DCC User Gateway Interface Design Specification

Main Document

Author: DCC
Version: 5.2a
Date: June 2023

Contents

1 Introduction

1.1 Document Purpose

The purpose of the DCC User Gateway Interface Design Specification documentation is to define the DCC User Interface at a technical level to enable DCC Service Users to integrate their IT infrastructure with the DCC Data Systems. This M2M interface enables suitably authorised DCC Service Users to call Service Requests to interact with Devices and services within the DCC, and to receive responses to those requests as well as Device and DCC Alerts.

1.2 Document Scope

This document is DUGIDS version 5.2~~1~~ and describes the behaviour of the DCC User Interface when operating at version 5.2~~1~~.

The DCC Data Systems will continue to support the DCC User Interface at version 3.x, 4.0 and 5.x, and the behaviour at these versions is also described in this version of DUGIDS. In some places behaviour which applies equally to multiple releases within a major release is abbreviated, e.g. behaviour for 3.0 and 3.1 is indicated by "3.x". Versions 1.0 and 2.0 of the DCC User Interface are no longer supported by DCC (see section 9.5.4).

Where there are differences in behaviour between versions of DUIS then these are called out in the detailed descriptions of Service Requests.

The DCC User Gateway Interface Design Specification (DUGIDS) documentation consists of 4 separate document parts:

1. Main document – describing how the interface works. This document.

2. Annex to the main document (Annex) – describing the Service Request and Response definitions in detail.

3. DUIS XML Schema (DUIS XML Schema) – describing the main DUIS interface XML definition (instructions on how to view the DUIS XML Schema are included in Appendix 2).

4. MMC XML Schema – describing the MMC (Message Mapping Catalogue) XML definition (instructions on how to view the MMC XML Schema are included in Appendix 3).

This document set details the interface provided to the DCC Service User to access the Service Requests and Responses.

Please note that the DUGIDS document set is dependent on the contents of the latest published GBCS document. The GBCS defines the data item content of commands and responses from Devices in line with the protocol definitions. This DUGIDS document describes behaviour of SMETS2 devices with GBCS versions up to and including v4.2.

Note that references throughout this document set to GBCS v1.0 and GBCS v2.0 should be taken to also include GBCS v1.1 and GBCS v2.1 respectively.

1.3 Document Structure

This document is structured as follows:

Section 1 **Introduction**, this section

Section 2 **Overview of Interface**, describes how the interface operates

Section 3 **Command Variant**, describes the method by which Service Request responses may be returned to the DCC Service User

Section 4 **Request and Response IDs**, describes the format of the Service Request and Service Response Identifiers

Section 5 **Scheduling,** describes the Use Cases that involve Scheduling either at the Meter or within the DCC Data Systems

Section 6 **Sequencing**, describes how Service Requests may be orchestrated into a sequenced chain of commands

Section 7 **Access Control**, defines how Access Control is managed for the interface

Section 8 **Security**, describes the Service Requests security requirements

Section 9 **Request and Response Definitions**, defines the Service Requests and Service Responses (including Device and DCC Alerts) Common Data Items and, for each Service Request, it defines whether it is Critical and/or Sensitive and which Modes of Operation and User Roles are applicable

Section 10 **Web Services Implementation**, describes the technical implementation of the DCC User Interface

Section 11 **Error Handling**, describes the error handling and retry strategy for this interface

Section 12 **Response and Status Codes**, describes the response codes generated by this interface

Section 13 **DCC Alerts List**, lists the DCC Alerts

Section 14 **Connection Mechanisms**, describes the connection mechanisms to DCC User Gateway Network

Section 15 **Connections – Certificate and Key Management**, references the DCCKI SEC documentation set, including Interface Specifications, Code of Connection and Policy documents.

Section 16 **Anomaly Detection**, describes the anomaly detection service for Service Request and Response processing

Appendix 1 **Glossary**, lists a Glossary of terms used in this document set

Appendix 2 **DUIS XML Schema Definition Instructions**, provides information on how to view the DUIS XML Schema document

Appendix 3 **MMC XML Schema Definition Instructions**, provides information on how to view the MMC XML Schema document

Appendix 4 **XML Data Type Ranges**, summarises the XML numeric data type ranges

Appendix 5 **GBCS Assumptions – Requests**, provides a list of assumptions made with respect to GBCS v2.0 Draft 5 which affect requests to the Device

Appendix 6 **GBCS Assumptions – Responses**, provides a list of assumptions made with respect to GBCS v2.0 Draft 5 which affect responses from the Device

Appendix 7 **SEC and GBCS Version Assumptions**, provides a list of assumptions made with respect to SEC and GBCS Version

Appendix 8 **SMI Device Status**, provides a set of entity lifecycle diagrams for Devices held within the Smart Metering Inventory

Appendix 9 **Error Handling and DCC Alerts**, provides a set of diagrams that outline the main Error Handling scenarios, including the DCC Alerts generated in each scenario

Appendix 10 **Service Request Variant – GBCS UC Mapping Versioning,** provides the mapping of Service Request Variant to GBCS Use Case(s) applicable to the different DUIS XSD, MMC XSD and GBCS versions

Appendix 11 **Use of Multiple EUI64 Identifiers,** provides a description of the use of multiple EUI64 Service User IDs for the same SEC Party and Role

Appendix 12 **Firmware Version Alerts,** provides a description of the business rules used when tracking Firmware Versions on devices

Appendix 13 **Non-Critical Configurable Events / Alerts,** provides a summary of Events / Alerts that are configurable on ESME and / or GSME

Appendix 14 **Combined Supplier User Role**, provides a description of the behaviour associated with the Combined Supplier User Role

Appendix 15 **Firmware Distribution Tracking State Diagram** illustrates the possible states for tracking of a Firmware Distribution to a device.

Appendix 16 **Changes for the ECoS Service** provides a description of the reasons why ECoS service changes were made in DUIS before implementation in a later release

Appendix 17 **Permitted Activities with Suspended Devices** provides guidance on restrictions on Service Users for Devices where the Device Status is Suspended

1.4 Referenced Documents

Key	Document Title	Issue	Dated
Annex	DCC User Gateway Interface Design Specification Service Request Definitions	5.2a	June 2023
DUIS XML Schema	DCC User Interface Specification XML Schema	5.2a 5.1a 5.0a 4.0b 3.1a 3.0c 2.0 (2.0d) 1.0 (0.8.2.1)	June 2023 June 2022 November 2021 November 2020 June 2019 May 2019 March 2018 February 2016
MMC XML Schema	DCC Service User Message Mapping Catalogue XML Schema	5.2a 5.1a 5.0a 4.0b 3.1a 3.0c 2.0 (2.0b) 1.0 (0.8.2.1)	June 2023 June 2022 November 2021 November 2020 May 2019 Aug 2018 May 2017 February 2016
Error Handling Strategy	Error Handling Strategy Procedure	5.2	June 2023
XMLDSIG XSD[1]	W3C XML Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/	2.0	2008/06/10

Key	Document Title	Issue	Dated
GBCS	Smart Metering Implementation Programme Great Britain Companion Specification (GBCS)	4.2 4.1 4.0 3.3 3.2 2.1 2.0 1.1 1.0	November 2022 November 2021 November 2020 November 2022 June 2019 June 2018 February 2018 November 2017 November 2017
SMETS (per Device Type)	Smart Metering Implementation Programme Smart Metering Equipment Technical Specifications	GSMETS v4.3 ESMETS v5.1 IHDTS v4.3 PPMIDTS v4.4 HCALCSTS v5.1 SAPCTS v5.0	November 21 November 22 November 21 November 21 November 21 November 21
SMETS	Smart Metering Implementation Programme Smart Metering Equipment Technical Specifications	5.0 4.2 3.0 2.0	November 2020 June 2019 February 2018 February 2017
CHTS	Smart Metering Implementation Programme Communications Hub Technical Specifications	1.6 1.5 1.4 1.3 1.1 1.0	November 2022 November 2021 November 2020 June 2019 February 2018 November 2017
SEC	Smart Energy Code	TBD	TBD
DUIS	SEC Subsidiary Document – DCC User Interface Specification	5.2 5.1 5.0 4.0 3.1 3.0 2.0 1.1	June 2023 June 2022 November 2021 November 2020 November 2020 November 2020 June 2018 November 2018
MMC	SEC Subsidiary Document – Message Mapping Catalogue	5.2 5.1 5.0 4.0 3.1 3.0 2.0 1.0	June 2023 June 2022 November 2021 November 2020 May 2020 July 2019 February 2018 November 2017
CoCo	SEC Subsidiary Document – DCC User Interface Code of Connection	5.14	Feb 2018

Key	Document Title	Issue	Dated
TADP	SEC Subsidiary Document – Threshold Anomaly Detection Procedures	5.14	Feb 2018
DCCKI	SEC Subsidiary Documents – DCC Key Infrastructure (see Section 15)	5.14	Feb 2018
SMETS1 Supporting Requirements	SEC SMETS1 Supporting Requirements	AM 12.0	December 2021
SRPD	SEC Appendix AB Service Request Processing Document	AB 6.0	November 2021

Table 1 Referenced Documents

[1] XSD that defines the XML Signature Syntax in the Service Request and Response XML messages

1.5 Term Alignment

There are a few definition discrepancies between this DUGIDS and the DCC User Interface Specification (DUIS) SEC Subsidiary document that the reader should be aware of. Where these terms have been used in DUGIDS they represent the same meaning as in DUIS.

DUGIDS term	DUIS term
DCC Data Systems	DCC Systems
DCC Only Services	Non Device Services
DCC Service User	User
DSP Scheduled	DCC Scheduled
Future Dated (Device)	Future Dated Response Pattern (Device)
Future Dated (DSP)	Future Dated Response Pattern (DSP)
SMETS1 Service Request (depending on context this may include DCC-only requests)	SMETS1 Supported Service Request (in DUIS this term includes DCC-only requests whereas "SMETS1 Service Request" excludes DCC-only requests)

Table 2 Term Alignment

In addition to the above, the following table details the correspondence between the DUGIDS and DUIS User Roles.

DUGIDS term	DUIS term
Electricity Import Supplier (EIS)	Import Supplier (IS)
Electricity Export Supplier (EES)	Export Supplier (ES)
Gas Import Supplier (GIS)	Gas Supplier (GS)

DUGIDS term	DUIS term
Supplier Nominated Agent (SNA)	Registered Supplier Agent (RSA)
Electricity Network Operator (ENO)	Electricity Distributor (ED)
Gas Network Operator (GNO)	Gas Transporter (GT)
Other User (OU)	Other User (OU)

Table 3 User Roles Term Alignment

1.6 XML Schema Precedence

The DUGIDS document set consists of many documents and 2 schemas. See section 1.2 for details.

For the avoidance of doubt, the DUIS/MMC XML Schema is provided as the authoritative source for data item definitions. Where any inconsistencies may exist between the definitions contained within the main text within this document and the DUIS/MMC XML Schema then the DUIS/MMC XML Schema shall take precedence.

2 Overview of Interface

2.1 Context

The DCC User Interface provides the means by which Service Users can send and receive Service Requests and Responses to/from Smart Metering Equipment, using the services of the Data Service Provider (DSP) and Communication Service Providers (CSPs).

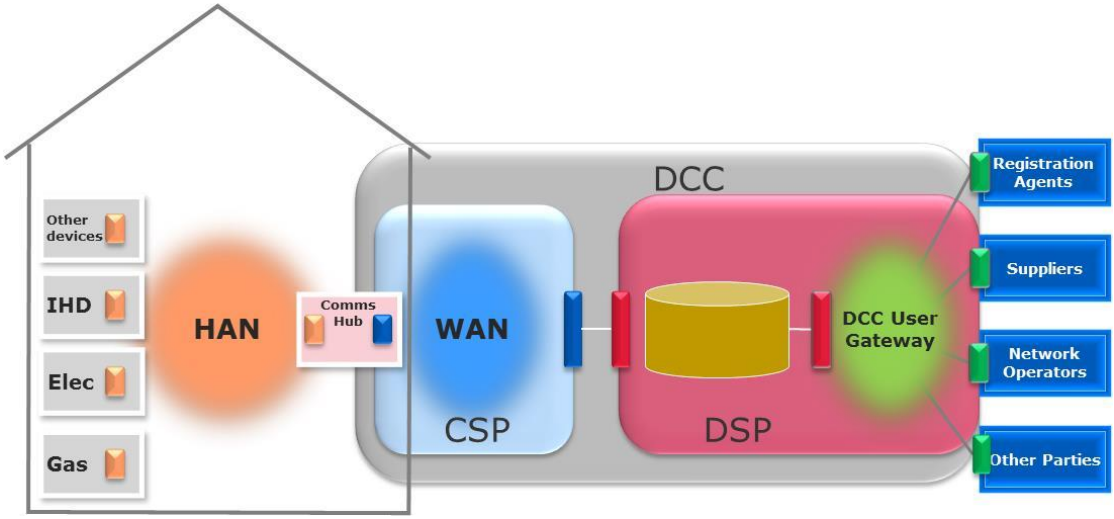


Figure 1 Overall Context

There are some Service Requests that do not involve interaction with Smart Metering Equipment, but the majority of usage for the DCC User Interface is for end to end messaging between DCC Service User systems and Devices within the customer premise.

The DCC User Interface has been designed to be a single common interface to enable communications for all SMETS devices, although some aspects of the DCC User Interface may be different for the two distinct sets of devices supported by the interface, namely those of;

- Devices conforming to SMETS2 or later versions of SMETS
- Devices conforming to SMETS1

The DCC User Interface was originally designed against SMETS2 Devices in v1.0, then extended in v2.0 to support SMETS Devices for later versions of SMETS than SMETS2, and further extended in v3.0 for support of SMETS1 devices.

2.2 Service Request Processing

The basic principles for Service Request processing involve a DCC Service User constructing a Service Request in the format described in this document (see section 9) and sending it to the DCC.

For Non-Critical Service Requests these are transformed to GB Companion Specification (GBCS) format and sent to the relevant Device.

For Critical Service Requests, the transformation to GBCS format is carried out by the DCC and the transformed request (a Pre-Command) is returned to the DCC Service User for checking and signing. The signed Pre-Command is returned to the DCC and is then sent to the relevant Device.

In both cases, a Service Response in GBCS format is sent by the Device to the DCC and the DCC forwards this response to the relevant DCC Service User.

Similarly, unsolicited Alerts in GBCS format are sent by the Device to the DCC and the DCC forwards the Alert to the relevant DCC Service User.

This basic Service Request/Response processing pattern is shown in Figure 2~~Figure 2~~ below.

There are, of course, variations on this basic processing pattern. These are introduced in section 2.3 and also described in more detail in section 3.

In addition, processing of SMETS1 Service Requests follows a variation on this pattern since SMETS1 devices do not use GBCS format messages. This is described in section 2.10.

Note that throughout this document the term Request is used to refer to both Service Requests and Signed Pre-Commands, where behaviour is applicable to both.

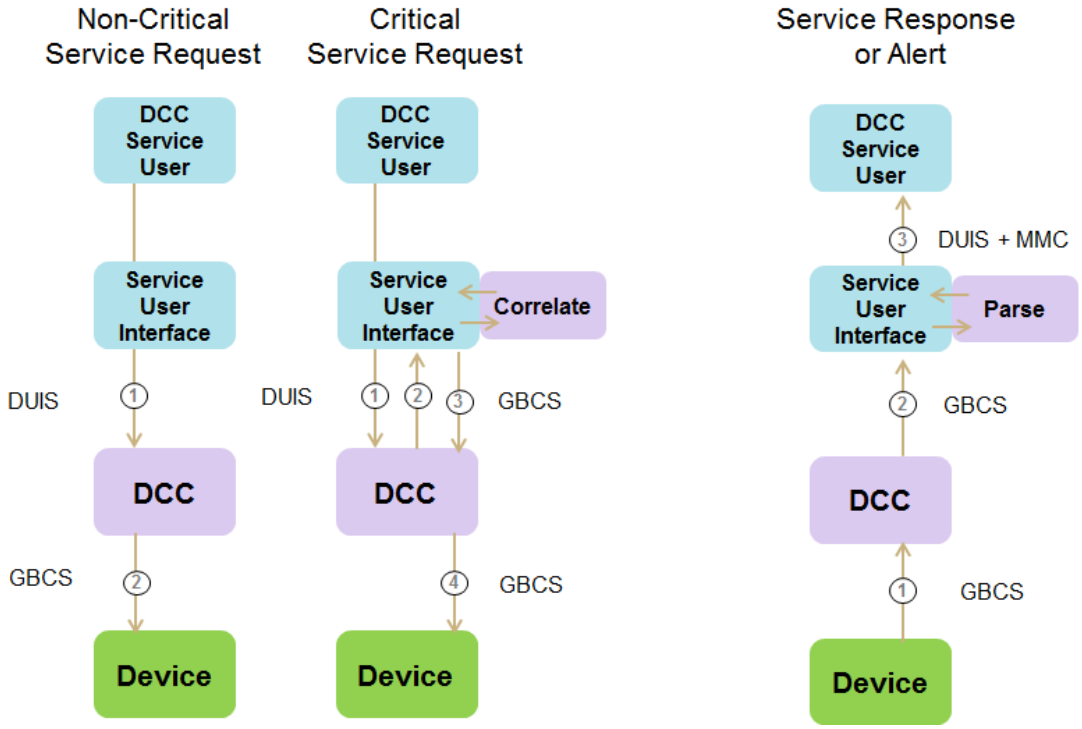


Figure 2 Basic Service Request Processing

An important factor in the end to end message processing for Service Users is the Parse & Correlate function (for which software is being made available by DCC).

The Correlate function supports the processing of Critical Service Requests and provides a mechanism to check that a returned Pre-Command in GBCS format is equivalent to (i.e. “correlates” with) the original DUIS format Service Request. Upon confirmation from the Correlate function, the DCC Service User can then sign and send the Pre-Command to the DCC.

The Parse function supports the processing of all Service Responses and Alerts from devices and provides a mechanism to transform GBCS format responses into a more accessible format. The output of the Parse function is referred to as the Parse Output and is defined in the Message Mapping Catalogue SEC Subsidiary document, however in order to provide a single design specification the format of responses produced by Parse are described in this DUGIDS document. See section 9.3.5 for more details.

2.3 Modes of Operation

As noted previously, there are a number of variations on the basic Service Request processing described above. There are some variations for Service Requests, Responses and Alerts that only require interaction with the DCC Data Systems and have no interaction with Devices. There are also variations in processing of Service Requests and Responses to/from Devices based on the scheduling requirements of when a Service Request needs to be executed.

Figure 3~~Figure 3~~ below shows these variations as “Modes of Operation”.

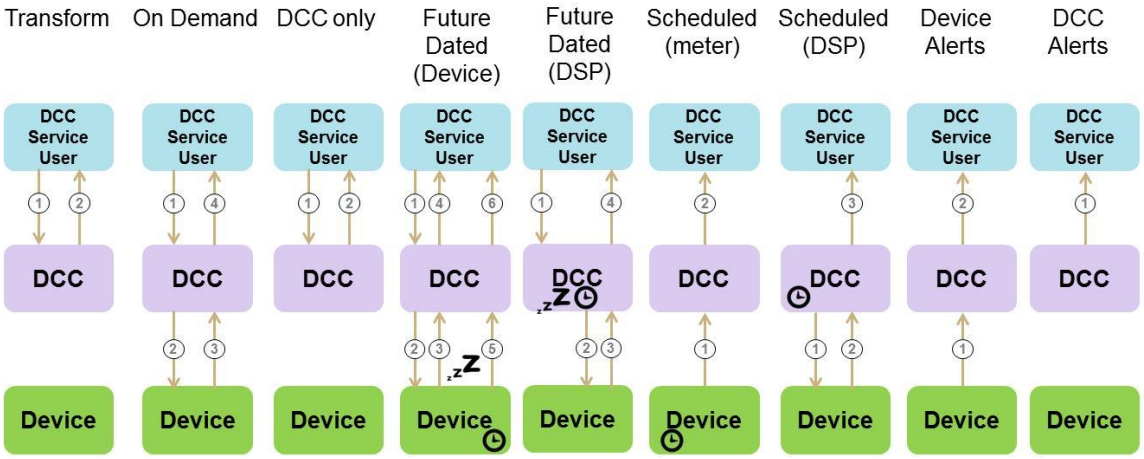


Figure 3 Modes of Operation

2.3.1 Transform

This Mode of Operation is only supported for SMETS2 or later Devices.

The Service Request in DUIS format is transformed to a GBCS Command and returned to the DCC Service User as a Pre-command to be digitally signed by the DCC Service User.

2.3.2 On Demand

A Non-Critical Service Request, Critical Service Request (for SMETS1 only) or Signed Pre-Command (for SMETS2 or later Critical Service Requests) is sent to the Device and the Device returns a Service Response.

2.3.3 DCC Only

The Service Request interacts with the DCC Data Systems only and a Service Response is sent to the Service User.

2.3.4 Future Dated (Device)

This Mode of Operation is only supported for SMETS2 or later Devices.

The Service Request or Signed Pre-Command is to be executed at a specified date/time in the future by the Device.

The Service Request with this future date/time is sent to the Device and the Device returns a Service Response confirming acceptance of the future command.

At the stated future date/time, the Device executes the command instructions and returns one Device Alert for each activation date-time, which the DCC Data Systems convert into Service Responses.

Note that, according to SMETS, a Device can only hold one future dated command per command type. Any new future dated command of the same type sent to a Device will simply overwrite the previous one (if not already executed).

The ability to set a particular Service Request for future dated execution on the device is driven by the definition of the relevant Use Case in GBCS (see section 9.4).

2.3.5 Future Dated (DSP)

Not all commands can be future dated at the Device and in this case the DSP is responsible for sending the Service Request to the Device at a specified date/time in the future. The Service Response is returned by the Device in response to that Service Request.

2.3.6 Meter Scheduled

This Mode of Operation is only supported for SMETS2 or later Devices.

The Meter Scheduled mode of operation is a special case where the Device holds a recurring schedule to send data to the Service User.

This mode of operation only applies to the Billing Calendar functionality within SMETS which sets a schedule for the Device to send a Billing Data Log Alert on a regular basis.

2.3.7 DSP Scheduled

A Service User can create a Schedule within the DCC that requires the DSP to send a Service Request on behalf of that Service User at regular intervals. The create Schedule response includes the DSP Schedule ID.

In line with the Schedule, the DCC Data Systems creates a Service Request and sends it to the relevant Device. The Device returns a Service Response and the DCC sends this Response, plus the DSP Schedule ID, to the Service User that created the Schedule.

Note that there are restrictions on what types of Service Request can be scheduled by the DSP (see section 9.4).

The rest of this section is additional information to provide guidance for Service Users.

As noted in section 5.1 (SRV 5.1 Create Schedule), for scheduling delivery of overnight readings based on data for a calendar day, Service Users are recommended to use the default setting for the start time.

The current DCC/DSP design for managing the DSP Scheduled Service Requests is as below:

- DSP creates a worklist containing all the scheduled Service Requests for each targeted Device per Service User with a run time (as specified by SRV 5.1) against each of the work items;
- DSP then works through the list, picking up any item from the list which has a run time in the past, at agreed rates per CSP/S1SP. DSP will select records using an approach which gives preference to those with older execution times for the same CSP/S1SP;
- the selection will not prioritise any Service User over another, and available capacity is distributed across ALL Service Users;
- On Demand messages for any Service User will always take precedence and will affect the delivery profile of requests/responses;
- the agreed rate for selection of schedules for execution is configurable on a per CSP/S1SP basis and should always be set to ensure that DCC is not operating at 100% capacity, so there should always be room to handle On Demand messages.
- it is not guaranteed that there will be an even spread across a particular Service Request or Service User;

- assuming Service User system capacity allows, there is no benefit for Service Users in staggering their Schedule Activation Times throughout the period; in fact, this could be detrimental since it means the DSP loses control over the scheduling. If Service Users stagger their activation times across the period, then we could end up with a lull in the processing because we can't action the next set of requests until 02:00 or 03:00 for example.

2.3.8 Device Alerts and SMETS1 Alerts

Unsolicited messages (Alerts) are generated by Devices and sent to the DCC. The DCC forwards these to the relevant Service User. The Alert recipient is defined in the message from the Device. The Device Alert list for SMETS2 or later Devices is mastered by GBCS.

SMETS1 Alerts are used to communicate Alert codes from a subset of GBCS Device Alert codes which are deemed also applicable to SMETS1 Devices, and additional Alert codes for SMETS1 Devices which are not in common with GBCS Alert codes. The SMETS1 Alert code list is mastered by DCC.

2.3.9 DCC Alerts and S1SP Alerts

The DCC Data Systems may generate unsolicited messages (DCC Alerts) which are sent to Service Users. Note that the DCC Alerts category includes Notifications to Service Users to inform them of actions taken within the DCC Data Systems.

Table 49~~Table 49~~ displays the list of DCC Alerts.

An S1SP Alert is a message originated by an S1SP and sent to the DSP for inclusion in a DCC Alert with a DCC Alert Code which indicates that it contains an S1SP Alert.

2.3.10 Firmware Distribution

SMETS2 or later

Although not explicitly a Mode of Operation, Services for delivery of new firmware images to Devices are a special use case for processing for both the DCC Data Systems and the CSP. Please note Firmware Distribution (Service References 11.1 and 11.4) is defined as Mode of Operation “DCC Only” in the rest of this documentation set.

Given the large volume of data involved for distribution of a firmware image, the responsibility for doing this is given to the CSP who may then optimise that distribution over the CSP SM WAN. For ESME, GSME and HCALCS this means there is a three stage process for delivering and applying a new firmware image to one or more Devices. This is shown in Figure 4~~Figure 4~~.

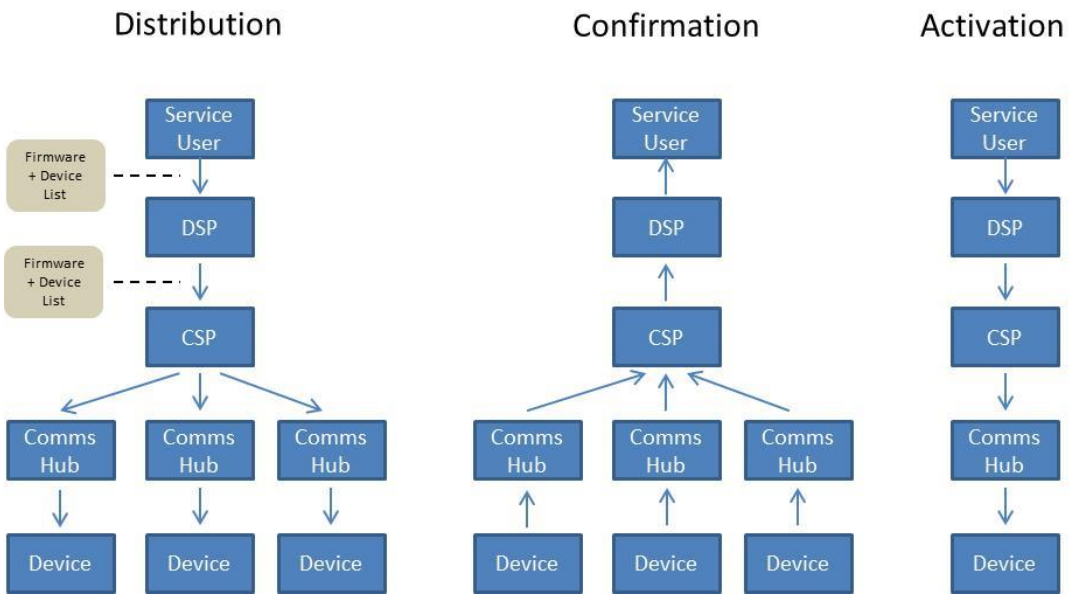


Figure 4: Firmware distribution process for ESME, GSME and HCALCS

The first stage is distribution of the new firmware image to one or more Devices. The DCC Service User sends the required firmware image and a list of Devices (Maximum Number of Devices = 50000) to the DSP in a standard Service Request. This firmware image and list of devices are then passed across to the CSPs for the CSPs to action. The CSPs will deliver the new firmware image to the relevant communication hub for each Device ready for onward transfer to the Device.

Upon completion of delivery of the firmware image by the Device, the Device will send a Device Alert to notify the DCC Service User that the firmware has been received.

Once a DCC Service User has received confirmation of successful delivery of the firmware image to a given device, then they are able to send an Activate Firmware command to that Device using the Activate Firmware Service Request.

For PPMIDs a separate activation request is not required. A PPMID automatically initiates the activation of a new firmware version upon successful receipt of a new firmware image. The PPMID will then notify its active Firmware Version to the DSP using a Device Alert and the DSP will forward this notification (via DCC Alerts) to all the Responsible Suppliers associated with its HAN. The process applicable to device type PPMID is shown in Figure 4~~Figure 4~~.1 below.

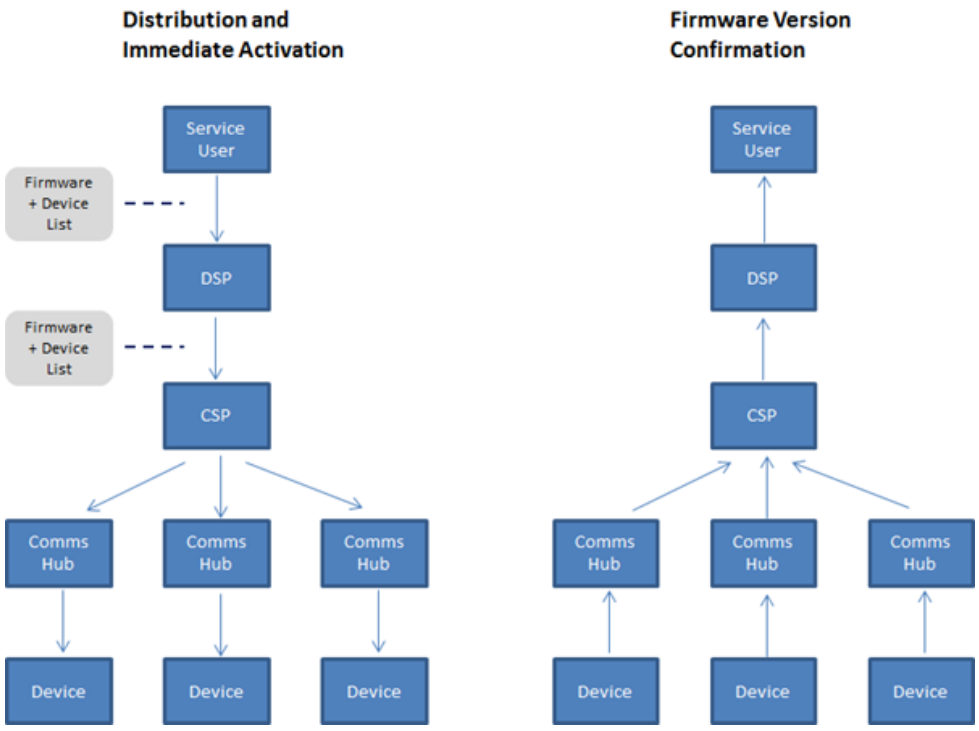


Figure 4~~Figure 4~~.1: Firmware distribution and activation for PPMID

For SMETS2 Devices, after a firmware image distribution has been initiated using the Service Requests 11.1 (for ESME, GSME and HCALCS) or 11.4 (for PPMID), the Service Users will be notified of its progress through different stages of processing within DCC Data systems. The following table lists the processing statuses related to firmware distribution and activation, and see Appendix 15 – Firmware Distribution Tracking State Diagram for a diagram showing valid progressions between Firmware Distribution Tracking states.

Processing Stage	Processing Status	Description	Notification Mechanism
Processing within DSP	Rejected by DSP	DSP validation checks failed, with one of the following reasons: • 'Invalid' • 'Not Commissioned' • 'Not Applicable Firmware' • 'Quarantine Reject' • 'Invalid GBCS Version'	Synchronous Response to SR 11.1/11.4
	Accepted by DSP	DSP validation checks successful	
Processing within CSP	Not Accepted by CSP	CSP validation checks failed or there is a communications failure with the CSP, with one of the following reasons: • 'Checksum provided did not match the firmware image' • 'Invalid delivery point' • 'Firmware image provided is too large' • 'Unable to deliver to CSP' • 'No firmware validation report' • 'Incomplete request'	DCC Alerts **N18, N19, N20, N22** or **N23**

Processing Stage	Processing Status	Description	Notification Mechanism
	Approved for Distribution	CSP Validation Checks Successful	DCC Alert **N59**, sent to other supplier only[3]
	Failed CH Transfer	Delivery to Comms Hub by CSP Failed. Only set if the previous status reported was 'APPROVED_FOR_DISTRIBUTION'.	DCC Alert **N60[1].**
	Successful CH Transfer	Delivered to Comms Hub by CSP. Only set if the previous status reported was 'APPROVED_FOR_DISTRIBUTION'.	DCC Alert **N61[1].**
Processing Within HAN	Not Delivered at HAN	Delivery to target Device by the Comms Hub failed, with one of the following GBCS reason codes: • '*imageDiscarded*' (1) • '*hardwareVersionMismatch*' (2) • '*fileTransferFailure*' (3)	DCC Alert **N62[1]** Information from GBCS Alert Code 0x8F89 indicated by one of the following TransferResponseCodes: • FirmwareImageDiscarded - where the Firmware is discarded at the Comms Hub • HardwareVersionMismatch - where the Firmware is rejected due to hardware version mismatch by the Comms Hub. • FileTransferFailure - where the Comms Hub failed to deliver to the target Device
	Successful HAN Transfer	Delivered to the target Device by the Comms Hub successfully	DCC Alert **N62[1]** Information from GBCS Alert Code 0x8F8A indicated by TransferResponseCode: • FileTransferSuccess
		Received (and validated) by the device.	GBCS Alert code 8F1C or 8F72 from ESME, GSME or HCALCS reporting the result of validation of the firmware.
Device Activation	Firmware Activated	For PPMIDs the firmware image activation happens upon its receipt, and successful activation is indicated by GBCS Device Alert 0x8F8B with Activate Image Result Code *ActivationSuccess* (0) Set with reason '8F8B Alert received'	DCC Alert **N39[2]** GBCS Alert Code is 0x8F8B (Applicable only for PPMIDs)

[1] Recipients that are on a version of DUIS earlier than 5.0 will receive an N999 Alert.

[2] Recipients that are on a version of DUIS earlier than 5.0 will receive the details of the 0x8F8B Device Alert, but without the activation outcome. SRV11.2 can be used to determine the firmware currently on the device

[3] Applies only to SMETS2 PPMIDs

Processing Stage	Processing Status	Description	Notification Mechanism
		For ESME / GSME / HCALCS, firmware activation is done by sending the SR 11.3. Response has ActivateImageResultCode of *success* (SMETS1) or response reports the new firmware is active (SMETS2). Set with reason '11.3 response received'	Response to SR 11.3
		11.2 response reports the new firmware is active. Set with reason '11.2 response received'	Response to SR11.2 DCC Alert N49
	Activation Failed	For PPMIDs the firmware image activation happens upon its receipt, and successful activation is indicated by GBCS Device Alert 0x8F8B with ActivateImageResultCode *ActivationFailure* (1) Set with reason '8F8B Alert received'	DCC Alert **N39** GBCS Alert Code is 0x8F8B (Applicable only for PPMIDs)
		For ESME / GSME / HCALCS, firmware activation is done by sending the SR 11.3. Response has an Activate Image Result Code indicating failure (SMETS1) or response reports a firmware version other than the new firmware (SMETS2). Set with reason '11.3 response received'.	Response to SR 11.3
Service Desk Intervention	Reset by DCC	Tracking status reset by DCC so that a new firmware distribution may be started	NA

Table 3~~Table 3~~.1 Firmware Distribution – Processing Statuses

SMETS1

The distribution of firmware to SMETS1 devices, including PPMIDs, follows the same distribution, confirmation and activation processing pattern as for SMETS2 non PPMID devices, with the SMETS1 Service Provider (S1SP) taking the role of the CSP. The status tracking DCC Alerts do not apply to SMETS1.

