

DCC User Gateway Interface Design Specification

Annex - Service Request Definitions 11 – Firmware Service

Author: DCC
Version: <u>5.2a</u>
Date: <u>June 2023</u>

Contents

11	Firmware Service (11 - FS)	3
11.1	Update Firmware (11.1)	4
11.1.1	Service Request	8
11.1.2	Responses	12
11.2	Read Firmware Version (11.2)	16
11.2.1	Service Request	19
11.2.2	Responses	20
11.3	Activate Firmware (11.3)	22
11.3.1	Service Request	25
11.3.2	Responses	27
11.4	Update PPMID Firmware (11.4)	30
11.4.1	Service Request	33
11.4.2	Responses	37 36

11 Firmware Service (11 - FS)

This section sets out the full content of the DCC Firmware Service by providing the overarching service content that includes: service request and response message types, data content items and User access roles.

Service Name	Firmware	Service Id	11
Service Objective	To enable a DCC Service User to upgrade the firmware on a Device for a specified device Id, such that the device can confirm that the operation has either completed or the reason for its failure.		
Business Context Statement	The DCC Service User wishes to manage the current version of firmware operating on a specified Device, e.g. following a firmware fix (or up-to-date version) being released by the Device manufacturer		
User Roles	<p>The following User Roles have access to some of the list of service requests which make up the Firmware Service:</p> <ul style="list-style-type: none"> Electricity Import Supplier (EIS) Electricity Export Supplier (EES) Gas Import Supplier (GIS) Supplier Nominated Agent (SNA) Electricity Network Operator (ENO) Gas Network Operator (GNO) Other User (OU) 		

Table 1 Overview of Firmware Service

The mapping between the Firmware Services and the Devices they apply to is defined as follows:

Service Reference	Service Reference Variant	Name	Business Target ID
11.1	11.1	Update Firmware	DSP Access Control Broker
11.2	11.2	Read Firmware Version	ESME GPF GSME CHF HCALCS PPMID
11.3	11.3	Activate Firmware	ESME GSME HCALCS CHF (only applicable to SMETS1) PPMID (only applicable to SMETS1)

Service Reference	Service Reference Variant	Name	Business Target ID
11.4	11.4	Update PPMID Firmware	DSP Access Control Broker (only applicable to SMETS2)

Table 2 FS - Service Requests / Devices

For each of the FS Service Requests supported by the DCC User Gateway, this section details:

- the reference to the appropriate section of the XML Schema (see XML Schema – document 3 of this documentation set)
- the structure of each Service Request and Response with examples (if specific to the Service Request)
- if applicable, Service Request specific Validation and Response Codes

This section should be read in conjunction with the Main Document of this documentation set sections 9 (which describes the general formatting for all Service Requests and Service Responses), 2.3.10 (which describes the Firmware Distribution and Activation process) and with the XSD (XML Schema - document 3 of this documentation set).

11.1 Update Firmware (11.1)

Service Request Name	UpdateFirmware
Service Reference	11.1
Service Request Variant Name	UpdateFirmware
Service Reference Variant	11.1
Service Request Objective	To enable a DCC Service User to request that the DCC distribute a specified Firmware Image to a specified ESME, GSME, HCALCS, SMETS1 CHF or SMETS1 PPMID for storage on the Device.
Business Context Statement	<p>The DCC Service User requires that an existing version of firmware operating on a specified ESME, GSME, HCALCS, SMETS1 CHF or SMETS1 PPMID is updated to the new specified version, e.g. following a firmware fix (or up-to-date version) being released by the Device manufacturer. The Firmware image is included within the Service Request.</p> <p>This Service Request is the first in a two-step process (the second step being to activate the firmware). This service can be used to distribute firmware to multiple device IDs.</p> <p>SRV11.4 should be used to distribute a Firmware Image to SMETS2 PPMIDs.</p>
User Role Access	<ul style="list-style-type: none"> Electricity Import Supplier (EIS) Gas Import Supplier (GIS)

Security Classification	Non-critical and non-sensitive SMETS2 or later: GBCS XREF: <i>SME.C.NC</i>
Service Request Narrative (SMETS2 or later)	<ol style="list-style-type: none"> 1. This Service can only be used for command delivery across the SM WAN. There are no local command delivery services for this service request. 2. The maximum number of Device IDs that can be included in a Service Request is 50,000. Each Service Request has to include the Firmware Image and version. 3. The Service Request Mode of Operation is “DCC Only” (see Main Document of this documentation set section 2.3.10 for details on Firmware Distribution Mode of Operation), i.e.: <ol style="list-style-type: none"> a. Business Target ID = DSP Broker ID b. Command Variant = 8 4. The DCC Data Systems apply the following specific authorisation and validation checks prior to the generation of the Service Response: <ol style="list-style-type: none"> a. The Firmware version specified in the Service Request matches an entry on the Central Products List, (approved Firmware version ID). The Firmware version is presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F, for example "1100EEFF" b. The DCC Service User is the Registered Import Supplier for each of the Device IDs in the list. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed c. Each Device ID in the list corresponds to a Device with a status of “Commissioned” . If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed Note: This validation will also allow Devices with a status of “Suspended”. d. The Firmware Version is applicable to each “Commissioned” Device's Device ID in the list. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed e. Each Device in the list is not already the subject of an Update Firmware Request that is in progress (with a Firmware Distribution Tracking status of ‘Accepted by DSP’, ‘Approved For Distribution’ or ‘Successful CH Transfer’ as described in the Main Document of this documentation set, section 2.3.10). If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed. f. If the Devices in the list are of type HCALCS, then the Firmware of the CHF on the same HAN must be GBCS v4.1 or later. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed. g. In addition to the check above, if the Devices in the list are of type HCALCS, then the current Firmware of each Device must be GBCS v4.1 or later. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed. This validation is not expected to fail as DCC Service Users should be aware of the GBCS Version of the target HCALCS Devices, as they are responsible for the version of the firmware on those Devices.

5. If the validation succeeds at least for one Device ID and the Service Request doesn't fail any anomaly detection checks, the DCC Data Systems distribute the Firmware to the Devices (via the appropriate CSPs) as described in the Main Document of this documentation set section 2.3.10.
6. Update Firmware Service Requests are subject to threshold anomaly detection (see Main Document of this documentation set section 16.3) but with a slight variation on the rules. Since a single Update Firmware Service Request may result in messages to many Devices, the message count for the purposes of anomaly detection will be increased by the total number of Devices listed in the Service Request rather than simply being increased by one.
7. Reporting of errors or Firmware Distribution Tracking status changes via DCC Alerts subsequent to DSP validation. Please note that, because one Update Firmware Service Request can be split into Commands to more than one CSP it is possible for one of the Commands to succeed and another to fail:
 - a. If the CSP detects a mismatch in Firmware Version / Hash, then the DCC Service User will be sent a DCC Alert N18.
 - b. If the CSP detects an invalid combination of Communications Hub / Device then the DCC Service User will be sent a DCC Alert N19.
 - c. If the CSP detects that the Firmware Image is too large then the DCC Service Users will be sent a DCC Alert N20.
 - d. If the Firmware Version is not recognised by the CSP then the DCC Service User will be sent a DCC Alert N21.
 - e. If the DCC cannot deliver the firmware image to the CSP, then the DCC Service User will be sent a DCC Alert N22 / N23.
 - f. If the firmware image has not been rejected by the CSP, all the Responsible Suppliers to that Device other than the sender will be sent a DCC Alert N59.
 - g. If the CSP cannot deliver the firmware image to the CHF, then the DCC Service User will be sent a DCC Alert N60.
 - h. If the CSP successfully delivers the firmware image to the CHF, then the DCC Service User will be sent a DCC Alert N61.
 - i. The Device Alerts received from the CHF indicating the following statuses will be sent to the DCC Service User using the DCC Alert N62:
 - i. CHF failed to deliver the firmware image to the target Device.
 - ii. The firmware image has been discarded at the CHF.
 - iii. The firmware image has been rejected due to hardware version mismatch of the target Device.
 - iv. The firmware image has been successfully delivered to the target Device by the CHF.
8. Each ESME, GSME or HCALCS that receives the Firmware will send a Device Alert to the Registered Supplier confirming success (0x8F72) / failure (0x8F1C).
9. It is the DCC Service User's responsibility to resend an Update Firmware Service Request to those Devices for which DSP, CSP or Device validation has failed or for which no successful response from the Device has been received. Note that in order to distinguish the Firmware Distribution Tracking between the original Upgrade Firmware Requests and resubmissions for the same Device and the same Firmware, the DCC Service User should use a new Service Request ID for each request.

