

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

MP205 ‘Updating terminology to align with the NCSC’

Legal text – version 0.2

About this document

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

Section A 'DEFINITIONS AND INTERPRETATION'

These changes have been redlined against Section A version 24.0.

Amend Section A 1.1 as follows:

A DEFINITIONS AND INTERPRETATION

A1. DEFINITIONS

A1.1 In this Code, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

SMI Status	means the status indicator of each Device recorded within the Smart Metering Inventory, which indicator may (as a minimum) be set to any one of the following: (a) 'pending', indicating that the Device has not yet been Commissioned; (b) 'installed not commissioned', indicating that the Device is ready to be Commissioned, but has not yet been Commissioned; (c) 'commissioned', indicating that the Device has been Commissioned; (d) 'decommissioned', indicating that the Device has been Decommissioned; (e) 'suspended', indicating that the Device has been Suspended; (f) 'white<u>allow</u>listed', indicating that a Device has been added to the Device Log of a Communications Hub Function but that communications between the Device and the Communications Hub Function may not yet have been established; (g) 'recovery', indicating that the processing of communications destined for the Device has been disabled (other than for communications originated by the DCC) in accordance with the SMKI Recovery Procedure; or (h) 'recovered', indicating that the Data comprising the Device Security Credentials have successfully been updated using Data from one or more OCA Certificates and/or Organisation Certificates for which DCC is the Subscriber as further described in the SMKI Recovery Procedure.
-------------------	--

Section H ‘DCC SERVICES’

These changes have been redlined against Section H version 14.0.

Amend Section H 3 as follows:

H3 DCC USER INTERFACE

Eligibility for Services Over the DCC User Interface

H3.9 Subject to Sections H3.10 and H3.10A, a User’s eligibility for a Service in respect of a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System) is also dependent upon the status of that Smart Metering System (or such a Device), such that:

- a) the Responsible Supplier may send Service Requests in respect of Devices that have an SMI Status of ‘pending’, ‘~~white~~allowlisted’, ‘installed not commissioned’, ‘commissioned’, or ‘suspended’;
- b) Users that are not the Responsible Supplier may only send Service Requests in respect of Devices that have an SMI Status of ‘installed not commissioned’ or ‘commissioned’; and
- c) Communication Services are not available in respect of a Smart Metering System until it has been Enrolled.

Schedule 8 ‘Smart Metering Implementation Programme

Great Britain Companion Specification (GBCS)’

These changes have been redlined against Schedule 8 version 4.1.

Amend Schedule 8 13 as follows:

13 Managing Security Credentials on Devices

13.7 Pair-wise Authorisation of Devices

13.7.1 Introduction to pair-wise Authorisation of Devices – informative

13.7.1.1 *The role of pair-wise Authorisation – informative*

This Section 0 includes the Use Cases related to the Authorisation (and the removal of Authorisation) for pair-wise, secure application layer interaction between two Devices on the same SMHAN. It also covers the related Use Cases for backing up and restoring the GPF Device Log.

The process of authorising two Devices to communicate is referred to as ‘Joining’³⁸. Removal of such authorisation is referred to as ‘Un-joining’. Correspondingly, Remote Party Commands are specified in this Section 0 for instructing Devices that they are to ‘Join’ or ‘Unjoin’.

In line with the SMETS and CHTS Device Log requirements, two Devices on a HAN must only be capable of interacting at the application layer if they are currently Joined. They must not be capable of interacting if (1) they have never been Joined or (2) they have been Unjoined.

The application layer interactions between Devices on the same SMHAN must conform to the Device Based Access Controls (DBAC) as defined in Section **Error! Reference source not found.**. For example, an ESME must not be capable of processing an ‘Enable Supply’ Command from an IHD or an HCALCS.

It is a precondition of Joining that both Devices have been ‘~~WhiteAllow~~-listed’ on to the HAN (as per Use Case ‘CCS01 Add Device to CHF Device log’) so that they are able to communicate over the HAN at the network layer (and so have network access). The GPF may be configured to be in the CHF’s Device Log at manufacture. A Device on a ~~whiteallow~~-list can be removed from the ~~whiteallow~~-list. It must then be unable to communicate over the HAN, and so unable to interact at the application layer with any Devices to which it was ‘Joined’.

In SMETS terminology:

- the CHF’s Device Log holds the list of currently ~~whiteallow~~-listed Devices on the SMHAN; and
- the Device Log on an ESME, SAPC, GSME, GPF, HCALCS or PPMID Device holds the Entity Identifiers, Device Types and related Security Credentials of other Devices on the HAN to which the Device is currently Joined (and so Authorised to interact with at an application layer).

The process of ~~whiteallow~~-listing a Device, and its subsequently obtaining network access, establishes a shared secret key between the Device and the Communications Hub. The Gas Proxy Function, which is

³⁸ This is unrelated to the ZSE meaning of ‘joining’

part of the Communications Hub, uses this shared secret key, combined with a Device being entered in to its Device Log, for application layer authorisation.

IHDs and other Type 2 Devices are not required to have a Device Log (as defined in SMETS). They are required to store security and related details of the Devices to which they are Joined as required by ZSE however (otherwise they would be cryptographically unable to understand the information being sent to them by the Joined Devices).

IHDs and other Type 2 Devices can only read application layer information from Devices to which they are Joined (either by requesting the information from the Device or by receiving information published by the Device). When a PPMID is joined to a GPF, the PPMID can only read information from the GPF to which it is Joined.