However, in some cases, SMETS1 devices activate the firmware as soon as it is delivered, therefore following the successful call of Service Request 11.1, the S1SP will generate a Firmware Verification Device Alert which is sent to the relevant DCC Service User. The Service User will then send an Activate Firmware Service Request to activate the firmware. On receipt of the Activate Firmware Service Request the S1SP will distribute the firmware which will activate automatically.

In addition to the Device Types for which Suppliers may update Firmware on SMETS2 or later Devices, the Lead Supplier of a SMETS1 HAN may also update the Firmware of a SMETS1 Communications Hub (which includes the associated GPF) or SMETS1 PPMID.

2.3.11 Change of Supplier

SMETS2 or later

The Service to support the Change of Supplier (CoS) process is a special use case for processing for the DCC Data Systems. In this case, a separate function within the DCC Total System called the CoS Party interacts with the main Access Control Broker (ACB) function to deliver an appropriately signed command to the Device. An overview of this interaction for a simple On Demand request is shown in Figure 5~~Figure 5~~.

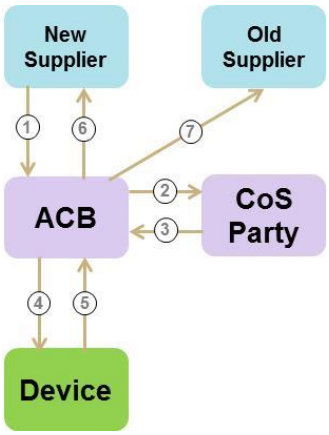


Figure 5: CoS On Demand Service Request processing

The new (gaining) Supplier sends a CoS Service Request to the DCC (step 1) which is acknowledged and processed by the ACB function. The ACB function then passes the request to the CoS Party function (step 2) which is responsible for creating a signed GBCS pre-command for the Device and returning it to the ACB (step 3). The ACB adds a MAC and sends the command to the Device (step 4) and receives a response (step 5). This response is then delivered to the new supplier (step 6) and the old (losing) supplier is notified of completion of the process via a DCC Alert N27 (step 7).

It is expected, however, that most CoS Service Requests will be Future Dated and in this case there is a further elaboration of the processing as shown in Figure 6~~Figure 6~~.

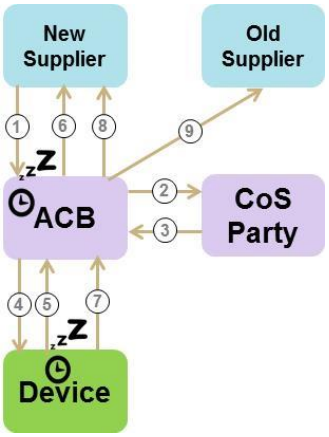


Figure 6: CoS Future Dated Service Request processing

If the CoS Service Request is sent by the new supplier to the DCC (step 1) more than 24 hours in advance of the stated Future Dated execution time or, (post CSS) the Registration has not reached Secured Active status, then the ACB function will hold this request until the time reaches 24 hours before the execution time[3]. At this point the ACB will schedule this request for processing and, when actioned, will forward the request to the CoS Party (step 2) and receive a signed future dated pre-command in return (step 3). The ACB will add a MAC and then deliver the signed future dated command to the Device (step 4) and receive a response confirming receipt by the device (step 5). This confirmation response is delivered to the new supplier (step 6). At the desired execution time, the Device will execute the command and send an execution response to the ACB (step 7). This execution response is then delivered to the new supplier (step 8) and the old supplier is notified of completion of the process via a DCC Alert N27 (step 9).

[3] If a Secured Active status update is not received then shortly before the execution time the request will fail with ResponseCode E4.

If the CoS Service Request is sent less than 24 hours before the stated Future Dated execution time and, (post CSS) the Registration has already reached Secured Active status, then the ACB function will not delay the passing of the request to the Cos Party (steps 1 to 2) but thereafter the processing is exactly the same as described above.

SMETS1

SMETS1 devices do not hold any Supplier certificates and therefore there is no need to support the full Change of Supplier (CoS) process as DCC operates for SMETS2 devices. However, the Service Request associated with the Change of Supplier process (SR6.23 - Update Security Credentials (CoS)) is supported for SMETS1 devices in order to allow the DCC Data Systems and the relevant SMETS1 Service Provider to track the specific DCC Service User ID that the Supplier intends to use with respect to that device.

Please note that this Service Request is a DCC Only Service Request and the sending of this Service Request to the DCC does not result in any interactions with the target Device ID as specified within the Service Request. The DCC retains security credential information associated with the Device, as defined in the SMETS1 Supporting Requirements Document.

For SMETS1 devices, Service Requests follow the same pattern as described for SMETS2 devices above, except that

- The CoS Party does not create (and ACB does not validate) a signed GBCS pre-command.
- For SMETS1 Devices a CoS Service Request is treated as pure Future Dated (DSP), rather than using the hybrid approach described above for SMETS2 or later Devices. The sending of the Service Request to the S1SP will be triggered by the DCC Data Systems when the CoS execution date and time is reached.

As with SMETS2 or later Devices, when the CoS is completed the old (losing) supplier is notified of completion of the process via a DCC Alert N27.

2.3.11.1 Move to Enduring Change of Supplier

The Transitional Change of Supplier (TCoS) solution is being replaced by the Enduring Change of Supplier (ECoS) solution[4]. The description above applies to both versions and this section explains the differences between the two solutions.

Each device that holds Supplier credentials has CoS Party credentials to support replacement of the Supplier credentials. These credentials currently all belong to the TCoS Party; over time the TCoS credentials will be replaced with ECoS credentials. Once the ECoS Party starts operation, new devices will be manufactured with ECoS credentials. Once all devices in the supply chain have ECoS credentials and all installed devices have had TCoS credentials replaced with ECoS credentials then the TCoS Party will be decommissioned.

Once the ECoS Party is in operation, the user experience will depend on whether the device they are sending the CoS Service Request to has TCoS or ECoS credentials. Further, all SMETS 1 CoS Service Requests will be sent to the ECoS Party.

The following changes will apply

[4] Please note that the the implementation of the new ECoS functionality is not part of the June 2022 Release (expected as part of the June 2023 Release). Please see Appendix 16 – Changes for the ECoS Service for further details.

- The check that the Service User is the Registered Supplier for the device will additionally be carried out against the Market Participant Identifier that is included within the certificate that is used to sign the CoS Service Request
    - On error E062306
- The DSP will determine the owner of the CoS certificate held in the transitionalCoS Trust Anchor Cell (slot 10) on the device according to the SMI
- The DSP will check that the identified party is an active CoS Party
    - On error E062305
- Where that party is the ECoS Party then the DSP will pass the request to the ECoS Party for processing.
    - On error E66, E67, E68, E69 or E71 will be returned using DCC Alert N26
    - The ECoS Party may generate a notification to the Service User, this will be delivered as DCC Alert N63
- Where that party is the TCoS Party then the DSP will pass the request to the TCoS Party for processing.
- After the CoS Party (either ECoS or TCoS) performs its processing and returns the request to the DSP, the DSP will carry out anomaly detection checks
    - On error the request is discarded (no quarantine), E70 will be returned using DCC Alert N26.

Where the Service User is using a version of DUIS prior to 5.1 then the response codes will be reported as follows:

DUIS 5.1 or later Response Code	Prior to DUIS 5.1 Response Code
E062306	E4
E66, E67, E68, E69, E70, E71	E19
E062305	E19

2.3.12 Power Outage Alerts

SMETS2 or later

To provide Network Operators with visibility of power outage events at customer premises, the DCC solution provides facilities to notify both power outage events and power restore events to the Network Operator.

Power Outage alerts are generated at the Comms Hub when power is lost and are notified via the CSP systems if the outage duration is greater than 3 minutes. The CSP systems notify the DSP via a dedicated power outage API and the DSP generates a DCC Alert AD1 for each Comms Hub that has been notified.

Power Restore events are recorded at the ESME and are notified via a GBCS Device Alert. There are different alert codes depending on the duration of the power outage and the phase that suffered the outage. In particular, the ESME will notify power restore events of less than 3 minutes as well as power restore events of greater than 3 minutes.

The overall processing for Power Outage and Power Restore alerts is shown in Figure 7~~Figure 7~~.

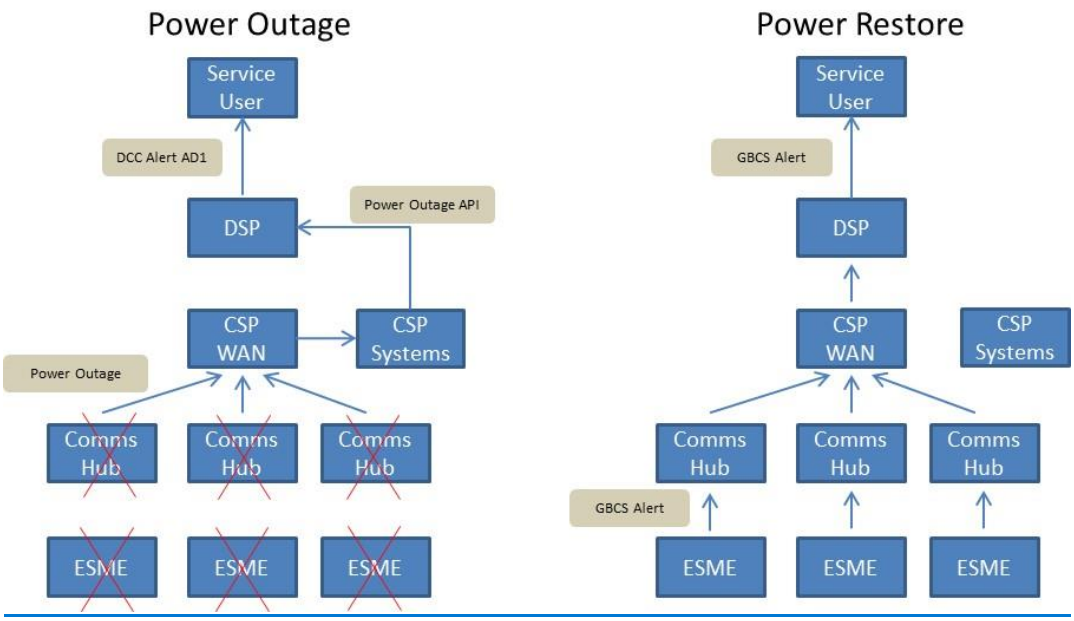


Figure 7: Power Outage and Power Restore alerts

As an exception to the above processing, an operational issue has been discovered where certain instances of a particular ESME device will cause power to be lost to the Comms Hub during the activation of new firmware on that ESME. This causes the Comms Hub to generate a Power Outage alert which is then notified all the way onwards to the Network Operator.

To prevent these spurious Power Outage alerts from reaching the Network Operator the DSP will track firmware activation requests to this particular set of ESME devices and will suppress any Power Outage alert from the associated Comms Hub that notifies an outage which started within [30 minutes] of the firmware activation.

2.4 Web Services

The technical implementation of the DCC User Interface is provided by using web services to allow Service Requests and Responses to be sent between the DCC Data Systems and the systems of the DCC Service Users.

To process Service Requests, there are three web services provided by the DCC Data Systems as follows:

- Transform Service – for SMETS2 or later Devices, a synchronous communication mechanism for transformation of Critical Service Requests into GBCS Format and the returning of a Pre-Command to the DCC Service User; for SMETS1 Devices, a SMETS1 Critical Service Request sent to this service is re-directed to the Send Command Service and follows the asynchronous communication mechanism for that service.

- DCC Only Service – a synchronous communication mechanism to process DCC Only Service Requests or a request for a Command to be returned by the DCC to the DCC Service User to be locally applied (via a Hand Held Terminal).

- Send Command Service – an asynchronous communication mechanism to which a DCC Service User must send any Non-Critical Service Request, Signed Pre-Command or Non-Critical SMETS1 Service Request where the DCC Service User

wishes the DCC only to send the associated Command to the Device specified in the message.

See section 2.10 for more details of differences in behaviour for SMETS1 Devices.

The Transform and DCC Only web services follow a synchronous processing pattern and return Service Response data to DCC Service Users upon completion of the web service call.

The Send Command web service also completes synchronously and returns a response, but this response simply provides an acknowledgement of acceptance of the Service Request by the DCC. The Service Response from the Device is then delivered asynchronously to the DCC Service User.

To receive asynchronous Service Responses and Alerts, the DCC Service User system must implement a web service as follows:

- Receive Response Service – a service to receive Service Responses and Alerts from the DCC Data Systems.

The Receive Response web service returns an acknowledgement of acceptance of the Service Response or Alert upon completion of the web service call. This same web service is used for receipt of both DCC Alerts and Device Alerts by DCC Service Users.

Figure 8~~Figure 8~~ below shows the Transform and DCC Only web services. Please note Correlate has been added to illustrate the End to End process, but it is not part of the Web Service.

Figure 9~~Figure 9~~ shows the Send Command and Receive Response web services. The Receive Response Service Ack dotted line represents the HTTP acknowledgement of the Web Service call. Please note Parse has been added to illustrate the End to End process, but it is not part of the Web Service.

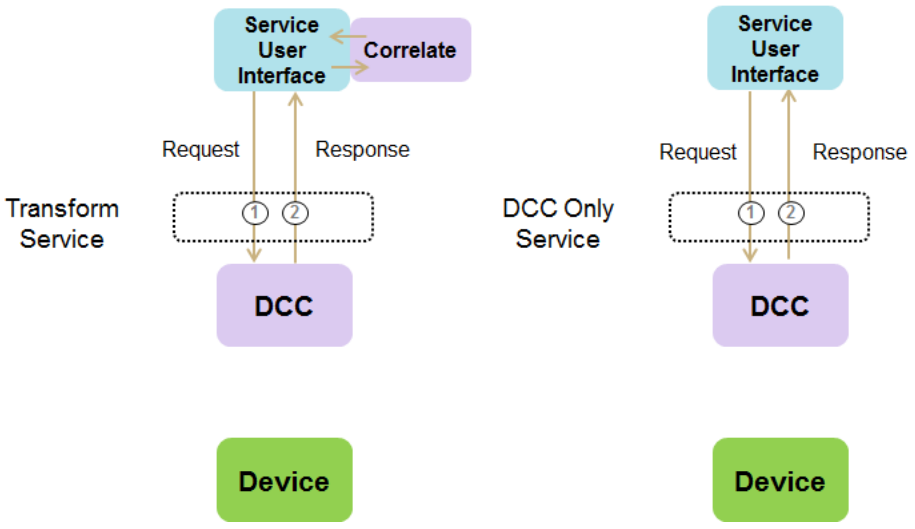


Figure 8 Transform and DCC Only services

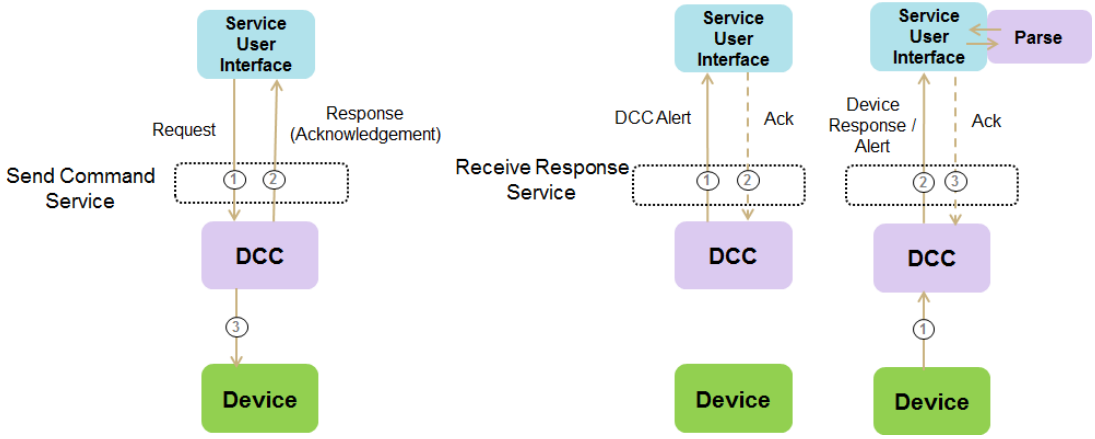


Figure 9 Send Command and Receive Response services

As an extension to the basic processing described above, Commands for local delivery are returned to the DCC Service User either as the response to the DCC Only service (if the command is not being sent to the Device), or they are returned asynchronously via a separate response delivered to the Receive Response service (if the command has been requested to be sent to the Device via the Send Command service). See section 3 for more details on these processing patterns.

For the purposes of supporting the measurement of Target Response Times, the concepts of 'receipt' and 'sending' are to be interpreted by Service Users and the DCC in the following manner:

For the Transform and DCC Only Services the DCC Data Systems shall record the date and time of Receipt of the Service Request from the DCC Service User and the date and time of Sending of the Service Response to the DCC Service User by those services.

For the Send Command Service the DCC Data Systems shall record the date and time of Receipt of the Service Request from the DCC Service User by the Send Command Service and then subsequently record the date and time of Sending of the Service Response to the DCC Service User's Receive Response Service.

For Device and DCC Alerts the DCC Data Systems shall record the date and time when the Alert is received/generated and the date and time of Sending of the Alert to the DCC Service User's Receive Response Service.

2.5 Use of the DCC User Gateway Network

Physical connectivity to the DCC Data Centres is provided by a dedicated private network which is referred to as the DCC User Gateway Network. The DCC is responsible for providing this network and for making available network services to allow DCC Service User organisations to obtain connectivity to the network. More details on the DCC User Gateway Network and connection mechanisms are contained in section 14.

DCC Service Users make use of this network to obtain secure connections to the DCC Data Systems and thus to gain access to the web services described in this Design Specification (see section 0).

An exception to this is an out of band mechanism which allows non domestic Energy Suppliers who do not wish to use DCC Services to opt out of the DCC Services. This mechanism provides the same details as contained within the "Service Opt Out" Service Request (Service Reference 8.5) but is delivered to the DCC outside of the DCC User Gateway Network.

2.6 Time

The DCC User Interface and DCC Data Systems shall use UTC (Coordinated Universal Time) for all Requests and Responses. All references to Time or Date-Time in this DUGIDS will use UTC. To avoid ambiguity, this should be indicated by using the trailing Z in the XML Date and Time formats.

For example;

xs:date data types shall be formatted as <Date>2015-12-25Z</Date>

xs:time data types shall be formatted as <Time>09:30:10.00Z</Time>

xs:dateTime data types shall be formatted as <DateTime>2015-12-25T09:30:10.00Z</DateTime>

All references to time for the DCC User Interface and DCC Systems shall use time with a format precision to 100th of a second.

Where time values are included within the “Body” of a Service Request, the values shall be populated in line with GBCS time definitions for the associated GBCS Use Case to the Service Request being sent by a User.

The DCC User Interface shall only process time values within Service Requests representing whole seconds for which the associated GBCS Use Case results in the creation of an ASN.1 Command as defined by GBCS, with 00 to represent whole second values as shown in the example above. The DCC User Interface shall process time values within Service Requests representing 100th of a second precision for which the associated GBCS Use Case results in the creation of a DLMS COSEM Command or a GBZ Command as defined by GBCS, with a value of 00 to 99 inclusive to represent 100th of a second precision.

Where time values are returned within Service Responses, the 100th of a second precision of time values will be populated where that precision is available otherwise it shall be populated with a value of 00.

For the avoidance of doubt all date-times specified within Service Requests by the User shall not be validated unless explicitly stated within the Service Request definitions.

For SMETS1 Devices, time values in Service Requests and Service Responses also shall be populated in line with the standard DUIS time definitions, in that all references to time shall use UTC time with a format precision to 100th of a second, unless otherwise directly stated.

2.7 Smart Metering Inventory – Device Status

The Smart Metering Inventory maintains Device Status. Some of the Service Requests submitted over the DUIS interface will change the Status of Devices in the Smart Metering Inventory (SMI). Individual Service Requests define what changes are to be applied to the SMI on successful completion. See Appendix 8 – SMI Device Status – Entity Lifecycle Diagrams for a summary of these changes.

For SMETS1 Devices accessed via DCC the DCC Data Systems shall maintain Device Status in the same ways as for SMETS2 or later Devices except that the following Device Statuses shall not apply:

- Whitelisted
- Recovery
- Recovered

See Appendix 8 – SMI Device Status – Entity Lifecycle Diagrams for SMETS1-specific diagrams.

2.8 Handling multiple GBCS versions

The DCC User Interface and DCC Data Systems must be able to support multiple versions of GBCS across the mixed estate of devices that will exist at any point in time.

Backward compatibility of GBCS Use Cases (unless mandated otherwise for a specific GBCS Use Case) will be supported, such that a new version of the DCC User Interface will support message codes for devices with older GBCS versions as well as the devices with the latest GBCS version.

Forward compatibility, meaning use of an older version of the DCC User Interface with a device running a newer GBCS version, will be supported for GBCS use cases which are in common between the older and newer GBCS versions. It will not be possible for a Service Request Variant (SRV) issued in an older version of the interface to be transformed to a GBCS use case/message code which was newly introduced in a later GBCS version.

The following diagram illustrates the basic principles of compatibility between versions of the DCC User Interface and versions of GBCS. SMETS1 devices are also shown on this diagram for completeness; see section 2.10 for more details of using SMETS1 devices via DUIS.

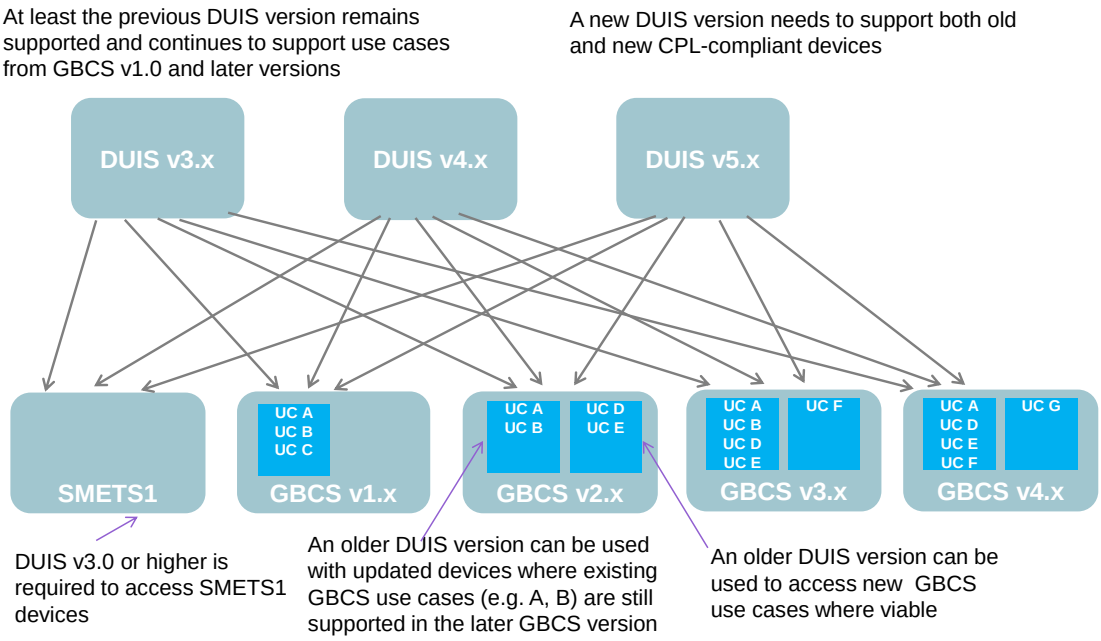


Figure 10 GBCS, SMETS1 and DUIS compatibility

NOTE: There are some specific exceptions to the above rule about not providing forward compatibility for new GBCS Use Cases, e.g. certain Service Requests in DUIS v3.0 can access new Use Cases in GBCS 4.0, but only where those Use Cases continue to support the functionality that is available in DUIS v3.0. This forward compatibility is described, where applicable, in the relevant Service Request Definition Annex.

2.9 Upgrading the DCC User Interface

This document describes the behaviour of the DCC User Interface up to version 5.21. To access version 5.21, DCC Service Users will use URLs as described in section 10.2.

Earlier DCC User Interfaces will also be supported where indicated in section 9.5.4 and will remain available at the existing URLs.

It is assumed that a DCC Service User will only use one version of the DCC User Interface at any point in time.

2.10 SMETS1

SMETS1 devices are supported by the DCC Data Systems in a similar fashion to SMETS2 or later devices. SMETS1 Service Requests are sent using the same Service Request definitions and SMETS1 Responses are sent using the same Service Response definitions. The most significant difference for SMETS1 devices is that the DCC Data Systems does not transform Requests and Responses to/from GBCS format.

Instead, the DUGIDS format Service Request is sent to the relevant SMETS1 Service Provider who is then responsible for transforming the Request to the required SMETS1 command format and sending it to the device. The SMETS1 Service Provider then receives the SMETS1 format response and transforms the response into a DUGIDS format SMETS1 Response which is returned to the DCC Data Systems and delivered to the DCC Service User as a Countersigned SMETS1 Response. This processing pattern is shown in Figure 11~~Figure 11~~ below.

A similar pattern is followed for SMETS1 Device Alerts which are processed by the SMETS1 Service Provider and transformed to a DUGIDS format for sending to the DCC Data Systems and then onwards to the DCC Service User as a Countersigned SMETS1 Alert.

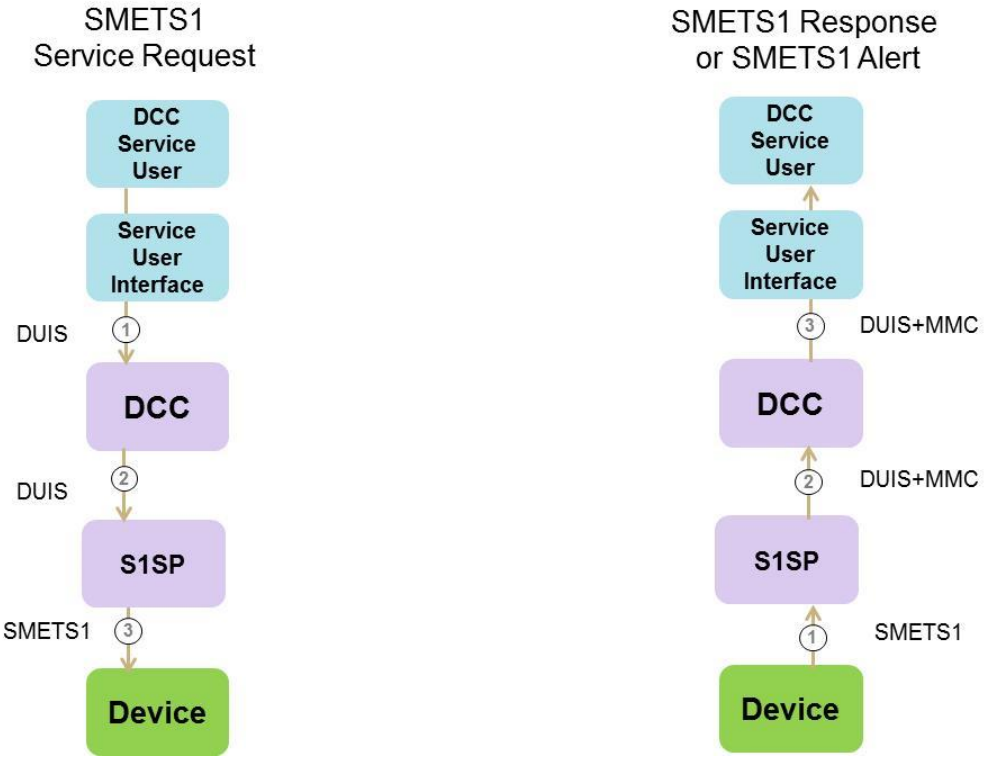


Figure 11 SMETS1 Service Request Processing

There is some difference in the processing pattern for SMETS1 Critical Service Requests compared to SMETS2 devices. SMETS1 Critical Service Requests should be submitted to the Transform Service with Command Variant 4, however instead of returning a Signed Pre-Command, the DCC will process the Service Request with the equivalent behaviour to a Non-Critical Command Variant 1 request to the Send Command Service.

References to the delivery, scheduling and retry of sending of Commands to a Device, where equivalent behaviour is supported by DCC for SMETS1 Devices, shall apply to the sending of instructions to a SMETS1 Device.

Service Users must use DUIS v3.0 or later for DCC SMETS1 Device functionality.

There are some validation conditions specific to SMETS1 Device functionality, including generic validation errors (e.g. E61) and validation conditions to specific Service Requests where appropriate.

2.11 APCs and SAPCs

2.11.1 Auxiliary Proportional Controllers

An Auxiliary Proportional Controller (APC) is a type of connected load control device that enables variable load as a percentage from 0-100%, rather than on or off as with ALCS and HCALCS.

In addition an APC may support two-directional load control, including input from the controlled load to the meter (i.e. export of energy) as well as output from the meter to the controlled load (i.e. import of energy).

From GBCS v4.0 the term “Auxiliary Controller” is a generic term for a connected load control Device, which may be an APC, ALCS or HCALCS.

ESME Devices of GBCS v4.0 or later may support up to 5 Auxiliary Controllers which may be any combination of APC, ALCS or HCALCS.

The presence of an APC in an ESME is indicated by the use of ESME Variant F, and this may occur in combination with other additional ESME Variants such as boost buttons.

As with other ESME Variant information, the CPL will record only variant A, B or C, and additional ESME Variant combinations are recorded for individual Devices when they are pre-notified using Service Request 12.2.

2.11.2 Standalone Auxiliary Proportional Controllers

A Standalone Auxiliary Proportional Controller (SAPC) is a Device which conforms to the requirements of SMETS2 section 9 (v5.0 or later).

SAPC Devices are implemented as Device Type ESME in DCC Data Systems and the CPL, and will be treated in the same way as other ESME devices for access control.

SAPCs will be implemented only as single element ESME Variant A, and will not exist in twin element or polyphase versions (ESME variant B and C respectively).

SAPCs will be identified by the inclusion of G in the ESME Variant combination, and may be in combination with other additional ESME Variants such as boost buttons.

As with other ESME Variant information, the CPL can record only variant A, B or C, and additional ESME Variant combinations are recorded for individual Devices when they are pre-notified using Service Request 12.2.

As with other ESME Devices conforming to GBCS v4.0 or later, an SAPC may support up to 5 Auxiliary Controllers, which may be any combination of APC, ALCS or HCALCS.

SAPC Devices need to conform to a minimum subset of GBCS Commands supported by an ESME, but do not need to conform to all GBCS Commands that would need to be supported by an ESME that is not an SAPC. Where an SAPC receives an ESME GBCS Command that it does not support, it will reject the request by issuing a Device Alert 0x8F85 (GBCS Use Case ECS100).

An ESME conforming to GBCS v4.0 or later may or may not be an SAPC. In this document set, where the term ESME is used it covers SAPCs as well, whether SAPCs are specifically mentioned or not, though the term SAPC is also used explicitly in some places to add clarity.

2.12 Throttling of Alerts

Throttling of Alerts will be triggered where multiple occurrences of the same Alert Code from the same Device exceeds a threshold rate. Where throttling is in progress, Alerts from that Device will be consolidated and an Alert sent to the DCC Service User only once for every N Alerts received or when a configurable time period has expired since the last Alert was sent.

Settings for parameters such as the threshold rate, 1 in N delivery rate and the maximum time period for delivery will be maintained as configurable parameters within the DCC Data Systems and any changes to these parameters will be discussed and agreed with Service Users through the SEC Operations group.

Alert storm protection applies to Device Alerts (SMETS2), SMETS1 Alerts and DCC Alerts (where a DCC Alert is used to deliver an Alert from a Device).

However, some Alert codes are excluded from Alert storm protection. The exclusion list will be discussed and agreed with SEC Operations as with other parameters.

Where an Alert is subject to throttling, consolidated Alerts will include additional fields showing that the Alert which has been sent is Alert “X” of a throttled sequence, and that it is a consolidation of “Y” Alerts since the previous forwarded Alert. The presence of these fields indicates that throttling is active for the Alert Code in question on that Device.

The specification of where throttling information is included in XML formats is in this document section 9.3.2 (Device Alerts) and 9.3.3 (DCC Alerts), and Annex 19 section 19.4.1 (SMETS1 Alerts).

For XML samples showing the use of throttling in Alerts, see Annex 15 section 15.2.3 (Device Alerts and SMETS1 Alerts) and Annex 16 section 16.2.2 (DCC Alerts).

3 Command Variant

The Command Variant is a common data item included in all DCC Service User Requests to indicate to the DCC Data Systems if a Request has to be:

- transformed to a GBCS Command and returned to the DCC Service User for signing
- sent to the Device via the CSP network
- returned to the DCC Service User to be locally applied (via a Hand Held Terminal)
- sent to the Device via the CSP network and returned to the DCC Service User to be locally applied (via a Hand Held Terminal)
- executed by the DCC Data Systems.

The following sections 3.1 to 3.12 describe the use of Command Variant in connection with SMETS2 or later Devices. The use of Command Variant in connection with SMETS1 Devices accessed via the DCC differs in some respects, and these differences are described in section 3.13.

3.1 Interface Message Types

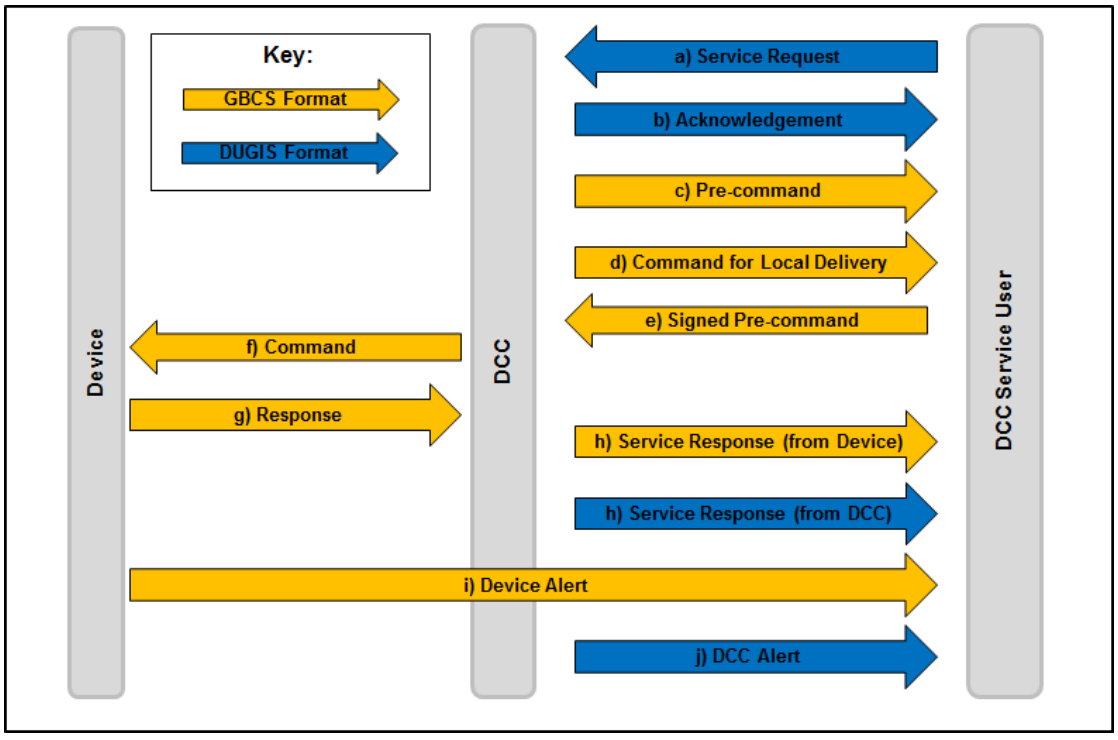


Figure 12 Interface Message Types – SMETS2 or Later

This diagram illustrates the message types supported by the interface.

a) Service Request. A request sent by a DCC Service User to be processed by the DCC Data Systems. Service Requests are listed in section 9.4;

b) Acknowledgement. Synchronous message sent by the DCC Data Systems to the DCC Service User, acknowledging receipt of a Non-Critical Service Request or Signed Pre-Command.