	<div>10. The Firmware Image (maximum size = 750 KB) has to be included in the Service Request in base 64 binary form (maximum length = 1024000). Please see GBCS section 11, for details of the Firmware Image contents, format and validation.</div> <div>11. The specified ESME, GSME or HCALCS will verify the Firmware Image received by verifying that the sending Users digital signature applied to the Firmware Image is the same as the digital signature held in the Supplier trust anchor cell on the specified Device.</div> <div>12. The Sending Users digital signature must be calculated across the Firmware image using the sending Users Digital Signing Key.</div> <div>13. The Authorisation Check allows the Device Status to be 'Suspended', but successful completion of the Service Request doesn't change the Device Status in the Smart Metering Inventory. Once the Firmware Version is activated via Service Request 11.3 (Activate Firmware), the DCC Data Systems shall update the Device Status to the value it held immediately prior to its Suspension. See section 11.3.</div> <div>14. Where a User receives a warning that an Update Firmware Request is in progress and does not believe that this is correct, then a service management incident should be raised so that the DCC's Firmware Distribution Tracking Status can be updated to 'Reset By DCC' to allow subsequent Update Firmware Requests to be accepted by the DCC.</div> <div>15. DCC Service Users are requested to maximise the efficiency of firmware distribution within the DCC by ensuring that as many Devices as possible are included within Update Firmware Service Requests. Sending Service Requests with single or low numbers of Devices reduces firmware download efficiencies and increases overall delivery timescales.</div> <div>16. <u>DCC Data Systems will perform validation to check that the OTA header conforms to GBCS Table 11.2.3 requirements for the construction of the OTA Upgrade Image (ZigBee OTA Header + Upgrade Image), including the content of the OTA upgrade file identifier, OTA Header version, OTA Header length, OTA Header Field control and ZigBee Stack version, and that the total length of the OTA Upgrade Image matches the Total image size declared in the header.</u></div>	
GBCS Cross Reference	Electricity	Gas
GBCS Message Code	N/A	N/A
GBCS Use Case	N/A	N/A
GBCS Use Case Name	N/A	N/A
SMETS1 Applicability	Yes for ESME, GSME, CHF and PPMID	
SMETS1 Service Request Narrative	<div>The behaviour of DSP for this Service Request with regard to SMETS1 Devices is equivalent to the behaviour for SMETS2 or later Devices except as follows:</div> <div>1. For Firmware updates of a SMETS1 CHF or SMETS1 PPMID the DCC Service User must be the Responsible Supplier for the SMETS1 ESME which is connected to the same home area network as the SMETS1 CHF / PPMID.</div> <div>2. The maximum length of a SMETS1 Firmware Image which may be uploaded to the DSP is 10240000 in base 64 binary (approx. 7.5 Mb).</div>	

3. Firmware Images are distributed by S1SPs.
4. Please see SEC SMETS1 Supporting Requirement Document for the composition and verification of Firmware Images.
5. Firmware verification success & failure are indicated using SMETS1 Alerts that are equivalent to the Device Alerts used for the same purpose.
6. Where the Firmware Image has been successfully verified and Devices of the Device Model identified by the OTA Header are not capable of having the Manufacturer Image distributed to them without that causing the firmware to activate, the S1SP shall retain the Manufacturer Image until receipt of the corresponding Firmware activation command (SRV11.3).
7. For SMETS1 CHF and PPMID Devices only, following receipt of SRV 11.1, for each successfully-validated Device ID a DCC Alert with DCC Alert code N57 will be sent to other Suppliers with an interest in the HAN. DCC Alerts N59, N60, N61, N62 are not generated for SMETS1 devices.
8. The Alerts sent to the Registered Supplier confirming success (0x8F72) / failure (0x8F1C) shall be sent as SMETS1 Alerts.
9. The check whether each Device already has an Update Firmware Request in progress does not apply.
10. Firmware Distribution Tracking is not performed for SMETS1 Devices.
11. The specification for OTA Upgrade Images targeted at SMETS1 Devices is defined in the SMETS1 Supporting Requirements document, though it should be noted that the definition is the same as the requirements of GBCS Table 11.2.3.

Table 3 Update Firmware Service Request

This section should be read in conjunction with the Main Document of this documentation set sections 9 (which describes the general formatting for all Service Requests and Service Responses) and 2.3.10 (which describes the Firmware Distribution and Activation process) and with the XSD (XML Schema - document 3 of this documentation set).

11.1.1 Service Request

11.1.1.1 Format

The Request Body XML element of the XSD (see XML Schema – document 3 of this documentation set) defines the structure of all the Service Requests. Its UpdateFirmware XML element defines this Service Request and contains the Firmware Image, its Version and the list of Device IDs the Firmware is to be distributed to.

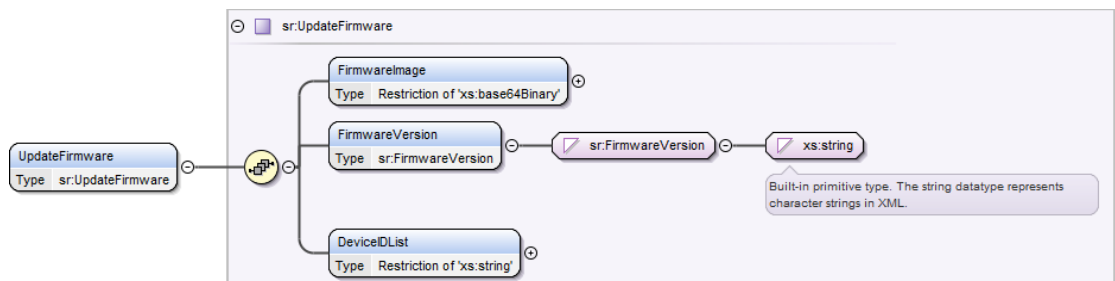


Figure 1 Update Firmware Service Request Structure

11.1.1.2 Specific Data Items Definition

The data items contained in the Service Request are defined as:

Table 4 Update Firmware Service Request Data Items

¹ List of Device IDs. Minimum 1 and maximum 50000

11.1.1.3 Applicable Modes of Operation

The Modes of Operation applicable to this Service Request are (see Main Document of this documentation set section 2.3 for Modes of Operation definitions):

Service	Transform	On Demand	DCC Only	Future Dated	DSP Scheduled
SMETS2 or later	No	No	Yes ¹	No	No
SMETS1	No	No	Yes ¹	No	No

Table 5 Update Firmware Modes of Operation

¹ See Main Document of this documentation set section 2.3.10 for details on Firmware Distribution Mode of Operation

11.1.1.4 Applicable Command Variant Values

The Command Variant values applicable to this Service Request are (see Main Document of this documentation set section 3 for Command Variant definitions):

Service	CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
SMETS2 or later	No	No	No	No	No	No	No	Yes
SMETS1	No	No	No	No	No	No	No	Yes

Table 6 Update Firmware Command Variant Values

11.1.1.5 Validation

This Service Request specific validation is as follows (see Main Document of this documentation set section 7 for generic access control checks):

Validation Check	Process	Response Code
Does the Firmware version ID match an entry on the Central Products List?	Check that the Firmware Version aligns with an entry on the Central Products List, i.e. it is an approved Firmware Version Id	E110101 ⁴
Are all the Devices in the list valid? ³	Check that each Device ID in the list exists and the DCC Service User, in the User Role defined in the Service Request, is the registered Import Supplier for all the Devices in the list, or for a SMETS1 CHF / SMETS1 PPMID the Lead Supplier	W110101 ²
Are all Devices in the list in a Status of 'Commissioned' or 'Suspended'? ¹	SMETS2 or later: Check that each Device ID in the list corresponds to a Meter or HCALCS in a status of 'Commissioned' or 'Suspended' SMETS1: Check that each Device ID in the list corresponds to a Meter, CHF or PPMID in a status of 'Commissioned' or 'Suspended'	W110101 ²
Is the Firmware Version applicable to each 'Commissioned' Device in the list?	Check that the Firmware Version is applicable to each 'Commissioned' Device ID in the list	W110101 ²

Validation Check	Process	Response Code
For SMETS2 or later Devices: Is there another firmware upgrade request already in progress for the Device in the list?	For SMETS2 or later Devices, check that the Device does not have another active firmware upgrade request in progress.	W110101 ²
For an HCALCS Device Type: Does the Device currently have a Firmware Version that is GBCS v4.1 or later?	For the HCALCS Device Type, check that the Device has a Firmware Version that is GBCS v4.1 or later.	W110101 ²
For an HCALCS Device Type: Does the CHF associated with the HCALCS have a Firmware Version that is GBCS v4.1 or later?	For the HCALCS Device Type, check that the Firmware Version of the CHF associated with the Device is GBCS v4.1 or later.	W110101 ²
Check that the firmware status value as per CPL is active?	Check the status of the firmware image against the CPL.	E110102
Check that the Firmware Hash of the Manufacturer Image part of the firmware image contained within the Service Request is the same as the Firmware Hash for that firmware image contained within the CPL	DCC Data Systems to compute the hash of the Manufacturer Image part of the firmware image and check this against the hash held for this version of firmware from the stored Central Products List (CPL)	E110103
Is the FirmwareImage well formed?	Check that the FirmwareImage contains both an OTA Header and a Firmware Image concatenated together, <u>conforms to GBCS requirements</u> , and if a non-SMETS1 Firmware image is within the non-SMETS1 size limit i.e. 1024000. Note that 1024000 is the base 64 equivalent of approx. 750kb.	E110105

Table 7 Update Firmware Service Request Validation

¹ This check supersedes the generic Authorisation Check associated to Response Code E5. See Main Document of this documentation set section 7.4

² The same Response Code is returned to indicate the Response contains a warning

³ This check supersedes the generic Authorisation Check associated to Response Code E4. See Main Document of this documentation set section 7.4

⁴ HCALCS Firmware Versions are not valid prior to DUIS v5.0

11.1.1.6 Sample Request

Sample requests are given in Annex Introduction Appendix 2. The specific information for this Service Request (Body) is as follows:

```
<UpdateFirmware>
  <FirmwareImage>ZGVmYXVsdA==</FirmwareImage>
  <FirmwareVersion>1100EEFF</FirmwareVersion>
  <DeviceIDList>11-00-AA-BB-CC-DD-EE-FF,22-00-AA-BB-CC-DD-EE-FF</DeviceIDList>
</UpdateFirmware>
```

Figure 2 Sample Update Firmware Service Request (Body) Format

11.1.2 Responses

The response messages for an “Update Firmware” Request follow the generic format for all “DCC Only” Service Responses. The generic responses applicable to this request are;

- Acknowledgement.
- Service Response (from DCC). Applicable if response includes a warning

See Main Document of this documentation set section 2.3.10 for details on the Firmware Distribution responses from the Devices.

11.1.2.1 Service Response (from DCC)

Applicable to cases where authorisation / validation failed for one or more of the Device IDs in the list to inform the DCC Service User of the Device IDs not included in the DCC Data Systems Request to the CSPs.

11.1.2.1.1 Format

This Service Request synchronous response is defined in the XSD DSPUpdateFirmwareWarning XML element, which contains the list(s) of Device IDs that failed DCC Authorisation / Validation.

