to PPMIDs and HCALCSs.

3.2 Forecasting firmware updates – Non-functional requirements

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

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

3.3 Adding PPMID/HCALCS Manufacturer Image Hashes to the CPL

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

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

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

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

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

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

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

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

3.4 Communications Hub memory considerations

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

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

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

3.5 Dual Supplier Scenarios

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

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

3.6 Anomaly Detection Thresholds

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

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

3.7 Activation date-time

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

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

4. Sending PPMID firmware Images

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

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

4.1 Sending a single Manufacturer Image to a PPMID

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

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

4.1.1 Supplier preparations

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

Obtain the following information:

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

Undertake the following checks on that information:

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

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

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

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

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

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

   OTA Header || Manufacturer Image

2. List of Device IDs

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

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

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

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

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

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

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

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

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

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

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

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

4.1.6 Communications Hub notification of Image availability to the PPMID

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

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

4.1.7 PPMID request for the details of the Image

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

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

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

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

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

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

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

4.1.9 PPMID download and authentication of the Image

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

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

4.1.10 Activation of the firmware Image

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

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

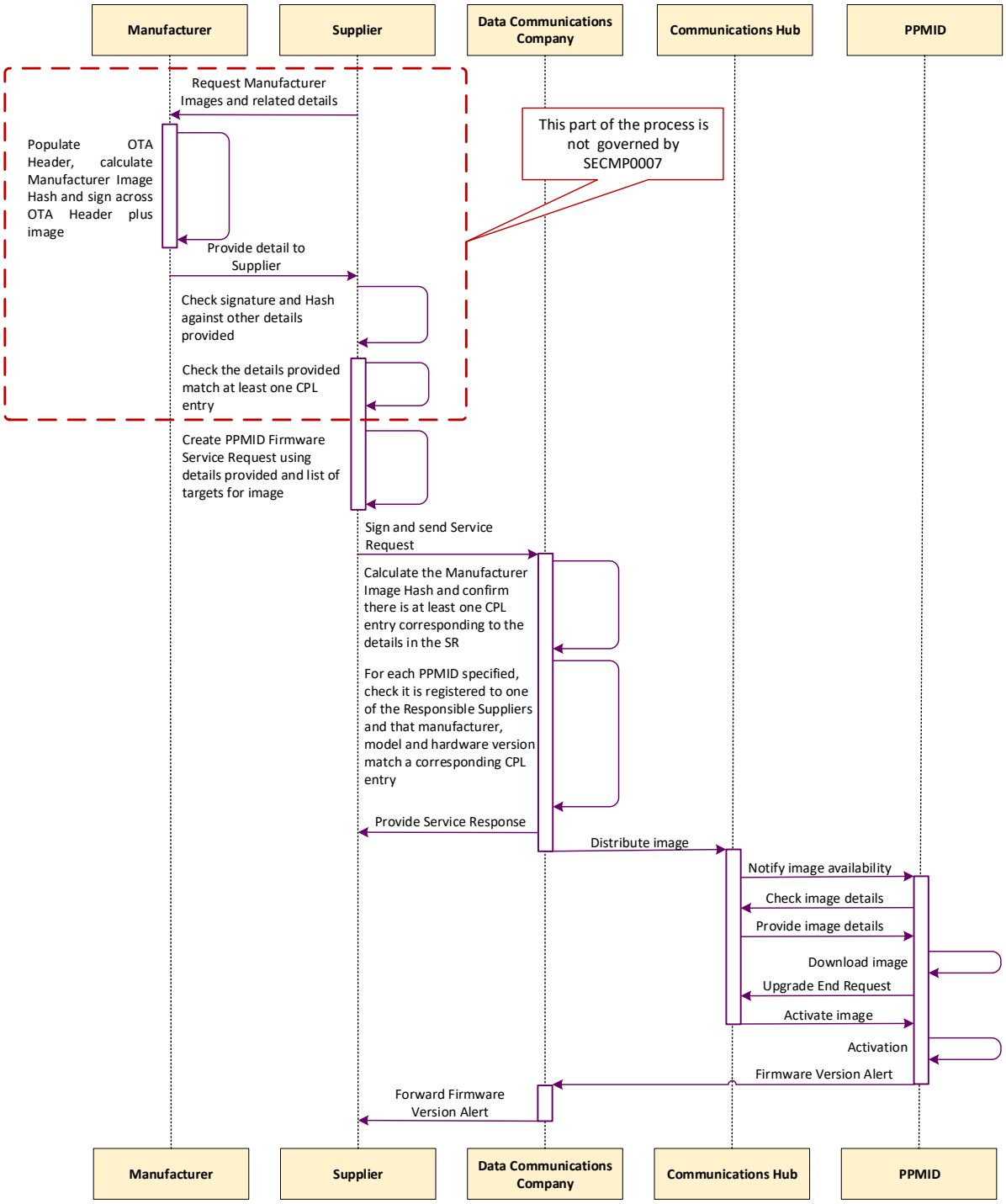
If the Device Alert is not received, the Supplier can send SR11.2 to the DCC. This will result in a Command to the PPMID to respond with its active firmware version. The DCC will forward the Response to the Supplier and update the SMI if the firmware version in the SMI is different. SR11.2 can also be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