- It is returned when:

- Access Control is successful. In those cases where no other synchronous response is returned
- or Access Control fails. In all Access Control failure scenarios

- It isn't returned when one of the following is returned synchronously in place of the Acknowledgement message:
  - A Pre-Command
  - A Service Response (from DCC)
  - A Command for Local Delivery

c) Pre-Command. Synchronous message sent from the DCC Data Systems to the DCC Service User for digital signing. It includes:

- Command, in the format required by the GBCS (but excluding MAC headers/footers and signatures), prepared in response to a Critical Service Request
- and successful Service Request Acknowledgement

d) Command for Local Delivery. Synchronous or Asynchronous message sent from the DCC Data Systems to the DCC Service User. It includes: (Please note this definition differs from that in the SEC2 Consultation to align with the technical solution)

- Command, in the format required by the GBCS, to be applied locally to the Device
- and successful Service Request or Signed Pre-command Acknowledgement

e) Signed Pre-Command. Pre-Command that has been Digitally Signed by a DCC Service User in relation to a Critical Service Request;

f) Command. Communication sent by the DCC Data Systems to a Device, in the format required by the GBCS. Signed Pre-Commands become Commands once the DCC has applied a Message Authentication Code;

g) Response. Sent by the Device to the DCC Data Systems in reply to a Command;

h) Service Response. Synchronous or Asynchronous message sent by the DCC Data Systems to the DCC Service User, in response to a Service Request. Service Responses may be generated by Devices (in which case they will be in GBCS format), or generated by the DCC Data Systems (in DUIS format), depending on the type of response;

i) Device Alert. Asynchronous message forwarded by the DCC Data Systems in response to a problem or the risk of a potential problem identified by a Device (see GBCS); and

j) DCC Alert. Asynchronous message generated by the DCC Data Systems. It is sub-divided in 2 sub-types (see Table 49~~Table 49~~):

- Alert: Message generated in response to a problem or the risk of a potential problem (e.g. the receipt by the DCC Data Systems of an Alert from a Communications Hub)
- Notification: Message generated in response to an event (e.g. the decommissioning of a Smart Meter Device) triggered within the DCC Data Systems processing

The rest of this document will use the term Request to generically refer to Service Request and Signed Pre-Command messages sent by the DCC Service User to the DCC Data Systems and Response to generically refer to solicited Service Responses and unsolicited Responses (Device Alerts and DCC Alerts) sent to the DCC Service User.

3.2 Command Variant Types

The list of possible Command Variant values, their descriptions, etc. is as follows (see section 3.1 for Interface Message Types); note that this table only covers SMETS2 or later Devices (see section 3.13.2 for applicability to SMETS1 Devices):

CV Value	Command Variant Description	Input	Output	Processing Pattern for DCC Service User	Return to Service User	Delivery Over SM WAN
1	Non Critical Service Request to be sent to a Device via the CSP Communications network	Service Request	Command	Asynch	No	Yes
2	Non Critical Service Request to be returned to the DCC Service User for local delivery to a Device	Service Request	Command for Local Delivery	Synch	Yes	No
3	Non Critical Service Request to be sent to a Device via the CSP Communications network as well as a copy to be returned to the DCC Service User for local delivery	Service Request	Command and Command for Local Delivery	Asynch	Yes (Command for local delivery only)	Yes
4	Transform Service Request and return Pre-command to DCC Service User for Correlation	Service Request	Pre-command	Synch	Yes	No
5	Critical Signed pre command to be sent to a Device via the CSP Communications network	Signed Pre-command	Command	Asynch	No	Yes
6	Critical Signed pre command to be returned to the DCC Service User for local delivery to a Device	Signed Pre-command	Command for Local Delivery	Synch	Yes	No
7	Critical Service Request to be sent to a Device via the CSP Communications network as well as a copy to be returned to the DCC Service User for local delivery.	Signed Pre-command	Command and Command for Local Delivery	Asynch	Yes (Command for local delivery only)	Yes
8	Request a DCC Only Service	Service Request	Service Response (from DCC)	Synch	Yes	No

Table 4 Command Variant Values – SMETS2 or Later

Please note that there is a Command Variant 9 which is generated internally by the DCC Data Systems for DSP Scheduled Requests. This Command Variant value is N/A to Service Requests. Response Code E12 will be returned for Service Requests where the Command Variant is 9.

The following sections describe the message types and interactions for the different Command Variant Values. The Access Control failure scenario is applicable to all cases and is described separately (see section 3.11.1 for CV = 1, 2, 3, 4 or 8 Access Control failure and section 3.11.2 for CV = 5, 6 or 7 Access Control failure).

3.3 CV = 1 (Non-Critical Service Request – Send Command over SM WAN)

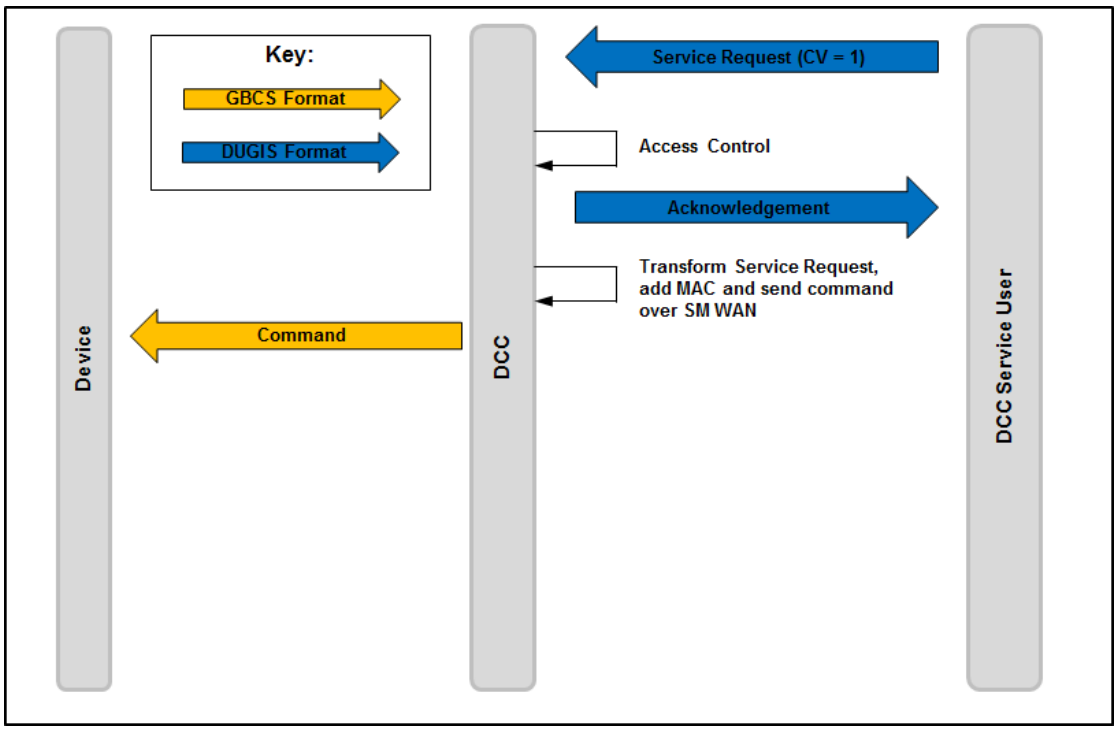


Figure 13 Command Variant = 1

Possible Service Responses:

- Service Response (from Device) if the Command is executed by the device
- Device Alert, if the Device rejects the Command, e.g. because it doesn't recognise the sender
- DCC Alert, if the Command fails to be delivered (see Table 49~~Table 49~~ DCC Alert Code N12)

3.4 CV = 2 (Non-Critical Service Request – Return Command for Local Delivery)

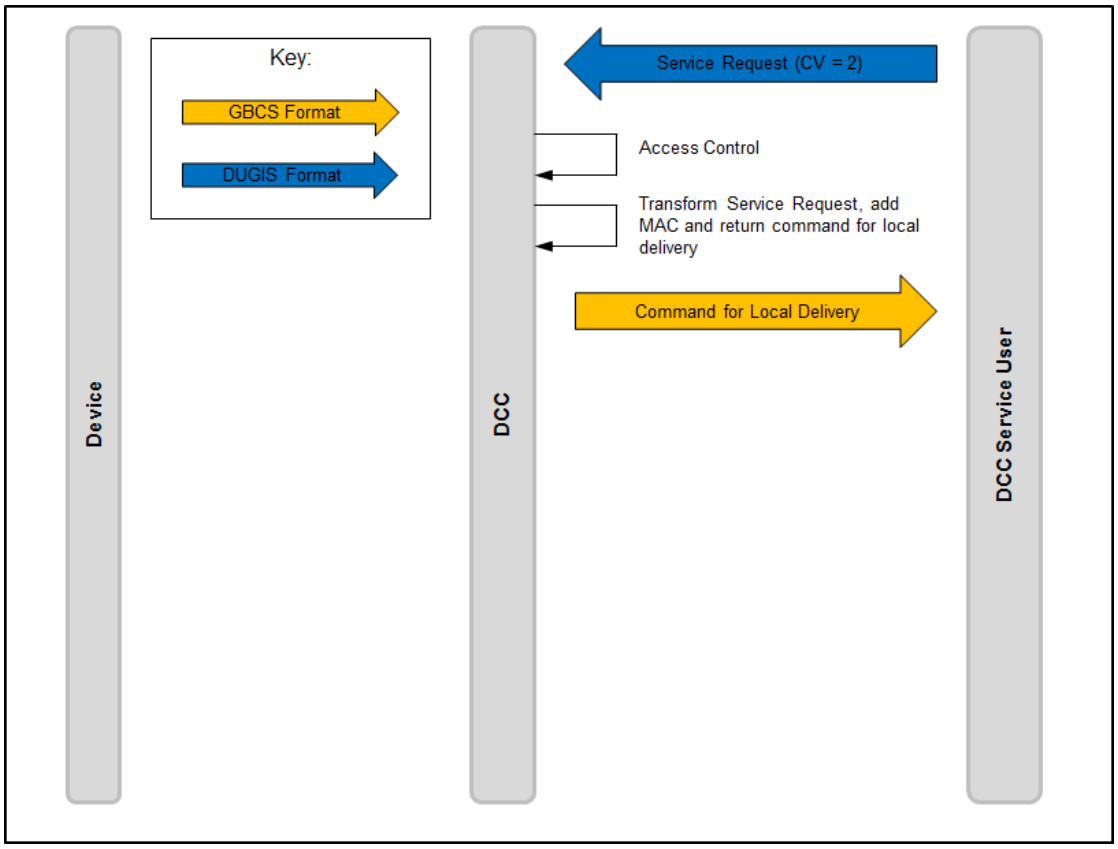


Figure 14 Command Variant = 2

Possible Service Responses:

- From DCC: Returning the Command for Local Delivery to the DCC Service User is the Service Response
- From DCC Service Users: After the Command has been applied locally, the DCC Service Users can upload the subsequent GBCS format response message from the Device to the DCC Data Systems via the “Return Local Command Response” (8.13) Service Request. Note that for certain Service Requests the DCC Service User **must** return the locally applied Command response to the DCC Data Systems. Please see Annex for a definition of Service Requests where this is required,
- From Device: If the SM WAN is available when the Device returns the Command Response to the Communications Hub during local delivery, it will be returned to the DCC Data Systems via the SM WAN channel and it will be processed as if the Command had been sent to the Device via the SM WAN. The DCC Data Systems will forward this message to the DCC Service Users as a Service Response (from Device).

3.5 CV = 3 (Non-Critical Service Request – Send Command over SM WAN and Return for Local Delivery)

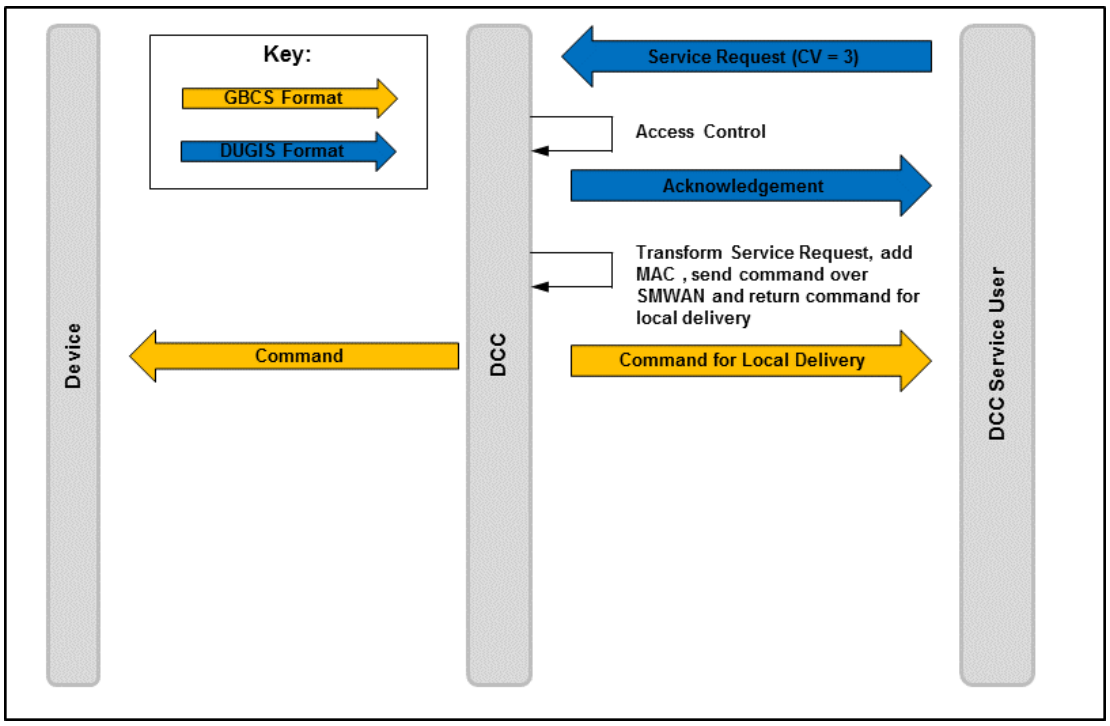


Figure 15 Command Variant = 3

Possible Service Responses:

- Command sent over SM WAN
    - Service Response (from Device) if the command is executed by the device
    - Device Alert, if the Device rejects the command, e.g. because it doesn't recognise the sender
    - DCC Alert, if the command fails to be delivered (see Table 49~~Table 49~~ DCC Alert Code N12)
- Command Delivered Locally
    - Returning the Command for Local Delivery to the DCC Service User is not the Service Response. The Service Users should only apply this command to the device if they receive no response to the Command sent over SM WAN. If the Command is delivered locally, its possible responses are as defined in section 3.4.

3.6 CV = 4 (Transform Service Request – Return Pre-Command)

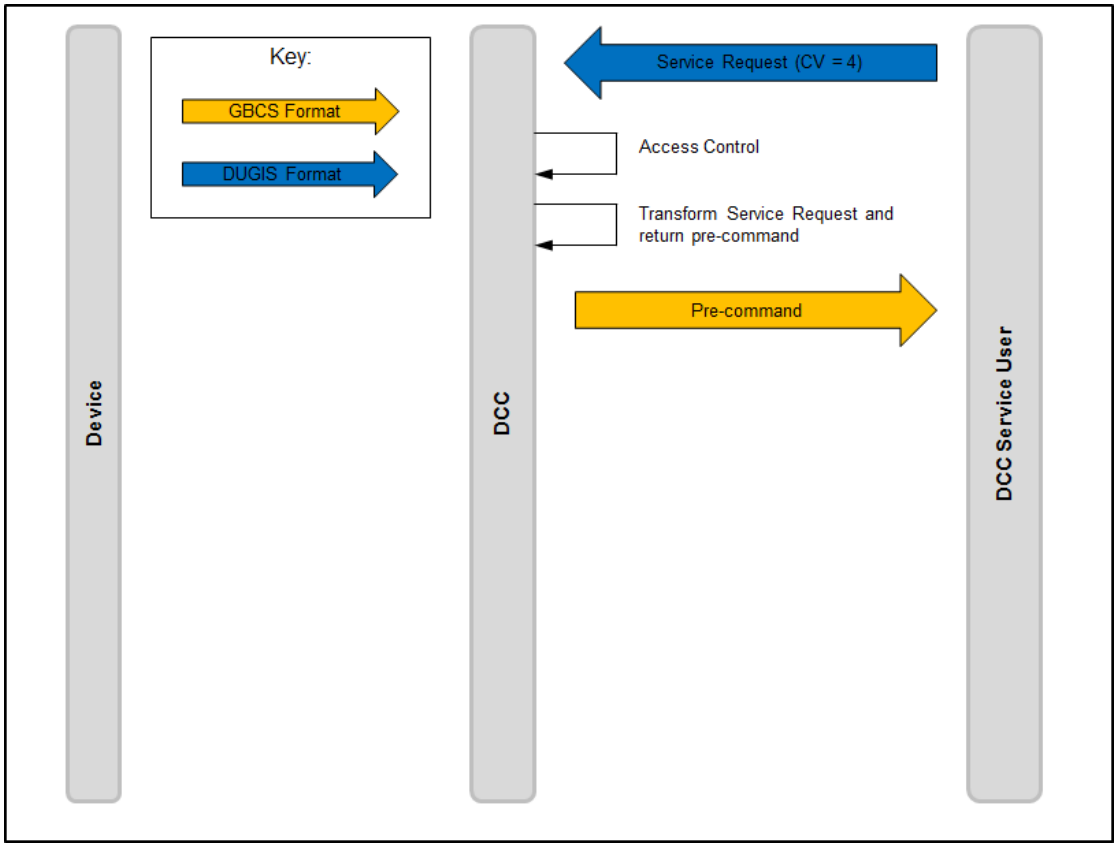


Figure 16 Command Variant = 4

Possible Service Responses:

- The Pre-command returned to the DCC Service User is the Service Response

3.7 CV = 5 (Signed Pre-command – Send Command over SM WAN)

The diagram includes the transformation of the Service Request to a Pre-command (CV = 4) as well as the CV = 5 itself.

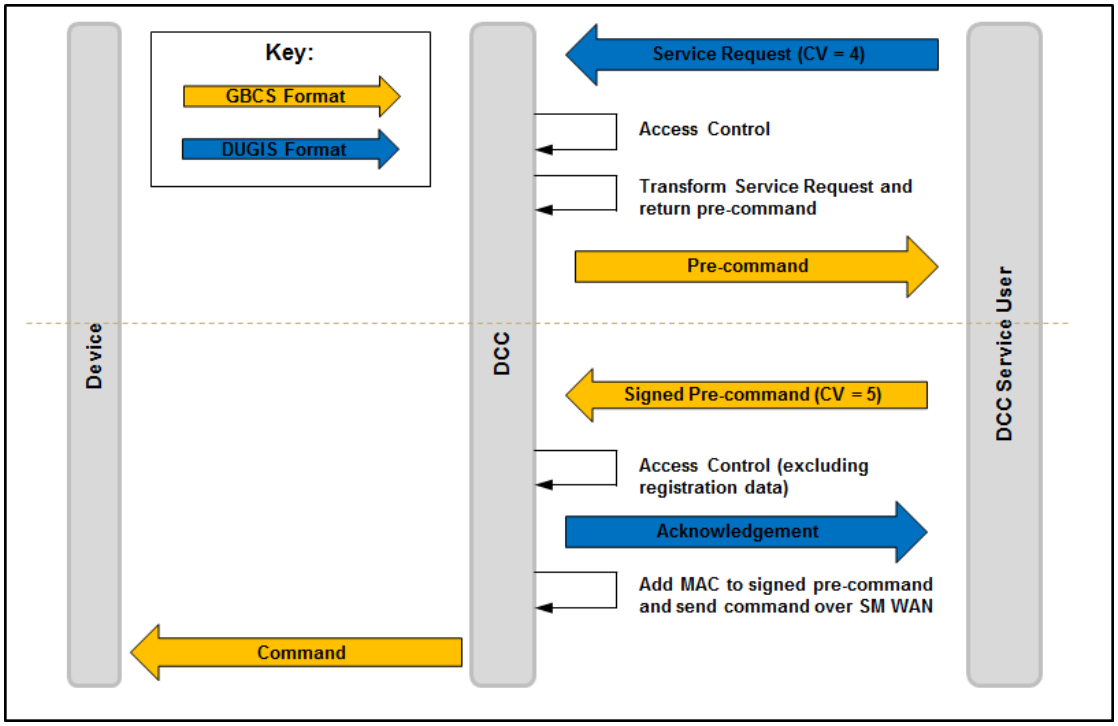


Figure 17 Command Variant = 4 and 5

Possible CV = 5 Service Responses (see section 3.6 for CV = 4 details):

- Service Response (from Device) if the Command is executed by the device
- Device Alert, if the Device rejects the Command, e.g. because it doesn't recognise the sender
- DCC Alert, if the Command fails to be delivered (see Table 49~~Table 49~~ DCC Alert Code N12)

3.8 CV = 6 (Signed Pre-command – Return Command for Local Delivery)

The diagram includes the transformation of the Service Request to a Pre-command (CV = 4) as well as the CV = 6 itself.

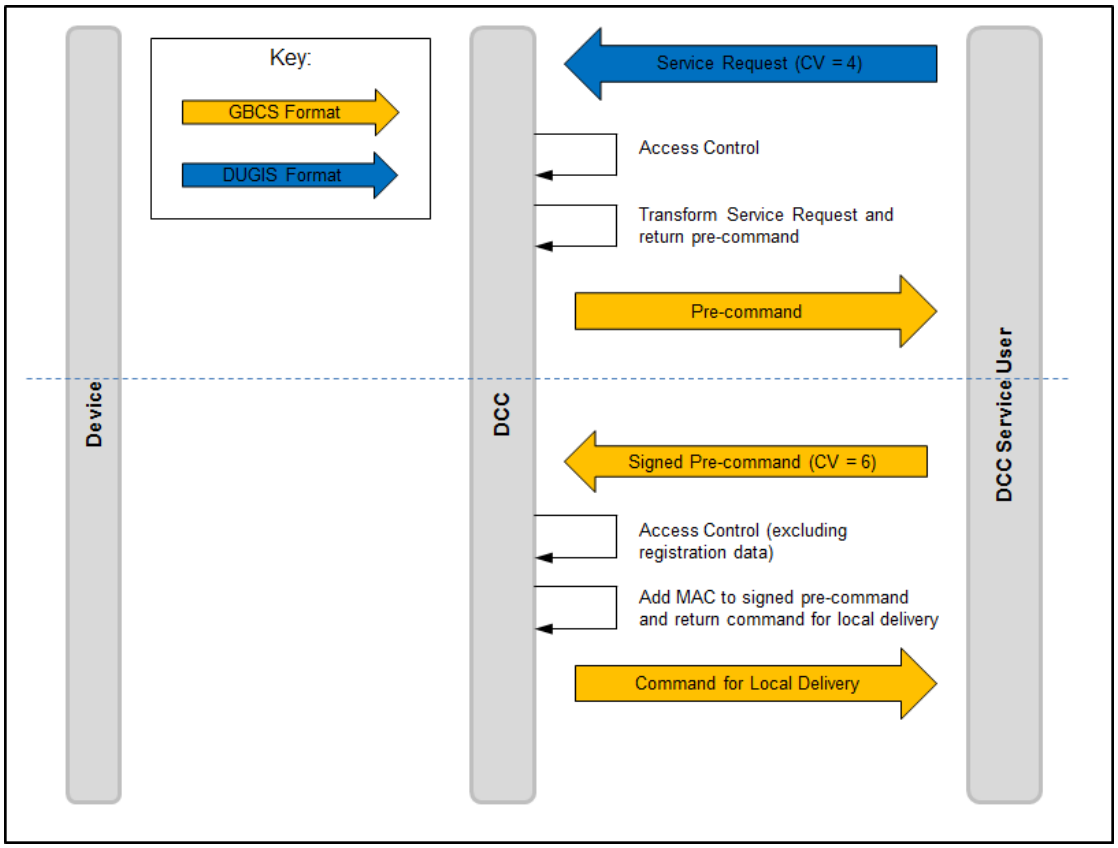


Figure 18 Command Variant = 4 and 6

See section 3.6 for CV = 4 Service Responses.

The Service Responses applicable to CV = 6 are those described in section 3.4.

3.9 CV = 7 (Signed Pre-command – Send Command over SM WAN and Return for Local Delivery)

The diagram includes the transformation of the Service Request to a pre-command (CV = 4) as well as the CV = 7 itself.

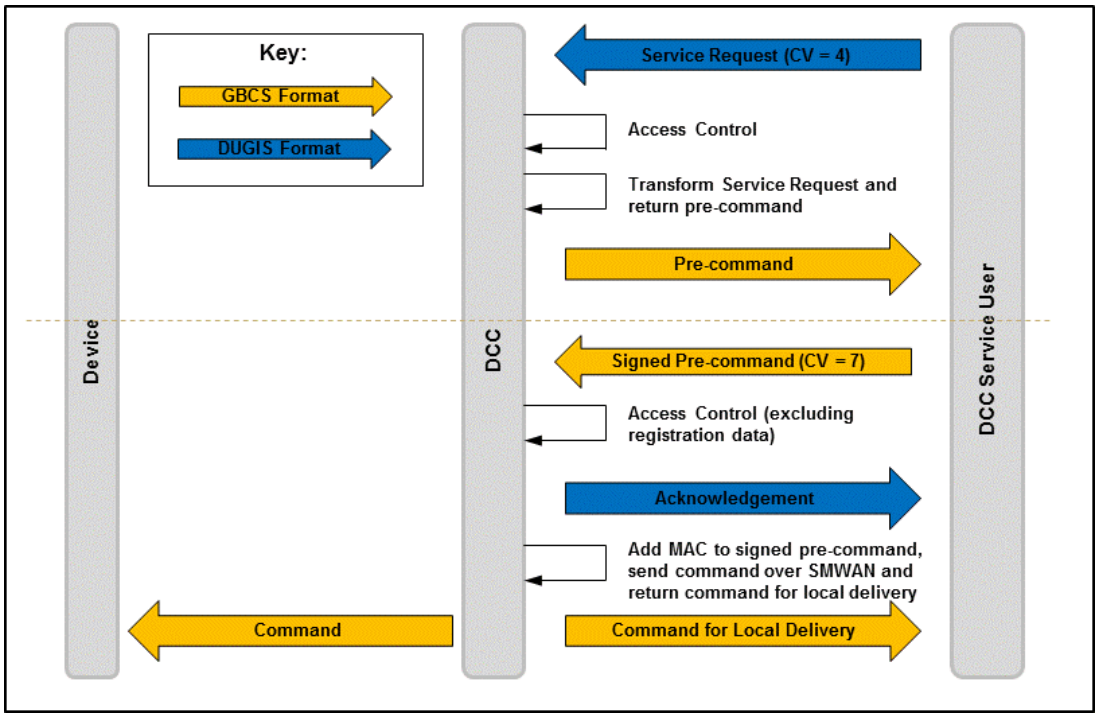


Figure 19 Command Variant = 4 and 7

Possible CV = 7 Service Responses (see section 3.6 for CV = 4 details):

- Command sent over SM WAN
  - Service Response (from Device) if the Command is executed by the device
  - Device Alert, if the Device rejects the Command, e.g. because it doesn't recognise the sender
  - DCC Alert, if the Command fails to be delivered (see Table 49~~Table 49~~ DCC Alert Code N12)
- Command Delivered Locally
  - Returning the Command for Local Delivery to the DCC Service User is not the Service Response. The Service Users should only apply this command to the device if they receive no response to the Command sent over SM WAN. If the Command is delivered locally, its possible responses are as defined in section 3.4.

3.10 CV = 8 (DCC Only Service Request – Service Response Returned)

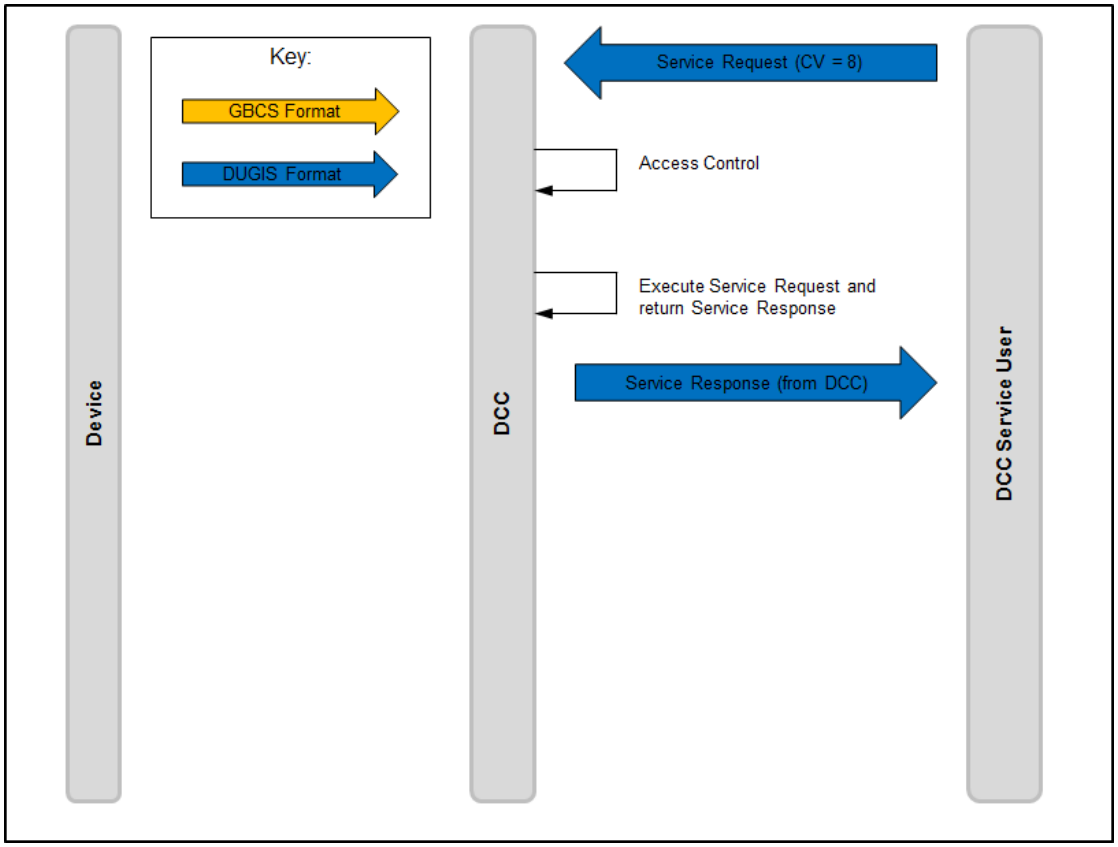


Figure 20 Command Variant = 8

Possible Service Responses:

- The Service Response (from DCC) is the Service Response

3.11 Access Control Failure

3.11.1 CV = 1, 2, 3, 4 or 8 Access Control Failure

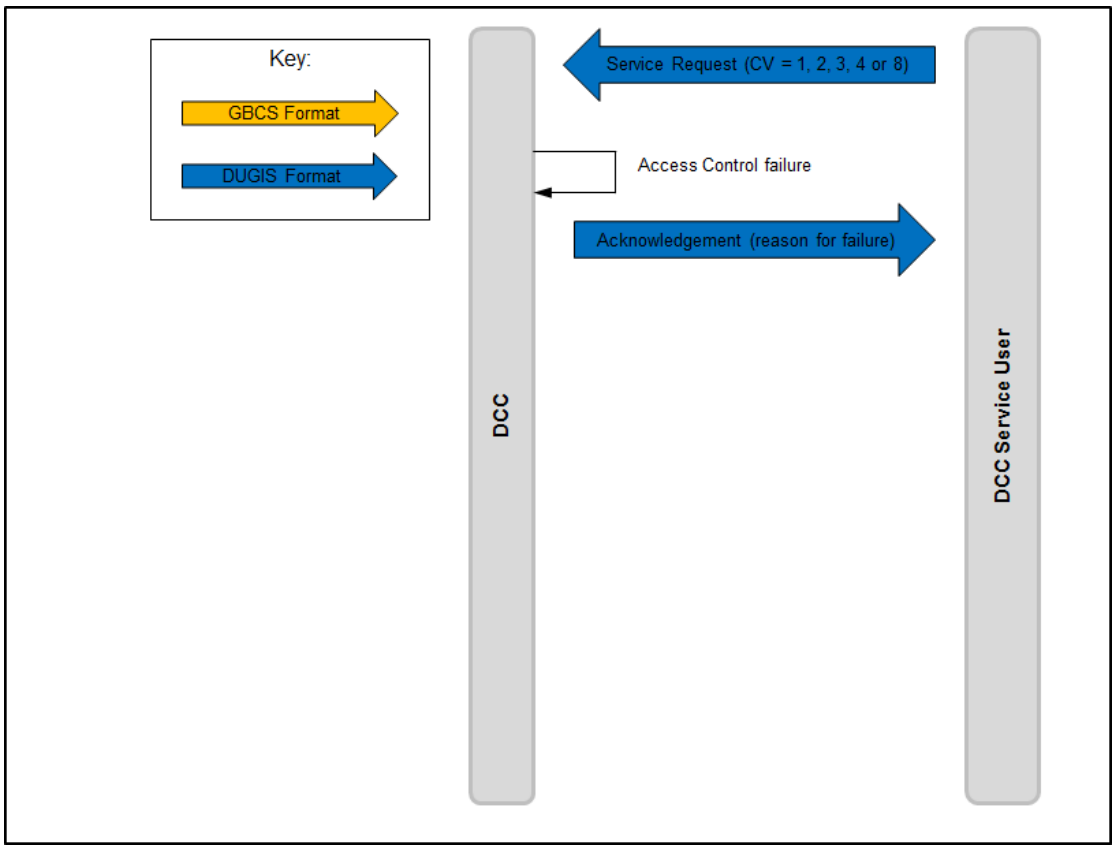


Figure 21 Command Variant = 1, 2, 3, 4 or 8 Access Control Failure

Possible Service Responses:

- The Acknowledgement message, which includes the reason why the Service Request failed Access Control (Response Code), is the Service Response

3.11.2 CV = 5, 6 or 7 Access Control Failure

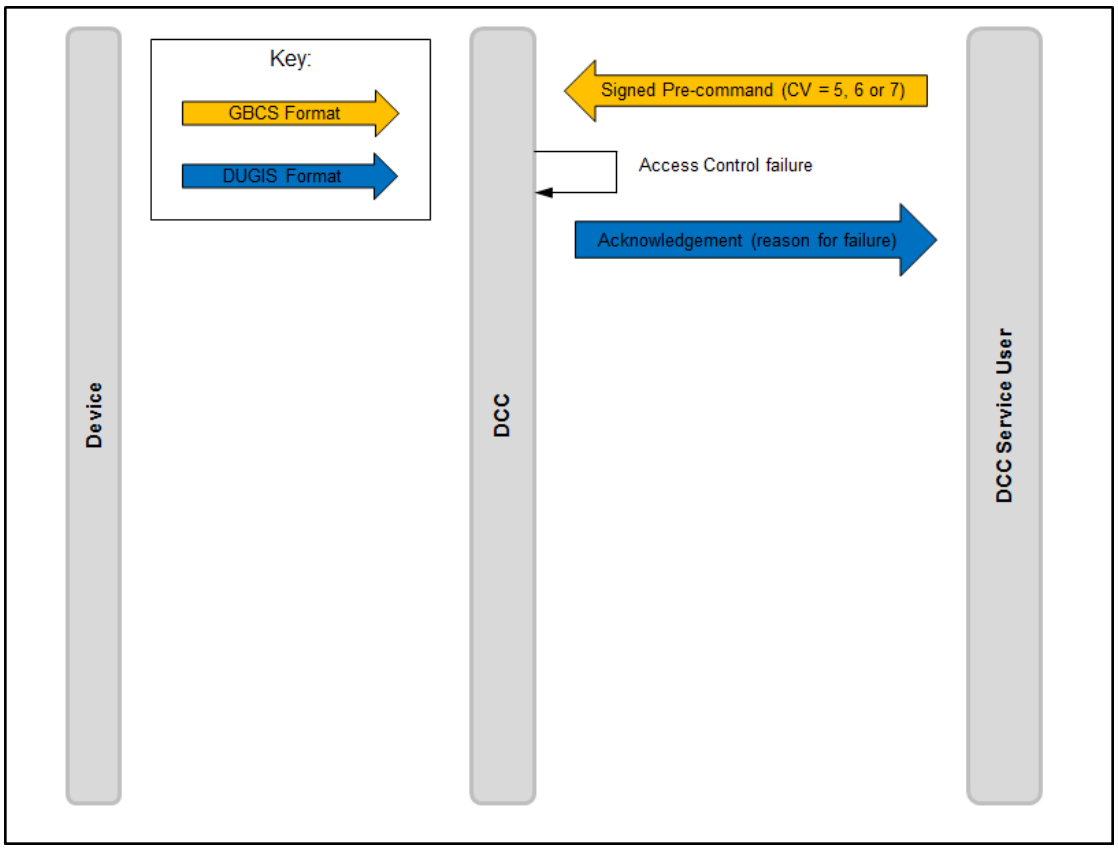


Figure 22 Command Variant = 5, 6 or 7 Access Control Failure

Possible Service Responses:

- The Acknowledgement message, which includes the reason why the Signed Pre-command failed Access Control (Response Code), is the Service Response

3.12 Command Variant / Mode of Operation and Web Services

The following table describes the relationship between a Request's Command Variant, Mode of Operation (see section 2.3) and Web Services (see section 0) (see section 3.13.3 for applicability to SMETS1 Devices):

Command Variant	Mode of Operation	Web Services	
		Request	Response
1	"On Demand", "Future Dated (DSP)"	Send Command Service	Receive Response Service
2[2]	"On Demand" [1]	DCC Only Service	Completion of DCC Only Service
3	"On Demand" [1]	Send Command Service	Receive Response Service
4	"Transform"	Transform Service	Completion of Transform Service
5	"On Demand", "Future Dated (Device)"	Send Command Service	Receive Response Service
6[2]	"On Demand" [1]	DCC Only Service	Completion of DCC Only Service
7	"On Demand" [1]	Send Command Service	Receive Response Service
8	"DCC Only"	DCC Only Service	Completion of DCC Only Service
N/A	"Meter Scheduled"	N/A	Receive Response Service
N/A	"DSP Scheduled"	N/A	Receive Response Service
N/A	"Device Alert"	N/A	Receive Response Service
N/A	"DCC Alert"	N/A	Receive Response Service

Table 5 Command Variant, Mode of Operation and Web Services – SMETS2 or Later

[1] "In those cases where a Command for Local Delivery is returned to the DCC Service User, the definition of "On Demand" is extended to "A Non-Critical Service Request or signed Pre-Command (for Critical Service Requests) is sent to the Device / returned to the DCC Service User immediately and, if sent to the device via SM WAN, the device returns a Service Response."