When other types of Device are Joined (e.g. HICALCS, PPMID), they can also exchange Commands and Responses at the application layer. For example, an ESME that is Joined to an HICALCS can send a Command to the HICALCS to turn its switch on and the HICALCS can send a Response saying whether it has done that. A PPMID can send an 'enable supply' Command to an ESME etc.

Appendix R 'Common Test Scenarios Document'

These changes have been redlined against Appendix R version 4.0.

Amend Appendix R 8 as follows:

8. Annex C: Test Scenarios

8.1.2. SMETS2+ Install and Commission

ID	IC01*
Title:	Install & Commission the following devices, when the Relevant Party will be supplying Gas: • Communication Hub specified for Region • Gas Meter
Prerequisite:	• Relevant Party holds a Gas Supply Licence • Connection to DCC Test Laboratory • Appropriate data • Available Meter and Communication Hubs • SM WAN Available • Appropriate Security Keys have been installed in the available metering equipment • Required security credentials are present on the Communications Hub

Note: the scope of this test is intentionally limited to only those activities where there is a prescribed order for the submission Service Requests and where failure to follow this order will lead to a failed installation.

Steps	Description	Objective	Actions	Acceptance Criteria
1	Pre-Installation	Notify DCC of Device ID and device details Ascertain the security credentials are installed on the devices	The following Service Requests have been designed to support Pre-Installation: DUIS SR 12.2 – Device Pre-notification * (n) devices	The DCC has received notification of the Device ID Acknowledgement received for relevant Service Request sent
2	WhiteAllow List Device	Identify the Communication Hub to Meter device relationship by: Add the HAN device to HAN device log, by including the MAC addresses and the install codes	Complete the following Service Request to support whiteallow listing of device: DUIS SR 8.11- Update HAN Device Log * (n) devices	Service Responses received for all Service Requests sent Service User will receive the following Alert code when the device has been added to the whiteallow list: DCC Alert N24
3	Commission	Send response to commission device service request to Service User Update inventory status Configure the Meter: Set Time	Complete the following Service Request to support device commission: DUIS SR 8.1.1 – Commission Device * (n) devices	Acknowledgement received for all Service Requests sent
4	Commission Gas Proxy	To hand over Gas Proxy Function from DSP to the Relevant Party, complete the following:	Complete the following Service Request to support Commission Gas Proxy Function:	Relevant Party receives an Service Response to confirm the credentials have been changed from the DSP to Relevant Party

		Send Service Request to change credentials to Relevant Party's credentials Ensure Relevant Party can update other credentials as required	DUIS SR 6.21 – Request Handover of DCC Controlled Device * (n) devices	
5	Join Device	Join Gas meter to GPF	The following Service Requests have been designed to support joining HAN devices: DUIS SR 8.7.2 – Join Service (Non-Critical) Note: The following DUIS SRs can be sent during this step, should they not have been sent during steps 1 to 3: DUIS SR 12.2 – Device Pre-notification * (n) devices DUIS SR 8.11- Update HAN Device Log * (n) devices	Relevant Party receives acknowledgement to confirm the HAN devices are joined Acknowledgement received for all Service Requests sent
6	Set MPxN on GSME for display purposes	Set MPxN on GSME for display purposes	Complete the following Service Request to support setting the MPxN on the GSME for display purposes DUIS SR 6.20.1 – Set Device Configuration (Import MPxN)	Relevant party receives a service response to confirm successful execution of the Service Request.

ID	IC02*
Title:	Install & Commission the following devices, when the Relevant Party will be supplying Electricity: Communication Hub specified for Region Electricity Meter
Prerequisite:	Relevant Party holds an Electricity Supply Licence Connection to DCC Test Laboratory Appropriate data Available Meter and Communication Hubs SM WAN Available Appropriate Security Keys have been installed in the available metering equipment Required security credentials are present on the Communications Hub

Note: the scope of this test is intentionally limited to only those activities where there is a prescribed order for the submission Service Requests and where failure to follow this order will lead to a failed installation.

Steps	Description	Objective	Actions	Acceptance Criteria
1	Pre-Installation	Notify DCC of Device ID and device details	The following Service Requests and Self-Service Interface Use Cases have	The DCC has received notification of the Device ID

		Ascertain the security credentials are installed on the devices	been designed to support Pre-Installation: DUIS SR 12.2 – Device Pre-notification * (n) devices	Acknowledgement received for relevant Service Requests sent
2	WhiteAllow List Device	Identify the Communication Hub to Meter device relationship by: Add the HAN device to HAN device log, by including the MAC addresses and the install codes	Complete the following Service Request to support whiteallow listing of device: DUIS SR 8.11 - Update HAN Device Log * (n) devices	Service Responses received for all Service Requests sent Service User will receive the following Alert code when the device has been added to the whiteallow list: DCC Alert N24
3	Commission	Send response to commission device Service Request to Service User Update Smart Metering Inventory status Configure the Meter: Set Time	Complete the following Service Request to support device commission: DUIS SR 8.1.1 – Commission Device * (n) devices	Acknowledgement received for all Service Requests sent
4	Set MPxN on ESME for display purposes	Set MPxN on ESME for display purposes	Complete the following Service Request to support setting the MPxN on the ESME for display purposes DUIS SR 6.20.1 – Set Device Configuration (Import MPxN)	Relevant party receives a service response to confirm successful execution of the Service Request.