Note that when the image has been received by the target device the device shall send an Alert (code 0x8F72 for success and 0x8F1C for failure) see Annex 15 for further information on these Alerts.

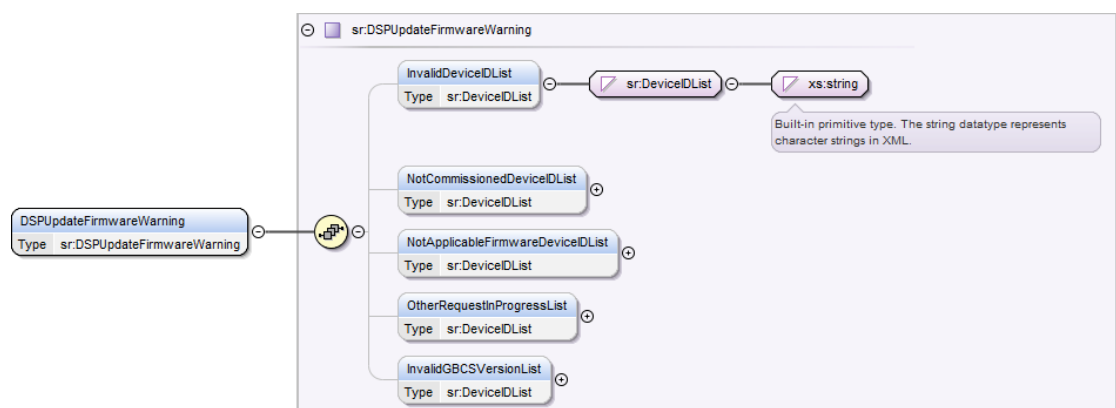


Figure 3 Update Firmware Service Response (from DCC) – Update Firmware Warning Structure

A DSPUpdateFirmwareWarning element is returned when ResponseCode is W110101.

Data Item	Description / Valid Set	Type	Mandatory ¹	Default	Units	Sensitivity
InvalidDeviceIDList	<p>Comma separated list of Device IDs for which the DCC Service User ID is not the registered Import Supplier or the Device IDs don't exist.</p> <p>Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)</p>	<p>sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){1,}([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){0,1})")</p>	No ¹	None	N/A	Non-Sensitive
NotCommissionedDeviceIDList	<p>SMETS2 or later: Comma separated list of Device IDs which aren't in a status of "Commissioned" or "Suspended" or the Device is not a Meter or HCALCS.</p> <p>SMETS1: Comma separated list of Device IDs which aren't in a status of "Commissioned" or "Suspended" or the Device is not a Meter or a SMETS1 CHF/PPMID.</p> <p>Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)</p>	<p>sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){1,}([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){0,1})")</p>	No ¹	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory ¹	Default	Units	Sensitivity
NotApplicableFirmwareDeviceIDList	Comma separated list of Device IDs for which the Firmware is not applicable. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})"*)	No ¹	None	N/A	Non-Sensitive
OtherRequestInProgressList	Comma separated list of Device IDs for which another Firmware Update request is in progress. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17). Prior to DUIS v5.0, Devices with in-progress updates will be included in the InvalidDeviceIDList. This list type is introduced in DUIS v5.0.	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})"*)	No ¹	None	N/A	Non-Sensitive
InvalidGBCSVersionList	Comma separated list of <ul style="list-style-type: none"> HCALCS Device IDs for which the GBCS Version of the associated CHF is prior to v4.1 HCALCS Device IDs for which the current GBCS Version is prior to v4.1 Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17). This list type is introduced in DUIS v5.0. Note: this list and the associated validation is primarily intended to check GBCS compatibility of the CHF Firmware Version. However the same list will also be used to report any validation failures for GBCS compatibility of the HCALCS Firmware Version.	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})"*)	No ¹	None	N/A	Non-Sensitive

Table 8 Update Firmware Service Response (from DCC) – Update Firmware Warning Data Items

¹ The DSPUpdateFirmwareWarning will contain at least one of the 5 Lists and it could contain all of them

11.1.2.1.3 Sample Responses

Sample responses are given in Annex Introduction Appendix 1. The specific information for this Service Request Response is as follows:

```
<ResponseMessage>
  <ServiceReference>11.1</ServiceReference>
  <ServiceReferenceVariant>11.1</ServiceReferenceVariant>
  <DSPUpdateFirmwareWarning>
    <NotCommissionedDeviceIDList>22-00-AA-BB-CC-DD-EE-FF</NotCommissionedDeviceIDList>
    <OtherRequestsInProgressList>22-00-AA-BB-CC-DD-EE-AA</OtherRequestsInProgressList>
  </DSPUpdateFirmwareWarning>
</ResponseMessage>
```

Figure 4 Sample Update Firmware Service Response (from DCC) – Update Firmware Warning Format

11.1.2.2 Unsuccessful Response

The Response Codes specific to this Service Request are:

Response Code	Response Code Name	Response Code Type	Description
E110101	Failed Validation – Firmware Version not approved	Error	The Firmware Version is not approved, i.e. it doesn't align with an entry on the Central Products List
W110101	Failed Authorisation – Invalid User / Device Registration Status and / or Firmware Version not applicable to Device	Warning	<p>The Update Firmware Warning contains between one and five lists of Device IDs for which the validation failed:</p> <ul style="list-style-type: none"> InvalidDeviceIDList. The Device ID doesn't exist or the DCC Service User is not the Device's registered Import Supplier NotCommissionedDeviceIDList. The Device's status is not 'Commissioned' or 'Suspended' or the Device is not a Meter, HCALCS, SMETS1 CHF or SMETS1 PPMID NotApplicableFirmwareDeviceIDList. The Firmware Version is not applicable to the Device OtherRequestsInProgressList. The Device already has another Firmware update request in progress InvalidGBCSVersionList: The CHF associated with the HCALCS Device has a GBCS Version prior to v4.1 (and so firmware updates are not supported); or additionally the target HCALCS Device has a GBCS Version prior to v4.1 (and so firmware updates are not supported).
E110102	Failed Validation – Firmware not active	Error	The firmware is not marked as active in the Central Products List and Smart Meter Inventory.
E110103	Failed Validation – Hash error	Error	The calculated hash value for the Manufacturer Image part of the firmware Image provided by the User within the Service Request differs from that held in the CPL for the specified FirmwareVersion.
E110105	Failed Validation – Firmware image not correctly formed	Error	The firmware image is not constructed as per the GBCS definition, e.g. the FirmwareImage does not contain both an OTA Header and a Firmware Image concatenated together, or the size is too large for the SMETS version.

Table 9 Failed Update Firmware Service Request Response Codes

11.2 Read Firmware Version (11.2)

Service Request Name	ReadFirmwareVersion
Service Reference	11.2
Service Request Variant Name	ReadFirmwareVersion
Service Reference Variant	11.2
Service Request Objective	To enable a DCC Service User to retrieve the firmware details that currently exists on a specified Device.
Business Context Statement	The DCC Service User requires the details of the current operating firmware version for a specified device
User Role Access	<ul style="list-style-type: none"> Electricity Import Supplier (EIS) Electricity Export Supplier (EES) Gas Import Supplier (GIS) Supplier Nominated Agent (SNA) Electricity Network Operator (ENO) Gas Network Operator (GNO) Other User (OU)
Security Classification	Non-critical and non-sensitive SMETS2 or later: GBCS XREF: SME.C.NC
Service Request Narrative (SMETS2 or Later)	<ol style="list-style-type: none"> The Gas Smart Meter Firmware Version can be read from the Gas Proxy Function (preferred) or from the Meter. This approach is recommended to preserve the battery life of the GSME. Upon receipt of a Response to this Service Request containing a Firmware Version value, <ol style="list-style-type: none"> if the Target Device Type is ESME, GSME, CHF, PPMID or HCALCS and the Firmware Version returned by the Device matches an entry on the CPL, but is different from that stored in the SMI, the DCC Data Systems will update the Firmware Version in the SMI to the value returned by the Device. Note that updating the Firmware Version may also update the Device's GBCS Version in the SMI <ol style="list-style-type: none"> If the target Device is CHF, the associated GPF Firmware Version will also be updated If the Firmware Version entry on the CPL has a status of "Current" and the Read Firmware Version Service Request wasn't submitted by the Responsible Import Supplier, DCC Alert N49 will be sent to the Responsible Import Supplier, or to all Responsible Import Suppliers where the Device is a PPMID. If the Device Status was 'Suspended' and the Firmware Version returned by the Device matches an entry on the CPL with a status of "Current" the DCC Data Systems shall update it to the status it held immediately prior to its Suspension and DCC Alert

	<p>N29 will be sent to the Responsible Import Supplier and, for ESMEs, GSMEs and GPFs, to the Responsible Network Operator.</p> <p>iv. If the Firmware Version entry on the CPL has a status of "Removed", the SMI Firmware Version will be updated, but the Device Status will not be set to 'Suspended'. In this case DCC Alert N50 will be sent to the Responsible Import Supplier as a warning, or to all Responsible Import Suppliers where the Device is a PPMID.</p> <p>b. if the Target Device Type is ESME, GSME, CHF, PPMID or HCALCS and the Firmware Version returned by the Device doesn't match an entry on the CPL DCC Alert N51 will be sent to the Responsible Import Supplier, or to all Responsible Import Suppliers where the Device is a PPMID, as a warning and the SMI Firmware Version will not be updated</p> <p>c. if the Target Device Type is GPF and the GSME Firmware Version returned by the GPF is different from that stored in the SMI, DCC Alert N52 will be sent to the Responsible Import Supplier as a warning and the SMI Firmware Version will not be updated</p> <p>d. Updates to the Smart Metering Inventory are carried out before the Service Response is generated. The other actions above are post-processing steps after the Service Response has been sent to the User</p> <p>3. In case of a SMETS2 or later PPMID, the Command will always be sent to the Device even if the version of the firmware recorded in the SMI indicates that the Device is not capable of returning the firmware version, as there is a possibility that the firmware has been updated but no activation alert has been received. If the PPMID does not in fact support the command, it will discard the command without sending a response, and will generate Device Alert 0x8F1E, which will cause DSP to generate a DCC Alert N39.</p>			
GBCS Cross Reference	Electricity / Communications Hub Function	Gas	PPMID	HCALCS
GBCS Message Code prior to GBCS v4.1	0x0059	0x0084	N/A ¹	N/A
GBCS Use Case prior to GBCS v4.1	ECS52	GCS38	N/A ¹	N/A
GBCS Use Case Name prior to GBCS v4.1	Read ESME/Comms Hub Firmware Version (prior to GBCS v4.0) Read ESME/SAPC/Comms Hub Firmware Version (GBCS v4.0 or later)	Read GSME Firmware Version	N/A ¹	N/A
GBCS Message Code v4.1 or later	0x0059	0x0084	0x0129	0x0129