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

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

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

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



4.2 Updating PPMID firmware comprised of multiple Manufacturer Images

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

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

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

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

The Manufacturer has split this upgrade data into two Images:

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

New CPL entry:

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

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

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

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

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

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

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

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

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

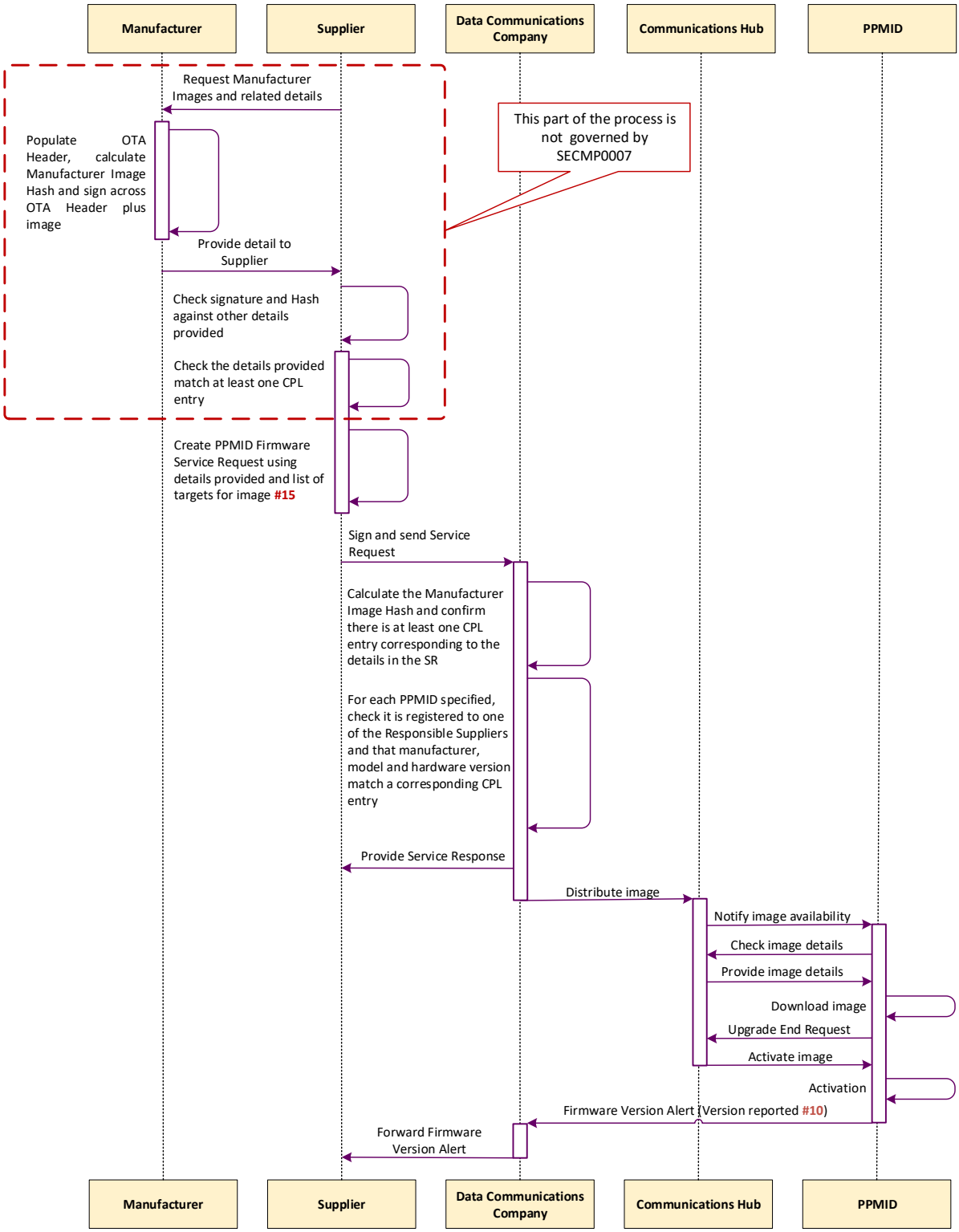
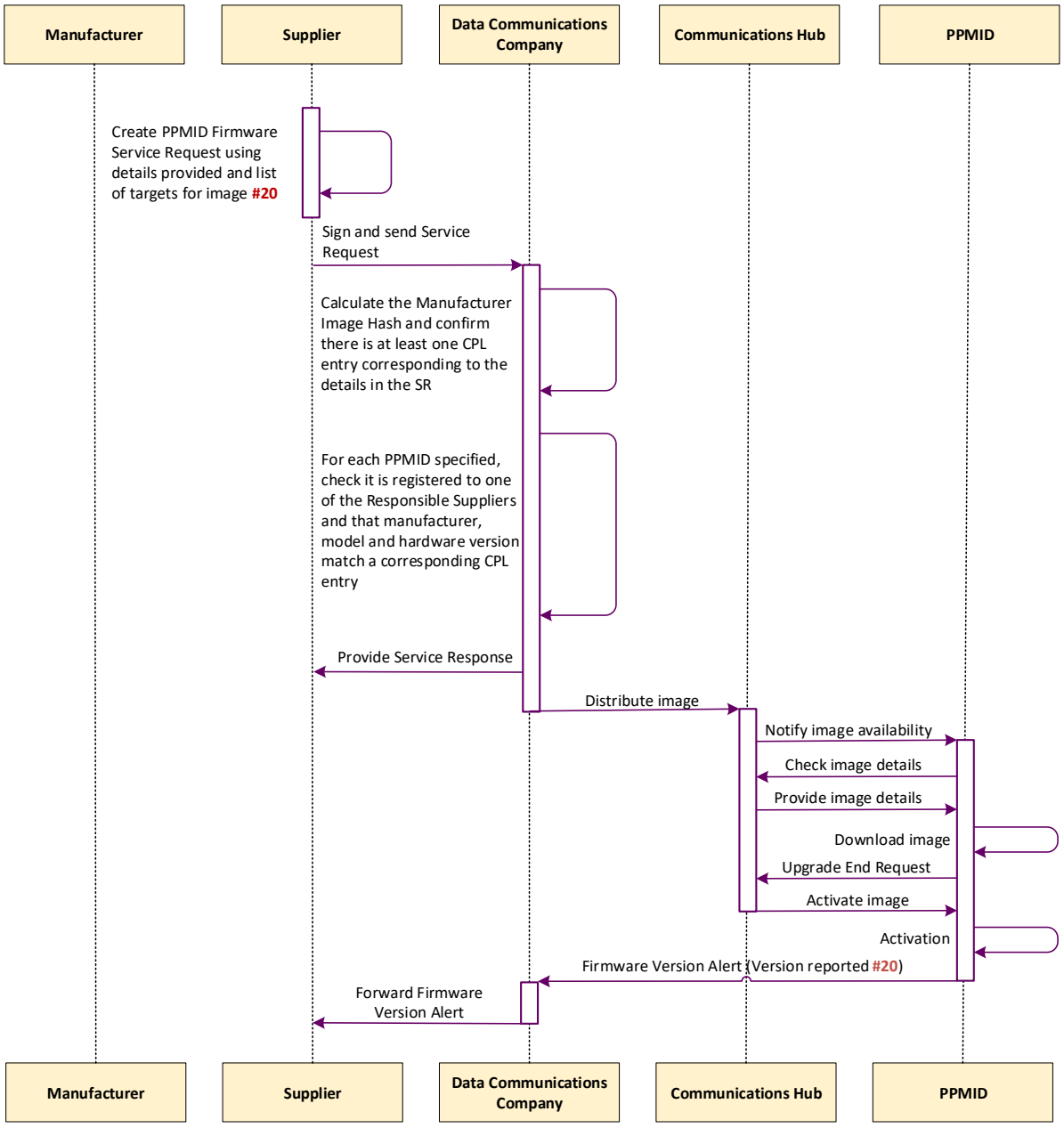


Figure 3: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2



5. Sending HCALCS Manufacturer Images

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

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

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

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

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

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

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

6. Glossary

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

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