[2] Although Mode Of Operation is "On Demand" (since the command is ultimately delivered locally to a Device), the initial interaction with the DCC follows the same processing pattern as "DCC Only" and hence uses the "DCC Only "services.

3.13 Command Variants and SMETS1 Devices

This section describes differences in the use of Command Variant in connection with SMETS1 Devices, as an addendum to usage with SMETS2 or later Devices as described in sections 3.1 to 3.12.

3.13.1 SMETS1 Interface Message Types

Message types in section 3.1 apply to SMETS1 Devices apart from exceptions as noted in this section.

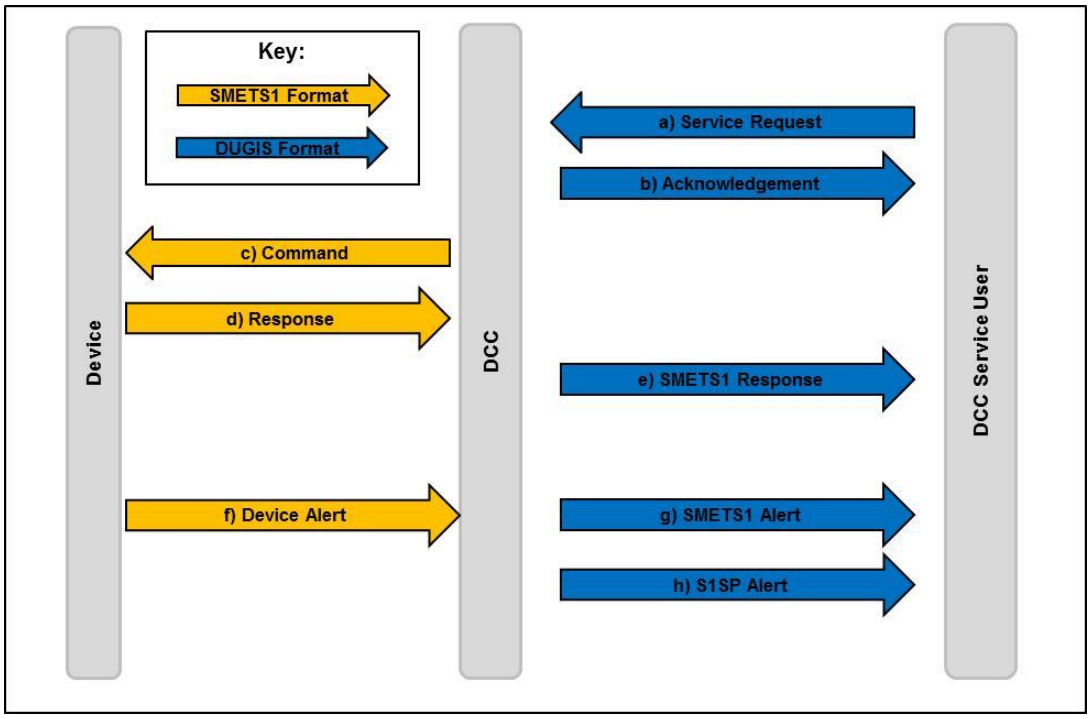


Figure 23 Interface Message Types – SMETS1

The following differences in message types and terminology are applicable to SMETS1 Devices:

- Countersigned SMETS1 Response. Synchronous or Asynchronous message sent by the DCC Data Systems to the DCC Service User, in response to a Service Request. A Countersigned SMETS1 Response wraps a SMETS1 Response provided by an S1SP. Where the term Service Response is used within DUGIDS it may, depending on the context, include Countersigned SMETS1 Responses;

- Countersigned SMETS1 Alert. Asynchronous message sent by the DCC Data Systems to the DCC Service User which wraps a SMETS1 Alert provided by an S1SP (see section 2.3.8). Where the term Device Alert is used within DUGIDS it may, depending on the context, include Countersigned SMETS1 Alerts;

- Countersigned S1SP Alert. Asynchronous message sent by the DCC Data Systems to the DCC Service User which is a DCC Alert with a DCC Alert Code that indicates it carries an S1SP Alert within it; an S1SP Alert is an asynchronous message signed by an S1SP. Where the term DCC Alert is used within DUGIDS it may, depending on the context, include Countersigned S1SP Alerts;

- Command. Although defined in connection with GBCS, as in section 3.1, this term shall also be used in DUGIDS, where applicable according to context, to mean a communication sent by the DCC Data Systems to a Device in a format required by SMETS1.

The following message types from section 3.1 do not apply to SMETS1 Devices:

- Pre-Command;

- Command for Local Delivery;
- Signed Pre-Command.

3.13.2 SMETS1 Command Variant Types

Note that in the following table "Command" should be interpreted as meaning SMETS1 formats, since they are in connection with SMETS1 Devices, instead of GBCS, as explained in section 3.13.1. That is generally the case throughout DUGIDS.

CV Value	Command Variant Description	Input	Output	Processing Pattern for DCC Service User	Return to Service User	Delivery Over SM WAN
1	Non Critical Service Request to be sent to a SMETS1 Device via the S1SP communications network	Service Request	Command	Asynch	No	Yes
2	SRV 2.2: SRV-specific redefinition for SMETS1 Devices; see Annex Section 2. N/A otherwise	Service Request	S1SP Alert	Asynch	Yes	No
3	SRV 2.2: SRV-specific redefinition for SMETS1 Devices; see Annex Section 2. N/A otherwise	Service Request	S1SP Alert and Command	Asynch	Yes (S1SP Alert only)	Yes
4	Send SMETS1 Critical Service Request to a SMETS1 Device via the S1SP communications network	Service Request	Command	Asynch	No	Yes
5	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A
8	Request a DCC Only Service	Service Request	Service Response (from DCC)	Synch	Yes	No

Table 6 Command Variant Values – SMETS1

3.13.3 SMETS1 Command Variant / Mode of Operation and Web Services

The following table describes the relationship between a Request's Command Variant, Mode of Operation (see section 2.3) and Web Services (see section 00) in connection with SMETS1 Devices (see section 3.12 for SMETS2 or later Devices):

Command Variant	Mode of Operation	Web Services	
		Request	Response
1	"On Demand", "Future Dated (DSP)"	Send Command Service	Receive Response Service
2 (SRV2.2 only)	"On Demand"	DCC Only Service	Receive Response Service
3 (SRV2.2 only)	"On Demand"	Send Command Service	Receive Response Service
4	"On Demand", "Future Dated (Device[1])"	Transform Service	Receive Response Service
8	"DCC Only"	DCC Only Service	Completion of DCC Only Service
N/A	"DSP Scheduled"	N/A	Receive Response Service
N/A	"Device Alert" (used for SMETS1 Alerts)	N/A	Receive Response Service
N/A	"DCC Alert" (including S1SP Alert)	N/A	Receive Response Service

Table 7 Command Variant, Mode of Operation and Web Services – SMETS1

[1] Future dating for Future Dated (Device) Service Requests targeted at SMETS1 Devices is implemented by DCC Data Systems

4 Request and Response IDs

Where a DCC Service User sends a Service Request or a Signed Pre-Command, the DCC Service User shall ensure that it contains a unique message identifier. This unique message identifier is the Request ID.

Each Request includes a unique Request ID. Depending on the interaction type, each Response includes the corresponding Request ID and / or a unique Response ID. See Table 8~~Table 8~~ for details.

Request and Response IDs are defined by GBCS. In line with the GBCS Message Identifier, both Request and Response IDs consist of 3 elements (concatenated with ":") both for "Device Services" and "Non-Device Services":

- Business Originator ID
- Business Target ID
- Originator Counter (the sender of the Request (DCC Service User or DSP Broker) needs to control the Originator Counter as per GBCS and keep incrementing it – does not need to be contiguous).

For Critical Service Requests for SMETS2 or later devices, the same Request ID is submitted twice. The first time to transform the Service Request into a Pre-command and the second time to send the Signed Command to the Device. See Table 8~~Table 8~~ for Response ID details.

For solicited Service User Device Requests for which the DCC Data Systems identify an issue, e.g. Command can't be delivered, the DCC will return a DCC Alert to the DCC Service User, with a DSP Broker Response ID different from that of the Service User request ID. In these cases, the Request ID of the DCC Service User Request will be part of the message payload.

Although SMETS1 Devices do not use GBCS, the SMETS1 Service Requests shall use the same format of Request and Response IDs in order to ensure commonality across the DCC User Interface. See Table 9~~Table 9~~ in section 4.19 to see how Request and Response IDs are applied to SMETS1 Devices.

The following table lists Request and Response IDs content in DUIS format (XML) for the different interaction types. Note that in some cases there are multiple interaction types for a single Command Variant, since the behaviour is different depending on whether the Service Request is being sent by a DCC Service User which is a Known Remote Party (KRP) or Unknown Remote Party (URP) to the Device. Where the DCC Service User is an Unknown Remote Party then the DSP Broker carries out the request on behalf of the DCC Service User. The BusinessOriginatorID and OriginatorCounter from within the RequestID contained within the DUIS XML format message shall be replaced with those used by the Access Control Broker required to enable communication with the Device and the original values provided by the User are transferred to the otherInformation field within the Command's GroupingHeader as defined by GBCS (added to Supplementary Remote Party ID and Supplementary Remote Party Counter respectively). The BusinessTargetID remains unchanged.

This table is applicable to SMETS2 or later Devices. See section 4.19 for information on applicability to SMETS1 Devices.

Request ID				Response ID				Response includes Request ID	Interaction Type
CV Type	Business Originator ID	Business Target ID	Originator Counter	Type	Business Originator ID	Business Target ID	Originator Counter		
1	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (KRP) – Command Response

Request ID				Response ID				Response includes Request ID	Interaction Type
CV Type	Business Originator ID	Business Target ID	Originator Counter	Type	Business Originator ID	Business Target ID	Originator Counter		
									(see section 4.1)
N/A	N/A	N/A	N/A	Future Dated Device Alert (unsolicited response to Service User)[5]	Device ID	DCC Service User ID	Device Originator Counter	Yes	Send Command and Receive Response (KRP) – FDEDA[4] (see section 4.2)
1	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (URP) (see section 4.3)
N/A	N/A	N/A	N/A	Future Dated Device Alert (unsolicited response to Service User)[5]	Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (URP) – FDEDA[6] (see section 4.4)
2	DCC Service User ID	Device ID	Service User Originator Counter	Command for Local Delivery (from DCC)	N/A	N/A	N/A	Yes	Return Command for Local Delivery (KRP) (see section 4.5)
2	DCC Service User ID	Device ID	Service User Originator Counter	Command for Local Delivery (from DCC)	N/A	N/A	N/A	Yes	Return Command for Local Delivery (URP) (see section 4.6)
3	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device) / Command for Local Delivery (from DCC)	Request's Device ID / N/A	Request's Service User ID / N/A	Request's Originator Counter / N/A	Yes / Yes	Send Command and Return for Local Delivery (KRP) (see section 4.1 and 4.7)
3	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device) / Command for Local Delivery (from DCC)	Request's Device ID / N/A	DSP Broker / N/A	Command's Originator Counter / N/A	Yes / Yes	Send Command and Return for Local Delivery (URP) (see section 4.3 and 4.8)
4	DCC Service User ID	Device ID	Service User Originator Counter	Pre-command (from DCC)	N/A	N/A	N/A	Yes	Transform Command (KRP) (see section 4.9)

Request ID				Response ID				Response includes Request ID	Interaction Type
CV Type	Business Originator ID	Business Target ID	Originator Counter	Type	Business Originator ID	Business Target ID	Originator Counter		
5	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Transformed Send Command and Receive Response (KRP) (see section 4.10)
N/A	N/A	N/A	N/A	Future Dated Device Alert (unsolicited response to Service User)[5]	Device ID	DCC Service User ID	Device Originator Counter	Yes	Transformed Send Command and Receive Response (KRP) – FDEDA[4] (see section 4.11)
6	DCC Service User ID	Device ID	Service User Originator Counter	Command for Local Delivery (from DCC)	N/A	N/A	N/A	Yes	Transform and Return Command for Local Delivery (KRP) (see section 4.12)
7	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device) / Command for Local Delivery (from DCC)	Request's Device ID / N/A	Request's Service User ID / N/A	Request's Originator Counter / N/A	Yes / Yes	Transformed Send and Return Command for Local Delivery (KRP) (see section 4.10 and 4.13)
8	DCC Service User ID	DSP Broker ID	Service User Originator Counter	Service Response (from DCC)	N/A	N/A	N/A	Yes	DCC Only (see section 4.14)
N/A	N/A	N/A	N/A	Device Alert (unsolicited response to Service User)[7]	Device ID	DCC Service User ID	Device Originator Counter	No	Device Alert (see section 4.15)
N/A	N/A	N/A	N/A	DCC Alert (unsolicited response to Service User)	DSP Broker ID	DCC Service User ID	DSP Broker Originator Counter	No	DCC Alert (see section 4.16)
9[1]	DSP Broker ID[2]	Device ID[2]	DSP Broker Originator Counter[2]	Service Response (from Device)[3]	Request's Device ID	DSP Broker ID	Request's DSP Broker Originator Counter	Yes[2]	DSP Scheduled Command and Response (see section 4.17)

Table 8 Request and Response IDs – SMETS2 or later Devices

[1] Command Variant 9 is an internal only value used for DSP Scheduled Command to a Device

[2] The Request ID is generated by the DSP Broker and included in the GBCS Command to the Device

[3] The Response XML and GBCS Payload include the DSP Schedule ID

[4] The Device holds the Remote Party ID, Message Code and Future Dated Counter (= Originator Counter) of the Command to be executed

[5] The Device Alert Payload includes the Command Message Code and Originator Counter of the executed Command

[6] This interaction is only applicable to Service Request 6.23 (Update Security Credentials (CoS)). The Device holds the Remote Party ID (CoS Party), Message Code and Future Dated Counter (= Originator Counter) of the Command to be executed. The DCC Data Systems hold the relationship between the Service Request ID (from the DCC Service User) and the Command (from the CoS Party)

[7] For Device Alerts with 2 recipients (as defined by GBCS), the second recipient's Response ID is: Business Originator ID = Device ID, Business Target ID = Device Alert Supplementary Remote Party ID, Originator Counter = Device Originator Counter

The following diagrams illustrate the content of Request and Response IDs in all the interaction types. The values in the diagrams indicate the originator and target rather than their IDs. See section 3 for Command Variants applicable to each case.

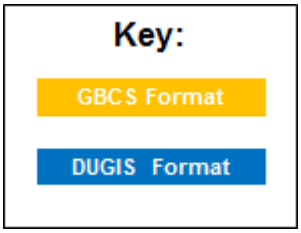


Figure 24 Request and Response IDs Diagrams Key

4.1 Send Command and Receive Response (KRP) – Command Response

Applicable to Non-Critical Service Requests Commands from a KRP delivered via SM WAN, where the response is either to an On Demand Command or the Device acceptance of a Future Dated (Device) Command. See section 4.2 for the Device Alert returned when the Future Dated (Device) Command is executed by the Device.

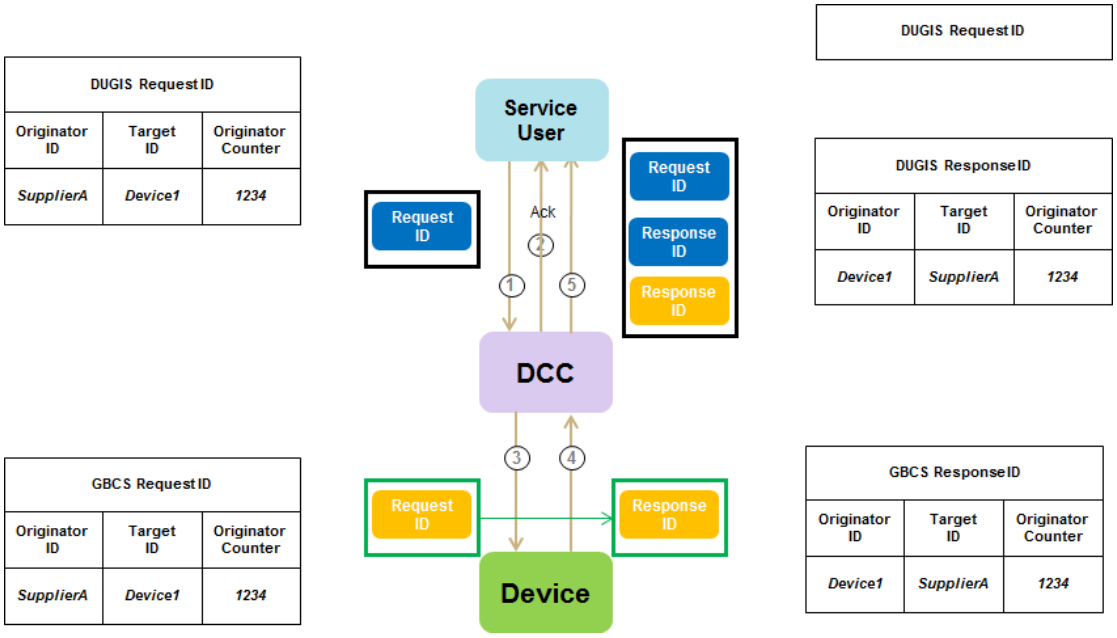


Figure 25 Send Command and Receive Response (KRP) – Command Response

Note that the synchronous Acknowledgement response (flow 2 on the diagram) returns only the original DUIS Request ID.

4.2 Send Command and Receive Response (KRP) – FDEDA

Applicable to Non-Critical Service Requests Commands from a KRP delivered via SM WAN, where the response is the Future Dated (Device) Execution Device Alert (FDEDA).

There are currently no instances of this interaction.

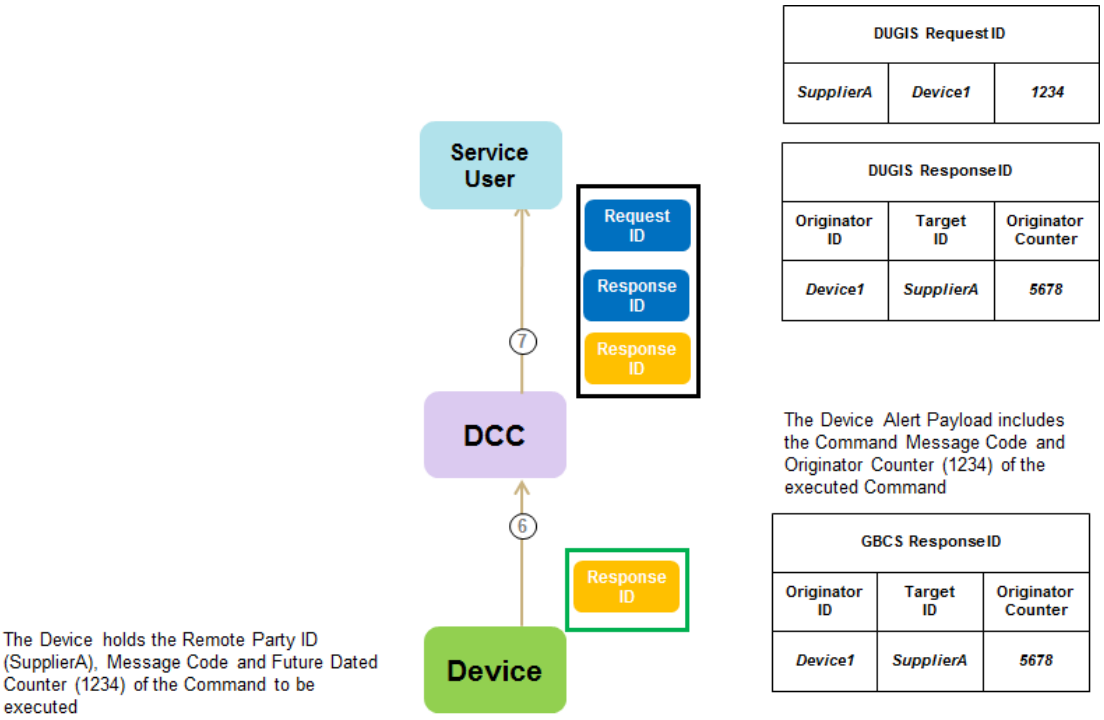


Figure 26 Send Command and Receive Response (KRP) – FDEDA

4.3 Send Command and Receive Response (URP)

Applicable to Non-Critical Service Requests Commands from a URP delivered via SM WAN. Also applicable to Service Requests 6.21 (Request Handover Of DCC Controlled Device) and 8.5 (Service Opt Out), because even though the DCC Service User submitting the Service

Request to the DCC Data Systems is a KRP, the Command is Critical and has to be digitally signed by the DSP Broker.

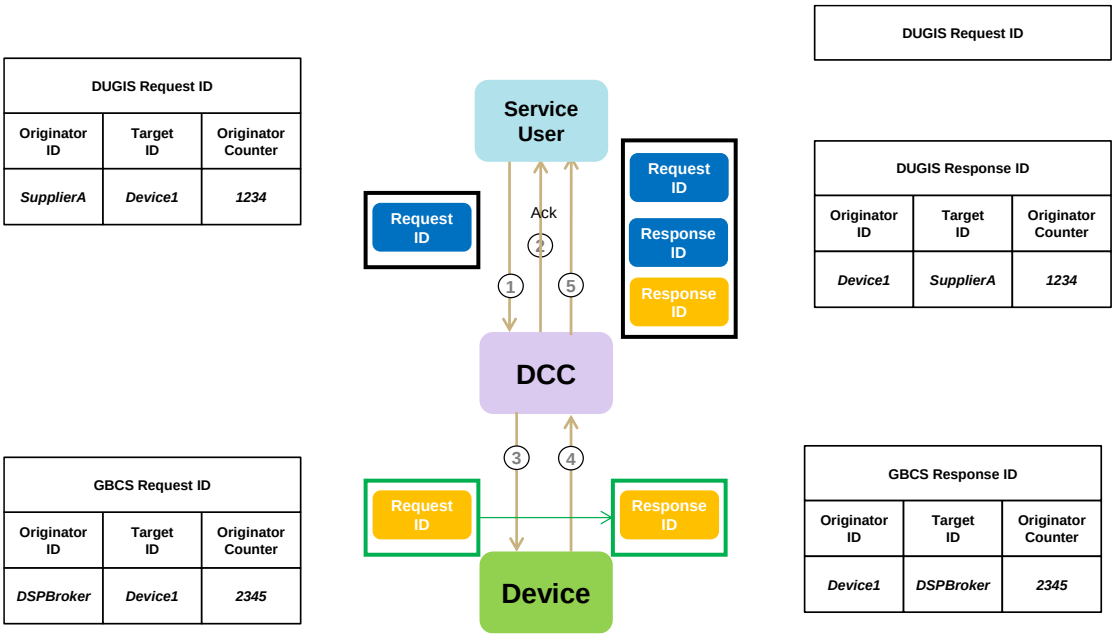


Figure 27 Send Command and Receive Response (URP)

4.4 Send Command and Receive Response (URP) – FDEDA

Applicable to Non-Critical Service Requests Commands from a URP delivered via SM WAN, where the response is the Future Dated (Device) Execution Device Alert (FDEDA).

The only instance of this interaction is Service Request 6.23 (Update Security Credentials (CoS)).

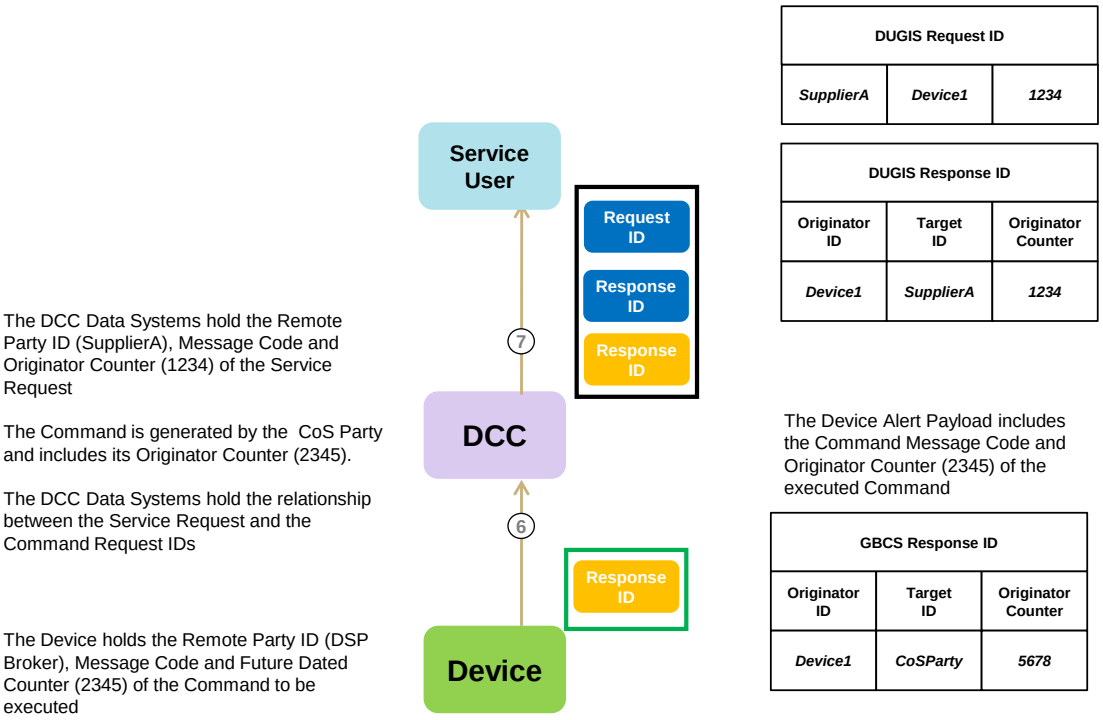


Figure 28 Send Command and Receive Response (URP) – FDEDA

4.5 Return Command for Local Delivery (KRP)

Applicable to Non-Critical Service Request Commands from a KRP returned to the DCC Service User for Local Delivery.

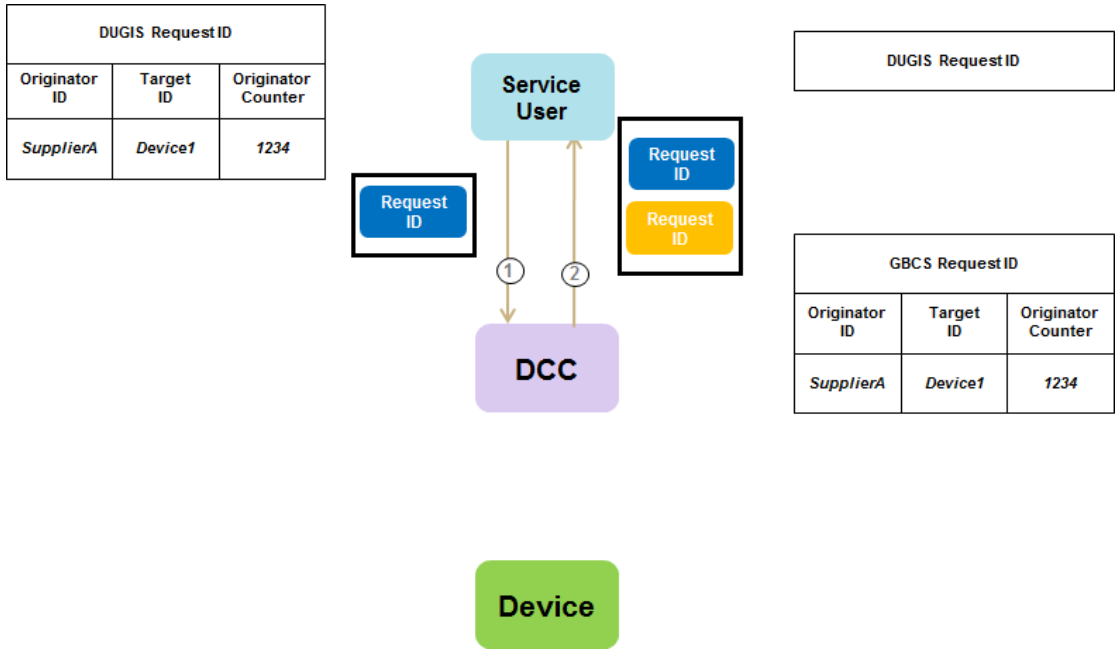


Figure 29 Return Command for Local Delivery (KRP)

4.6 Return Command for Local Delivery (URP)

Applicable to Non-Critical Service Request Commands from a URP returned to the DCC Service User for Local Delivery.

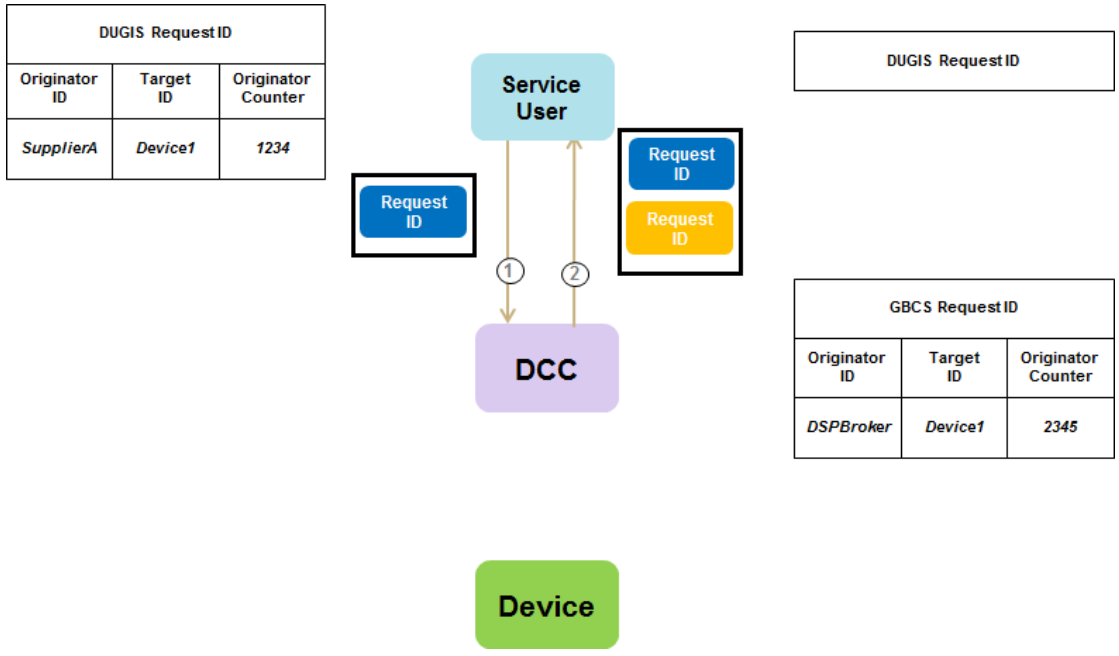


Figure 30 Return Command for Local Delivery (URP)

4.7 Send Command and Return for Local Delivery (KRP)

Applicable to Non-Critical Service Request Commands from a KRP delivered via SM WAN and returned to the DCC Service User for Local Delivery.

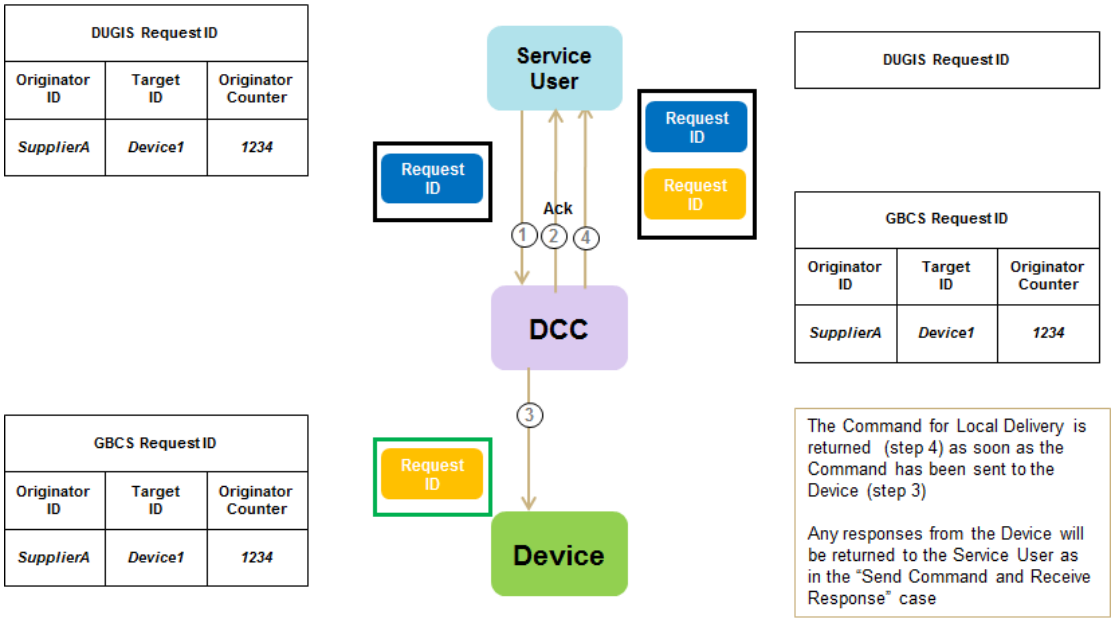


Figure 31 Send Command and Return for Local Delivery (KRP)

4.8 Send Command and Return for Local Delivery (URP)

Applicable to Non-Critical Service Request Commands from a URP delivered via SM WAN and returned to the DCC Service User for Local Delivery.