GBCS Use Case v4.1 or later	ECS52	GCS38	CS08	CS08
GBCS Use Case Name v4.1 or later	Read ESME/SAPC/Comms Hub Firmware Version	Read GSME Firmware Version	Read PPMID/HCALCS Firmware Version	Read PPMID/HCALCS Firmware Version
SMETS1 Applicability	Yes	Yes	Yes	No
Service Request Narrative (SMETS1)	The behaviour of DSP for this Service Request with regard to SMETS1 Devices is equivalent to the behaviour for SMETS2 or later Devices except: <div>1. Steps 2a and 2b in the SMETS2 or later narrative above, for SMETS1 CHF and PPMID, the alerts N49, N50 and N51 are only sent to the Responsible Import Supplier for the ESME on the same HAN.</div>			
GBCS Commands - Versioning Details				
DCC Data System creates the following GBCS Commands or Response Codes based on the following combinations				
Device Type			ESME	
Device’s firmware version for Business Target Device ID specified within SRV and contained within SMI			GBCS v1.0 or later	
DEFAULT - No specific XML criteria			ECS52	
Device Type			GSME	
Device’s firmware version for Business Target Device ID specified within SRV and contained within SMI			GBCS v1.0 or later	
DEFAULT - No specific XML criteria			GCS38	
Device Type			PPMID	
Device’s firmware version for Business Target Device ID specified within SRV and contained within SMI			GBCS prior to v4.1	GBCS v4.1 or later
DEFAULT - No specific XML criteria			CS08 ¹	CS08
Device Type			HCALCS	
Device’s firmware version for Business Target Device ID specified within SRV and contained within SMI			GBCS prior to v4.1	GBCS v4.1 or later
DEFAULT - No specific XML criteria			Response Code - E57	CS08

Table 10 Read Firmware Version Service Request

¹ For a SMETS2 PPMID, DSP will create a GBCS Command conforming to GBCS Use Case CS08 regardless of the firmware version for the Business Target Device ID specified within the SRV and contained within SMI (see narrative point 3 for further information); this is to enable the DCC Service User to query the Device in the event that a Device with a GBCS version prior to v4.1 has been updated to GBCS v4.1 or later successfully but the SMI record was not updated to show that (e.g. the activation alert was not received). Note that this is not applicable to HCALCS because (unlike PPMID) it is not feasible to update the firmware of an HCALCS Device with GBCS version prior to v4.1.

This section should be read in conjunction with Main Document of this documentation set section 9 (which describes the general formatting for all Service Requests and Service Responses) and with the XSD (XML Schema – document 3 of this documentation set).

11.2.1 Service Request

11.2.1.1 Format

The Request Body XML element of the XSD (see XML Schema – document 3 of this documentation set) defines the structure of all the Service Requests. Its ReadFirmwareVersion XML element defines this Service Request and only contains the Execution Date and Time for Future Dated Requests.

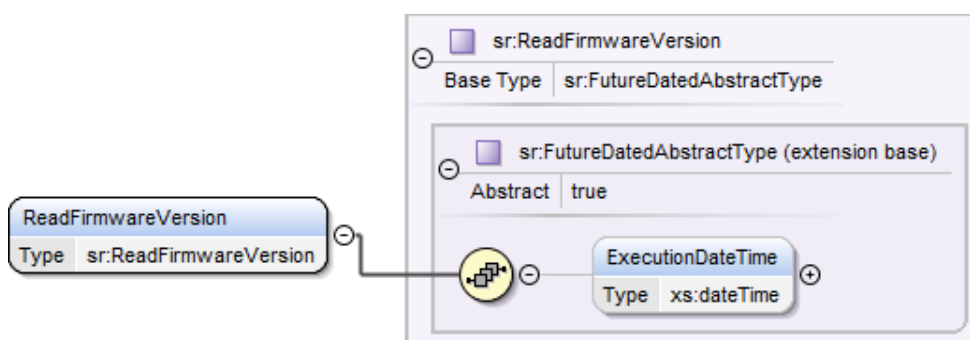


Figure 5 Read Firmware Version Service Request Structure

11.2.1.2 Specific Data Items Definition

The data items contained in the Service Request are defined as:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ExecutionDateTime	The UTC date and time the DCC User requires the command to be executed on the Device ID <ul style="list-style-type: none"> Date-time in the future that is either <= current date + 30 days or the date = 31/12/3000 	xs:dateTime	No	None	UTC Date-Time	Non-Sensitive

Table 11 Read Firmware Service Request Data Items

11.2.1.3 Applicable Modes of Operation

The Modes of Operation applicable to this Service Request are (see Main Document of this documentation set section 2.3 for Modes of Operation definitions):

Service	Transform	On Demand	DCC Only	Future Dated	DSP Scheduled
SMETS2 or later	No	Yes	No	DSP	No

Service	Transform	On Demand	DCC Only	Future Dated	DSP Scheduled
SMETS1	No	Yes	No	DSP	No

Table 12 Read Firmware Version Modes of Operation

11.2.1.4 Applicable Command Variant Values

The Command Variant values applicable to this Service Request are (see Main Document of this documentation set section 3 for Command Variant definitions):

Service	CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
SMETS2 or later	Yes	Yes	Yes	No	No	No	No	No
SMETS1	Yes	No	No	No	No	No	No	No

Table 13 Read Firmware Version Command Variant Values

11.2.1.5 Validation

This Service Request has no specific validation. See Main Document of this documentation set section 7 for generic access control checks and Annex section 17.2 for Execution Date Time validation.

11.2.1.6 Sample Request

Sample requests are given in Annex Introduction Appendix 2. The specific information for this Service Request (Body) is as follows:

<ReadFirmwareVersion/>

Figure 6 Sample Read Firmware Version Service Request (Body) Format

11.2.2 Responses

The response messages for a "Read Firmware Version" Request follow the generic format for all "Device" response messages, the generic responses applicable to this request are;

- Acknowledgement
- Service Response (from Device) - GBCSPayload. Service Response Specific Payload
- Command for Local Delivery
- Parse Output / SMETS1 Response.

See Main Document of this documentation set section 4 for Response IDs returned to DCC Service Users that are Known Remote Parties (KRP) or Unknown Remote Parties (URP) to the Device.

Sample responses are given in Annex Introduction Appendix 1, response specific information details are given below.

11.2.2.1 Parse Output / SMETS1 Response Format

11.2.2.1.1 Format - ReadFirmwareVersionRsp

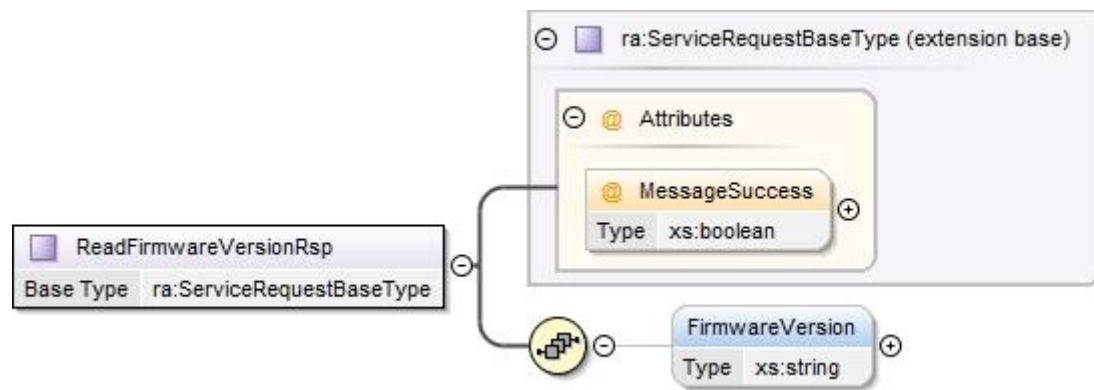


Figure 7 - Read Firmware Version Parse Response / SMETS1 Response Structure

11.2.2.1.2 Specific Header Data Items Definition

Data Item	Electricity Response	Gas Response	CHF/PPMID Response (SMETS1 only)	HCALCS	PPMID (SMETS2 only)
GBCSHexadecimalMessageCode	0059	0084	0059	0129	0129
GBCS Use Case Number (for information only - not in header)	ECS52	GCS38	n/a	CS08	CS08
GBCS Use Case Name (for information only - not in header)	Read ESME/Comms Hub Firmware Version (prior to GBCS v4.0) Read ESME/SAPC/Comms Hub Firmware Version (GBCS v4.0 or later)	Read GSME Firmware Version	Read ESME/Comms Hub Firmware Version	Read PPMID / HCALCS Firmware Version	Read PPMID / HCALCS Firmware Version
SupplementaryRemotePartyID	Present if originator is a URP	Present if originator is a URP	Present	Present if originator is a URP	Present
SupplementaryRemotePartyCounter	Present if originator is a URP	Present if originator is a URP	Present	Present if originator is a URP	Present
SupplementaryOriginatorCounter	Not Present	Not Present	Not Present	Not Present	Not Present
Timestamp	Not Present	Not Present	Not Present	Not Present	Not Present

Table 14 - Read Firmware Version Parse Response Header Data Items

See DUGIDS main document sections 8.1.1 and 4 for circumstances in which Users are a KRP or URP to a Device.