8.1.19. DCC Alert Tests – IS

Reference	Name	Test Scenario	Applicable User Role
N17	DSP Schedule Removal – Schedule removal due to Change of Supplier	Mandatory	Previously Registered IS
N24	Update HAN Device Log Result – Successful Communications Hub Function WhiteAllow list Update	Mandatory SMETS2+	IS
N27	Change of Supplier – Device Change of Supplier	Mandatory	Previously Registered IS
N49, N50, N51, N52	Firmware Version Mismatch	Optional	IS
N53	Command Not Delivered To ESME	Mandatory SMETS2+	IS
N54	Dual Band CH Sub GHz Alert	Mandatory SMETS2+	IS
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	IS
N56	SMETS1 Service Provider Provision of prepayment top-up UTRN	Mandatory SMETS1	IS

8.1.20. DCC Alert Tests – GS

Reference	Name	Test Scenario	Applicable User Role
-----------	------	---------------	----------------------

N17	DSP Schedule Removal – Schedule removal due to Change of Supplier	Mandatory	Previously Registered GS
N24	Update HAN Device Log Result – Successful Communications Hub Function White Allowlist Update	Mandatory SMETS2+	GS
N27	Change of Supplier – Device Change of Supplier	Mandatory SMETS2+	Previously Registered GS
N49, N50, N51, N52	Firmware Version Mismatch	Optional SMETS2+	GS
N54	Dual Band CH Sub GHz Alert	Mandatory SMETS2+	GS
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	GS
N56	SMETS1 Service Provider Provision of prepayment top-up UTRN	Mandatory SMETS1	GS
N57	SMETS1 CH Firmware notification	Mandatory SMETS1	GS

8.1.25. DCC Alert Tests - OU

Reference	Name	Test Scenario	Applicable User Role
N24	Update HAN Device Log Result - Successful Communications Hub Function White Allowlist Update	Mandatory SMETS2+	OU
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	OU

Appendix AB 'Service Request Processing Document'

These changes have been redlined against Appendix AB version 6.0.

Amend Appendix AB 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) 'whiteallowlisted'; 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 or a Standalone Auxiliary Proportional Controller 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);
- 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; and
- n) in the case of SMETS1 'Activate Firmware' Service Requests, where the target Device is a SMETS1 CHF or a SMETS1 PPMID, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPANs in the Smart Metering Inventory) that the User sending the Service Request is the Import Supplier for the ESME on the same home area network.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 5.0.

Amend Appendix AC 4 and 8 as follows:

4. Commissioning

Adding Devices to Communication Hub Functions' Device Logs

- 4.3 Following the Successful Execution of an 'Update HAN Device Log' Service Request requesting the addition of a Device to the Device Log of a Communications Hub Function, the DCC shall:
- (a) update the Smart Metering Inventory to Associate the Device with the applicable Communications Hub Function;
 - (b) in the case of Smart Meters and Standalone Auxiliary Proportional Controllers only, record the MPAN(s) or MPRN (as applicable) provided within the Service Request against that Device and notify the Electricity Distributor or Gas Transporter (as applicable) of the MPAN(s) and/or MPRN and of the Device's Device ID and Device Type; and
 - (c) other than in the case of a Type 2 Device, set the SMI Status of the Device to '~~white~~allowlisted'.

8. Reactivating Decommissioned or Suspended Devices

- 8.1 Where the Responsible Supplier wishes to change the SMI Status of any Device (other than a Type 2 Device) from 'decommissioned' or '~~white~~allowlisted' to 'pending', then the Responsible Supplier shall send the DCC a Service Request to that effect. Provided the Device in question is of (or is part of) a Device Model that is identified in the Central Products List, the DCC shall change the SMI Status to 'pending'.

Appendix AD ‘DCC User Interface Specification’

These changes have been redlined against Appendix AD version 5.0.

Amend Appendix AD 3 as follows:

3 MESSAGES SENT OVER THE INTERFACE

3.2 Access Control

3.2.4 Authorisation

The DCC shall verify that the User has permission to send the Service Request or Pre-Command as per the following steps and where authorisation checks are failed the following Response Code shall be added by the DCC to the Service Response that is sent to the sending User;

Authorisation Check	Process	Response Code
Verify that the Service Request or Signed Pre-Command is applicable to the Device status	This is a check to confirm that the target Device has a status within the Smart Metering Inventory that enables the User to send it the particular Service Request or Signed Pre-Command This check is not applicable to Service Requests 8.2 (Read Inventory) and 12.1 (Request WAN Matrix) or to Critical Service Requests or Signed Pre-Commands. With the exception that it is applied for Signed Pre-Commands when the Device Status is ‘Recovery’. Devices can only be communicated with in response to a Request if they are in a status of ‘Commissioned’, ‘InstalledNotCommissioned’, ‘WhiteAllowlisted’, ‘Pending’ or ‘Recovered’ in the Smart Metering Inventory. The DCC shall, where the Device has a Smart Metering Inventory (SMI) Status of ‘Suspended’ prevent any Non-Critical Service Requests from being processed with the exception of, Service Requests 11.1 (Update Firmware), 11.2 (Read Firmware Version) and 6.23 (Update Security Credentials (CoS)). The DCC shall, where a Device has a Smart Metering Inventory (SMI) Status of ‘Recovery’ prevent any Service Requests relating to that Device from being processed with the exception of Non-Device Service Requests (subject to their specific validation).Note that where a Device has an SMI Status of ‘Recovered’ the Device’s SMI Status immediately prior to it having the SMI Status of ‘Recovery’ shall be used in validation.	E5