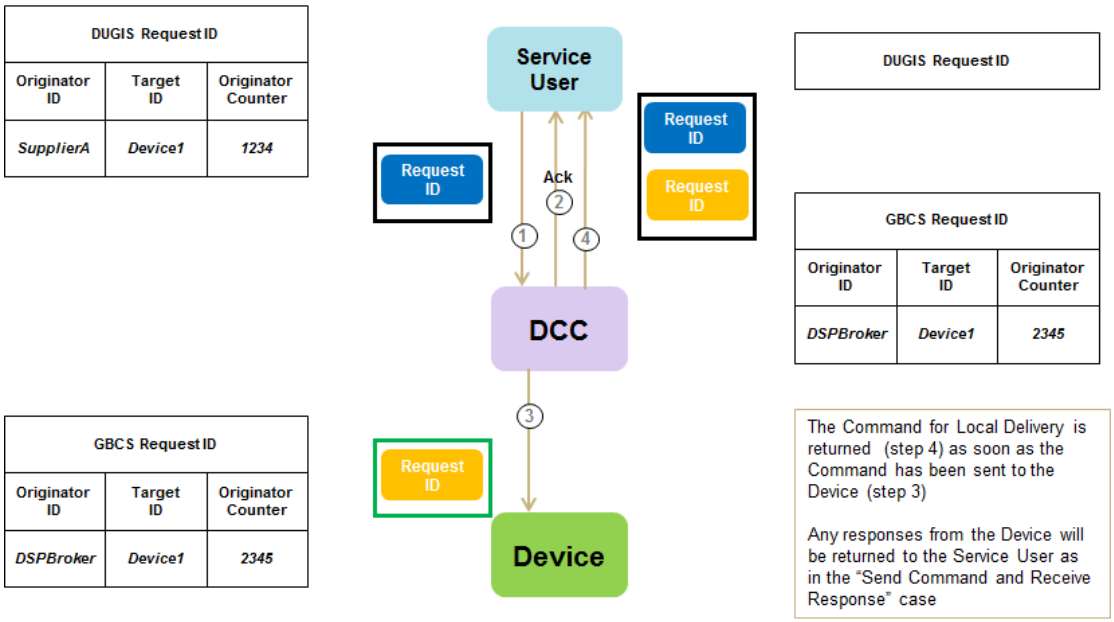


Figure 32 Send Command and Return for Local Delivery (URP)

4.9 Transform Command (KRP)

Applicable to Critical Service Request Commands.

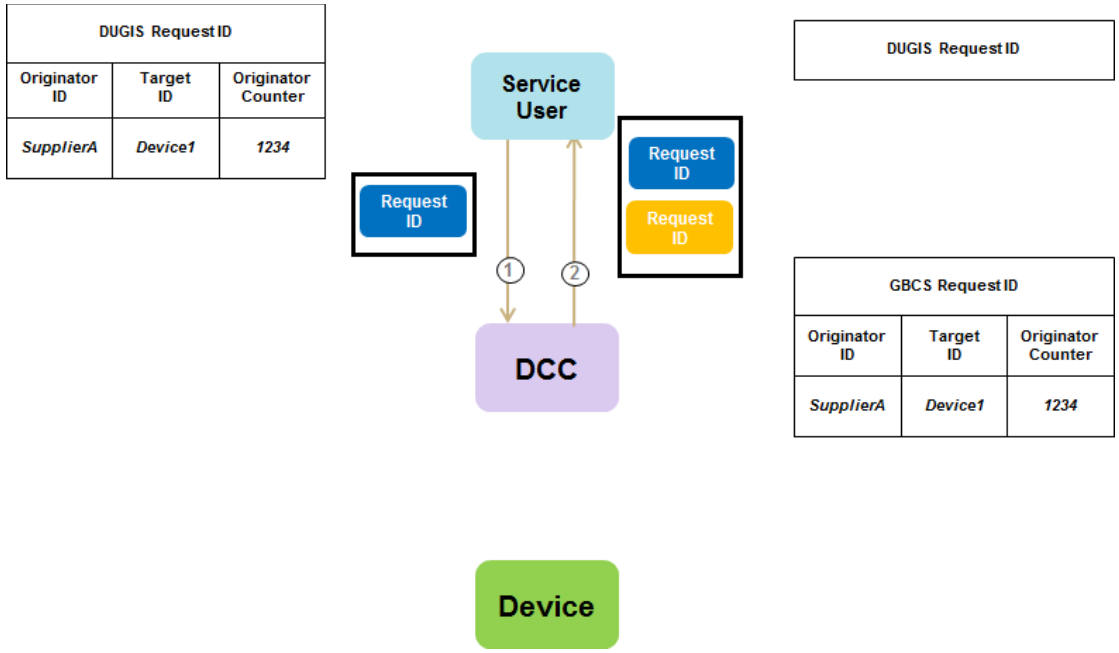


Figure 33 Transform Command (KRP)

4.10 Transformed Send Command and Receive Response (KRP)

Applicable to Signed Pre-Commands delivered via SM WAN, where the response is either to an On Demand Command or the Device acceptance of a Future Dated (Device) Command. See section 4.11 for the Device Alert returned when the Future Dated (Device) Command is executed by the Device.

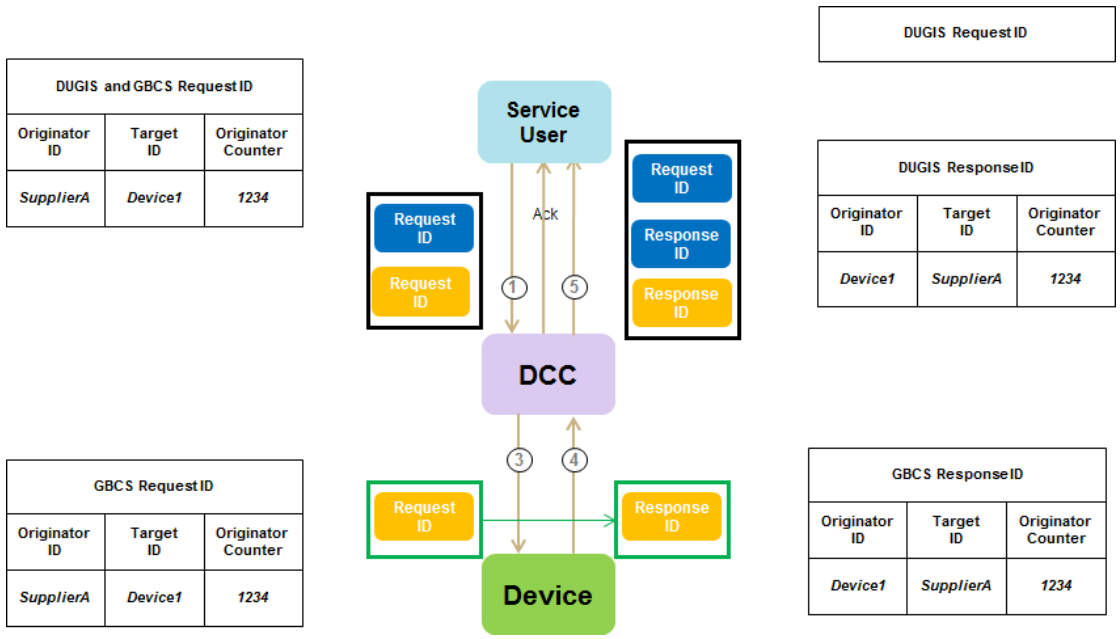


Figure 34 Transformed Send Command and Receive Response (KRP)

Note that the synchronous Acknowledgement response (flow 2 on the diagram) returns only the original DUIS Request ID.

4.11 Transformed Send Command and Receive Response (KRP) – FDEDA

Applicable to Signed Pre-Commands from a KRP delivered via SM WAN, where the response is the Future Dated (Device) Execution Device Alert (FDEDA).

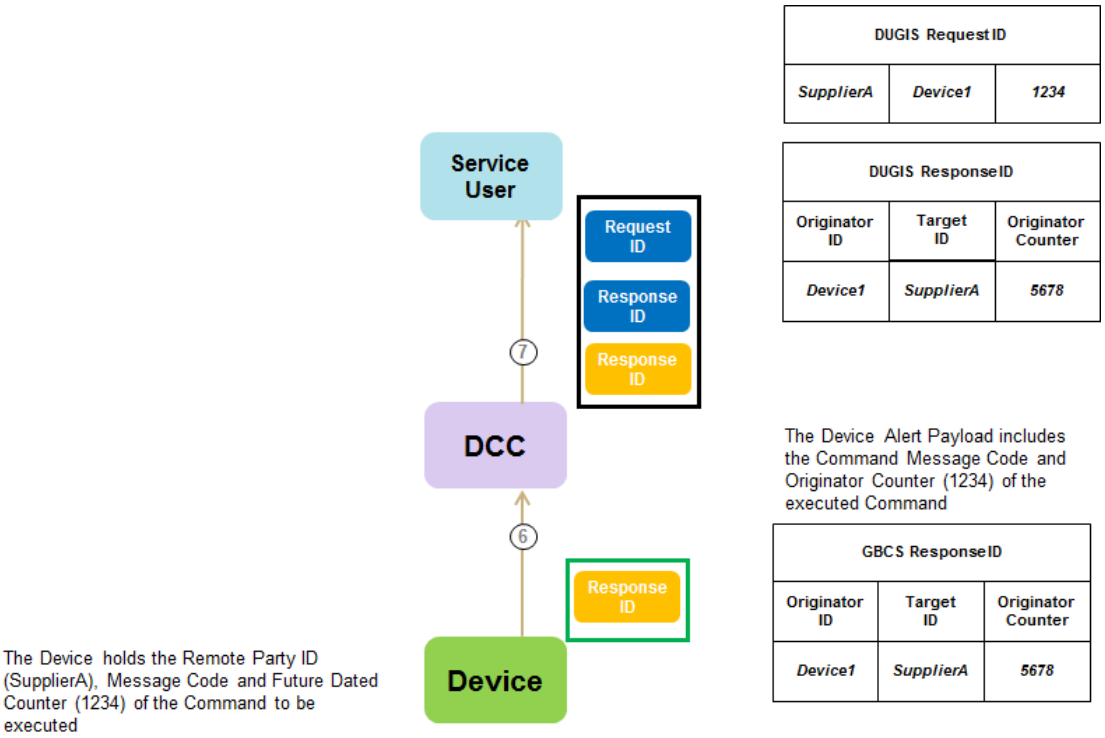


Figure 35 Transformed Send Command and Receive Response (KRP) – FDEDA

4.12 Transform and Return Command for Local Delivery (KRP)

Applicable to Critical Service Request Commands returned to the DCC Service User for Local Delivery.

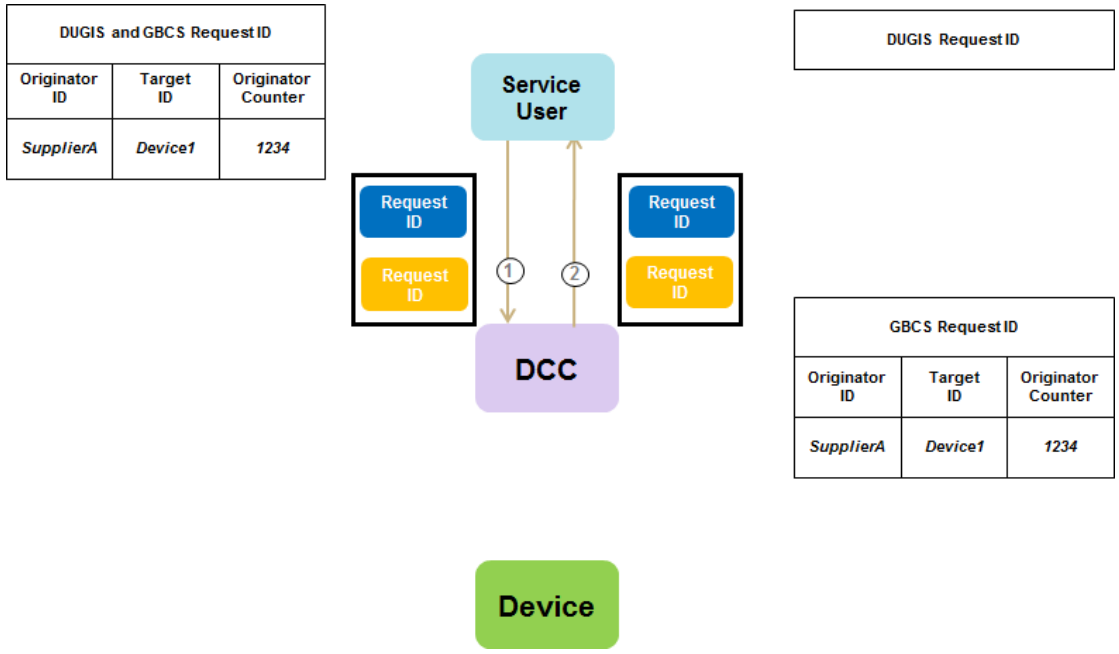


Figure 36 Transform and Return Command for Local Delivery (KRP)

4.13 Transformed Send and Return Command for Local Delivery (KRP)

Applicable to Signed Pre-Commands delivered via SM WAN and returned to the DCC Service User for Local Delivery.

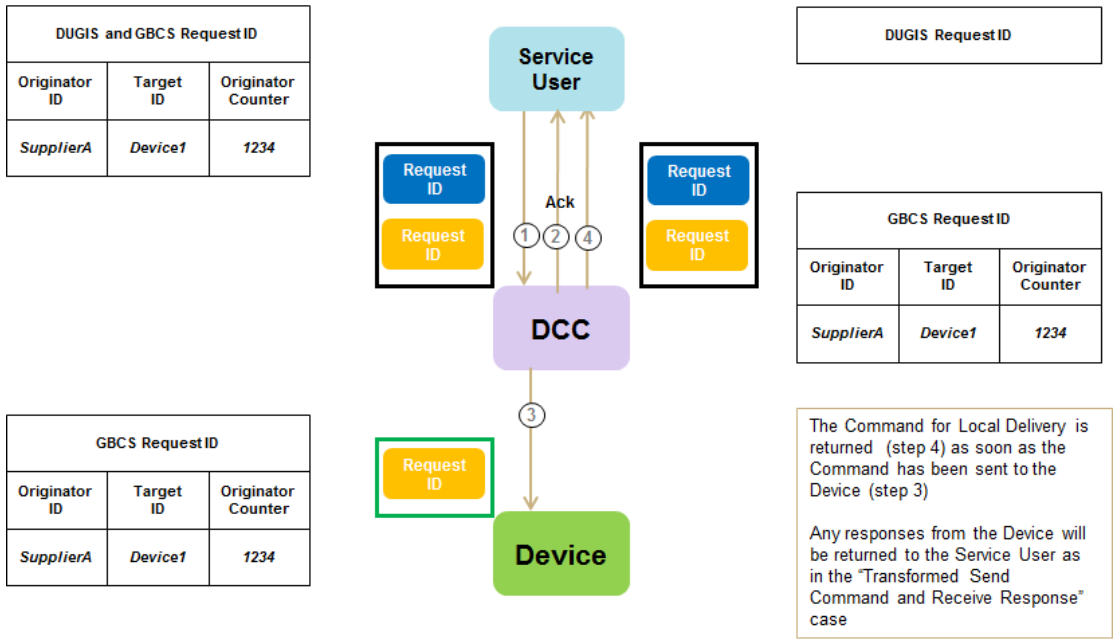


Figure 37 Transformed Send and Return Command for Local Delivery (KRP)

4.14 DCC Only

Applicable to “DCC Only” Service Requests.

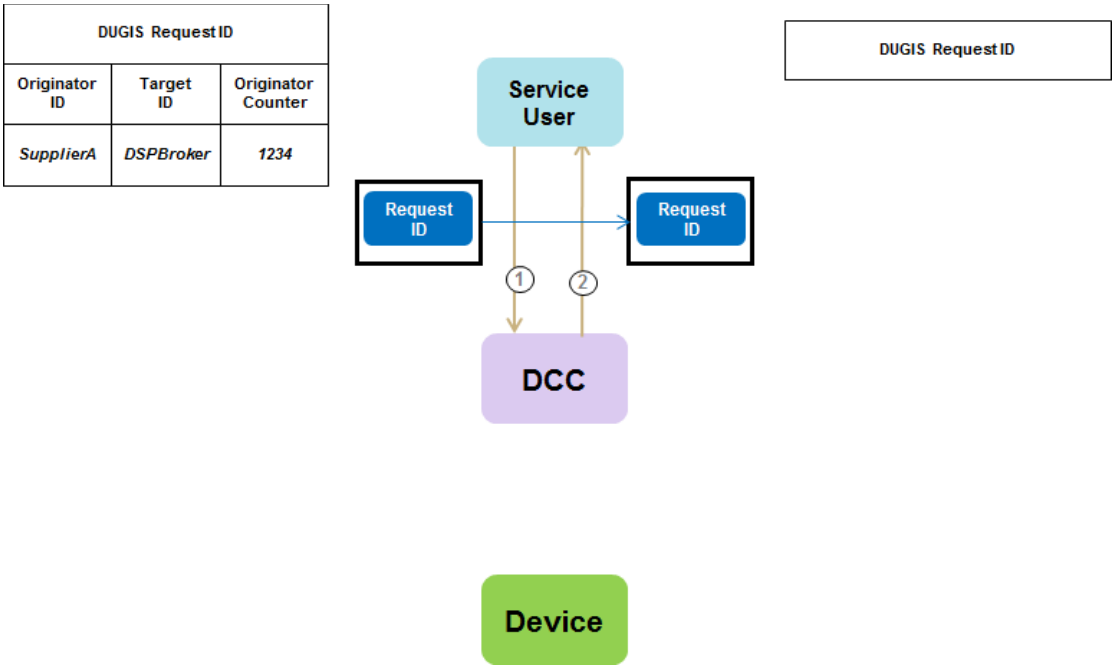


Figure 38 DCC Only

4.15 Device Alert (including Billing Data Alert)

Unsolicited response (Device Alert). The Device sends “Meter Scheduled” Billing Data Log data as an Alert.

For Device Alerts with 2 recipients (as defined by GBCS), the second recipient’s DUIS Response ID is: Business Originator ID = Device ID, Business Target ID = Device Alert Supplementary Remote Party ID, Originator Counter = Device Originator Counter

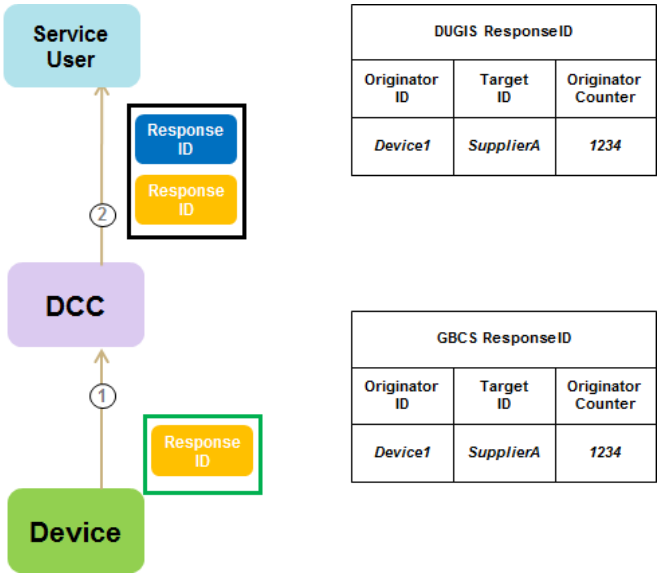
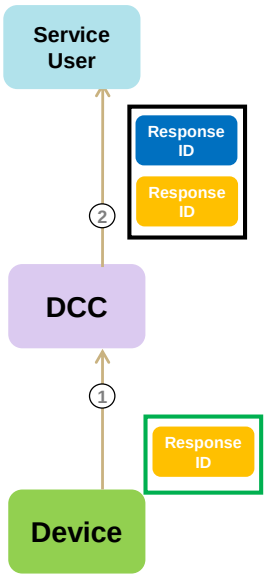


Figure 39 Device Alert (including Billing Data Alert)



DUGIS Response ID – First Recipient		
Originator ID	Target ID	Originator Counter
Device1	*SupplierA*	*1234*

DUGIS Response ID – Second Recipient		
Originator ID	Target ID	Originator Counter
Device1	*NOperatorB*	*1234*

Originator ID = Device ID, Target ID = Device Alert Supplementary Remote Party ID, Originator Counter = Device Counter

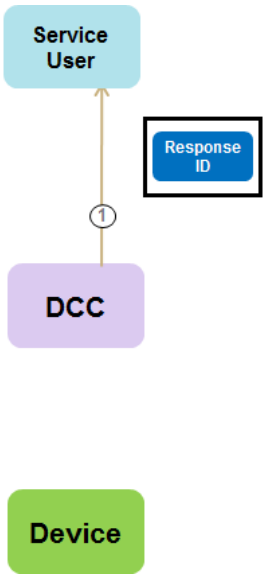
GBCS Response ID		
Originator ID	Target ID	Originator Counter
Device1	*SupplierA*	*1234*

Device Alert Supplementary Remote Party ID = Target ID of Second Recipient (NOperatorB)

Figure 39~~Figure 39~~.1 Device Alert With Two Recipients

4.16 DCC Alert

Unsolicited response (DCC Alert).



DUGIS ResponseID		
Originator ID	Target ID	Originator Counter
DSPBroker	*SupplierA*	*1234*

Figure 40 DCC Alert

4.17 DSP Scheduled Command and Response

Unsolicited response to DCC Service User (request generated by DSP Broker). The Response XML and GBCS Payload include the DSP Schedule ID.

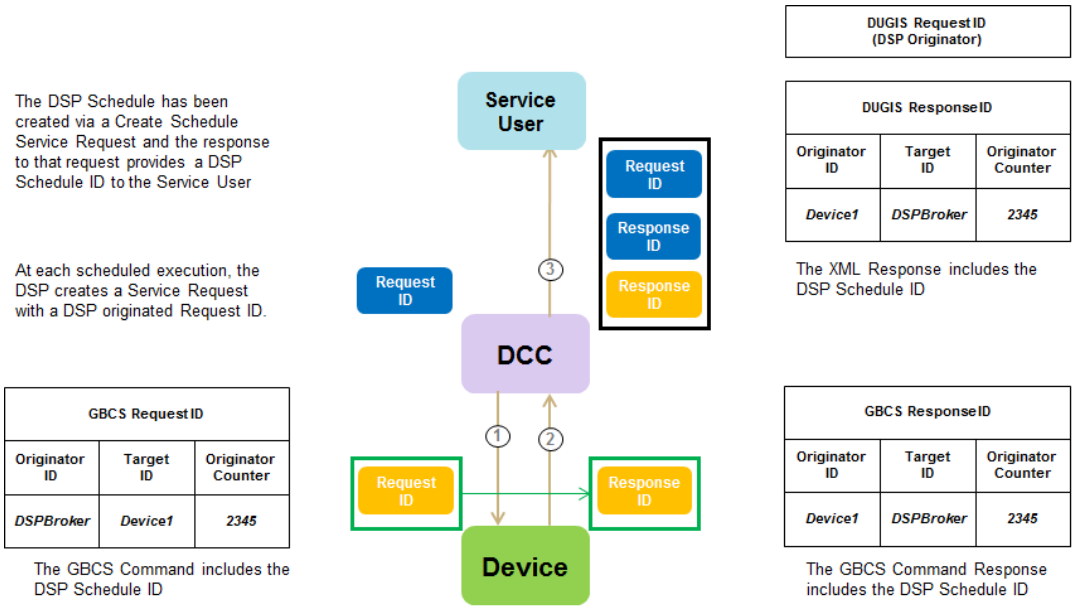


Figure 41 DSP Scheduled Command and Response

4.18 Originator Counters and Anti-Replay

This section is specific to SMETS2 or later Devices. Please see section 4.19.5 for applicability to SMETS1 or later Devices.

The Originator Counter within the Request ID plays a crucial part in providing protection against replay of Commands at the Device. This is explained in detail in GBCS, however this section attempts to summarise the behaviour for DCC Service Users.

Each Device maintains one Execution Counter per Known Remote Party (KRP) and Command type combination for all Commands that are marked as requiring 'Protection Against Replay' as defined in GBCS. The Device shall reject a Command where the Originator Counter in the request is not greater than the value of the Execution Counter held for that Command type and Remote Party.

Therefore, if the Command being sent to the Device has "Protection Against Replay Required" as defined by GBCS then the Device will store the Originator Counter of that Command when processed and only process higher value counters for that Command type and Remote Party combination. This means that the order of processing of Commands on Devices is important for these Commands to ensure that they are successfully processed by the Device. If a DCC Service User sends multiple Service Requests of the same type that require "Protection Against Replay" to the same Device then the DCC Service User must ensure that they are sent and confirmed as completed in order.

Service Requests which are Future Dated at the DSP (see section 5.1.2) have the additional complication that if before the corresponding Command is sent to the Device the DCC Service User sends an On Demand Service Request of the same Command type to the same Device, then when the Future Dated Command is subsequently sent by the DSP to the Device it will fail in the Device. DCC Service Users will need to manage this risk.

If "Protection Against Replay" is not required then DCC Service Users are free to send Service Requests to the device in any order and the originator counter values are not checked by the device.

Table 36~~Table 36~~ in section 9.4 indicates which Service Requests use Commands that require "Protection Against Replay".

4.19 SMETS1 Request and Response IDs

This section describes differences in the use of Request and Response IDs in connection with SMETS1 Devices,

Although SMETS1 Devices do not use GBCS, the SMETS1 Service Requests shall use the same format of Request and Response IDs in order to ensure commonality across the DCC User Interface. The following table shows the use of Request and Response IDs for SMETS1 Devices, and is the SMETS1 equivalent of Table 8~~Table 8~~ in section 4.

Request ID				Response ID				Response includes Request ID	Interaction Type
CV Type	Business Originator ID	Business Target ID	Originator Counter	Type	Business Originator ID	Business Target ID	Originator Counter		
1	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (KRP) (see section 4.19.1)
1	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (URP)

Request ID				Response ID				Response includes Request ID	Interaction Type
CV Type	Business Originator ID	Business Target ID	Originator Counter	Type	Business Originator ID	Business Target ID	Originator Counter		
									(see section 4.19.1)
2 (SRV 2.2 only)	DCC Service User ID	Device ID	Service User Originator Counter	UTRN S1SP Alert (from DCC)	N/A	N/A	N/A	Yes	Generate and return UTRN (see section 4.19.2)
3 (SRV 2.2 only)	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device) / UTRN S1SP Alert (from DCC)	Request's Device ID / N/A	Request's Service User ID / N/A	Request's Originator Counter / N/A	Yes / Yes	Generate, return and send UTRN (see sections 4.19.1 and 4.19.2)
4	DCC Service User ID	Device ID	Service User Originator Counter	Service Response (from Device)	Request's Device ID	Request's Service User ID	Request's Originator Counter	Yes	Send Command and Receive Response (KRP) (see section 4.19.1)
8	DCC Service User ID	DSP Broker ID	Service User Originator Counter	Service Response (from DCC)	N/A	N/A	N/A	Yes	DCC Only (see section 4.14)
N/A	N/A	N/A	N/A	SMETS1 Alert (unsolicited response to Service User)[7]	Device ID	DCC Service User ID	Device-specific Originator Counter generated by the S1SP	No	SMETS1 Alert (see section 4.19.3)
N/A	N/A	N/A	N/A	DCC Alert (unsolicited response to Service User) other than S1SP Alert	DSP Broker ID	DCC Service User ID	DSP Broker Originator Counter	No	DCC Alert other than S1SP Alert (see section 4.16)
N/A	N/A	N/A	N/A	DCC Alert (unsolicited response to Service User) which is an S1SP Alert	DSP Broker ID	DCC Service User ID	DSP Broker Originator Counter	Yes (of corresponding Service Request)	DCC Alert which is an S1SP Alert (see section 4.19.2)
9[1]	DSP Broker ID[2]	Device ID[2]	DSP Broker Originator Counter[2]	Service Response (from Device)[3]	Request's Device ID	DSP Broker ID	Request's DSP Broker Originator Counter	Yes[2]	DSP Scheduled Command and Response (see section 4.19.4)

Table 9 Request and Response IDs – SMETS1 Devices

[1] Command Variant 9 is an internal only value used for DSP Scheduled Command to a Device

[2] The Request ID is generated by the DSP Broker and included in the Request to the S1SP

[3] The Response XML includes the DSP Schedule ID

4.19.1 SMETS1: Service Responses

In the Response to a SMETS1 Service Request originated by a Service User where a SMETS1 Device is the target, for both the Countersigned SMETS1 Response (i.e. the corresponding Service Response created by the DCC Data Systems) and the SMETS1 Response (i.e. the message contained within it which was created by an S1SP) the following shall be populated:

- The Business Originator ID shall be the value of the Business Target ID in the Request ID, which shall be the Device;
- the Business Target ID shall be the value of the Business Originator ID in the Request ID, which shall be the originating Service User;
- the Originator Counter shall be the value of the Originator Counter in the Request, as created by the originating Service User.

This shall apply regardless of whether the equivalent request to a SMETS2 or later Device would be KRP or URP.

4.19.2 SMETS1: S1SP Alerts

See section 2.3.9 for a description of S1SP Alerts.

The payload of an S1SP Alert, which is delivered in a DCC Alert, includes the Request ID of the Service Request to which it corresponds.

An S1SP Alert may correspond to a Service Request in the following ways:

- Validation error. For any Service Request sent to an S1SP, the S1SP may reject it because of a validation condition, and that shall be communicated by sending an S1SP Alert contained in a DCC Alert with DCC Alert Code N55;
- notification. An S1SP may initiate a notification in connection with a SMETS1 device, and that shall be communicated by sending an S1SP Alert contained in a DCC Alert with DCC Alert Code N55;
- delivery of a UTRN. Where a Service Request 2.2 is sent to an S1SP with CV2 or CV3, the S1SP shall generate a UTRN and it will be sent to the requesting Service User as an S1SP Alert contained in a DCC Alert with DCC Alert Code N56.

4.19.3 SMETS1: SMETS1 Alerts

See section 2.3.8 for a description of SMETS1 Alerts.

As defined in the SMETS1 Supporting Requirements Document, the Request ID of a SMETS1 Alert includes an originator counter created by the relevant S1SP.

SMETS1 Alerts are delivered using DUIS XML elements which incorporate the MMC Device Alert format.

4.19.4 SMETS1: Scheduled Responses

Where a Countersigned SMETS1 Response is the response to a DSP Scheduled request, for both the Countersigned SMETS1 Response (i.e. the corresponding Service Response created

by the DCC Data Systems) and the SMETS1 Response (i.e. the message contained within it which was created by an S1SP) the following shall be populated:

- The Business Originator ID shall be the value of the Business Target ID in the Request ID, which shall be the Device;
- the Business Target ID shall be the Access Control Broker;
- the Originator Counter shall be the value of the Originator Counter created by the Access Control Broker in the scheduled Request.

4.19.5 SMETS1: Originator Counters and Anti-Replay

This section is specific to SMETS1 Devices and provides information supplementary to section 4.18.

For SMETS1 Service Requests, protection against Replay is performed by DCC Data Systems and S1SPs instead of Devices, as defined in the SMETS1 Supporting Requirements Document.

The set of SRVs for which protection against Replay is required with regard to SMETS1 Devices is not exactly the same as for SMETS2 Devices. It is defined in DUIS and can also be seen in the Service Request Matrix in this document section 9.4 by use of footnotes 8 and 9 to the “Protection Against Replay” column.

DCC Data Systems and S1SPs shall maintain Execution Counters on a per-SRV, per-Role and per-Device basis where Replay protection is required, with the exception of SRV 6.23, for which the requirement is to maintain Execution Counters on a per-Supplier basis.

If a SMETS1 Service Request is rejected by the DCC Data Systems because of protection against Replay, the Service User will receive a validation error by synchronous response, and the error will be indicated by error code E63.

If a SMETS1 Service Request is rejected by the S1SP because of protection against Replay, the Service User will receive an S1SP Alert which indicates a validation error due to protection against Replay.

Execution Counters maintained by the DCC shall be established as zero for a new Device with the exception of SRV 6.15.1 Update Device Security Credentials. For SRV 6.15.1 the Execution Counter for a new Device shall be set such that it prevents use of the SRV until SRV 6.21 Handover of DCC-Controlled Device has been used successfully for a Remote Party Role, following which the floor counter for that Role for SRV 6.15.1 shall be set to zero.

Where the DCC accepts a Service Request for which it maintains Execution Counters, the Execution Counter for that SRV and Role shall be updated to the originator counter of that Service Request.

Where an SRV 6.23 Update Security Credentials (CoS) is accepted for processing by the DCC for a SMETS1 Device, the Execution Counters maintained by the DCC, for the Supplier Role for that Device for SRVs other than SRV 6.21 and the SRV 6.23 itself, shall be updated to the SupplierFloorSeqNumber supplied in the Service Request, with effect from the execution date and time of the request.

It shall not be possible to reset Execution Counters maintained by the DCC other than by the mechanisms described in this section, and the remote party floor sequence number parameters of SRV 6.15.1 Update Device Security Credentials or SRV 6.21 Handover of DCC-Controlled Device shall not be used to change Execution Counters maintained by the DCC.

5 Scheduling

There are four main use cases which involve some sort of scheduling, either at the meter or within the DCC Data Systems, as shown in Figure 42~~Figure 42~~.

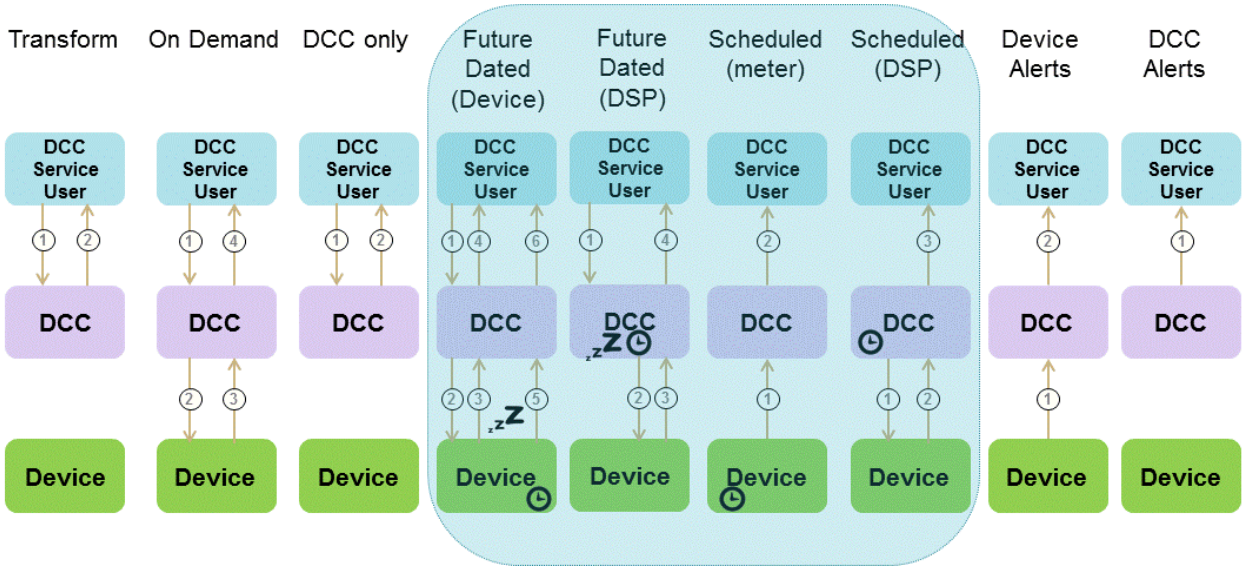


Figure 42: Scheduled Use Cases

5.1 Future Dated

Future Dated Service Requests incorporate an element of scheduling in that they are retained by either the device or the DCC Data Systems for execution at a specified time and date in the future.

Service Requests which support the ability to be Future Dated have an optional attribute for execution date/time defined within the Service Request Definition (see Annex). If this attribute is set then the Service Request is treated as Future Dated.

For Critical Service Requests which are to be Future Dated at the Device, the initial Transform Service Request requires this attribute to be set in order for the Pre-Command to be created with the required execution date/time. In all cases, the Signed Pre-Command must also include the execution date/time to allow the DSP to schedule and/or track the completion of the Future Dated request.