11.2.2.1.3 Specific Body Data Items Definition

The data items contained in the parse response are.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
FirmwareVersion	<p>Current version number in manufacturer format.</p> <p>The Firmware version as held in the CPL and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F.</p> <p>This data item matches the value on the CPL (excluding the colon separator between octet values)</p> <p>The value shall be four octets in length and shall correspond to the File Version field in the ZSE OTA Header structure.</p>	xs:string (maxLength = 8)	No	None	N/A	Non-Sensitive

Table 15 - Read Firmware Version Parse Response / SMETS1 Response Body Data Items

11.2.2.1.4 Sample Response

```
<ra:ReadFirmwareVersionRsp MessageSuccess="true">
  <ra:FirmwareVersion>1100EEFF</ra:FirmwareVersion>
</ra:ReadFirmwareVersionRsp>
```

Figure 8 - Read Firmware Version Parse Response Sample

11.3 Activate Firmware (11.3)

Service Request Name	ActivateFirmware
Service Reference	11.3
Service Request Variant Name	ActivateFirmware
Service Reference Variant	11.3
Service Request Objective	To enable a DCC Service User to activate the specified firmware image stored on a specified ESME, GSME, HCALCS, SMETS1 CHF or SMETS1 PPMID.
Business Context Statement	The DCC Service User requires that the current version of firmware operating on a specified device is updated to the required version, e.g. following a firmware fix (or up-to-date version) being released by the device manufacturer.
User Role Access	<ul style="list-style-type: none"> Electricity Import Supplier (EIS) Gas Import Supplier (GIS)

Security Classification	Critical and non-sensitive SMETS2 or later: GBCS XREF: SME.C.C		
Service Request Narrative (SMETS2 or later)	<ol style="list-style-type: none"> 1. Pre-Condition - To successfully execute this Service Request a DCC Service User Must first have sent and received successful confirmation that a new firmware image is stored on the target Device ready for activation as a result of sending Service Request 11.1 UpdateFirmware. 2. A DCC Service User will know this to be true if and / or when they will have received a GBCS Alert (Alert Code 0x8F72). 3. The DCC Data Systems shall monitor all Responses received to this Service Request. Where the DCC identifies any Response where the current Firmware Version returned by the Device matches an entry on the CPL for that Device Model and that Firmware Version is different to the value currently held in the Smart Metering Inventory for that Device, an update to the Smart Metering Inventory shall be made. <ol style="list-style-type: none"> a. The DCC Data Systems shall update the DeviceFirmwareVersion data item within the Smart Metering Inventory to record the new DeviceFirmwareVersion value for the specified Device ID received in the Response. b. If the Device Status was 'Suspended' and the Firmware Version returned by the Device matches an entry on the CPL with a status of "Current" the DCC Data Systems shall update it to the status it held immediately prior to its Suspension and DCC Alert N29 will be sent to the Responsible Import Supplier and, for ESMES, GSMES and GPFs, to the Responsible Network Operator. c. If the Firmware Version returned by the Device matches an entry on the CPL with a status of "Removed", the SMI Firmware Version will be updated, but the Device Status will not be set to 'Suspended'. In this case DCC Alert N50 will be sent to the Responsible Import Supplier as a warning. d. Note that if the Firmware Version returned by the Device is invalid (doesn't match an entry on the CPL) DCC Alert N51 will be sent to the Responsible Import Supplier as a warning and the Smart Metering Inventory Firmware Version will not be updated. e. Updates to the Smart Metering Inventory are carried out before the Service Response is generated. The other actions above are post-processing steps after the Service Response has been sent to the User. 4. The Firmware Hash value included in the Service Request shall be calculated by the DCC Service User using the algorithm as defined in the SEC definition of Firmware Hash. 5. <u>Some specific ESME Devices have a known issue that causes power to be lost to the comms hub as a side effect of activating a firmware update. This causes the comms hub to generate a spurious power outage alert. To manage this issue, DCC Data System will track firmware activation commands sent to affected ESMES and will suppress any power outage message received from the comms hub that notifies an outage which started within [30 minutes] of such a firmware activation. The Devices affected are identified by Device ID and are limited to a subset of SMETS2 ESMES. See section 2.3.12 of the main DUGIDS document for more information about power outage alerts.</u> 		
GBCS Cross Reference	Electricity (ESME)	Gas	HICALCS
GBCS prior to v4.1 Message Code	0x0012	0x0012	N/A

GBCS prior to v4.1 Use Case	CS06	CS06	N/A
GBCS prior to v4.1 Use Case Name	Activate Firmware	Activate Firmware	N/A
GBCS v4.1 or later Message Code	0x0012	0x0012	0x0012
GBCS v4.1 or later Use Case	CS06	CS06	CS06
GBCS v4.1 or later Use Case Name	Activate Firmware	Activate Firmware	Activate Firmware
SMETS1 Applicability	Yes for ESME, GSME, CHF and PPMID		
Service Request Narrative (SMETS1)	<p>The behaviour of DSP for this Service Request with regard to SMETS1 Devices is equivalent to the behaviour for SMETS2 or later Devices except:</p> <ol style="list-style-type: none">1. In addition to ESME and GSME, Firmware of a SMETS1 CHF or a SMETS1 PPMID can be updated by this Service Request (by the Responsible Supplier for the SMETS1 ESME which is connected to the same home area network as the SMETS1 CHF / PPMID; note that response code E4 would be returned if this is attempted by the GIS).2. For SMETS1 Devices the Alert Code 0x8F72 will be sent as a SMETS1 Alert rather than as a GBCS Alert.3. If the activation of the Firmware update to a SMETS1 CHF or SMETS1 PPMID is successful, then DCC Alert N57 will be sent to all Suppliers with an interest in the HAN except for the Supplier that originated the Service Request.4. Where the Device is a SMETS1 CHF, the behaviour documented in 3b above regarding returning from Device Status Suspended applies also to the corresponding GPF.5. For SMETS1 devices the SMI Firmware Version will be updated only where the response indicates success.		
GBCS Commands - Versioning Details			
DCC Data System creates the following GBCS Commands or Response Codes based on the following combinations			
Device Type		ESME	
Device's firmware version for Business Target Device ID specified within SRV and contained within SMI		GBCS v1.0 or later	
DEFAULT - No specific XML criteria		CS06	

Device Type	GSME	
Device's firmware version for Business Target Device ID specified within SRV and contained within SMI	GBCS v1.0 or later	
DEFAULT - No specific XML criteria	CS06	
Device Type	HCALCS	
Device's firmware version for Business Target Device ID specified within SRV and contained within SMI	GBCS prior to v4.1	GBCS v4.1 or later
Prior to DUIS v5.0: DEFAULT - No specific XML criteria	Response Code - E57	Response Code - E57
DUIS v5.0 or later: DEFAULT - No specific XML criteria	Response Code - E57	CS06

Table 16 Activate Firmware Service Request

This section should be read in conjunction with the Main Document of this documentation set section 9 (which describes the general formatting for all Service Requests and Service Responses) and with the XSD (XML Schema – document 3 of this documentation set).

11.3.1 Service Request

11.3.1.1 Format

The Request Body XML element of the XSD (see XML Schema – document 3 of this documentation set) defines the structure of all the Service Requests. Its ActivateFirmware XML element defines this Service Request and contains the Firmware Hash and, for Future Dated, the Execution Date and Time.

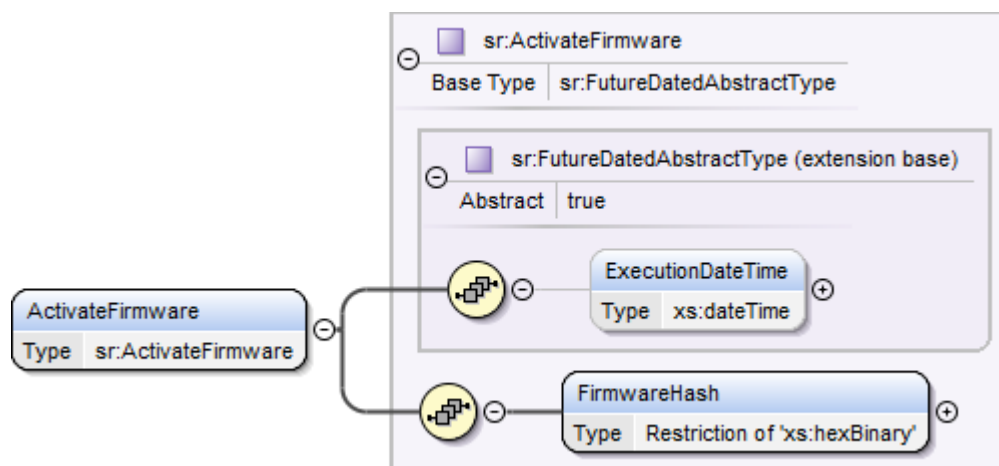


Figure 9 Activate Firmware Service Request Structure

11.3.1.2 Specific Data Items Definition

The data items contained in the Service Request are defined as:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ExecutionDateTime	The date and time at which the firmware will be activated Valid set: <ul style="list-style-type: none"> Date-time in the future that is either <= current date + 30 days or the date = 31/12/3000 	xs:dateTime	No	None	N.A	Non-Sensitive
FirmwareHash	Hash calculated over the Firmware Image The Firmware hash as held in the CPL and presented in the format XX.XX (64 characters) where each X is one of the characters 0 to 9 or A to F. This data item must match the value on the CPL (excluding the colon separator between octet values) Note that a hexBinary value of length 32 is defined as 32 octets, an octet is represented as 2 characters.	Restriction of xs:hexBinary (minLength = 32, maxLength = 32)	Yes	None	N/A	Non-Sensitive

Table 17 Activate Firmware Service Request Data Items

11.3.1.3 Applicable Modes of Operation

The Modes of Operation applicable to this Service Request are (see Main Document of this documentation set section 2.3 for Modes of Operation definitions):

Service	Transform	On Demand	DC C Only	Future Dated	DSP Scheduled
SMETS2 or later	Yes	Yes	No	Device	No
SMETS1	No	Yes	No	DSP	No

Table 18 Activate Firmware Modes of Operation

11.3.1.4 Applicable Command Variant Values

The Command Variant values applicable to this Service Request are (see Main Document of this documentation set section 3 for Command Variant definitions):

Service	CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
SMETS2 or later	No	No	No	Yes	Yes	Yes	Yes	No
SMETS1	No	No	No	Yes	No	No	No	No

Table 19 Activate Firmware Command Variant Values

11.3.1.5 Validation

This Service Request has no specific validation. See Main Document of this documentation set section 7 for generic access control checks and Annex section 17.2 for Execution Date Time validation.