Authorisation Check	Process	Response Code
Verify that the Service Request or Signed Pre-Command is available for Local Command Services	This is a check to confirm that a Service Request or Signed Pre-Command is available to Users for local delivery to a Device using Local Command Services including additional reference to the requesting User Role and SMI Status combination. A Service Request or Signed Pre-Command is not available to Users for local delivery using Local Command Services where the Service Request or Signed Pre-Command is one of the following; - A Service Reference Variant of 8.1.1 – Commission Device - A Future Dated Service as defined by clause Error! Reference source not found. In addition, a Service Request or Signed Pre-Command can only be delivered locally in the following combinations of requesting User Role and SMI Status of the target Device: - Where the User Role of the sender is either IS, ES or GS, the target Device within the request must have an SMI Status of either “Pending”, “WhiteAllowlisted”, “InstalledNotCommissioned” or “Commissioned”. - Where the User Role of the sender is either ED, GT, RSA or OU, the target Device within the request must have an SMI Status of either “InstalledNotCommissioned” or “Commissioned”. Note that where a Device has an SMI Status of ‘Recovered’ the Device’s SMI Status immediately prior to it having the SMI Status of ‘Recovery’ shall be used in validation.	E17

Table 1 : Authorisation checks

3.6 Device Alerts and DCC Alerts

3.6.3 DCC Alerts - DCCAlertMessage Format

3.6.3.3 DCC Alert Codes

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	Device Applicability
N21	Unknown Firmware Version	Unknown Firmware Version	CSP or S1SP unable to process request, because it doesn't recognise the Firmware Version	Update Firmware request sender	All
N22	Failure to deliver Update Firmware Command to CSP	Failure to deliver Update Firmware Command to CSP	Failure to receive an acknowledgement notification from a CSP or S1SP via the SM WAN for an Update Firmware Command	Update Firmware request sender	All

Managed by

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	Device Applicability
N24	Successful Communications Hub Function White Allowlist Update	Communications Hub Function White Allowlist Update	The DCC has received positive confirmation that the requested addition to the Communications Hub Function's white allowlist resulted in establishing communications with the Device	Update HAN Device Log request sender	All
N25	Potentially Unsuccessful Communications Hub Function White Allowlist Update	Communications Hub Function White Allowlist Update	The DCC has not received positive confirmation that the requested addition to the Communications Hub Function's white allowlist resulted in establishing communications with the Device	Update HAN Device Log request sender	All
N36	Cancellation of Future Dated Response Pattern (DSP) requests because of CHF Withdrawal	Cancellation of all Future Dated Response Pattern (DSP) Services not yet submitted to the CHF and Devices in its White Allowlist	Upon successful completion of Service Request 8.4 Update Inventory for a CHF Withdrawal	All applicable Future Dated Response Pattern (DSP) Request senders	SMETS 2+
N37	Schedule removal because of CHF Withdrawal	"DCC Scheduled" schedule removal for ESME, GSME and GPF in the White Allowlist	Upon successful completion of Service Request 8.4 Update Inventory for a CHF Withdrawal	All applicable Schedule "owners"	SMETS 2+
N52	GSME Firmware Version Mismatch	GSME's Firmware Version returned by the GPF is different from that in the Smart Metering Inventory	Upon successful completion of Service Request 11.2 Read Firmware Version where the target Device is GPF and the GSME Firmware Version returned by the GPF is different from that in the SMI	GS	All

Table 2 : DCC Alert Codes

3.8 Service Request Definitions

3.8.104 Read Inventory

3.8.104.4 Specific Data Items in the Response

This Service Response is defined in the XSD ResponseMessage DSPInventory XML element, which contains the DSP Inventory details applicable to a single premises or Device.

The DCC shall return the following data items which are specific to this Service Response:

Data Item	Description / Values	Type	Mandatory	Default	Units
Per Device (complex type sr:Device) found at that Smart Metering System:					
DeviceStatus	An indicator giving the status of the device Valid set: - Pending WhiteAllowlisted - InstalledNotCommissioned - Commissioned - Decommissioned - Withdrawn - Suspended - Recovery - Recovered Device Status is not applicable to Type 2 Devices, i.e. IHD and CAD	sr:DeviceStatus (Restriction of xs:string (Enumeration))	Device Type = Type 2(IHD, CAD): N/A Otherwise: Yes	None	N/A

Table 3 : Device (sr:Device) data items

3.8.106 Update Inventory

3.8.106.3 Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for Device Existence validation.

Response Code	Response Code Description
E080414	The Device Status does not allow the MPxN to be updated. The Device Status must be one of “ WhiteAllow listed”, “Installed Not Commissioned” or “Commissioned” if the MPxN update is to succeed.

3.8.106.4 Additional DCC System Processing

When a User sends an Update Inventory Service Request to the DCC in respect of a Communications Hub, the DeviceId specified within the Service Request shall be that of the Communications Hub Function and not the Gas Proxy Function.

Note that where a Device has an SMI Status of ‘Recovered’ the Device’s SMI Status immediately prior to it having the SMI Status of ‘Recovery’ shall be used in validation.