5.1.1 Future Dated (Device)

The set of commands which can be future dated at the Device is defined by the GBCS. For these commands the DCC actions the Service Request or Signed Pre-Command immediately and sends the command to the device where it is stored for execution at a later date. The device sends a Service Response to indicate acceptance of the future dated command and upon execution sends an Alert to confirm execution. Where the Command includes more than one instruction the Device sends one Alert per activation date-time instruction. This is illustrated in Figure 43~~Figure 43~~.

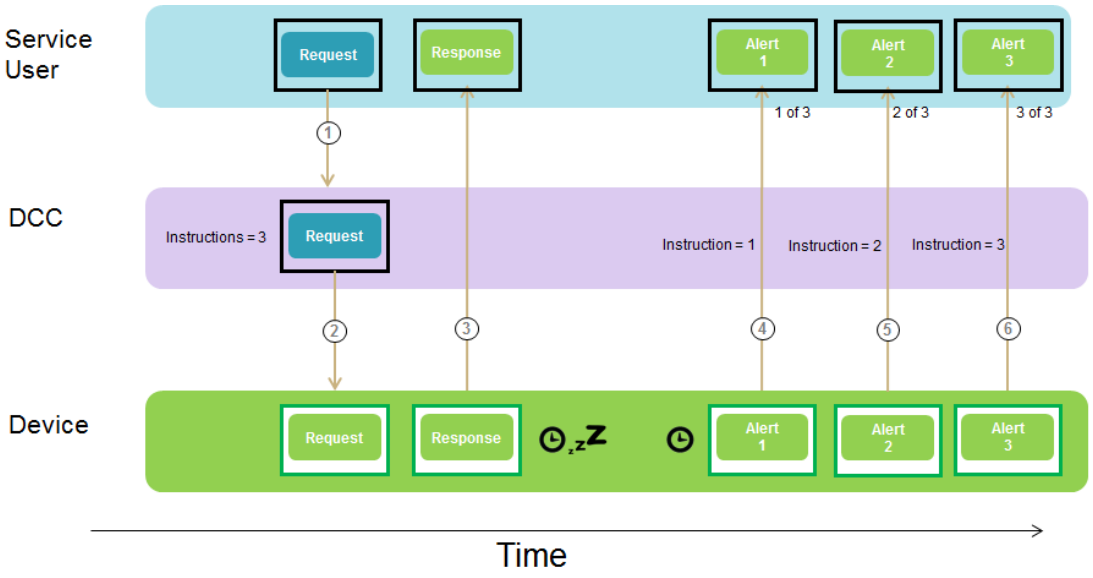


Figure 43 Future Dated Device – Processing Pattern

For a list of Service Requests that can be Future Dated at the Device see Table 36~~Table 36~~, where "Future Dated" column is set to "Device". For further details on how Responses are constructed see section 9.3.7. For details on how many instructions are contained in each Command please refer to the relevant Annexes.

If a Service Request that can be Future Dated at the Device is run On Demand, the Device will simply return a Service Response to confirm execution, in line with the standard On Demand processing pattern.

To cancel a Future Dated Service Request held at the Device, the DCC Service User has to send another Service Request of the same Service Reference Variant (mapping to the same GBCS Use Case and Message Code) with an execution date of 31/12/3000 to the same Device. The Device will cancel the original Command and return a Response to the Cancellation Service Request's Command but no further Response or Alert will be sent for the original Command being cancelled.

To modify a Future Dated Service Request held at the Device, the DCC Service User has to send another Service Request of the same Service Reference Variant (mapping to the same GBCS Use Case and Message Code) (with an execution date different from 31/12/3000) to the same Device. The Device will overwrite the values of the old Command with those of the new one.

If there is a change of Supplier on a Device which is after a future dated Command is stored but before it is activated, the change of control process will cancel that Command at the point of updating the Security Credentials. No Response or Alert will be returned by the Device to either the old or new Supplier in relation to any such cancellations. See GBCS for details.

5.1.2 Future Dated (DSP)

If a command cannot be Future Dated at the Device then the DCC can provide a similar function within the DCC Data Systems. In this case the Command is stored within the DCC Data Systems for a future scheduled delivery. This scheduling will be activated at the requested execution date and time and will be delivered in line with the relevant Target Response Time for Future Dated commands. Upon delivery the Device then sends a Service Response to confirm execution as it would for any other immediate execution of a command. For a list of Service Requests that can be Future Dated at the DSP see Table 36~~Table 36~~, where "Future Dated" column is set to "DSP". Please note that only Non Critical Service Requests can be Future Dated (DSP) for SMETS2 or later devices. For SMETS1 devices both Critical and Non-Critical Service Requests can be Future Dated (DSP).

To cancel a Future Dated Service Request held at the DSP, the DCC Service User has to send another Service Request of the same Service Reference Variant with an execution date of 31/12/3000 to the same Device. The DCC Data Systems will cancel the original Service Request and return a Service Response to the cancellation Service Request, but no further Service Response will be sent for the original Service Request being cancelled. Note that, if it isn't possible to cancel the original Service Request, e.g. because it had already been submitted to the Device, the Service Response will include failure Response Code E52.

To modify a Future Dated Service Request held at the DSP, the DCC Service User has to send another Service Request of the same Service Reference Variant (with an execution date different from 31/12/3000) to the same Device. The DCC Data Systems will only treat this Request as a modification if they can identify the Service Request to be modified as one not yet submitted to the Device, in which case the values of the old Service Request will be overwritten with those of the new one. Otherwise the Request won't be considered a modification and will be processed as a new one instead.

For SMETS1 Devices only, where an On Demand Service Request is received for a Device, any stored Future Dated (DSP) Critical Service Request of the same Service Reference Variant shall not be sent to the Device by the DCC Data Systems. The Service User shall receive an N11 DCC Alert which shall be actioned at the time at which the execution would have taken place.

5.2 Meter Scheduled

Electricity and Gas Smart Meters are capable of maintaining a meter held schedule for delivery of data from the Billing Data Log as defined in SMETS. The schedule is set by the Registered Energy Supplier using the Update Billing Configuration Calendar Service Request 6.8, with this request being passed directly to the meter the same as any other configuration command. Once the billing calendar has been set, the meter will initiate the sending of billing data as a specific Billing Data Log Device Alert at the stated date/time as per the schedule.

The DCC Data Systems receives these scheduled Device Alerts as unsolicited messages and processes them accordingly, forwarding them to the relevant DCC Service User.

5.3 DSP Scheduled

DCC Service Users may create schedules for sending Service Requests which are maintained and executed by the DCC Data Systems. Such schedules are created using the Create Schedule Service Request 5.1 and are stored within DCC Data Systems. At the relevant date and time, the DCC Data Systems sends the required Service Request to the Device and receives the Service Response. This Service Response is then returned to the DCC Service User that set up the schedule.

On successful creation of a Schedule, the Service Response to Service Request 5.1 includes a unique Schedule Id which is returned to the DCC Service User. When subsequent Service Requests are sent according to this schedule then the corresponding Service Responses will identify the Schedule Id from which they were created.

Each DCC Service User shall ensure that the number of active schedules created by themselves for any specified Device does not exceed 99 Schedules.

6 Sequencing

A DCC Service User has the option to orchestrate a number of Service Requests and Signed Pre-Commands into a business process through the use of sequencing. Each Service Request or Signed Pre-Command in the sequence is only released for execution once the previous one in the sequence has completed successfully.

Sequencing is applicable to SMETS1 Devices where Modes of Operation are supported, as can be seen in section 2.3 (e.g. Future Dated (Device) Requests are not supported on SMETS1 Devices).

For SMETS1 Devices the success of a Request in a sequence is determined from the SMETS1 Response outcome, rather than from the Command response which is applicable to SMETS 2 or later Devices.

In this section the term Request is used to refer to Service Requests or Signed Pre-Commands, where the behaviour is applicable to both.

Sequencing is only applicable to Requests that are for execution on Devices and more specifically (see section 3 and section 2.3):

- non-Critical Service Requests
- Critical Service Requests (SMETS1 only)
- and Critical Signed Pre-commands
    - Critical Requests for SMETS2 or later are submitted to the DCC Data Systems twice, both times with the same Request ID. First as a Service Request to be transformed to a Pre-command and second as a Signed Pre-command to be executed by the Device. When sent as part of a sequence, both Requests will include the sequencing related common data items, i.e. First In Sequence flag and / or Preceding Request ID (see section 9.2). The DCC Data Systems will ignore these data items in the Service Request for transformation but will use them in the Signed Pre-command. This is in line with the general sequencing orchestration rule to only release a Request for execution once the previous one has completed

CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
Yes	No	No	No	Yes	No	No	No

Table 10 Command Variant Values valid for sequencing

Note that for Future Dated Service Requests:

- Future Dated (Device). The trigger to release the following Command in the Sequence, where applicable, is when all the Future Dated Alerts corresponding to the Future Dated (Device) Command have been received by the DCC Data Systems and they are all successful
- Future Dated (DSP). The Service Request can only be the first in the Sequence

Sequencing is not applicable to:

- Transformation of Service Requests
    - See Critical Signed Pre-commands bullet point above
- DCC Only Service Requests. These Service Requests should be atomic in their own right and the purpose of sequencing is only to guarantee the order of Command execution on a Device

- Commands to be delivered locally. For these Requests the DCC Data Systems could ensure the order in which the Commands are returned to the DCC Service User, but not the order in which the Commands are delivered to the Device which makes the service redundant

- DSP Scheduled Service Requests

- All Gas Service Requests that return encrypted data in SMETS2 or later responses. In this case the DSP cannot read the message which includes the Response Code from the Device indicating successful execution or error reason and so cannot determine when to release subsequent Service Requests to the Device. See Table 36~~Table 36~~ for details. Please note that this Sequencing restriction applies at the SRV level and therefore also applies to SMETS1 devices.

The DCC Data Systems will process sequenced Requests in the order specified by the DCC Service User.

The following diagram illustrates the successful processing of a sequence of 3 “On Demand” Non-Critical Requests (Request ID = 1 is the “First In Sequence”. Request ID = 2 “Preceding Service Request ID” = 1 and Request ID = 3 “Preceding Service Request ID” = 2):

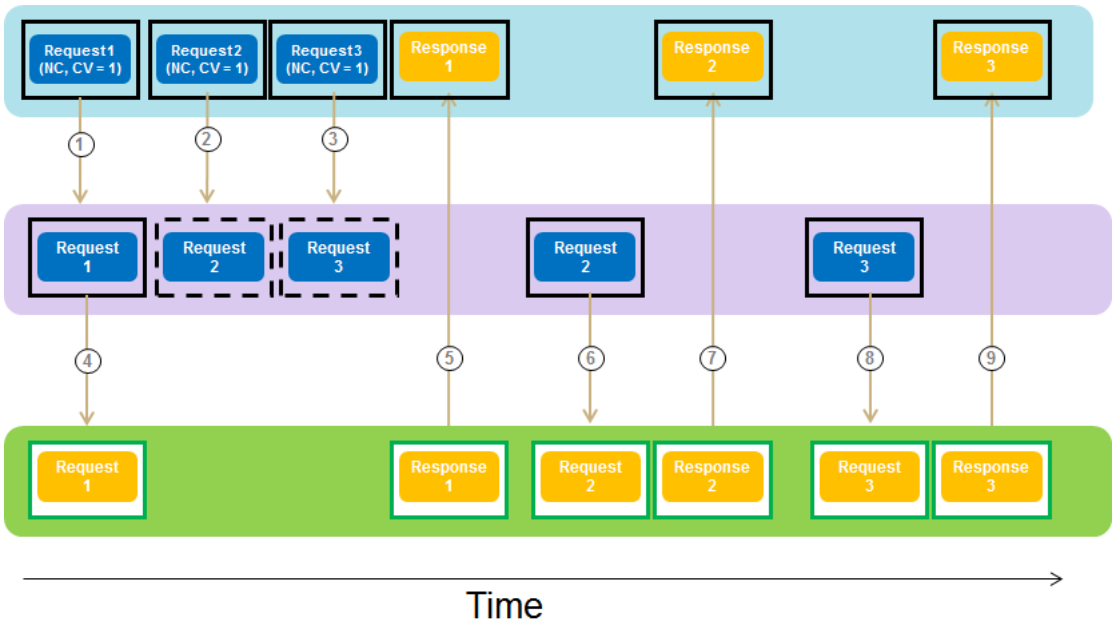


Figure 44 Sequencing – “On Demand” Non-Critical Requests

6.1 Starting a Sequence

The first Request in a sequence will have the First In Sequence flag set to true and no Preceding Request ID.

The DCC Data Systems treat the first Request in a sequence as a non-sequenced Request, except

- the First In Sequence flag being set to true is used to identify that its Command completion has to be monitored

6.2 Continuing a Sequence

The DCC Data Systems shall process all Requests in a sequence in the order specified by the DCC Service User. All Requests in a sequence, except the first one, will have the First In

Sequence flag set to false and the Preceding Request ID set to the Request ID of an earlier Request in the sequence.

Each Request that is intended to be sequenced from another Request shall only trigger the release of a single Request. The DCC Service User shall not link multiple Requests to a single Preceding Request ID.

If a Request is part of a sequence, its associated Command is only released by the DCC Data Systems to the specified Device for execution once its preceding Request's associated Command has completed successfully on the Device and a response is received by the DCC Data Systems.

6.3 Ending a Sequence

The DCC Data Systems will identify the last Request in the sequence in one of two ways:

- as the Request that makes the number of Requests in the Sequence reach the maximum number of Requests supported in a Sequence (currently set to a maximum of 99)
- as the last Request with a Preceding Request ID and with its Request ID not being the Preceding Request ID of another Request
    - The DCC Data Systems will wait for up to 2 minutes from the reception of a sequenced Request to determine if it is the last in the Sequence

If after the Last Request in the Sequence has been determined a subsequent Request is received, itself and any subsequent Requests will be set to errored.

- Their Acknowledgement Message Response Code will be set to E46 (provided they don't fail XSD validation or Access Control)

Note that the Sequence itself won't be failed and all Requests up to the last in the sequence that are still held, will be processed as defined in section 6.2.

6.4 Failed Sequenced Requests

Should a Request in a chain of sequenced Requests fail validation or execution, then all held Requests (including any already received out of order) in the Sequence that are dependent on the failed one will themselves be marked as failed and a DCC Alert will be sent to the DCC Service User. See Table 49~~Table 49~~ (DCC Alert Code N14) and Annex section 16.

For subsequent Requests received after this, the Acknowledgement Message Response Code will be set to E43 and no DCC Alert will be returned to the DCC Service User.

There is no attempt to reverse the action of the preceding successful Requests and it is the responsibility of the DCC Service User to resend corrected failed Requests (either as non-sequenced or as part of a new sequence), having first examined the failure reason given in the response message and corrected the underlying fault.

6.5 Quarantining of Sequenced Requests

In the event that a Request received as part of a sequence is identified as anomalous and is Quarantined, all not yet processed Requests identified as being part of that sequence shall also be held alongside the anomalous Request and processed or rejected as a set in accordance with the DCC Service User's instruction.

6.6 Out of Order Sequenced Requests

If sequenced Requests are received out of order, the DCC Data Systems shall cache the request for a "Wait Period" of 2 minutes from the reception of the Request to allow the missing Request to be received. If the missing Request is received within that period then the processing shall proceed as normal. If not, then the cached Request is not executed, the

Sequence is marked as failed and a DCC Alert is sent to the DCC Service User. See Table 49~~Table 49~~ (DCC Alert Code N15) and Annex section 16.

Any held subsequent Requests in the sequence dependent on the one just failed, will also be marked as failed and a DCC Alert (DCC Alert Code N15) sent to the DCC Service User.

For subsequent Requests received after the Sequence had failed (and provided they don't fail XSD validation or Access Control), the Acknowledgement Message Response Code will be set to E44 and no DCC Alert will be returned to the DCC Service User.

If the missing Request is received once the "Wait Period" has elapsed, it will be treated as the subsequent Requests received once the Sequence has failed.

6.7 No Sequence Number

The use of Sequencing is optional. Where the data items that indicate a Request is part of a Sequence (First In Sequence or Preceding Request ID) aren't included in Requests, the ordering of execution of Requests for a given device is not guaranteed.

7 Access Control

All Service Requests and Signed Pre-Commands submitted by the DCC Service User via the DCC User Interface undergo three logical modes of Access Control, namely: Authentication, Validation and Authorisation.

(In this section the term Request is used to refer to Service Requests or Signed Pre-Commands, where the behaviour is applicable to both.)

Authentication is based on two form factors: one covering the establishment of a secure communications channel, the other authentication of individual Requests. Similarly, Validation consists of both XSD Schema validation and data content validation. The DCC shall perform five stages of Access Control for all Service Requests and Signed Pre-Commands. These are executed in five stages as per the following table, See Table 11~~Table 11~~.

Stage	Description
Communications Authentication	Has the DCC Service User established a secure communications channel with the DCC, using a valid corporate TLS certificate issued by the DCC key Infrastructure (DCCKI)?
XSD Validation	Is the Request consistent with the DUIS XML Schema?
Request Authentication	Has the Request been signed with a valid certificate issued by the Smart Meters Key Infrastructure (SMKI)?
Request Authorisation	Is the DCC Service User organisation and associated User Role a valid SEC party of active status? If so, does the User Role specified have access rights to perform the Request for the specified Device?
Data Validation	Is the Request valid and complete?

Table 11 Access Control Stages

The checks carried out as part of the various Access Control stages meet the obligations as outlined in SEC, including the obligation to Verify the Service Request meets the requirements of the DCC User Interface Specification.

The DCC shall only successfully process Service Requests and Signed Pre-Commands where all five stages are passed.

As soon as any one Access Control check fails, the processing of the Request is halted and an error response is returned to the DCC Service User with an appropriate response code or HTTP status code indicating the error reason.

Authorisation and Data Validation is also applied for a second time at the point a “DSP Scheduled” Command or a “CoS Update Security Credentials” Command are generated by the DCC.

7.1 Stage 1 – Communications Authentication

All communications between the DCC and DCC Service Users shall be via a secure communications channel. Individual XML Requests will flow over this secure communications channel.

The communications channel will consist of an encrypted and authenticated session between a DCC and DCC Service User Policy Enforcement Point (PEP). This session will be based on the Transport Layer Security (TLS) v1.2 protocol standard and will make use of mutual authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret (TLS-RSA) with AES-128-GCM-SHA256 for communications encryption. The RSA Signing Key is the PEP corporate Digital Signing Key. This may support more than one organisation as defined by the Smart Meter Key Infrastructure (SMKI) organisation id. If this Authentication step fails then a TLS message of Access Denied will be returned to the DCC Service User. See section 15 for details.

The RSA (public) Signing Key will be issued to the DCC Key Infrastructure along with a PKCS #3 Certificate Signing Request. The Certificates for both PEPs keys will be stored on the DCC Public Key Store. The process for Certificate request / verification is described in section 15.

The establishment of this communications channel is illustrated in Figure 45 Secure Communications Channel~~Figure 45 Secure Communications Channel~~.

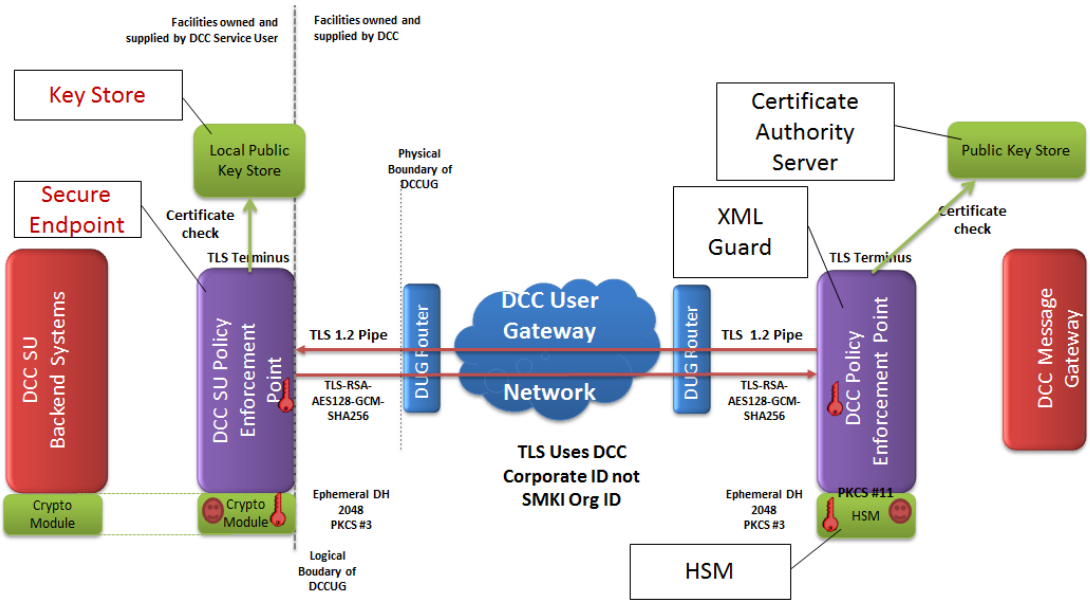


Figure 45 Secure Communications Channel

Facilities on the left hand side of the Logical Boundary of the DCCUG are owned and supplied by the DCC Service User. These reflect the expectation that each DCC Service User will put in place a boundary protection device that is capable of enforcing the TLS controls specified. The PEP must have logical access to a key store for TLS authentication and be able to create or import keys in a secure fashion such as via a Cryptographic Module. What provides the PEP capability, whether there is an Cryptographic Module in operation and the nature of the Local Public Key Store is at the discretion of the DCC Service User and their own risk assessment and risk treatment, subject to SEC conditions.

7.2 Stage 2 – XSD Validation

All Requests sent to the DCC User Interface will be subject to XSD Schema Validation.

If validation fails, the DCC Data Systems won't return a Synchronous Response as defined in section 9.3.1. Instead an HTTP status code 400 will be returned to the DCC Service User.

It is the DCC Service Users responsibility to ensure their Requests have been XSD Schema validated.

Validation Check	Process
Is the Service Reference valid?	Check that the Service Reference contained within an incoming Request from a DCC Service User is a valid and recognised request that can be received and processed by the DCC Data Systems.
Is the Service Reference format valid?	Check that the format of the Request is valid as per the Service Reference but not the content of the individual data items
Is the Request syntactically correct?	Check that the Request structure is syntactically correct with respect to the XML schema.

Validation Check	Process
Are the Request's data items valid?	Check that all the data items in the Request are valid according to the XSD. See DUIS XML Schema

Table 12 XSD Validation Checks

7.3 Stage 3 – Request Authentication

Where XSD validation is passed then the Request will be authenticated through the consumption of a Digital Signature applied to each and every XML format Request. This Digital Signature will be the organisational P-256 bit Elliptic Curve Digital Signature Algorithm (ECDSA) key generated under the auspices of the Smart Meter Key Infrastructure (SMKI).

This is illustrated in the diagram below.

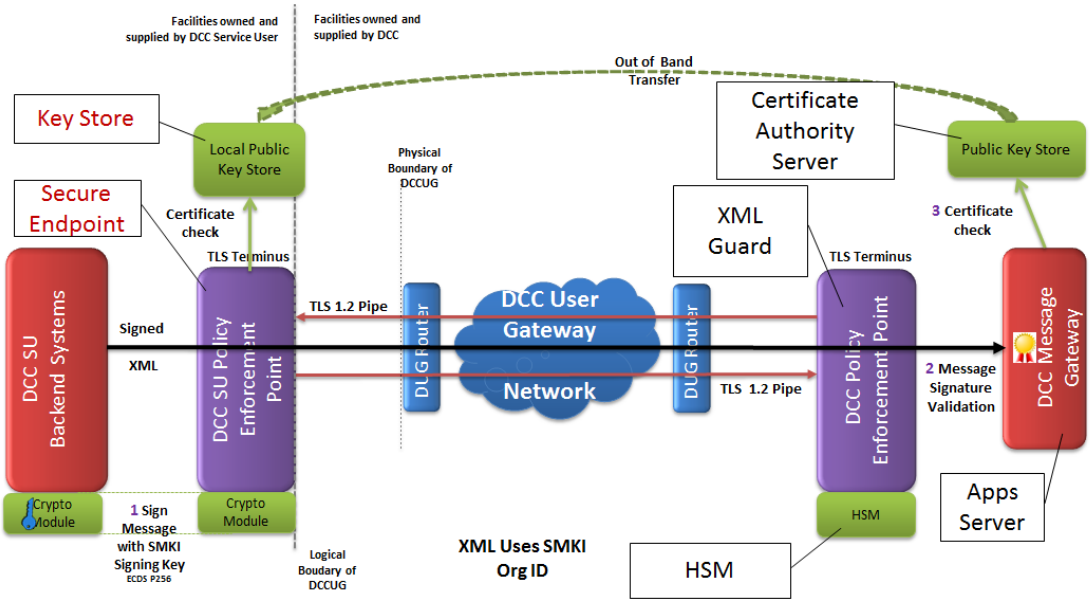


Figure 46 XML Request Authentication

To support graceful transition when approaching certificate expiry (or graceful non-emergency certificate revocation) the XML Digital Signature element `KeyInfo` must be included in the digital signature and it must define the certificate used to sign the request using a single `X509IssuerSerial` element (in a single `X509Data` element). This enables support for overlapping certificates for a period of time during a certificate transition.

In the case of all XML format Requests received by the DCC Data Systems via the DCC User Interface, the DCC will conduct the following checks.

Message Authentication Check	Process	Response Code (if checks are failed)
Validate the Remote Party Role of the DCC Service User's Organisation Certificate	Check that the Remote Party Role of the DCC Service User's Organisation Certificate is xmlSign.	E65[1]
Has the DCC Service User presented a valid SMKI client certificate?	The SMKI digital certificate referred to in the Request XML is verified to prove that the DCC Service User is eligible to communicate with the DCC Data Systems and the Request is intended for the DCC Data Systems. Checks undertaken[1]: 1. Check that the DCC Service User organisation ID in the Request Business Originator ID is consistent with the corporate ID used to secure the TLS connection (see section 15) 2. Use the `KeyInfo` in the Request to access the DCC Service User's signing certificate and check that it matches the signing certificate of the Request Business Originator ID 3. Use the public key from the DCC Service User's certificate to verify the authenticity of the Request 4. Verify the certificate's chain of trust up to the DCC root CA 5. Check the Certificate Revocation List to verify that no certificates in the chain of trust have expired or been revoked	E100[1]

Table 13 Authentication Check Steps

Requests that fail authentication will not be processed by the DCC Data Systems. The DCC Service User will be advised should authentication fail as part of the Service Response or Acknowledgment generated and sent to the requesting DCC Service User with an appropriate Response Code as listed in Table 13~~Table 13~~ above.

[1] For users on DUIS versions prior to 5.1, E100 is also used in place of E65.

7.4 Stage 4 – Request Authorisation

The permissions associated with the presented SMKI Certificate are checked to ensure that it has permission to perform the method requested.

This check is comprised of the following steps:

Authorisation Check	Process	Response Code
Does the DCC Service User have a valid User Role?	The sending organisation (DCC Service User) and their associated User Role are checked to confirm it is a valid SEC party / User Role combination	E1
Does the DCC User Role allow them to call that Request?	This is a User Role based check for the mapping between Requests and DCC Service User Roles (see section 9.4)	E2
Does the DCC Service User's status allow them to call that Request?	This is a status based check to find out if the DCC Service User is suspended (not allowed to run that Request) during the period against which the Request is placed for	E3

Authorisation Check	Process	Response Code
Is the DCC Service User, in the User Role defined in the Request, a "legitimate Registered Party" for the Device?[1]	This check is based on the registration data for the Device, and the date of execution of the Request or, for historical data, on the date-time period for which the data is required	E4
Is the Service Reference applicable to the Device status?[2]	This is a check to confirm that the target Device has a status within the Smart Metering Inventory that enables the DCC Service User to send it the particular Request [3]	E5
Does the User Role / Device status allow the Request to be delivered locally?	This is a check to confirm that if a Request is to be delivered locally (see section 3) the DCC User Role / Device status combination allows it (see section 9.4.1)	E17
Does the Device exist?[4]	This is a check to confirm that the target Device exists	E19

Table 14 Authorisation Check Steps

[1] The registration data check only applies to Energy Suppliers, Network Operators or Supplier Nominated Agents and is not applied for SMETS2 or later devices for Critical Service Requests and Signed Pre-Commands.

- A "legitimate Registered Party" means that a given DCC Service User is associated with an energy market participant having an industry registration data record for a given MPxN and in a given User Role on a given date, where there is not a Change of Supplier Objection against the industry registration data Supplier relationship effective on that date, with a status of Objection Raised or Objection Upheld
    - Where there is an Objection with one of the statuses given above against the Supplier relationship effective on that date, then the "legitimate Registered Party" is the DCC Service User associated with the previous industry registration data record for the same MPxN and in the same User Role without such an Objection.
    - Note that the "legitimate registered party" in the Supplier Nominated Agent role is dependent on any Objection raised against a Supplier relationship with a Meter Point, because the Supplier Nominated Agent is nominated by a particular Supplier. During the Change of Supplier process, the system must take account of which Supplier Nominated Agent registration corresponds to which Supplier registration. (Note that the generic Supplier Nominated Agent role corresponds to Meter Operator for electricity and Meter Asset Manager for gas.)
    - Where a Change of Supplier Request from a new Supplier has been withdrawn by the new Supplier, this means that the previous Supplier becomes the legitimate registered Supplier (with no end date). This scenario is recorded in the industry registration data as an Objection with status Registration Withdrawn, and therefore the access control rules treat Objection statuses of Objection Raised, Objection Upheld and Registration Withdrawn in the same way."
    - The DCC Data Systems will store historical registration data for 24 months. Requests from a DCC Service User that had ceased to be a "legitimate Registered Party" more than 24 months ago will be rejected.
- If the Device Type is a Communications Hub, this check is done on the Device(s) being added to or already existing on the same HAN for which the Service User / User Role is a Registered Party.
- If the Device Type is a 'Type 1', 'Type 2' or Gas Proxy Function, this check is done on the Device(s) in the same HAN Device Log for which the Service User / User Role is a Registered Party.
- Authorisation is done using the device specified in the business target id except for "DCC Only" Service Requests, where the Target Device ID is specified in the Request itself, where applicable.
- This check is not applicable to Service Request 8.2 (Read Inventory), 12.1 (Request WAN Matrix) or 12.2 (Device Pre-notification)
- This check is not applicable to Service Request 8.11 (Update HAN Device Log) where an IHD is being added to the Device Log and the command is for Local Delivery only.
- If Service Request 11.3 Activate Firmware is sent by a GIS and the target Device is a SMETS1 CHF or SMETS1 PPMID, it would be rejected with response code E4 because only the EIS is able to update the firmware in these cases.

[2] 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. As an exception, this

check will be carried out for Signed Pre-Commands if the Device Status is 'Recovery' (see footnote below).

[3] Devices can only be communicated with if they are in a status of 'Commissioned', 'Installed Not Commissioned', 'Whitelisted', 'Pending' or 'Recovered'. As an exception, Service Requests 11.1 (Update Firmware), 11.2 (Read Firmware Version), 11.4 (Update PPMID Firmware) and 6.23 (Update Security Credentials (CoS)), and, only for SMETS1 Devices, 2.2 (Top Up Device) with CV2, will be allowed if the Device Status is 'Suspended'. If the Device Status is 'Recovery' DCC Only Service Requests are allowed, subject to their specific validation.

[4] For DCC Only Service Requests this Response Code will be returned if the Business Target ID is not the DSP Access Control Broker ID.

If any of these checks fails at the point the Request is received by the DCC Data Systems, the Request is errored, no further checks are carried out and a Service Response is generated with the appropriate Response Code (error message) to inform the DCC Service User of the issue identified. See section 12.3 for Response Code details.

If any of these checks fails at the point a "DSP Scheduled" Command or a "CoS Update Security Credentials" Command is being generated, the associated Service Request is also errored, no further checks are carried out and a Service Response (see Table 49~~Table 49~~) is generated with the appropriate Response Code (error message) to inform the DCC Service User of the issue identified.

7.5 Stage 5 – Data Validation

All Requests sent to the DCC User Interface will be subject to Data Validation. Data Validation is driven by application functionality rather than syntax.

Service Request specific validation is included in the Annex Service Request Definitions. The table below describes common validation checks.

Data validation checks (see section 12.3 for more information on Response Code details):

Validation Check	Process	Response Code
Is the Request applicable to the Device type and, for Electricity Smart Meter, its variant? [2]	Check that the Request content is applicable to the Device type (and, for Electricity Smart Meter, the first character of its variant), e.g. Service Request 14.1 Record Network Data (Gas) is only applicable to a Gas Smart Meter[1]	E11
Is the Request's Command Variant valid?	Check that the Command Variant (see section 3) is applicable to the Request[5]	E12
Is the Request valid for the Web Service?	Check that the Request has been sent to the correct Web Service. See section 0	E13
Is the first request in a sequence valid?	Check that if the Request includes the FirstInSequence flag set to true, it doesn't include a PrecedingRequestID	E40
Is the sequenced Request's PrecedingRequestID the PrecedingRequestID of another Request?	Check that the sequenced Request's PrecedingRequestID is not the PrecedingRequestID of another Request	E41

Validation Check	Process	Response Code
Does the sequence contain a circular reference?	Check that there are no circular references in the sequence, i.e. a Request's PrecedingRequestID is not its own RequestID or the PrecedingRequestID of a Preceding Request in the sequence is not the currently processed Request's RequestID	E42
Have any of the sequenced Request's Preceding Requests failed?	Check that none of the Request's Preceding Requests have failed	E43
Have all the sequenced Request's Preceding Requests been received?[3]	Check that all Request's Preceding Requests in the sequence have been received during their "Wait Period" (see section 6.6)	E44
Is the sequenced Request's Command Variant valid?	Check that the Command Variant (see section 3) is applicable to sequenced Requests (see section 6)	E45
Has the sequenced Request been received before the Last in Sequence has been determined?[3]	Check that the Request does not follow a Request that has been determined to be the Last In Sequence (see section 6.3)	E46
Have any of the sequenced Request's Preceding Request Responses been received?	Check that the Request has not been received after the Sequence has been failed because of no response received from the Device to a previous Command	E47
Is the ServiceReference / ServiceReferenceVariant combination valid?	Check that the combination of Service Reference and Service Reference Variant is correct, i.e. it aligns to the definitions in Table 36~~Table 36~~.	E48
Is the Request Format correct for the Request? [2]	Check that the actual Request format matches the Service Reference Variant in the message header	E49
Is the Command for Local Delivery returned??	Check that Service Request requesting a Command for Local Delivery has returned a Command	E50
Is the Signed Pre-Command GBCS message code correct?[4]	Check that the GBCS message code in the Signed Pre-Command is consistent with the Service Reference Variant contained in the XML Request Header	E51
Is the Request to cancel a Future Dated (DSP) Service Request valid?	Check that if the Service Request is the cancellation of a Service Request Future Dated (DSP), the corresponding Service Request can be found and it hasn't yet been submitted to the Device	E52
Is the sequenced Future Dated (DSP) Request valid?	Check that if the Service Request is Future Dated (DSP) and it is part of a Sequence, it is the first Request in the Sequence	E53
Is the sequenced Gas Service Request valid?	Check that if the sequenced Service Request returns Gas Data, the response is not encrypted (See Table 36~~Table 36~~ for details)	E54
Is the Request ID a duplicate?	Check that the Request ID is not the duplicate of another Request which is currently being processed by the DCC Data Systems	E55
Is the Service Request still supported by the DCC Data Systems?	Check that the requested Service Request is still supported by the DCC Data Systems. This error will only occur if a Service Request which exists in an older version of the DUIS schema can no longer be accepted by the DCC Data Systems on that version of the interface.	E56

Validation Check	Process	Response Code
Is the Request applicable to the Device GBCS version[2]	Check that the Request content is applicable to the Device GBCS version, e.g. Service Request 6.26 Update Device Configuration (daily resetting of Tariff Block Counter Matrix) is only applicable to an Electricity Smart Meter at GBCS version 2.0 or later [1]	E57
Is the Request applicable to SMETS1?	Check that if the target Device's SMETS version is SMETS1, the Service Request is applicable to SMETS1 (Table 36~~Table 36~~ 'SMETS1 Applicability' set to Yes)	E60
Is the SMETS1 Service Request's Command Variant valid?	Check that if the target Device's SMETS version is SMETS1, the Command Variant (see section 3) is applicable to SMETS1 Service Requests[6]	E61
If DCC protection against Replay is required, has the Service Request been processed already?	Apply protection against Replay checks where DCC protection against Replay is required, as specified in the Service Request Processing Document.	E63
If DCC protection against Replay is required, does the Service Request come from the correct Supplier or Network Operator ID?	Where DCC protection against Replay is required, check that the Originator ID in the Service Request matches the Notified Critical Supplier ID or Notified Critical Network Operator ID as stored by the DCC Data Systems.	E64

Table 15 Data Validation Checks

[1] This check is not applicable to DCC Only Service Requests, except for Service Request 5.1 (Create Schedule) where it does apply to the Scheduled Service Request

[2] Validation is only applied to the XML data within the Request. There is no validation of the format of the GBCS Command held within a Signed Pre-Command. The E57 check is not applicable for Service Request 11.2 if the target Device is a PPMID, to cater for the scenario where a firmware update has been executed on a Device but the confirmation Device Alert was not received and processed by DSP, so the Firmware Version ID in the SMI is misleading.