11.3.1.6 Sample Request

There are three versions applicable to this Service Request

- Transform Service Request
- Signed Pre-command
- SMETS1 Service Request. Same format as Transform Service Request

Sample requests are given in Annex Introduction Appendix 2. The specific information for this Service Request (Body) is as follows:

```
<ActivateFirmware>  
<FirmwareHash>0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF</FirmwareHash>  
</ActivateFirmware>
```

Figure 10 Sample Activate Firmware Transform Request (Body) Format

11.3.2 Responses

The response messages for an “Activate Firmware” Request follow the generic format for all “Device” response messages, the generic responses applicable to this request are;

- Pre-command
- Acknowledgement
- Service Response (from Device) - GBCSPayload
- Service Response (from Device) - FutureDatedDeviceAlertMessage
- Command for Local Delivery
- Parse Output / SMETS1 Response

Sample responses are given in Annex Introduction Appendix 1, response specific information details are given below.

11.3.2.1 Device Responses and Future Dating

For SMETS2 or later Devices this Service Request's Command contains a fixed number of instructions ('n' = 1) and activation date-time instructions ('m' = 1). See Main Document of this documentation set section 9.3.6 for details of the Device Responses returned in the different scenarios. Apart from in the exception cases described there, e.g. cancellation, the relationship between Mode of Operation and Response message types is as follows:

1. On Demand.
 - a. Service Response (from Device) – GBCSPayload
 - i. One Device Response (Command execution outcome containing 'n' results).
2. Future Dated (Device).
 - a. Service Response (from Device) – GBCSPayload
 - i. One Device Response (Command storage outcome containing 'n' results)
 - b. Service Response (from Device) – FutureDatedDeviceAlertMessage

- i. 'm' Device Alerts (Command instruction execution outcome). These Device Alerts are described in Annex section 15.4.4. The Device Alert payloads for this particular Service Request will be of the type described in Annex section 15.4.4.3.4.

For SMETS1 Devices this Service Request is only available for Mode of Operation On Demand or Future Dated (DSP). In both cases, the Response message type is a single SMETS1 Device Response.

11.3.2.2 Parse Output / SMETS1 Response Format

11.3.2.2.1 Format - ActivateFirmwareResp

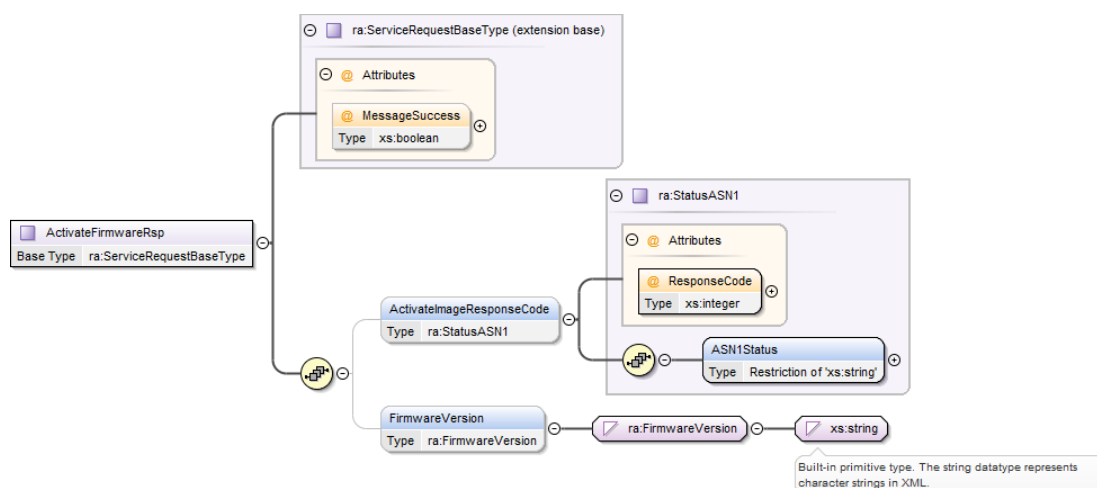


Figure 11 – Activate Firmware Parse Response / SMETS1 Response Structure

11.3.2.2.2 Specific Header Data Items Definition

Data Item	Electricity/HCALCS Response	Gas Response	CHF/PPMID Response (SMETS1 only)
GBCSHexadecimalMessageCode	0012	0012	0012
GBCS Use Case Number (for information only - not in header)	CS06	CS06	N/A
GBCS Use Case Name (for information only - not in header)	Activate Firmware	Activate Firmware	Activate Firmware
SupplementaryRemotePartyID	Not Present	Not Present	Present
SupplementaryRemotePartyCounter	Not Present	Not Present	Present
SupplementaryOriginatorCounter	Not Present	Not Present	Not Present
Timestamp	Present	Present	Present

Table 20 - Activate Firmware Parse Response Header Data Items

11.3.2.2.3 Specific Body Data Items

Responses to on demand execution requests will carry the data in the table below.

Parse Responses: See section 11.3.2.1 for description of the responses to Future Dated execution requests. Where an immediate response to a request for Future Dated execution indicates successful placing of the Command on the Device, it will be returned as a status-only response. Please see Annex section 18.9 for a description of how status-only responses are represented in the MMC XML schema.

Data Item	Description / Valid Set	Type	Default	Units	Sensitivity
ActivateImageResponseCode	Outcome of the request for each replacement. Valid Set: <ul style="list-style-type: none"> success noImageHeld hashMismatch activationFailure Only present in responses to on demand execution requests. Not present in responses to requests for future dated execution.	Restriction base xs:string (Enumeration)	None	N/A	Non-Sensitive
FirmwareVersion	A unique identifier representing a firmware image that has been approved for release by the DCC User concerned. The Firmware version as held in the CPL and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F. This data item matches the value on the CPL (excluding the colon separator between octet values) . Only present in responses to on demand execution requests. Not present in responses to requests for future dated execution.	ra:FirmwareVersion (restriction of xs:string, (maxLength = 8)			

Table 21 - Activate Firmware Parse Response / SMETS1 Response Body Data Items

11.3.2.2.4 Sample Response body

```
<ra:ActivateFirmwareRsp MessageSuccess="true">
  <ra:ActivateImageResponseCode ResponseCode="0">
    <ra:ASN1Status>success</ra:ASN1Status>
  </ra:ActivateImageResponseCode>
  <ra:FirmwareVersion>1100EEFF</ra:FirmwareVersion>
</ra:ActivateFirmwareRsp>
```

Figure 12 - Activate Firmware Parse Response Sample

11.4 Update PPMID Firmware (11.4)

Service Request Name	UpdatePPMIDFirmware
Service Reference	11.4
Service Request Variant Name	UpdatePPMIDFirmware
Service Reference Variant	11.4
Service Request Objective	To enable a DCC Service User to request that the DCC distribute a specified Firmware Image to a specified PPMID for storage and activation.
Business Context Statement	<p>The DCC Service User requires that an existing version of firmware operating on a specified PPMID is updated to the new specified version, e.g. following a firmware fix (or up-to-date version) being released for the PPMIDs.</p> <p>This Service Request is used to distribute and activate firmware to multiple PPMIDs. The Firmware image is included within the Service Request.</p>
User Role Access	<ul style="list-style-type: none"> Electricity Import Supplier (EIS) Gas Import Supplier (GIS)
Security Classification	<p>Non-critical and non-sensitive</p> <p>SMETS2 or later: GBCS XREF: SME.C.NC</p>
Service Request Narrative (SMETS2 or later)	<ol style="list-style-type: none"> This Service can only be used for command delivery across the SM WAN. There are no local command delivery services for this service request. The maximum number of Device IDs that can be included in a Service Request is 50,000. Each Service Request has to include the Firmware Image and version. The Service Request Mode of Operation is “DCC Only” (see Main Document of this documentation set section 2.3.10 for details on Firmware Distribution Mode of Operation), i.e.: <ol style="list-style-type: none"> Business Target ID = DSP Broker ID Command Variant = 8 The DCC Data Systems apply the following specific authorisation and validation checks prior to the generation of the Service Response: <ol style="list-style-type: none"> The Firmware version specified in the Service Request matches an entry on the Central Products List, (approved Firmware version ID). The Firmware version is presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F, for example "1100EEFF" The DCC Service User is the Registered Import Supplier for one of the meters connected to the same home area network as each of the Device IDs in the list. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed Each Device ID in the list corresponds to a Device with a status of “Commissioned”. If this validation fails for at least one of the Devices, the

Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed.

Note: This validation will also allow Devices with a status of "Suspended".