This Service Request can be used by Users to perform the following four functions;

1. Update Device details within the Smart Metering Inventory provided via Pre-Notification
 - a. This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request.
 - b. Only the User who originally added the Device to the Smart Metering Inventory may update these device details whilst the Device has a status of 'Pending'.
 - c. For Devices that have SMI Status values, only Devices in a status of 'Pending' can be updated.
 - d. Type 2 (IHD and CAD) Devices can be updated at any time.
 - e. Update most of the Device details that were initially provided to the DCC via Service Request 12.2 – Device Pre-notification (see clause **Error! Reference source not found.**)
 - f. It isn't possible to update a Device ID (including the GPF Device ID associated to a CHF). If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause **Error! Reference source not found.**).
 - g. It isn't possible to update a Device Type. If it has been entered in error it has to be deleted via this Service Request and re-added via Service Request 12.2 – Device Pre-notification (see clause **Error! Reference source not found.**).
 - h. Any updates to the details shared between a CHF and a GPF will be applied to both. The Device ID in the Service Request has to be that of the CHF.
2. Delete Device details from the Smart Metering Inventory provided via Pre-Notification which have not been installed.
 - a. This functionality of the Service Request is available to all the Eligible User Roles associated with this Service Request.
 - b. Only the User who originally added the Device to the Smart Metering Inventory may delete these device details.
 - c. For Devices that have SMI Status values, only Devices in a status of 'Pending' can be deleted.
 - d. Type 2 (IHD and CAD) Devices can be deleted at any time.
 - e. Deleting a CHF will also delete its associated GPF.

3. Update SMI Status within the Smart Metering Inventory

- a. This functionality of the Service Request is ONLY available to the Eligible User Roles of Import Supplier and Gas Supplier who are the Responsible Supplier to the Device being updated.
- b. Different options exist for which device SMI Status values can be updated by Users depending on Device type. Functionality allows,
 - i. Update the Device status for all Device Types, other than the CHF and the GPF and where the old and new status apply to the Device Type
 1. From 'Pending' to 'InstalledNotCommissioned'
 2. From '~~White~~Allowlisted' to 'Pending'
- c. Update the Device SMI Status for a CHF (and its associated GPF)
 - i. To support the Install & Leave process and / or Install & Commission after Decommissioning or Withdrawal:
 1. From 'Pending' to 'InstalledNotCommissioned' (GPF from 'Pending' to 'InstalledNotCommissioned')
 2. From 'InstalledNotCommissioned' to 'Commissioned' (GPF no status transition)
 3. From 'Pending' to 'Commissioned' (GPF from 'Pending' to 'InstalledNotCommissioned')
 - ii. From 'Commissioned' to 'Withdrawn' (GPF from 'Commissioned' to 'Withdrawn' or from 'Installed Not Commissioned' to 'Withdrawn'). This is the equivalent of Service Request 8.5 – Service Opt Out (see clause **Error! Reference source not found.**) for other Device Types. On successful completion of the Service Request, the DCC Systems will:
 1. automatically delete all active DSP Schedules on all Devices in the CHF ~~White~~Allowlist. For each deleted DSP Schedule a DCC Alert N37 will be sent to the User that owned it.
 2. automatically cancel all Future Dated (DSP) requests not yet sent to the Device for that CHF and all the Devices in its ~~White~~Allowlist. For each cancelled request a DCC Alert N36 will be sent to the sender of the Future Dated request.

- 4) Update MPxN associated with the Device (or add a new association) within the Smart Metering Inventory
- This functionality of the Service Request shall ONLY be available to either:
 - the Registered Supplier Party for the MPxN of the type specified in UpdateMPxN, as recorded in the Smart Metering Inventory against the DeviceID; or
 - where no such MPxN is recorded in the Smart Metering Inventory against the DeviceID, any Supplier Party
 - The new MPxN must be consistent with the type of Device, for example if the Secondary MPAN is updated then the device must be a twin element ESME.
 - ONLY a single MPxN association change be changed per Service Request call
 - If the MPxN is successfully updated in the Smart Metering Inventory, then a DCC Alert N16 is sent to the Meter's Network Operator.

3.8.114 Update HAN Device Log

3.8.114.2 Specific Data Items for this Request

UpdateHANDeviceLog Definition

Data Item	Description / Values	Type	Mandatory	Default	Units
DeviceID	Device ID of a Device to be added to or removed from the Communications Hub Function WhiteAllow list or removed from it. A User must send one Service Request per Device to add or remove from the Communications Hub Function (CHF) Device Log.	sr:EUI (See clause Error! Reference source not found.)	Yes	None	N/A
RequestType	Indicates whether the request is to add or remove the Device form the Communications Hub Function WhiteAllow list. Valid set: - Add - Remove	Restriction of xs:string (Enumeration)	Yes	None	N/A
AddDeviceToCHF WhiteAllow list	List of data items required to add the Device to the Communications Hub Function WhiteAllow list.	sr:AddDeviceToCHF WhiteAllow list	Device to be added to WhiteAllow list: Yes Device to be removed from	None	N/A

			WhiteAllowlist: N/A		
--	--	--	------------------------	--	--

Table 4 : UpdateHANDeviceLog (sr:UpdateHANDeviceLog) data items

AddDeviceToCHFWhiteAllowlist Definition

Data Item	Description / Values	Type	Mandatory	Default	Units
JoinTimePeriod	Defines the time period in seconds during which the Communications Hub Function will permit the device being added to join the HAN and communicate with the Communications Hub Function.	Restriction of xs:positiveInteger (minInclusive = 1, maxInclusive = 3600)	Yes	None	Seconds
InstallCode	Installation Credentials. Minimum length 6 (octets) to Maximum Length 16 (octets) equating to from 12 to 32 characters	Restriction of xs:hexBinary (minLength = 6, maxLength = 16)	Yes	None	N/A
ImportMPxN	The reference number identifying an electricity or a gas metering point.	sr:ImportMPxN (Restriction of xs:string (minLength = 1, maxLength = 13))	ESME, HCALCS and GSME: Yes Otherwise: N/A	None	N/A
SecondaryImportMPAN	The reference number identifying a Twin Element Import electricity secondary metering point.	sr:MPAN (Restriction of xs:string (minLength = 13, maxLength = 13))	No	None	N/A
ExportMPAN	The reference number identifying an Export electricity metering point.	sr:MPAN (Restriction of xs:string (minLength = 13, maxLength = 13))	No	None	N/A

Table 5 : AddDeviceToCHFWhiteAllowlist (sr:AddDeviceToCHFWhiteAllowlist) data items

3.8.114.3 Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for Execution Date Time validation.