[3] Validation takes into account Out of Order Sequenced Requests Rules (see section 6.6) and it will only fail if the "Wait Period" for the Preceding Requests has elapsed

[4] Validation only applicable to GBCS Command held within a Signed Pre-Command

[5] The valid combinations of Command Variant and Mode Of Operation are defined in Table 5~~Table 5~~

[6] The valid combinations of Command Variant, Mode Of Operation and SMETS1 Services are defined in Table 6~~Table 6~~

7.6 Responses and Alerts

When sending Responses and Alerts to DCC Service Users, the DCC Data Systems have to determine the correct recipient of those Responses or Alerts. This is the only relevant "access control" carried out for Responses or Alerts.

The rules below describe how this is determined:

1. Device Response. The DCC Data Systems forward the Device Response to the Business Target ID specified in the Device Response. Where the Business Target ID is the Access Control Broker acting on behalf of a URP the DCC Data Systems forward the Device Response to the DCC Service User that made the original Request. There is no checking against Registration data to determine Response routing.

2. Device Alert. The DCC Data Systems forward the Device Alert to the Business Target ID in the Device Alert and, for those with two recipients, also to the Supplementary Remote

Party ID in the Device Alert. There is no checking against Registration data to determine Alert routing.

3. DCC Alert. The DCC Data Systems generates the Alert in response to a trigger and sends it to the Recipient(s) associated to that DCC Alert (see Table 49~~Table 49~~) via checking against Registration data to determine the registered recipient, where applicable.

8 Security

8.1 Introduction

Much of the content, processing and structure of Remote Party Messages (as defined in GBCS) are common across multiple Messages. This Section lays out such common requirements with a specific focus on interactions between the DCC Service User and DCC User Gateway Services.

The following Section includes use cases between the DCC and DCC Service User that fall outside the scope of the GB Companion specification as they do not involve Device communications. It also includes use cases that are included within the GB Companion Specification but with embellishments supplied in relation to the interaction between and actions of the DCC and the DCC Service User.

Please note; one significant clarification that has been made with respect to those diagrams in the GB Companion Specification is that the Transform Service (DCC) (see section 0) is a dedicated function solely to support Critical Command Transformation and Signing. For Non-Critical Commands, transformation is seen as part of the core DCC Send Command Service and is performed within that service.

It should be noted that while there may be overlap between the sequence diagrams in section 8.3 and those within the GB Companion Specification, it is only those items shown within yellow notes boxes in the sequence diagrams that form part of the formal GB Companion Specification. For such items the GB Companion Specification takes precedence. This document represents the definitive specification for all other activities shown within the sequence diagrams included below.

This is fully consistent with the GB Companion Specification itself, which states that "*only those parts of the sequence diagrams within yellow notes boxes are within the scope of the GBCS. The steps outside such boxes are provided for context and, where mandated, are mandated through mechanisms outside the GBCS, for example the Smart Energy Code*."

Embellishments to our sequence diagrams include:

- clarification of the use of XML Messaging between DCC Service User and the DCC;
- clarification that Signatures are required to be applied to the XML messages (see section 8.2 for details of keys that are used);
- confirmation that the DCC issues an Acknowledgement message in response to Service Request and Signed Pre Commands for all Asynchronous communications;
- clarification as to the specific DCC service with which a DCC Service User interacts where applicable, e.g. Send Command Service, Transform Service etc.;
- clarification as to the format of each DCC Service User to DCC Communication.

Note that all Service Responses and Alerts go via the Receive Response Service.

Where such use cases include Device communications we have generally included those communications and Device operations to provide context. We have simplified these where possible while retaining the essence of the use case flow.

8.1.1 Device KRP and URP

For a SMETS2 or later Device, where a Remote Party is known to a Device by way of that Remote Party's Security Credentials being stored on the Device, the Remote Party is referred to as a Known Remote Party (KRP). Otherwise, it is referred to as an Unknown Remote Party (URP). See GBCS for details.

For a SMETS1 Device, the Remote Party is KRP to a Device if the Relevant S1SP is required to hold either a current Notified Critical Supplier ID or a current Notified Critical Network

Operator ID (according to the Remote Party's Role) for the SMETS1 Device in question, and URP otherwise, which is equivalent to the distinction for SMETS2 or later Devices. See the SMETS1 Supporting Requirements Document for details.

SMETS 2 or later

In all cases where a User Role doesn't map to a Device KRP, but SEC states that the User Role has access to a Service Request, the User Role is a URP and the Command is sent to the Device by the Access Control Broker, i.e. the DSP Broker, and the Device Response is returned to the Access Control Broker.

Where a User Role is a URP the DCC shall create the associated Command to the Device on behalf of the User using the DSP Access Control Broker Security Credentials. The RequestID of the Command created by the DCC shall be different to that of the original Service Request received by the DCC. Where the Response to a Service Request Variant of this type requires encryption within the Service Response, the Service User is required to include an additional data item (KAPublicSecurityCredentials) within the body of the Service Request as defined within the Service Request Definitions in the Annex. This data item is added to the otherInformation field within the associated Commands GroupingHeader as defined by GBCS (added to Supplementary Remote Party Key Agreement Certificate).

SMETS1

Where a Service User sends a Service Request targeted at a SMETS1 Devices, whether the Service User has a KRP or URP relationship to the Device, the DCC Data Systems shall pass the whole Service Request to the S1SP. This means that for URP cases, where the S1SP responds to the originator of the request it targets the response directly at the Service User, rather than to the Access Control Broker as in the corresponding SMETS2 or later case. See section 4.19.1.

The following table summarises (as defined in GBCS) which User Roles are Known Remote Parties to which SMETS2 or later Devices:

Known Remote Party				Device Type					
User Role	Remote Party Role	Key Usage	Cell Usage	ESME	GSME	CHF	GPF	HCALCS	PPMID
EIS	Supplier	Digital Signature	Management	✓				✓	
EIS	Supplier	Key Agreement	Management	✓					
EIS	Supplier	Key Agreement	Pre Payment Top Up	✓					
GIS	Supplier	Digital Signature	Management		✓		✓		
GIS	Supplier	Key Agreement	Management		✓		✓		
GIS	Supplier	Key Agreement	Pre Payment Top Up		✓				
ENO	Network Operator	Digital Signature	Management	✓					
ENO	Network Operator	Key Agreement	Management	✓					
GNO	Network Operator	Digital Signature	Management				✓		
GNO	Network Operator	Key Agreement	Management				✓		
N/A	Access Control Broker	Digital Signature	Management			✓			✓

Known Remote Party				Device Type					
User Role	Remote Party Role	Key Usage	Cell Usage	ESME	GSME	CHF	GPF	HCALCS	PPMID
N/A	Access Control Broker	Key Agreement	Management	✓	✓	✓	✓	✓	✓
N/A	WAN Provider	Digital Signature	Management			✓			
N/A	Transitional CoS	Digital Signature	Management	✓	✓		✓	✓	
N/A	Root	Key Certificate Signing	Management	✓	✓		✓	✓	
N/A	Load Controller [2]	Digital Signature	Management	✓ [1]					
N/A	Load Controller [2]	Key Agreement	Management	✓ [1]					

Table 16 User Roles and Device KRPs

[1] GBCS v4.0 or later

[2] In this version of the interface, these may be updated only by a Supplier since there is no regulatory support enabling SMKI Organisation Certificates to be issued with the Load Controller SMKI Remote Party Role.

8.2 Key Cryptographic Operations

The following Cryptographic operations protect all DUIS XML format messages that are sent and received by DCC Service Users across the DCC User Interface and are in addition to those specified within the GB Companion Specification which are used to Digitally Sign Commands.

The DCC and each DCC Service User shall Digitally Sign all DUIS XML format messages using the following method for each of the DUIS signing activity listed below. All these DUIS signing activities shall be signed with an organisational P-256 bit Elliptic Curve Digital Signature Algorithm (ECDSA) key generated under the auspices of the Smart Meter Key Infrastructure (SMKI). This signature should be generated in accordance with NSA Suite B.

8.2.1 DUIS XML Service Request Signing

Each DCC Service User shall Digitally Sign every XML format Service Request and Signed Pre-Command using an XML User Role Signing Private Key. For clarity, this is a separate dedicated key pair that shall not be used for communication with Devices.

A separate XML User Role Signing Private Key must be used per User Id in use for each DCC Service User.

Each DCC Service User may use the same XML User Role Signing Private Key for Service Requests and SMETS1 Service Requests.

The DCC shall check that the DCC Service User has used an XML User Role Signing Private Key to Digitally Sign each Service Request and Signed Pre-Command, and shall cease processing the communication and notify the DCC Service User if this is not the case.

See section 7.3 for additional details.

8.2.2 Transform Service Response Signature Validation

The DCC shall Digitally Sign all XML format Service Responses containing Pre-Commands sent to DCC Service Users using an XML DSP Role Signing Private Key. This is a separate dedicated key pair that shall not be used for communication with Devices.

The DCC Service User shall verify the Digital Signature of Pre-Commands sent by the DCC (this includes Certificate status checking and Certificate Path Validation of the Public Key Certificate of the DCC Transform Service).

8.2.3 DCC Signed Service Responses

The DCC shall Digitally Sign the following XML format Service Responses sent to DCC Service Users, using an XML DSP Role Signing Private Key. This is a separate dedicated key pair that shall not be used for communication with Devices

- all DCC Alert messages, originating from the DCC, including DCC Alerts containing S1SP Alerts (see section 3.13.1);
- all Service Responses to DCC Only Service Requests that return data;
- all Service Responses returning Command(s) for Local Delivery;
- all Service Responses to Commands created by a DSP Schedule;
- For SMETS2 or later, all Service Responses to Commands from an Unknown Remote Party. Also applicable to Service Requests 6.21 (Request Handover Of DCC Controlled Device), 6.23 (Update Security Credentials (CoS)), 6.24.1 (Retrieve Device Security Credentials (KRP)), 8.5 (Service Opt Out), 8.9 (Read Device Log) where the Target Device Type is HCALCS and 8.12.2 (Restore GPF Device Log)
- All SMETS1 Response and SMETS1 Alert Messages (see section 3.13.1)

The DCC shall use the same XML DSP Role Signing Private Key for each of the XML format Service Responses sent to DCC Service Users defined above regardless of SMETS device type,

The DCC Service User shall verify the Digital Signature of such DCC Signed Service Responses. This shall include Certificate status checking and Certificate Path Validation of the Public Key Certificate of the DCC Access Control Broker Service.

To support graceful transition when approaching certificate expiry (or graceful non-emergency certificate revocation) the XML Digital Signature element `KeyInfo` is included in the digital signature of signed responses and it defines the certificate used to sign the request using a single `X509IssuerSerial` element (in a single `X509Data` element). DCC Service Users must support overlapping certificates for a period of time during a certificate transition.

8.2.4 XML Digital Signatures

The DUIS XML is signed with a Digital Signature (XMLDSig), there are a number of parameters that are required as part of the algorithm, these parameters define the transform, signing, canonicalization and digest algorithms to be used, as well as the XML node which is signed. Note that the Reference URI is defined as “”, which indicates that signature applies from the root of the document;

Parameter	Value
Reference URI	“”
Transform Algorithm	**http://www.w3.org/2000/09/xmldsig#enveloped-signature**
CanonicalizationMethod Algorithm	**http://www.w3.org/2001/10/xml-exc-c14n#**

Parameter	Value
SignatureMethod Algorithm	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
DigestMethod Algorithm	http://www.w3.org/2001/04/xmlenc#sha256

8.3 Sequence Diagrams

The sequence diagrams in the figures in this section 8 illustrate the generic processing stages and common processing requirements, where a Device is operated via the DCC.

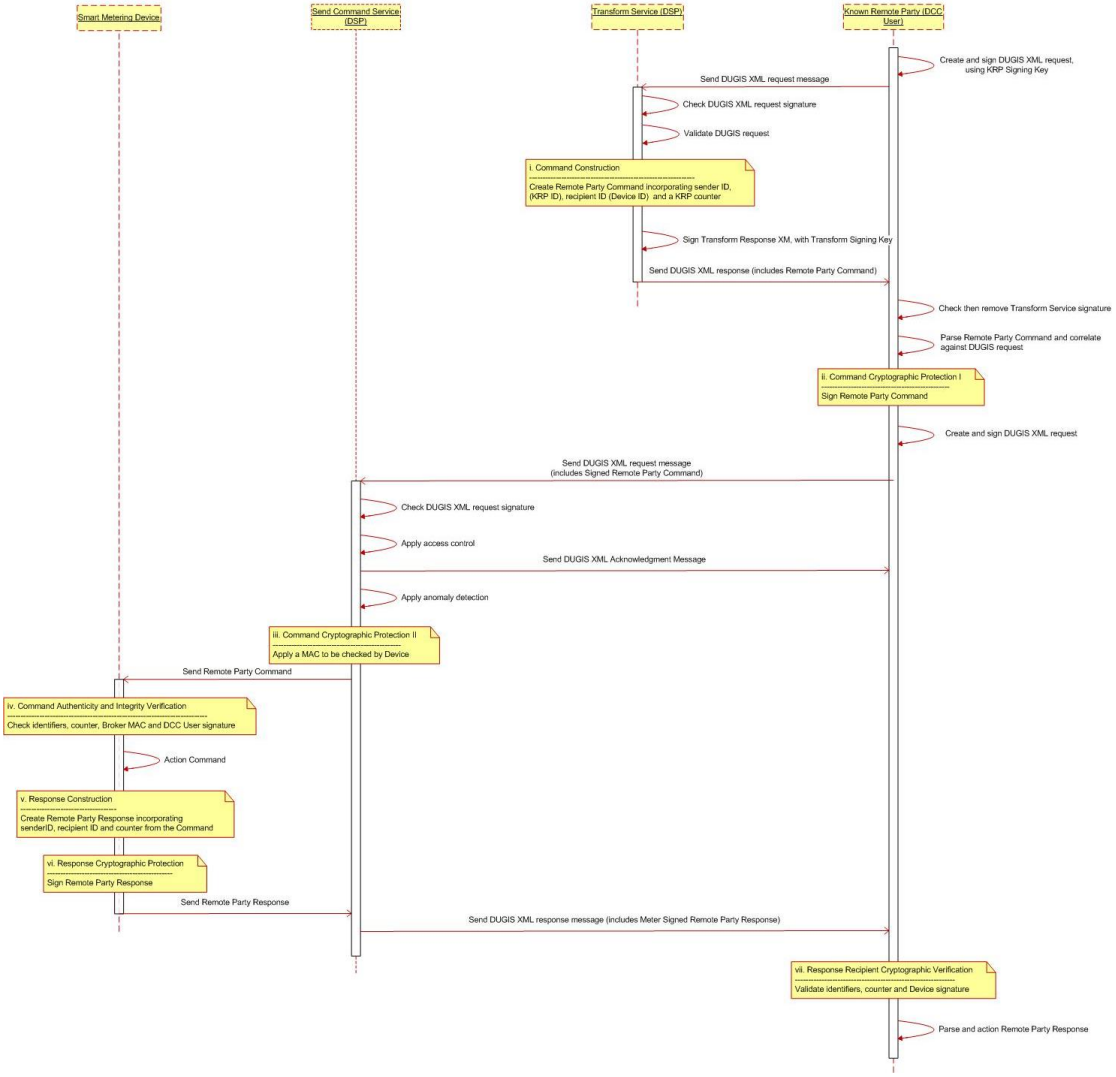
Note that those parts of the sequence diagrams within yellow notes boxes are within the scope of the GBCS. The steps outside such boxes are mandated via this Design Specification.

For readability, these diagrams use the term “DSP Broker” to refer to the DCC Access Control Broker.

These sequence diagrams are applicable only to SMETS2 or later Devices.

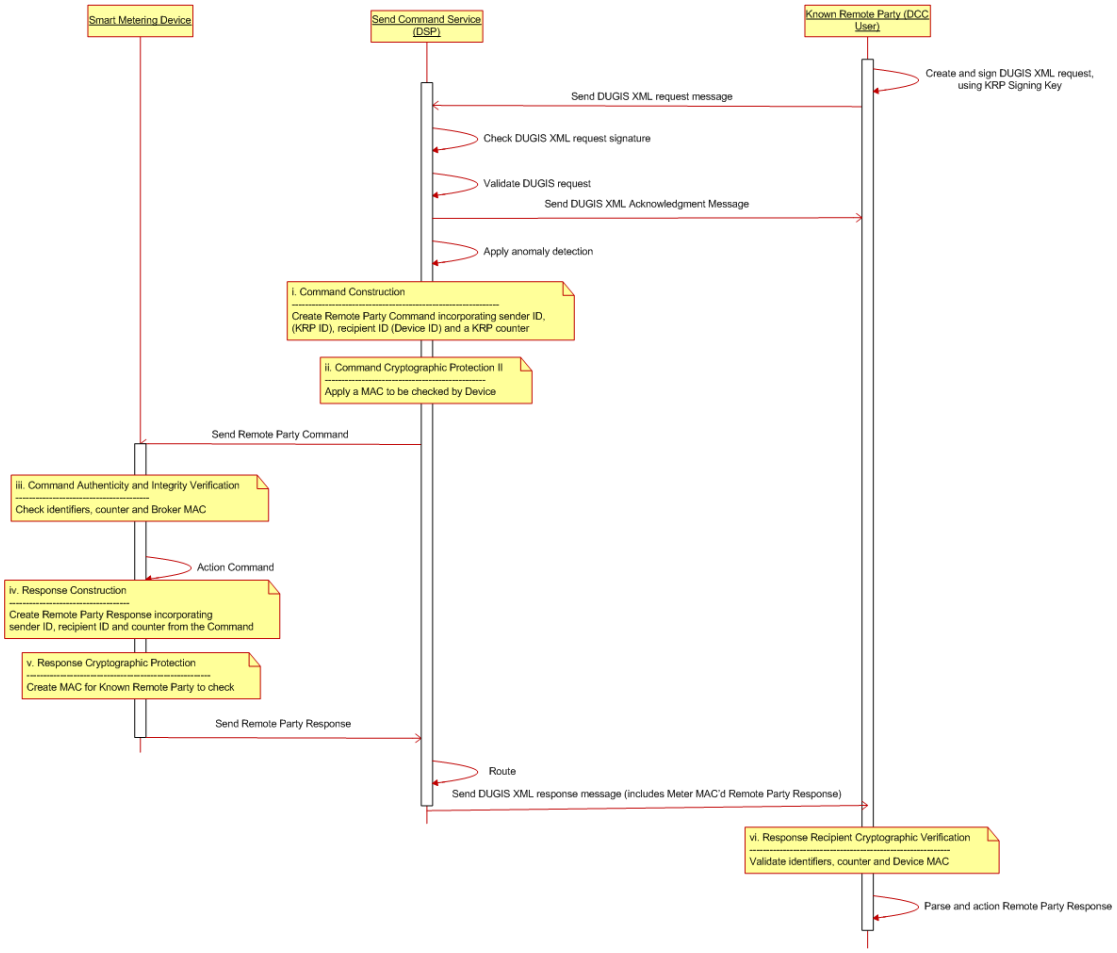
8.3.1 SME.C.C – Critical Command from Known Remote Party (KRP)

This service request follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.



8.3.2 SME.C.NC.KRP – Non-Critical Command from Known Remote Party (KRP)

This command follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.



Note: If the Response contains sensitive data then the Device will additionally encrypt the sensitive data for the KRP to decrypt.

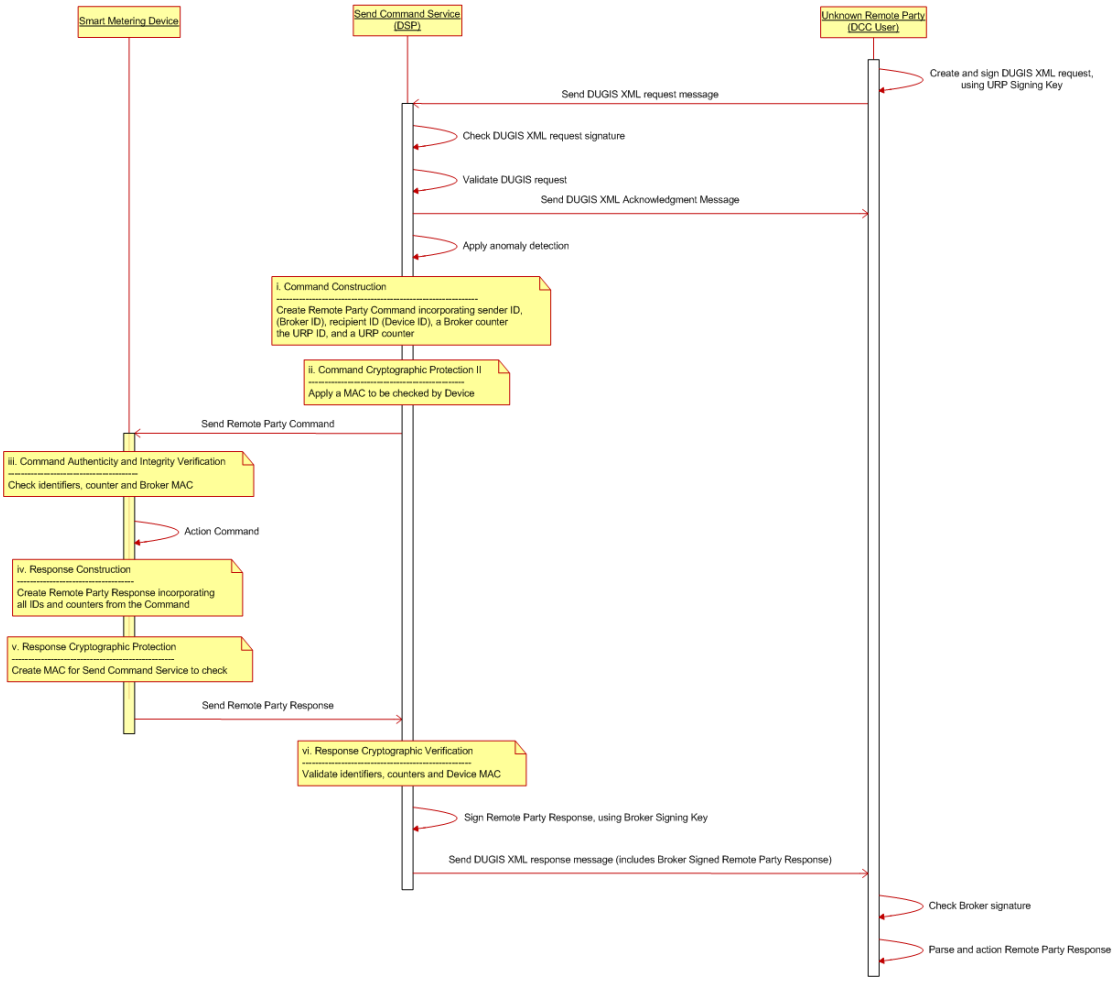
8.3.3 SME.C.NC.URP – Non-Critical Command from Unknown Remote Party (URP)

This command follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.

It varies from SME.C.NC.KRP in that the Device is not aware of the Unknown Remote Party, its associated keys, etc. and hence has to relay the response through the Send Command Service.

To support this the Send Command Service has to apply its own message counter to the outbound command to enable the Device to generate a response GMAC'd for the Send

Command Service which then has to validate this GMAC and sign the XML message to the Unknown Remote Party.



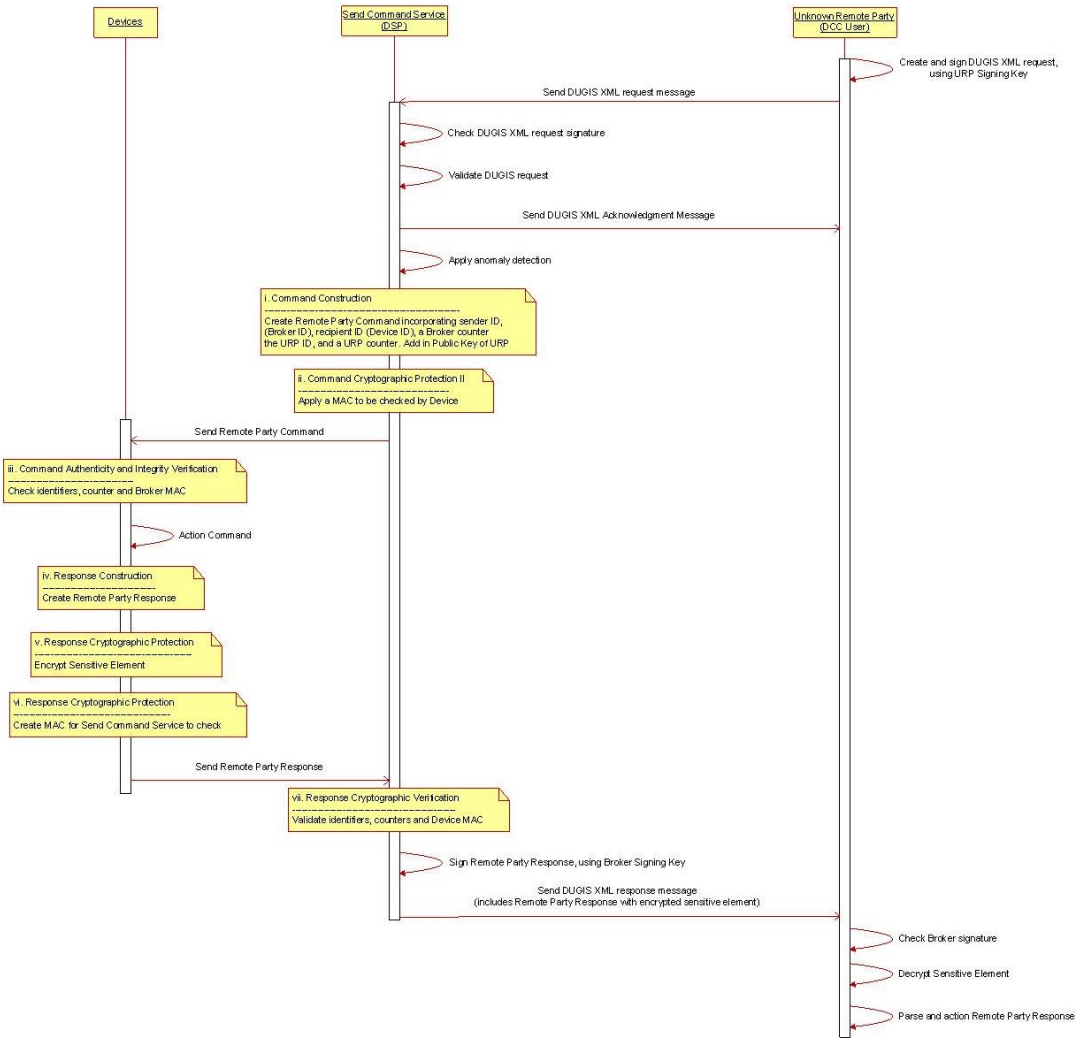
8.3.4 SME.C.NC.URP.SEN – Non-Critical Command from Unknown Remote Party (Sensitive Response)

This Service Request follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.

It builds on and varies from SME.C.NC.KRP in that the Device has to encrypt the sensitive element of the response message, such that the sensitive element cannot be read by anyone other than the Unknown Remote Party (URP).

To support this the Send Command Service has to apply both its own counter and add the public key of the URP to the outbound command to enable the Device to generate a response GMAC'd for the Send Command Service and encrypt the sensitive element for the URP.

The Send Command Service then has to validate this GMAC on the service response and Sign the XML message to the URP. The URP is able to decrypt the sensitive element through generation of the Device shared Secret, generated via Elliptic Curve Diffie Helman (ECDH) based on the URP and Device key agreement keys.

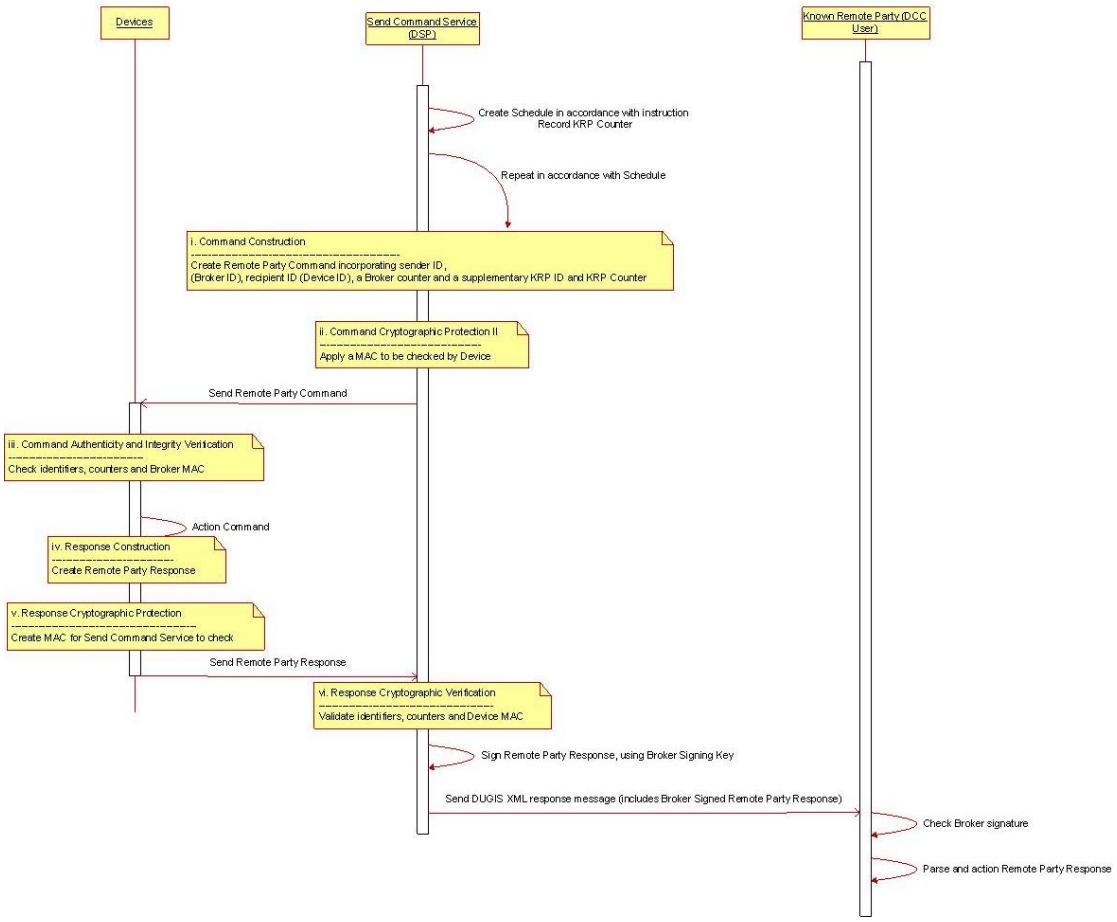


8.3.5 SME.C.NC.KRP.SCH – Non-Critical Command from Known Remote Party (DSP Scheduled)

This Service Request follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.

It builds on and varies from SME.C.NC.KRP, through the addition of a Send Command Service scheduling function. Note that we have not reiterated in this diagram how the Send Command Service receives the schedule in the first place which is no different from how it receives any other Non-Critical Command.

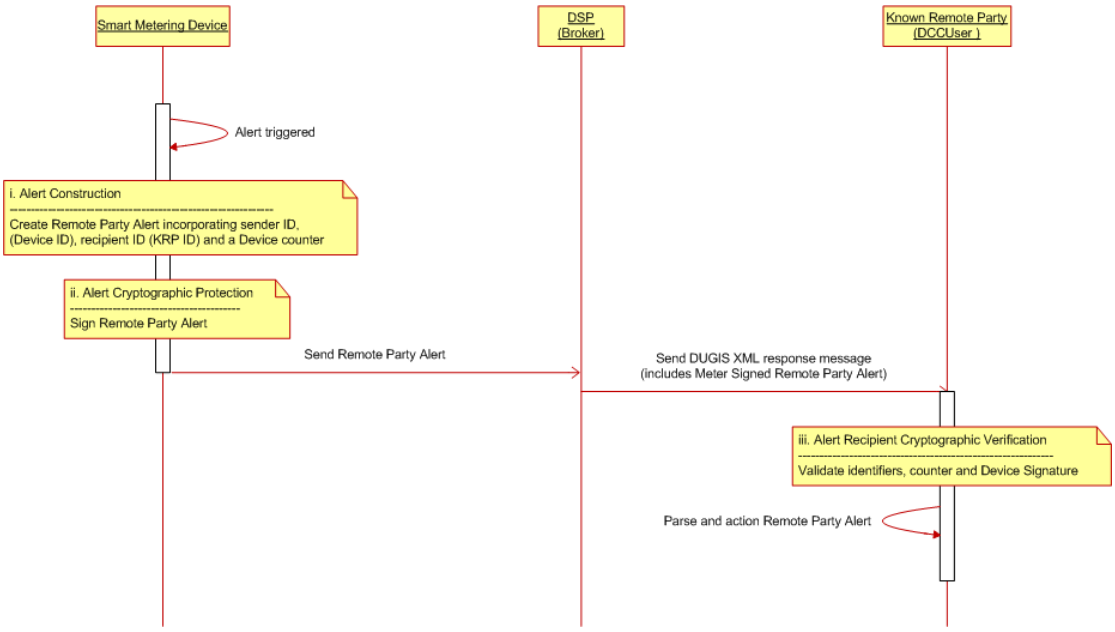
To support this the Send Command Service has to apply its own message counter to the outbound command to enable the Device to generate a response GMAC'd for the Send Command Service which then has to validate this GMAC and sign the XML message to the Known Remote Party.



Note: If the Response contains sensitive data then the Device will additionally encrypt the sensitive data for the KRP to decrypt,

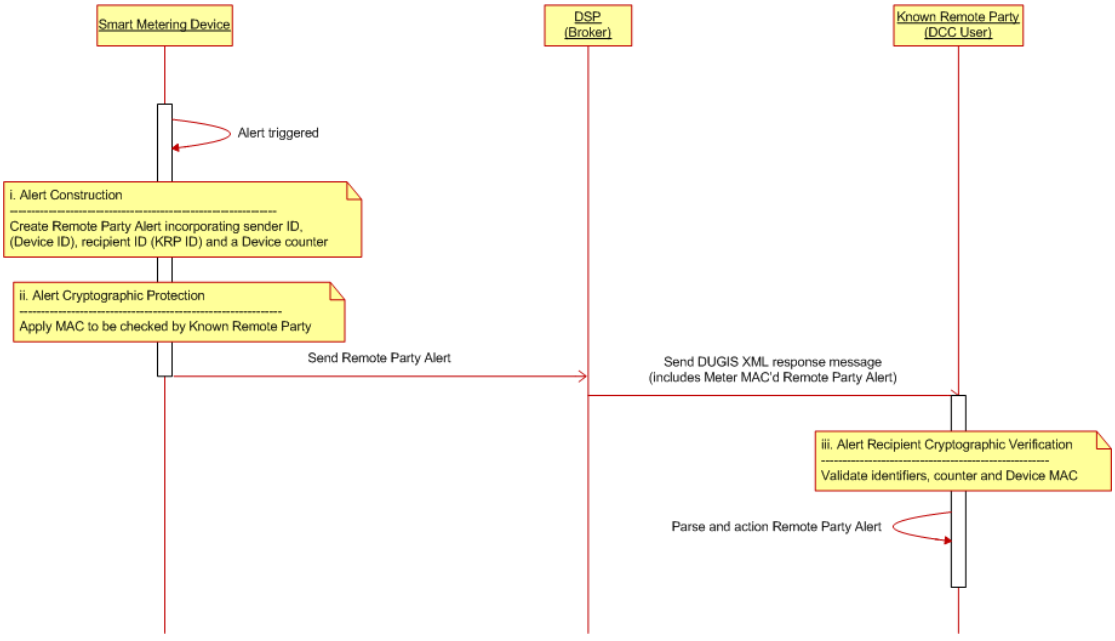
8.3.6 SME.A.C – Critical Alert to Known Remote Party

This command follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1.