- d. The Firmware Version is applicable to each "Commissioned" Device's Device ID in the list. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed.
 - e. Each Device in the list is not already the subject of an Update Firmware Request that is in progress (with a Firmware Distribution Tracking status of 'Accepted by DSP', 'Approved For Distribution' or 'Successful CH Transfer' as described in the Main Document of this documentation set, section 2.3.10). If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed.
 - f. The Firmware of the CHF on the same HAN must be GBCS v4.1 or later. If this validation fails for at least one of the Devices, the Service Response (from DCC) will include a warning and the list of all the Device IDs for which the validation failed.
5. If the validation succeeds at least for one Device ID and the Service Request doesn't fail any anomaly detection checks, the DCC Data Systems distribute the Firmware to the PPMIDs (via the appropriate CSPs) as described in the Main Document of this documentation set section 2.3.10.
 6. Update PPMID Firmware Service Requests are subject to threshold anomaly detection (see Main Document of this documentation set section 16.3) but with a slight variation on the rules. Since a single Update PPMID Firmware Service Request may result in messages to many Devices, the message count for the purposes of anomaly detection will be increased by the total number of Devices listed in the Service Request rather than simply being increased by one.
 7. Reporting of errors or Firmware Distribution Tracking status changes via DCC Alerts subsequent to DSP validation. Please note that, because one Update PPMID Firmware Service Request can be split into Commands to more than one CSP it is possible for one of the Commands to succeed and another to fail:
 - a. If the CSP detects a mismatch in Firmware Version / Hash, then the DCC Service User will be sent a DCC Alert N18.
 - b. If the CSP detects an invalid combination of Communications Hub / PPMID IDs then the DCC Service User will be sent a DCC Alert N19.
 - c. If the CSP detects that the Firmware Image is too large then the DCC Service Users will be sent a DCC Alert N20.
 - d. If the Firmware Version is not recognised by the CSP then the DCC Service User will be sent a DCC Alert N21.
 - e. If the DCC cannot deliver the firmware image to the CSP, then the DCC Service User will be sent a DCC Alert N22 / N23.
 - f. If the firmware image has not been rejected by the CSP, all the Responsible Suppliers to that Device other than the sender will be sent a DCC Alert N59.
 - g. If the CSP cannot deliver the firmware image to the CHF, then the DCC Service User will be sent a DCC Alert N60.
 - h. If the CSP successfully delivers the firmware image to the CHF, then the DCC Service User will be sent a DCC Alert N61.

- i. The Device Alerts received from the CHF indicating the following statuses will be sent to the DCC Service User using the DCC Alert N62:
 - i. CHF failed to deliver the firmware image to the target Device.
 - ii. The firmware image has been discarded at the CHF.
 - iii. The firmware image has been rejected due to hardware version mismatch of the target Device.
 - iv. The firmware image has been successfully delivered to the target Device by the CHF.
8. The Device Alert received from the PPMID indicating the activation outcome (8F8B) will be sent to all the Responsible Suppliers to that Device using the DCC Alert N39

If the firmware update for a PPMIDfirmware is successfully activated on the PPMID, then:

 - a. The DCC Data Systems shall update the DeviceFirmwareVersion data item within the Smart Metering Inventory to record the new DeviceFirmwareVersion value for the Device ID of the Device that sent the Device Alert.
 - b. If the Device Status was 'Suspended' and the Firmware Version in the Device Alert matches an entry on the CPL with a status of "Current" the DCC Data Systems shall update it to the status it held immediately prior to its Suspension and DCC Alert N29 will be sent to the Responsible Import Suppliers.
 - c. If the Firmware Version in the Device Alert matches an entry on the CPL with a status of "Removed", the SMI Firmware Version will be updated, but the Device Status will not be set to 'Suspended'. In this case DCC Alert N50 will be sent to the Responsible Import Suppliers as a warning.
 - d. Note that if the Firmware Version in the Device Alert is invalid (doesn't match an entry on the CPL) DCC Alert N51 will be sent to the Responsible Import Suppliers as a warning and the Smart Metering Inventory Firmware Version will not be updated.
 - e. Updates to the Smart Metering Inventory are carried out before the N39 DCC Alert is generated. The other actions above are post-processing steps after the DCC Alert N39 has been sent to the User.
 - f. Note that those Responsible Suppliers using a DUIS version prior to v5.0 will only receive the Device Alert Code 8F8B (without the activation outcome). In this case, Service Request 11.2 can be used to read the Firmware Version currently active on the device.
9. It is the DCC Service User's responsibility to resend an Update Firmware Service Request to those Devices for which DSP, CSP or Device validation has failed or for which no successful response from the Device has been received. Note that in order to distinguish the Firmware Distribution Tracking between the original Upgrade Firmware Requests and resubmissions for the same Device and the same Firmware, the DCC Service User should use a new Service Request ID for each request.
10. The Firmware Image (maximum size = 750 KB) has to be included in the Service Request in base 64 binary form (maximum length = 1024000). Please see GBCS section 11, for details of the Firmware Image contents, format and validation.
11. Where a User receives a warning that an Update PPMID Firmware Request is in progress and does not believe that this is correct, then a service management incident should be raised so that the DCC's Firmware Distribution Tracking Status

	<p>can be updated to 'Reset By DCC' to allow subsequent Update Firmware Requests to be accepted by the DCC.</p> <p>12. DCC Service Users are requested to maximise the efficiency of firmware distribution within the DCC by ensuring that as many Devices as possible are included within Update Firmware Service Requests. Sending Service Requests with single or low numbers of Devices reduces firmware download efficiencies and increases overall delivery timescales.</p> <p>13. DCC Service Users are requested to send Service Request 11.2 Read Firmware Version to each PPMID before attempting to update the firmware, in order to ensure that the Device is turned on and ready to accept firmware updates; following this good practice will minimise the likelihood of DCC Service Users needing to raise technical queries and wasting DCC capacity.</p> <p>14. <u>DCC Data Systems will perform validation to check that the OTA header conforms to GBCS Table 11.2.3 requirements for the construction of the OTA Upgrade Image (ZigBee OTA Header + Upgrade Image), including the content of the OTA upgrade file identifier, OTA Header version, OTA Header length, OTA Header Field control and ZigBee Stack version, and that the total length of the OTA Upgrade Image matches the Total image size declared in the header.</u></p>
GBCS Cross Reference	PPMID
GBCS Message Code	N/A
GBCS Use Case	N/A
GBCS Use Case Name	N/A
SMETS1 Applicability	No

Table 22 Update PPMID Firmware Service Request

This section should be read in conjunction with the Main Document of this documentation set sections 9 (which describes the general formatting for all Service Requests and Service Responses) and 2.3.10 (which describes the Firmware Distribution and Activation process) and with the XSD (XML Schema - document 3 of this documentation set).

11.4.1 Service Request

11.4.1.1 Format

The Request Body XML element of the XSD (see XML Schema – document 3 of this documentation set) defines the structure of all the Service Requests. Its UpdatePPMIDFirmware XML element defines this Service Request and contains the Firmware Image, its Version and the list of Device IDs the Firmware is to be distributed to.

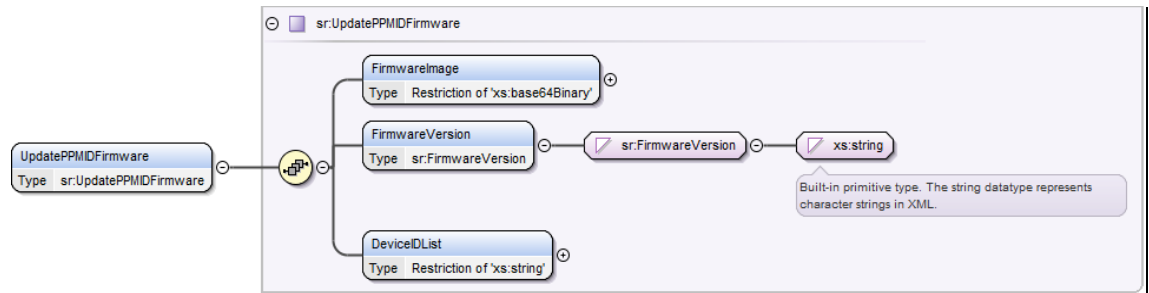


Figure 13 Update PPMID Firmware Service Request Structure

11.4.1.2 Specific Data Items Definition

The data items contained in the Service Request are defined as:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
FirmwareImage	<p>The Firmware Image corresponding to the Firmware Version</p> <p>The Firmware Image is the full OTA Upgrade Image as defined in GBCS. Note that this includes not only the Manufacturer Image but also additional signature and OTA Header information.</p> <p>Please see GBCS for details of how to construct the OTA Upgrade Image.</p> <p>The max length value in the XML schema is large enough to allow for SMETS1 Firmware images (for consistency with 11.1), whereas non-SMETS1 Firmware image size is restricted further; see validation error E110405.</p>	Restriction of xs:base64Binary (max Length = 10240000)	Yes	None	N/A	Non-Sensitive
FirmwareVersion	<p>A unique identifier representing a firmware image that has been approved for release by the DCC User concerned.</p> <p>The Firmware version as held in the CPL and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F.</p> <p>This value must align with the firmware version value listed on the Central Products List (excluding the colon separator between octet values) pursuant to SEC Section F2.</p> <p>For avoidance of doubt, there is no direct comparison made between this FirmwareVersion value to the File Version value contained in the OTA Header (as defined by GBCS).</p>	sr::FirmwareVersion (Restriction of xs:string (minLength = 1, maxLength = 8))	Yes	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
DeviceIDList	Comma separated list of Device IDs. Containing a minimum of 1 and a maximum of 50000 Device IDs, each as defined by sr:EUI (see Annex section 17)	Restriction of xs:string (min length = 23 max length = 1199999 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})*([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})")	Yes ¹	None	N/A	Non-Sensitive

Table 23 Update PPMID Firmware Service Request Data Items

¹ List of Device IDs. Minimum 1 and maximum 50000

11.4.1.3 Applicable Modes of Operation

The Modes of Operation applicable to this Service Request are (see Main Document of this documentation set section 2.3 for Modes of Operation definitions):

Service	Transform	On Demand	DCC Only	Future Dated	DSP Scheduled
SMETS2 or later	No	No	Yes ¹	No	No