For this Request, the general Authorisation Checks as defined below shall not be carried out where an IHD is being added to the Device Log by a User and the command is requested for Local Delivery only.

- a Response Code of E4 as defined in clause 3.2.4 “Verify that the User, in the User Role defined in the Service Request is a Eligible User for the Device”

Response Code	Response Code Description
E081101	The Device ID of a Device to be added to the CHF WhiteAllow list is already associated with another CHF WhiteAllow list
E081102	The Device ID of a Device to be removed is not included in the CHF WhiteAllow list
E081104	The Device Type of the Device to be added to the WhiteAllow list is invalid, e.g. if it is a Communications Hub Function or Gas Proxy Function
E081105	The status of the Device being added to the WhiteAllow list is not ‘Pending’ or ‘ WhiteAllow listed’
E081106	If the Request Type is: • ‘Add’. It doesn’t include the Add Device CHF WhiteAllowlist element • ‘Remove’. It does include the Add Device CHF WhiteAllowlist element
E081107	The Device ID of the Device to be added to or removed from the WhiteAllow list does not exist

3.8.114.4 Additional DCC System Processing

Upon receipt of a successful Response resulting from the UpdateHANDeviceLog Service Request to Add a Device, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following action.

- Update the Smart Metering Inventory and set the Device status of the DeviceId to ‘~~WhiteAllow~~listed’
- Where the DeviceID to be added to HANDeviceLog is an Electricity Smart Meter or a Gas Smart Meter, the association between the DeviceID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor(s) or Gas Transporter (as applicable)

The DCC Systems shall wait for a timeout period to receive the updated Device Log from the CHF following the successful execution of an UpdateHANDeviceLog Service Request to Add a Device. The timeout period that the DCC Systems shall wait for the Alert is defined as “JoinTimePeriod” as specified within the Service Request plus a configurable network transmission time to allow delivery of the Alert over the SM WAN.

- If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is received within the timeout period, then the DCC Systems shall notify the Responsible Supplier for the specified Device via a DCC Alert N24, and;
 - For ESME, GSME, HCALCS and PPMID the Device Status is set to ‘InstalledNotCommissioned’ in the Smart Metering Inventory

- b) If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is not received within the timeout period, then the DCC Systems informs the User via a DCC Alert N25.

When a User requests the Request Type “Add” variant of this Service Request 8.11, then an unsuccessful Command Response indicates that the CHF did not execute the Command, the details provided in the Service Request have NOT been successfully added to the CHF Device Log and no further actions are triggered by the DCC Systems.

When a User requests the Request Type “Remove” variant of this Service Request 8.11, then the Command Response indicates whether the specified Device provided in the Service Request was either successfully removed from the CHF Device Log or the removal was unsuccessful. Upon receipt of a successful Response resulting from the UpdateHANDeviceLog Service Request to Remove a Device, the DCC shall, where the Device Status is currently ‘WhiteAllowlisted’, set the Device status to ‘Pending’. No additional DCC Alerts are produced by the DCC Systems.

3.8.115 Restore HAN Device Log

3.8.115.3 Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for ‘Old CHF Device’ Existence validation.

Response Code	Response Code Description
E081202	The Old CHF ID doesn’t correspond to a Device of Type Communications Hub Function
E081204	The Device Status of the new Communications Hub Function is invalid
E081205	The User is not a Responsible Supplier to any of the MPxNs associated with Device(s) in the Old CHF ID <u>WhiteAllow</u> list

3.8.116 Restore Gas Proxy Function Device Log

3.8.116.3 Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for ‘Old GPF Device’ Existence validation.

Response Code	Response Code Description
E081221	The Old GPF ID doesn’t correspond to a Device of Type Gas Proxy Function
E081222	The Device Status of the new Gas Proxy Function is invalid
E081223	The User is not an Import Supplier to any of the MPxNs associated with Device(s) in the CHF ID <u>WhiteAllow</u> list associated to the BusinessTargetID GPF

3.8.117 Return Local Command Response

3.8.117.3 Specific Data Items for this Request

The following table lists the Service Requests Responses and Device Alerts needed by the DCC Systems from Users via the return Local Command Response Service Request if these are collected from execution of Local Commands on Devices. Note that a HHT will receive all Alerts / Responses from all HAN Devices whilst it is connected; these may or may not be related to the execution of Local Commands.

Alerts
Device Addition To / Removal From HAN White <u>Allow</u> list Alerts used by DCC to manage the CHF/GPF Device Log Backup process (GBCS Alert Codes: 0x8F12 – CHF Device Log Updated)
GPF Device Log Backup Alert (GBCS Alert Code: 0x8071)

DCC Alert Messages

Specific Data Items in the DCC Alert Message

Each Alert Code being reported as a DCC Alert shall conform to the DCC Alert format as defined in 0 3.6 **Device Alerts and DCC Alerts**

3.6.3 DCC Alerts - DCCAlertMessage Format. The DCC shall ensure that the Body of each DCC Alert (DCCAlert XML element) conforms to one of these fourteen DCC Alert formats as defined in the table below:

DCCAlert Definition

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
UpdateHANDeviceLogResult	The trigger event indicates if a Command to Update a Communications Hub White Allowlist Update. (addition ONLY) has succeeded or no Alert has been received by the DCC. .	sr:UpdateHANDeviceLogResult See Error! Reference source not found.	N24 and N25	None	N/A

Table 6 : DCCAlert (sr:DCCAlert) data items

Appendix AL 'SMETS1 Transition and Migration Approach Document'

These changes have been redlined against Appendix AL version 18.0.

