This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECMP0007 'Firmware updates to IHDs and PPMIDs'

Annex B

Legal text – version 1.0

About this document

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

SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2'

These changes have been redlined against Schedule 10 version 1.3.

Add Section 7.4.7 as follows:

7.4.7.5 Firmware

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

Add Sections 7.5.2.5 and 7.5.2.6 as follows:

7.5.2.5 Activate Firmware

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

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

7.5.2.6 Receive Firmware

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

Add Section 7.6.4 as follows:

7.6.4 Operational data

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

7.6.4.1 Firmware Version

The active version of Firmware of the PPMID.

Amend Section 8.4.4.1 as follows:

8.4.4 Security

8.4.4.1 General

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

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

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

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

Add Section 8.4.4.5 as follows:

8.4.4.5 Firmware

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

Add Sections 8.5.1.7 and 8.5.1.8 as follows:

8.5.1.7 Activate Firmware

A Command to activate Firmware.

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

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

8.5.1.8 Receive Firmware

A Command to receive Firmware.

In executing the Command the HCALCS shall be capable of:

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

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

Add Section 8.6.3 as follows:

8.6.3 Operational data

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

8.6.3.1 Firmware Version

The active version of Firmware of the HCALCS.

These changes have been redlined against Schedule 10 version 1.3.

Amend Section 4.4.4 as follows:

Buffering

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

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

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

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

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

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

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

Appendix E ‘DCC User Interface Services Schedule’

These changes have been redlined against Appendix E version 3.0.

Amend Service Reference 11.1 ‘Update Firmware’ as follows:

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

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

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

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

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

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

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

Appendix R 'Common Test Scenarios Document'

These changes have been redlined against Appendix R version 2.0.

Amend Table 8.1.5 as follows:

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

Update the total values for Table 8.1.5 as follows:

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

Amend Table 8.1.6 as follows:

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

Update the total values for Table 8.1.6 as follows:

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

Appendix AB 'Service Request Processing Document'

These changes have been redlined against Appendix AB version 3.0.

Amend Section 2 as follows:

2 Obligations of Users: Suspended Devices and Firmware

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

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

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

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

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

(a) the User has received the following information:

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

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

(iii) the Hash of the replacement Manufacturer Image;

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

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

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

Amend Section 6 as follows:

6 Obligations of the DCC: Processing Service Requests

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

(a) Verify the Service Request;

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

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

(d) Check Cryptographic Protection for the Service Request;

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

the Service Request;

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

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

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

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

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

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

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

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

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

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

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

Housekeeping amendment to Section 12.4 as follows:

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

Amend Section 18 as follows:

18 Obligations of the DCC: Non-Device Service Requests

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

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

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

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

(A) 'Update Inventory';

(B) 'Read Inventory';

(C) 'Request WAN Matrix';

(D) 'Device Pre-notification';

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

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

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

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

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

(A) 'Read Inventory';

(B) 'Request WAN Matrix';

(C) 'Device Pre-notification';

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix AF 'Message Mapping Catalogue'

These changes have been redlined against Appendix AF version 3.1.

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

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

4.1.3.3 Status Response Codes

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

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

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

Table 8 : ASN.1 Response Codes

Amend Section 4.2 as follows:

Device Alerts

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

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

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

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

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

Table 9 : Data Items within the DeviceAlertContent element

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

Amend Sections 5.106 and 5.107 as follows:

5.106 Read Firmware Version

5.106.1 Service Description

Service Request Name	ReadFirmwareVersion
Service Reference	11.2
Service Reference Variant	11.2

5.106.2 MMC Output Format

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

5.106.2.1 Specific Header Data Items

GBCS v1.0:

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

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

GBCS v4.x[1]:

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

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

5.106.2.2 Specific Body Data Items

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

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

5.107 Activate Firmware

5.107.1 Service Description

Service Request Name	ActivateFirmware
Service Reference	11.3
Service Reference Variant	11.3

5.107.2 MMC Output Format

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

5.107.2.1 Specific Header Data Items

GBCS v1.0:

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

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

Timestamp	xs:dateTime

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

GBCS v4.x[2]:

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

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

5.107.2.2 Specific Body Data Items

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

Table 245 : Activate Firmware MMC Output Format Body data items

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