Table 24 Update PPMID Firmware Modes of Operation

¹ See Main Document of this documentation set section 2.3.10 for details on Firmware Distribution Mode of Operation

11.4.1.4 Applicable Command Variant Values

The Command Variant values applicable to this Service Request are (see Main Document of this documentation set section 3 for Command Variant definitions):

[illegible]

Table 25 Update PPMID Firmware Command Variant Values

11.4.1.5 Validation

This Service Request specific validation is as follows (see Main Document of this documentation set section 7 for generic access control checks):

Validation Check	Process	Response Code
Does the Firmware version ID match an entry on the Central Products List?	Check that the Firmware Version aligns with an entry on the Central Products List, i.e. it is an approved Firmware Version Id	E110401

Validation Check	Process	Response Code
Are all the Devices in the list valid? ³	Check that each Device ID in the list exists and the DCC Service User, in the User Role defined in the Service Request, is a Responsible Supplier for all the Devices in the list	W110401 ²
Are all Devices in the list in a Status of 'Commissioned' or 'Suspended'? ¹	Check that each Device ID in the list corresponds to a PPMID in a status of 'Commissioned' or 'Suspended'	W110401 ²
Is the Firmware Version applicable to each 'Commissioned' Device in the list?	Check that the Firmware Version is applicable to each 'Commissioned' Device ID in the list	W110401 ²
Is there another firmware upgrade request already in progress for the Device in the list?	Check that the Device does not have another active firmware upgrade request in progress.	W110401 ²
Does the CHF associated with the target Device have a Firmware Version that is GBCS v4.1 or later?	Check that the Firmware Version of the CHF associated with the Target Device is GBCS v4.1 or later.	W110401 ²
Check that the firmware status value as per CPL is active?	Check the status of the firmware image against the CPL.	E110402
Check that the Firmware Hash of the Manufacturer Image part of the firmware image contained within the Service Request is the same as the Firmware Hash for that firmware image contained within the CPL	DCC Data Systems to compute the hash of the Manufacturer Image part of the firmware image and check this against the hash held for this version of firmware from the stored Central Products List (CPL)	E110403
Is the FirmwareImage well formed?	Check that the FirmwareImage contains both an OTA Header and a Firmware Image concatenated together, conforms to GBCS requirements , and is within the size limit i.e. 1024000. Note that 1024000 is the base 64 equivalent of approx. 750kb.	E110405

Table 26 Update PPMID Firmware Service Request Validation

¹ This check supersedes the generic Authorisation Check associated to Response Code E5. See Main Document of this documentation set section 7.4

² The same Response Code is returned to indicate the Response contains a warning

³ This check supersedes the generic Authorisation Check associated to Response Code E4. See Main Document of this documentation set section 7.4

11.4.1.6 Sample Request

Sample requests are given in Annex Introduction Appendix 2. The specific information for this Service Request (Body) is as follows:

```
<UpdatePPMIDFirmware>
  <FirmwareImage>ZGVmYXVsdA==</FirmwareImage>
  <FirmwareVersion>1100EEFF</FirmwareVersion>
  <DeviceIDList>11-00-AA-BB-CC-DD-EE-FF,22-00-AA-BB-CC-DD-EE-FF</DeviceIDList>
</UpdatePPMIDFirmware>
```

Figure 14 Sample Update PPMID Firmware Service Request (Body) Format

11.4.2 Responses

The response messages for an “Update PPMID Firmware” Request follow the generic format for all “DCC Only” Service Responses. The generic responses applicable to this request are;

- Acknowledgement.
- Service Response (from DCC). Applicable if response includes a warning

See Main Document of this documentation set section 2.3.10 for details on the Firmware Distribution responses from the Devices.

11.4.2.1 Service Response (from DCC)

Applicable to cases where authorisation / validation failed for one or more of the Device IDs in the list to inform the DCC Service User of the Device IDs not included in the DCC Data Systems Request to the CSPs.

11.4.2.1.1 Format

This Service Request synchronous response is defined in the XSD DSPUpdatePPMIDFirmwareWarning XML element, which contains the list(s) of Device IDs that failed DCC Authorisation / Validation.

Note that when the image has been received by the target PPMID it shall activate the firmware and send an Alert to notify the successful activation.

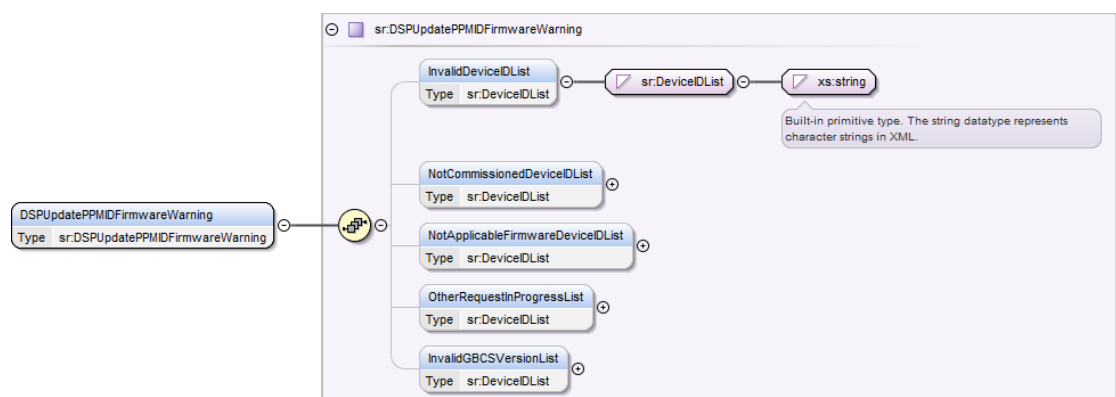


Figure 15 Update PPMID Firmware Service Response (from DCC) – Update PPMID Firmware Warning Structure

11.4.2.1.2 Specific Data Items

A DSPUpdateFirmwareWarning element is returned when ResponseCode is W110401.

Data Item	Description / Valid Set	Type	Mandatory ¹	Default	Units	Sensitivity
InvalidDeviceIDList	Comma separated list of Device IDs for which the DCC Service User ID is not a Responsible Supplier or the Device IDs don't exist. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){1,3}"))	No ¹	None	N/A	Non-Sensitive
NotCommissionedDeviceIDList	Comma separated list of Device IDs which aren't in a status of "Commissioned" or "Suspended" or the Device is not a SMETS2 PPMID Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){1,3}"))	No ¹	None	N/A	Non-Sensitive
NotApplicableFirmwareDeviceIDList	Comma separated list of Device IDs for which the Firmware is not applicable. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}){1,3}"))	No ¹	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory ¹	Default	Units	Sensitivity
OtherRequestInProgressList	Comma separated list of Device IDs for which another Firmware Update request is in progress. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17)	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})"*)	No ¹	None	N/A	Non-Sensitive
InvalidGBCSVersionList	Comma separated list of Device IDs for which the associated CHF has a GBCS version prior to v4.1. Containing a minimum of 1 Device ID, each as defined by sr:EUI (see Annex section 17).	sr:DeviceIDList (Restriction of xs:string (min length = 23 pattern = "([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})"*)	No ¹	None	N/A	Non-Sensitive

Table 27 Update PPMID Firmware Service Response (from DCC) – Update PPMID Firmware Warning Data Items

¹ The DSPUpdateFirmwareWarning will contain at least one of the 5 Lists and it could contain all of them

11.4.2.1.3 Sample Responses

Sample responses are given in Annex Introduction Appendix 1. The specific information for this Service Request Response is as follows:

```
<ResponseMessage>
  <ServiceReference>11.4</ServiceReference>
  <ServiceReferenceVariant>11.4</ServiceReferenceVariant>
  <DSPUpdatePPMIDFirmwareWarning>
    <NotCommissionedDeviceIDList>22-00-AA-BB-CC-DD-EE-FF</NotCommissionedDeviceIDList>
    <InvalidGBCSVersionList>22-00-AA-BB-CC-DD-EE-AA</InvalidGBCSVersionList>
  </DSPUpdatePPMIDFirmwareWarning>
</ResponseMessage>
```

Figure 16 Sample Update PPMID Firmware Service Response (from DCC) – Update PPMID Firmware Warning Format

11.4.2.2 Unsuccessful Response

The Response Codes specific to this Service Request are:

Response Code	Response Code Name	Response Code Type	Description
E110401	Failed Validation – Firmware Version not approved	Error	The Firmware Version is not approved, i.e. it doesn't align with an entry on the Central Products List
W110401	Failed Authorisation – Invalid User / Device Registration Status and / or Firmware Version not applicable to Device	Warning	<p>The Update PPMID Firmware Warning contains between one and five lists of Device IDs for which the validation failed:</p> <ul style="list-style-type: none"> InvalidDeviceIDList. The Device ID doesn't exist or the DCC Service User is not a Responsible Supplier of the Device. NotCommissionedDeviceIDList. The Device's status is not 'Commissioned' or 'Suspended' or the Device is not a SMETS2 PPMID NotApplicableFirmwareDeviceIDList. The Firmware Version is not applicable to the Device OtherRequestsInProgressList. The Device already has another Firmware update request in progress. InvalidCHFGBCSVersionList: The CHF associated with the Target Device has a GBCS Version prior to v4.1 (and so firmware updates are not supported).
E110402	Failed Validation – Firmware not active	Error	The firmware is not marked as active in the Central Products List and Smart Meter Inventory.
E110403	Failed Validation – Hash error	Error	The calculated hash value for the Manufacturer Image part of the firmware Image provided by the User within the Service Request differs from that held in the CPL for the specified FirmwareVersion.
E110405	Failed Validation – Firmware image not correctly formed	Error	The firmware image is not constructed as per the GBCS definition, e.g. the FirmwareImage does not contain both an OTA Header and a Firmware Image concatenated together, or the size is too large.

Table 28 Failed Update PPMID Firmware Service Request Response Codes