Amend Appendix AL 1, 12, 13, 14, 15, 16, Appendix A, Appendix B and Appendix C as follows:

1. Defined Terms and Interpretations

Term	Meaning
CHF WhiteAllow list	In relation to a SMETS1 Installation, shall include the list of Device IDs, being IEEE media access control addresses, held on the SMETS1 CHF detailing the set of Devices which are currently authorised to communicate over the ZigBee network to which the CHF controls access. For clarity this list never includes Device IDs for a CHF or a GPF, and in the case of an ESME only includes the Device ID where that ESME communicates with the CHF using a ZigBee network. For clarity, the CHF WhiteAllowlist, for GroupIDs specified in Clauses 12, 13, 14, 15 and 16, includes, for each IEEE media access control address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

12 Requirements specific to GroupID = "AA"

S1SP / DCO Commissioning of SMETS1 Installation

12.9 The checks at Table 12.9 shall be the 'S1SP / DCO Commissioning of SMETS1 Installation' for this GroupID.

Only the following lines in the table needs amending

Step Number	Check and processing	Critical?	Supporting Data
12.9.1.X	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this GroupID, as specified in Appendix A of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF WhiteAllow list. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.
12.9.4	Where the CHF is of a Device Model which requires the ESME Device Identifier to be in the CHF WhiteAllow list, check that the ESME Device Identifier, included in the Migration Common File for this SMETS1 Installation, is included in the CHF WhiteAllow list retrieved at StepNumber 1.	Yes	

12.9.5	Where a GSME Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that GSME Device Identifier is included in the CHF WhiteAllowlist retrieved at StepNumber 12.9.1.	Yes	
12.9.6	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF WhiteAllowlist retrieved at StepNumber 12.9.1.	Yes	

CHF [WhiteAllowlist](#)

12.11 The CHF [WhiteAllowlist](#) shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

12.12 The CHF [WhiteAllowlist](#) shall never include Device IDs for a CHF or a GPF and shall always include the Device ID for an ESME.

13 Requirements specific to GroupID = “BA”

CHF [WhiteAllowlist](#)

13.13 The CHF [WhiteAllowlist](#) shall, for this GroupIDs, include, for each IEEE address, either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

13.14 The CHF [WhiteAllowlist](#) shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

14 Requirements specific to GroupID = “CA” or “CB”

CHF [WhiteAllowlist](#)

14.12 The CHF [WhiteAllowlist](#) shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

14.13 The CHF [WhiteAllowlist](#) shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

15 Requirements specific to GroupID = “EA” or “EB”

S1SP / DCO Commissioning of SMETS1 Installation

15.9 The checks at Table 15.9 shall be the ‘S1SP / DCO Commissioning of SMETS1 Installation’ for these GroupIDs.

Only the following lines in the table needs amending

Step Number	Check and processing	Critical?	Supporting Data
-------------	----------------------	-----------	-----------------

15.9.1.X	The checks and processing required for ‘Installing a SMETS1 Electricity Meter’ for this Group ID, as specified Appendix B of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF WhiteAllow list. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.
15.9.4	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF WhiteAllow list retrieved at StepNumber 15.9.1.	Yes	

Table 15.9

16 Requirements specific to GroupID = “DA”

S1SP / DCO Commissioning of SMETS1 Installation

16.9 The steps at Table 16.9 may be carried out by the DCC up to 7 days in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.

Only the following linee in the table needs amending

Step Number	Check and processing	Critical?	Supporting Data
16.9.1.x	The checks and processing required for ‘Installing a SMETS1 Electricity Meter’ for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF WhiteAllow list. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.4	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF WhiteAllow list retrieved at StepNumber 16.9.1.	Yes	

Table 16.9

CHF [WhiteAllow](#)list

16.12 The CHF [WhiteAllow](#)list shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

16.13 The CHF [WhiteAllow](#)list shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF.

Appendix A Device installation – For GroupIDs “AA”, “BA”, “CA” and “CB”

Installing a SMETS1 Electricity Meter

A2 The checks and processing at Table A2 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' for relevant GroupID and shall take place in the order specified in that Table.

Only the following line in the table needs amending

Error code on failure	S1SP checks and processing	DCO checks and processing	Supporting Data
ET05	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the CHFDetails: confirm the successful creation of an Application Association with the Device, read the CHF WhiteAllowlist, confirm the Device ID for ESME is included in CHF WhiteAllowlist where the GroupID = "AA", read the serial number of the Device, confirm the serial number of the Device is same as in SerialNumbers\CHF element for the SMETS1 Installation in Migration Group File close the Application Association securely store each key and its association with: its 'key type' the 'name of Application Association' the Device ID the serial number of the Device		1, 2, 3, 4, 5, 6 or 7 reflecting the sub step which failed

Table A2

Installing a SMETS1 GSME

A3 The processing at Table A3 shall be that required of the S1SP and DCO for 'Installing a SMETS1 GSME' for this GroupID.

Only the following line in the table needs amending

Error code on failure	S1SP checks and processing	DCO checks and processing	Supporting Data
GT01	Using the DeviceID for the CHF on which the GSME should have been whiteallowlisted: ve the AuthenticationKey and EncryptionKey for the Extended Data Collection Application Association those keys, confirm the successful creation of an Application Association with the Device, he CHF WhiteAllowlist m that the GSME's Device ID is on that CHF WhiteAllowlist and that the GSME has communicated in the last 72 hours, close the Application Association		1, 2, 3, 4, or 5 reflecting the sub step which failed

Table A3

Appendix B Device installation – For GroupIDs “EA” and “EB”

Installing a SMETS1 Electricity Meter

B2 The checks and processing at Table B2 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' and shall take place in the order specified in that Table.

Only the following line in the table needs amending

Error code on failure	S1SP checks and processing	Supporting Data
ET01	Using the DeviceCertificate in the CHFDetails\DeviceCertificate element which the ESME is associated with, use network connection with CHF confirming successful responses to messages from the successful creation of a TLS session with the CHF in question. The CHF WhiteAllow list, confirm the Device ID in the Migration Common File for the ESME is included in the CHF WhiteAllow list,	1, 2, 3, 4 reflecting the sub step which failed

Table B2

Installing a SMETS1 GSME

B3 The processing at Table B3 shall be that required of the S1SP for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table.

Only the following line in the table needs amending

Error code on failure	S1SP checks and processing	DCO checks and processing	Supporting Data
GT01	Using the DeviceCertificate in the CHFDetails\DeviceCertificate element which the GSME is associated with, use network connection with CHF confirming successful responses to messages from the successful creation of a TLS session with the CHF in question, The CHF WhiteAllow list, confirm the Device ID in the Migration Common File for the GSME is included in CHF WhiteAllow list,		1, 2, 3 or 4 reflecting the sub step which failed

Table B3

Appendix C Device installation – For GroupIDs “DA”

Installing a SMETS1 GSME

C2 The processing at Table C2 shall be that required of the DCC for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table.

Only the following line in the table needs amending

Error code on failure	DCC checks and processing	Supporting Data

GT01	Using the DeviceID for the CHF on which the GSME should have been whitelisted: the CHF WhiteAllow list and confirm that the GSME's Device ID is on that CHF WhiteAllow list and that the GSME has communicated in the last 24 hours.	1, 2, 3 or 4 reflecting the sub step which failed
------	---	--

Table C2

Appendix AM ‘SMETS1 Supporting Requirements’

These changes have been redlined against Appendix AM version 12.0.

Amend Section 13.1 as follows:

Configuration pre-requisites for operating a SMETS1 Device through the DCC

- 13.1 Some SMETS1 Devices may support features which are additional to those required by SMETS1 and which cannot be configured through the DCC. Table 5 lays out a number of such features. Where a Device supports, or is capable of supporting, one or more of the features in Table 5, the Responsible Supplier shall (unless to do so would result in a material delay to the Migration of the relevant SMETS1 Installation), ensure that before the relevant SMETS1 Installation is Migrated, any such features are configured according to the requirements of Table 5.

Only the following line in the table needs amending

Feature	Type of Device	Required configuration
' BlackDeny listing' of access to the HAN	SMETS1 CHF	The Device shall be configured so that only ' whiteallow listed' Devices recorded on the SMI as being associated with the SMETS1 CHF can have access to the HAN, and that access is not controlled via any ' blackdeny listing' mechanism.

Appendix AP 'S1SPKI Certificate Policy

Secure S1SP Certificate Policy for the Secure Cohort'

These changes have been redlined against Appendix AP version 1.0.

Amend Appendix AP 14 Annex E as follows:

14 Annex E: SS1SP PKI RAPP

14.3 SS1SP PKI Registration Authority Roles

- (A) The SS1SP PKI RA consists of the following roles:
 - (i) SS1SPCA Systems technical RA role; and
 - (ii) SS1SPCA Personnel requesting and approving Certificates for issuance.
- (B) The Subordinate SS1SPCA Device CA acts as a technical RA for Certificates requested by Secure SMETS1 Devices only. The SS1SPCA Systems have been authorised to act as technical RAs through a combination of access controls and IP ~~white~~allowlisting. Only valid Secure SMETS1 Devices may request a Certificate. Therefore, acting as an Authorised Subscriber for such SS1SP End Entity Certificates.
- (C) Authorised and approved SS1SPCA Personnel are responsible for requesting and issuing all other SS1SPCA End Entity Certificates using SS1SPA Systems. Thereby acting as an Authorised Subscriber.
- (D) Only SS1SPCA Personnel with Privileged User rights can request and approve Certificate requests through the SS1SPCA Systems. This is enforced through:
 - (i) Pre-authorised and pre-approved access to SS1SPCA Systems for such SS1SPCA Personnel;
 - (ii) Access control to the SS1SPCA Systems;
 - (iii) User account management (audit and logging);
 - (iv) Dedicated named accounts on the SS1SPCA System;
- (E) Prior to being granted access to SS1SPCA Systems, all such SS1SPCA Personnel with Privileged User rights will either have:
 - (i) identities checked in line with personnel security standard BS7858;
 - (ii) background clearance checks performed in accordance with security check (SC) cleared to an appropriate level (in accordance with the latest version of the HMG Cabinet Office Security Policy; and/or
 - (iii) Screening and background verifications equivalent to BS7858. The personnel and key personnel, based in India, engaged in providing support for Smart metering services and solutions shall comply at all times with a background verification equivalent to personnel security British Standard BS 7858:2012 (Security Screening of Individuals Employed in Security Environment - Code of Practice),