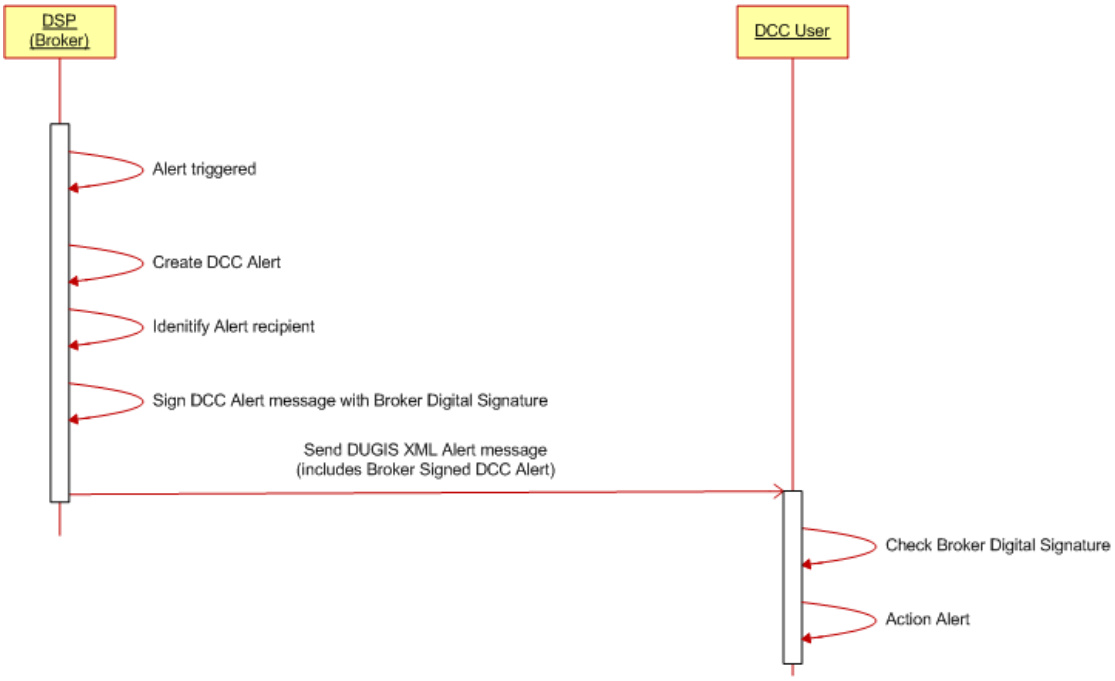
8.3.7 SME.A.NC – Non-Critical Alert to Known Remote Party

This command follows the pattern of that specified in GB Companion Specification subject to the above clarifications described in section 8.1. Note that all Alerts go via the Receive Response Service.



8.3.8 DCC.A – Alert from DSP to DCC Service User

This Alert represents a DCC to DCC Service User interaction that falls outside of the Scope of the GB Companion Specification described in section 8.1. Note that all Alerts go via the Receive Response Service.

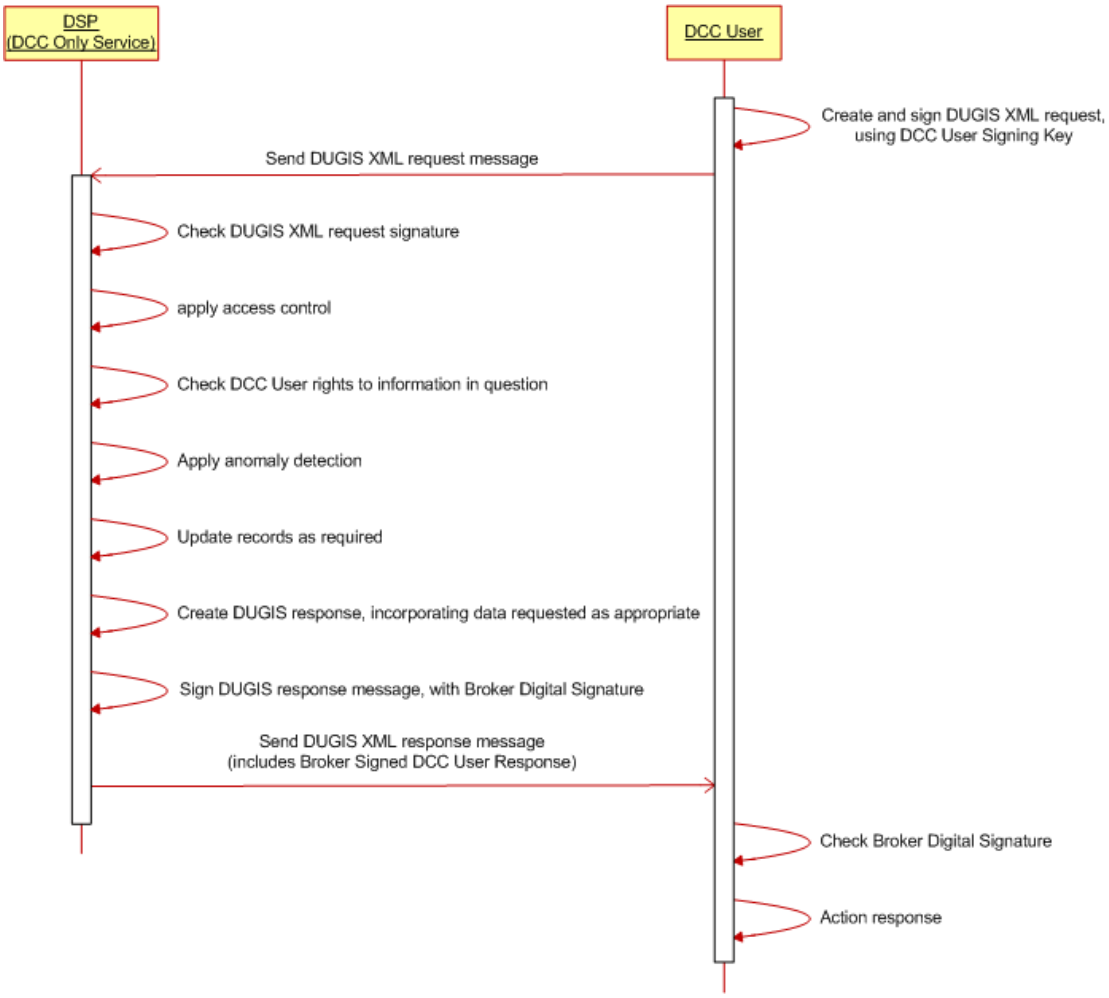


8.3.9 DCC.C – Command from DCC Service User to DCC

This command represents a DCC to DCC Service User interaction that falls outside of the scope of the GB Companion Specification.

It shows how a DCC Service User issues a Service Request via XML to the DCC Only Service; what steps the DCC Only Service takes in terms of its processing, from a security perspective;

and the form of the response. Note that communications in both directions are via XML messages signed using the digital signing key of the sending party.



9 Request and Response Definitions

This section defines the Request and Response Formats and their Header and Common Data Items. The more detailed data attributes associated with each Service Request, Service Response, Device Alert and DCC Alert are contained within the Annex – Service Request Definitions document (Annex).

The DCC User Interface has been designed to be a single common interface to enable communications between DCC and Service Users for all SMETS Devices and so the following Request and Response Definitions are common for all communications regardless of the SMETS version of the Device, except where indicated otherwise.

This documentation set uses the data types defined in XML (prefixed with xs:) and data types defined in this documentation set (prefixed with sr:).

9.1 Request and Response XSD Diagrams

The XSD diagrams in the following 2 sections and in the Annex consist of the following components, described in this example diagram:

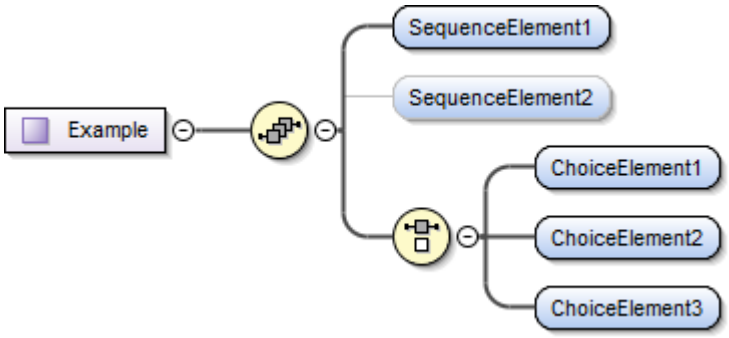


Figure 47 XSD Diagram Components

Example is a complex element consisting of:

- A sequence of
  - Mandatory SequenceElement1
  - Optional SequenceElement2
  - A mandatory choice of one of
    - ChoiceElement1
    - ChoiceElement2
    - ChoiceElement3

Note that all diagrams include the Schema version attribute for the top level element – see section 9.5 for a description of how versions are used.

9.2 Request Format

The Request format is defined in the Request XML element of the XSD (see DUIS XML Schema).

Note that the Request format is common to the DCC User Interface at versions 1.0, 2.0, 3.x. 4.0 and 5.x.

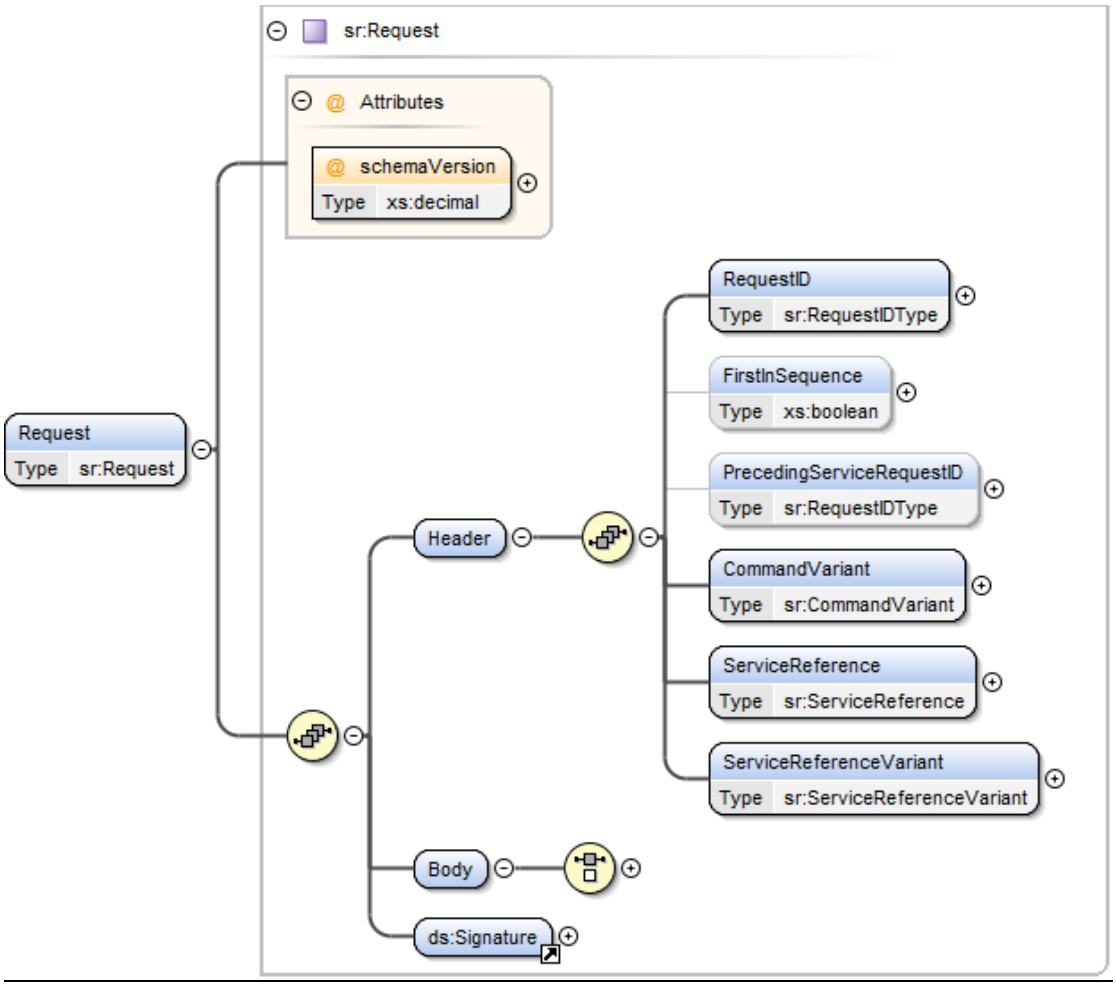


Figure 48 Request Structure

The above diagram is to be read as:

- A Request is a sequence of
    - A mandatory Header. It contains the Request Header Data Items. See Table 17~~Table 17~~
    - A mandatory Body. It contains the choice of Service Request Variants and Signed Pre-command. See section 9.2.1
    - A mandatory Digital Signature (defined in a separate schema). See XMLDSIG XSD for details on the signature schema. It contains the DCC Service User SMKI digital signature of the XML message. See section 8.2.

The following table details the data items in the Header:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
RequestID	Concatenation of BusinessOriginatorID, BusinessTargetID and OriginatorCounter as defined in GBCS, separated by ":". See section 4 for usage	sr:RequestIDType (see Annex section 17)	Yes	None	N/A	Non-Sensitive
FirstInSequence	Flag to indicate that a Request is the first in a sequence. See section 6 Valid set: • true. (Yes) • false. (No)	xs:boolean The User shall add to the first Request in a sequence when using sequencing functionality	No	None	N/A	Non-Sensitive
PrecedingServiceRequestID	The unique identifier (RequestID) of a preceding Request when this particular Request is intended to be executed specifically after the preceding Request. See section 6	sr:RequestIDType (see Annex section 17) The User shall add to a Request in a sequence (other the first) when using sequencing functionality	No	None	N/A	Non-Sensitive
CommandVariant	Value to indicate to the DCC Data Systems if a Request has to be: • transformed to a GBCS command • or sent via the CSP network, returned to the DCC Service User to be locally applied (via a Hand Held Terminal or in some cases via the customer entering a code on the device or PPMID) or both • or executed by DCC See section 3 Possible Values 1. Send (Non-Critical) 2. Return for local delivery (Non-Critical) 3. Send and Return for local delivery (Non-Critical) 4. Transform 5. Send (Critical) 6. Return for local delivery (Critical) 7. Send and Return for local delivery (Critical) 8. DCC Only Request	sr:CommandVariant (see Annex section 17)	Yes	None	N/A	Non-Sensitive
ServiceReference	Identifier that signals the particular type of Request to DCC (and is driven from the DCC Service User's selection of Request) See 'Service Reference' column in Table 36~~Table 36~~	sr:ServiceReference (see Annex section 17)	Yes	None	N/A	Non-Sensitive
ServiceReferenceVariant	Identifier that signals the particular Request Variant to DCC (and is driven from the DCC Service User's selection of Request) See 'Service Reference Variant' column in Table 36~~Table 36~~	sr:ServiceReferenceVariant (see Annex section 17)	Yes	None	N/A	Non-Sensitive

Table 17 Request Header Data Items

9.2.1 Request Body Format

The Request Body includes the list (as a choice) of all the Service Request Variants and the Signed Pre-command. This list can be sub-divided as follows:

- "Device" Service Requests. For the full list please see Table 36~~Table 36~~ where "DCC Only " is "No".
- "Non-Device" Service Requests. For the full list please see Table 36~~Table 36~~ where "DCC Only " is "Yes".
- Signed Pre-command. Applicable to those Service Request Variants in Table 36~~Table 36~~ where "DCC Only " is "No" and "Critical" is "Yes".

In all cases the Request Body has to include the XML element specific to that request.

For Service Requests that include data items the XML element will include the Service Request Name and the data items.

For Service Requests that don't include data items, the XML element will only contain the name in one of 2 ways:

<ServiceRequestName1></ServiceRequestName1>
Or
<ServiceRequestName1/>

9.2.1.1 "Device" Service Requests Format

The "Device" format is applicable to all Service Requests where the Business Target ID is a Device ID. For Critical Service Requests, this is the Service Request sent to the Transform Service. See section 3.

The Service Request specific XML section depends on the actual Service Request. It can either contain plain text (non-Sensitive) or a combination of plain text (non-Sensitive) and encrypted data (Sensitive). See Annex for details of each "Device" Request.

Figure 49~~Figure 49~~ includes a 'choice' of "Device" Service Requests (Service Reference Variants). For readability reasons, this 'choice' includes only a subset of "Device" Service Requests. For the full list please see Table 36~~Table 36~~ where "DCC Only " is "No".

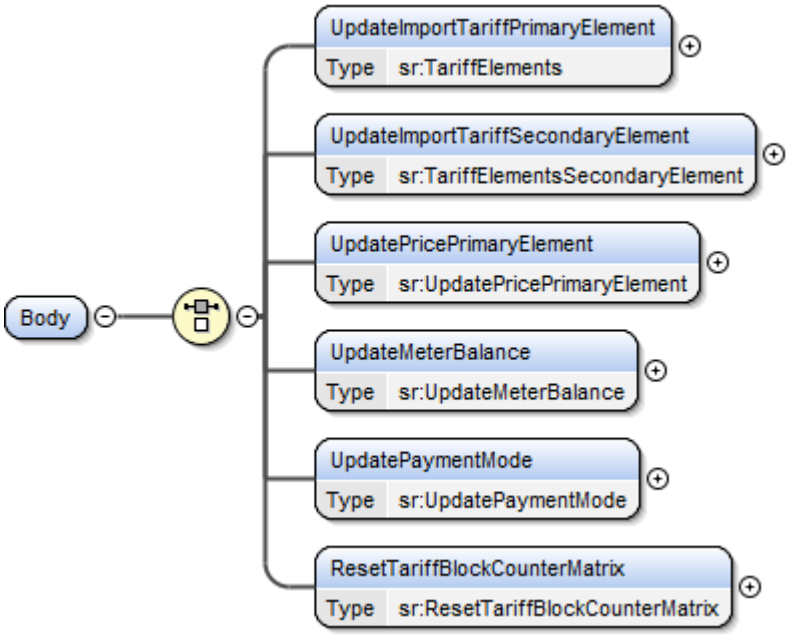


Figure 49 Request Body Structure ("Device" Service Requests subset)

9.2.1.1.1 Non-Critical "Device" Service Requests – Applicable Command Variant Values

The Command Variant values applicable to Non-Critical "Device" Service Requests are (see section 3 for Command Variant definitions):

CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
Yes	Yes	Yes	No	No	No	No	No

Table 18 Non-Critical "Device" Service Requests Command Variant Values

9.2.1.1.2 Critical "Device" Service Requests – Applicable Command Variant Values

The Command Variant values applicable to Critical "Device" Service Requests (Transform Requests) are (see section 3 for Command Variant definitions):

CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
No	No	No	Yes	No	No	No	No

Table 19 Critical "Device" Service Requests Command Variant Values

9.2.1.2 "Non-Device" Service Requests Format

The "Non-Device" format is applicable to all Service Requests where the Business Target ID is the DSP Access Control Broker ID.

The Service Request specific XML section depends on the actual Service Request. See Annex for details of each "DCC Only" Request.

Figure 50~~Figure 50~~ includes the 'choice' of "Non-Device" Service Requests (Service Reference Variants). Please see Table 36~~Table 36~~ where "DCC Only " is "Yes".

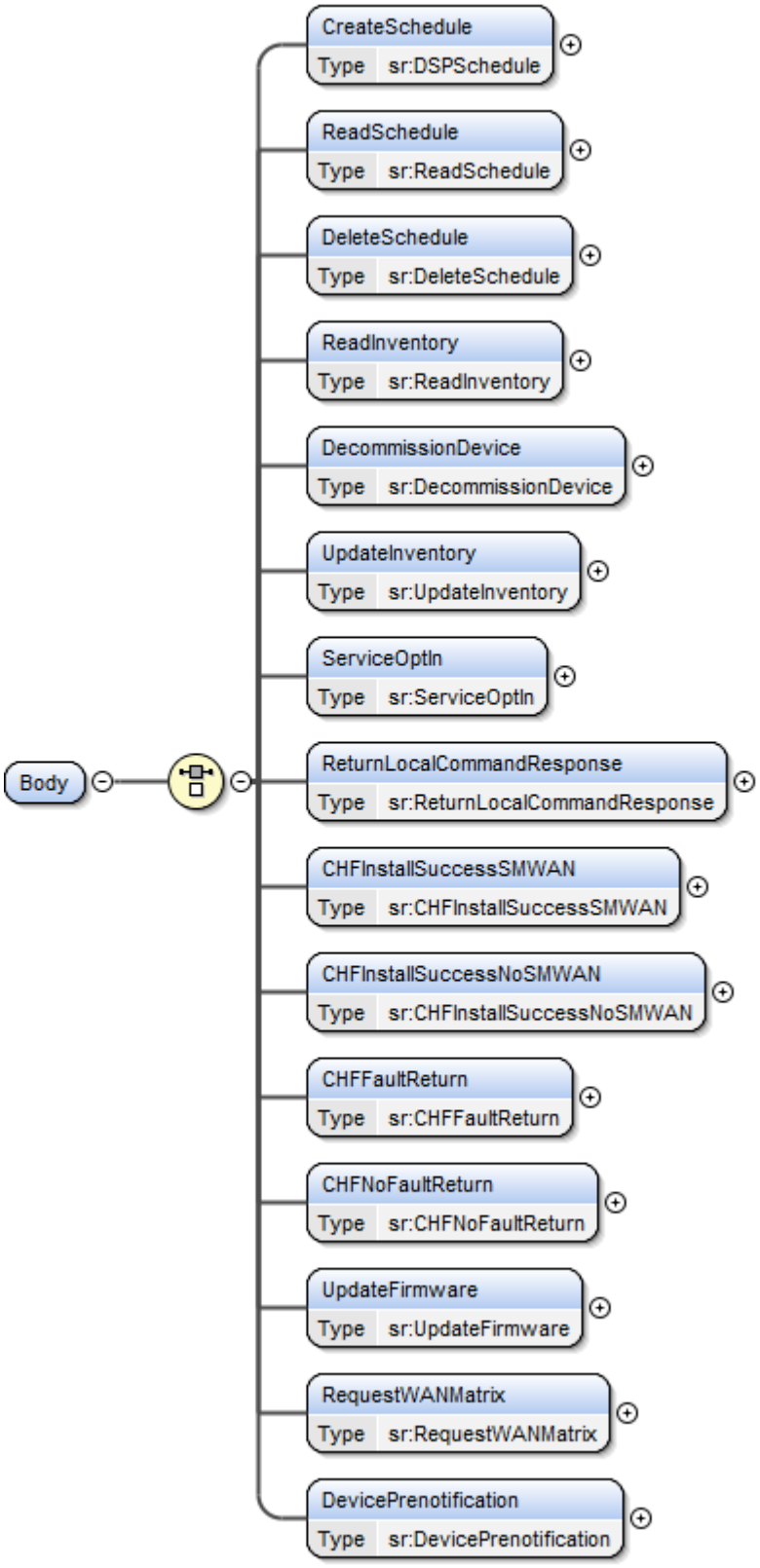


Figure 50 Service Request Body Structure (“Non-Device” Service Requests)

9.2.1.2.1 “Non-Device” Service Requests – Applicable Command Variant Values

The Command Variant values applicable to “Non-Device” Service Requests are (see section 3 for Command Variant definitions):

CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
No	No	No	No	No	No	No	Yes

Table 20 "Non-Device" Service Requests Command Variant Values

9.2.1.3 Signed Pre-command Format

The Signed Pre-command is applicable to those Service Request Variants in Table 36~~Table 36~~ where "DCC Only " is "No" and "Critical" is "Yes". See section 3.

The Signed Pre-command XML section contains the GBCSpayload which is the transformed Command signed by the DCC Service User. It may also contain a Future Dated Execution date/time (see section 5.1).

Figure 51~~Figure 51~~ includes a 'choice' of Signed Pre-command.

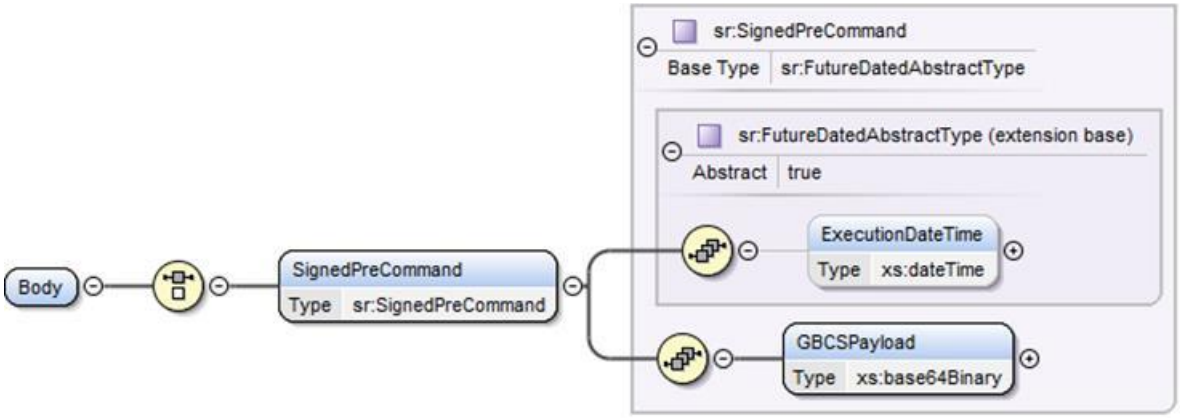


Figure 51 Request Body Structure (Signed Pre-command subset)

The additional data items included alongside the GBCSpayload are as follows.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ExecutionDateTime	For Future Dated requests, the UTC date and time the DCC Service User requires the command to be executed on the Device ID Valid set: • Date-time in the future that is either <= current date + 30 days or the date = 31/12/3000	xs:dateTime	Future Dated requests: Yes Otherwise: N/A	None	UTC Date-Time	Non-Sensitive

Table 21 Signed Pre-Command Additional Data Items

9.2.1.3.1 Signed Pre-command – Applicable Command Variant Values

The Command Variant values applicable to Signed Pre-commands are (see section 3 for Command Variant definitions):

CV = 1	CV = 2	CV = 3	CV = 4	CV = 5	CV = 6	CV = 7	CV = 8
No	No	No	No	Yes	Yes	Yes	No

Table 22 Signed Pre-command Command Variant Values

9.3 Response Format

A Response is composed of an XML document, identifying (where applicable) the original Service Request, the Device, the DCC Service User and the data (XML or GBCS) and / or response code for the request.

The Response format is defined in the Response XML element of the XSD (see DUIS XML Schema).

Note that the SMETS1ResponseMessage definition which includes SMETS1 Responses and SMETS1 Alerts was added to the Response format in version 3.0.

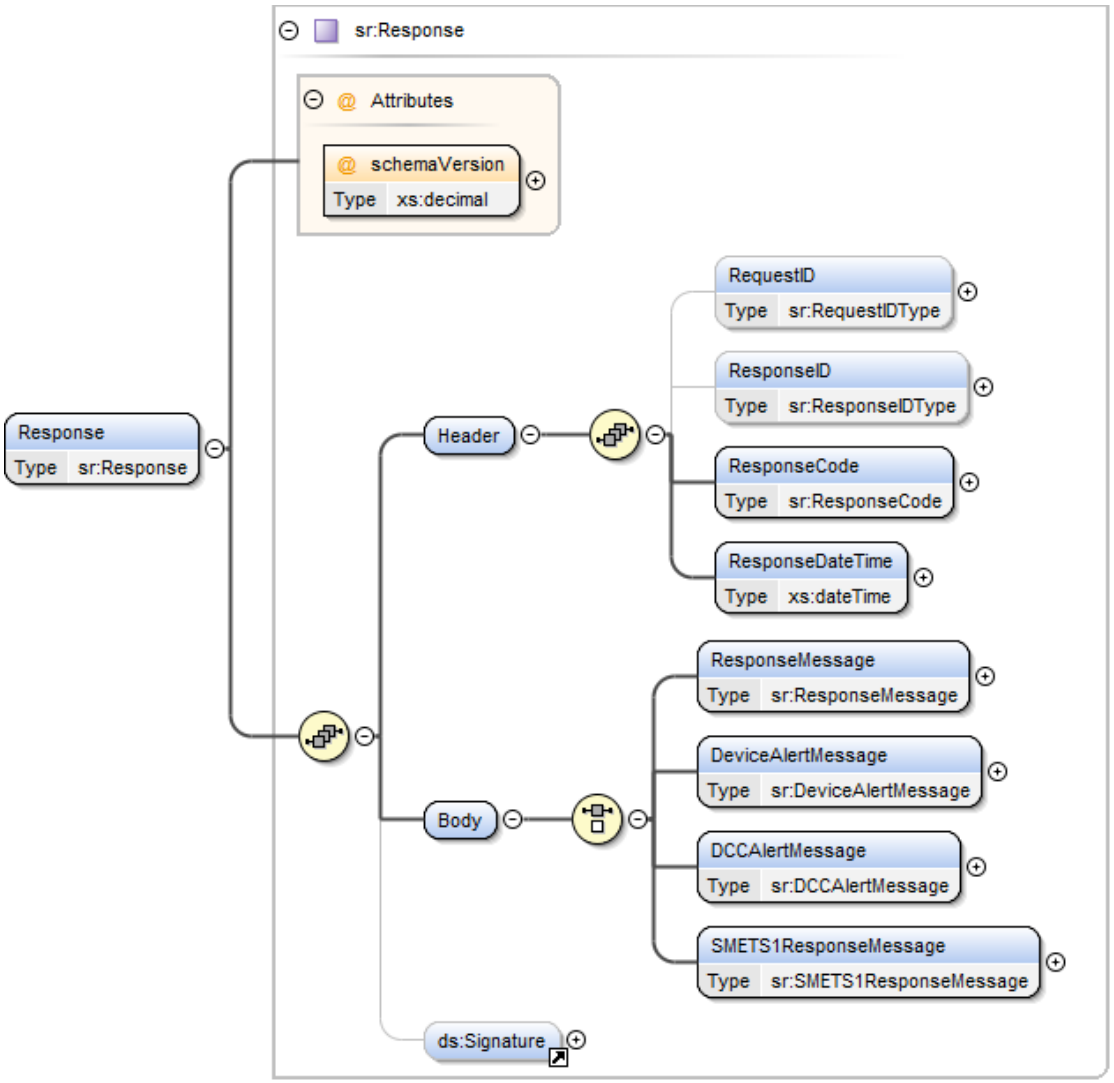


Figure 52 Response Structure

The above diagram is to be read as:

- A Response is a sequence of
  - A mandatory Header. It contains the Request Header Data Items. See Table 23~~Table 23~~
  - A mandatory Body. It contains a choice of Response Message, Device Alert, DCC Alert and SMETS1 Response Message. See section 9.3.1, 9.3.2, 9.3.3 and 9.3.4.

- An optional Digital Signature (defined in a separate schema). See XMLDSIG XSD for details on the signature schema. See section 8.2 for details of which signatures are used on which Responses.

The following table details the data items in the Header:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
RequestID	Concatenation of BusinessOriginatorID, BusinessTargetID and OriginatorCounter as defined in GBCS, separated by ":". See section 4 for usage	sr:RequestIDType (see Annex section 17)	solicited response from DCC: Yes solicited response from Device: Yes unsolicited response (Device or DCC Alert): N/A	None	N/A	Non-Sensitive
ResponseID	Concatenation of Response BusinessOriginatorID, BusinessTargetID and OriginatorCounter as defined in GBCS, separated by ":". See section 4 for usage	sr:ResponseIDType (see Annex section 17)	solicited response from DCC: N/A solicited response from Device: Yes unsolicited response (Device or DCC Alert): Yes	None	N/A	Non-Sensitive
ResponseCode	Code indicating the success or exceptions generated by the original request. These codes are listed in this document or at a Service Request level where there is a specific response code for that request. For Device responses, the Response Code will always be success. Any error codes will be included in the GBCS response form the device Valid set: See section 12.3, Annex section 15 and Annex 1 to Annex 16 validation sections.	Sr:ResponseCode (see Annex section 17)	Yes	None	N/A	Non-Sensitive
ResponseDateTime	Date and time extracted from Device Response, if available, or added to the response by DCC when sending message to the DCC Service User Valid set: • Valid date-time	xs:dateTime	Yes	None	UTC date-time	Non-Sensitive

Table 23 Response Header Data Items

The Response Types defined in the following sections are:

SMETS version Applicability	Response Type	Response Delivery Pattern
All	Acknowledgement	Synchronous
All	Service Response from DCC (DCC Only)	Synchronous
SMETS2 or later	Pre-command	Synchronous
SMETS2 or later	Command for Local Delivery	Synchronous / Asynchronous
SMETS2 or later	Service Response (from Device)	Asynchronous
SMETS2 or later	Device Alert	Asynchronous
All	DCC Alert	Asynchronous
SMETS1	SMETS1 Response	Asynchronous
SMETS2 or later	Parse Output	Asynchronous

Table 24 Response Types and Response Delivery Pattern

The initial response to a DCC Service User Request is returned to the DCC Service User synchronously. All other responses (solicited and unsolicited) are returned asynchronously.

9.3.1 Response – ResponseMessage Formats

The ResponseMessage format is used for all solicited Responses related to SMETS2 Requests and for Acknowledgement and "Service Response from DCC (DCC Only)" related to Requests for SMETS1 Devices.

There are several different types of Response which use this format, but they all include the Service Reference from the original Request. The following table details the common data items in the ResponseMessage format:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ServiceReference	Identifier that signals the particular Request to DCC (and is driven from the DCC Service User's selection of Request) See 'Service Reference' column in Table 36~~Table 36~~	sr:ServiceReference (see Annex section 17)	Yes	None	N/A	Non-Sensitive
ServiceReferenceVariant	Identifier that signals the particular Request Variant to DCC (and is driven from the DCC Service User's selection of Request) See 'Service Reference Variant' column in Table 36~~Table 36~~	sr:ServiceReferenceVariant (see Annex section 17)	Yes	None	N/A	Non-Sensitive

Table 25 Response – ResponseMessage Common Data Items

Note: For DSP Scheduled responses, the ServiceReference and ServiceReferenceVariant are those of the ServiceReferenceVariant being scheduled, e.g. if SR 5.1 Create Schedule includes DSPScheduledServiceReference = 4.8 and DSPScheduledServiceReferenceVariant = 4.8.1, each activation instance response will include ServiceReference = 4.8 and ServiceReferenceVariant = 4.8.1

The following ResponseMessage formats do not apply to Service Responses associated with SMETS1 Devices:

- PreCommand Format
- LocalCommand Format

- GBCSPayload Format
- CINMessage Format
- DSPScheduledMessage Format
- FutureDatedDeviceAlertMessage Format

9.3.1.1 Acknowledgement Message Format

The Acknowledgement Message format is applicable to:

- All “Device” Service Requests that are to be delivered over the SM WAN
- all Service Responses to DCC Only Service Requests that don’t return data
- All Service Requests that fail Access Control
- All Signed Pre-Commands that are to be delivered over the SM WAN

The only items included in the response are the common data items that are included in all Responses. For the avoidance of doubt there is no further payload in an Acknowledgement message.

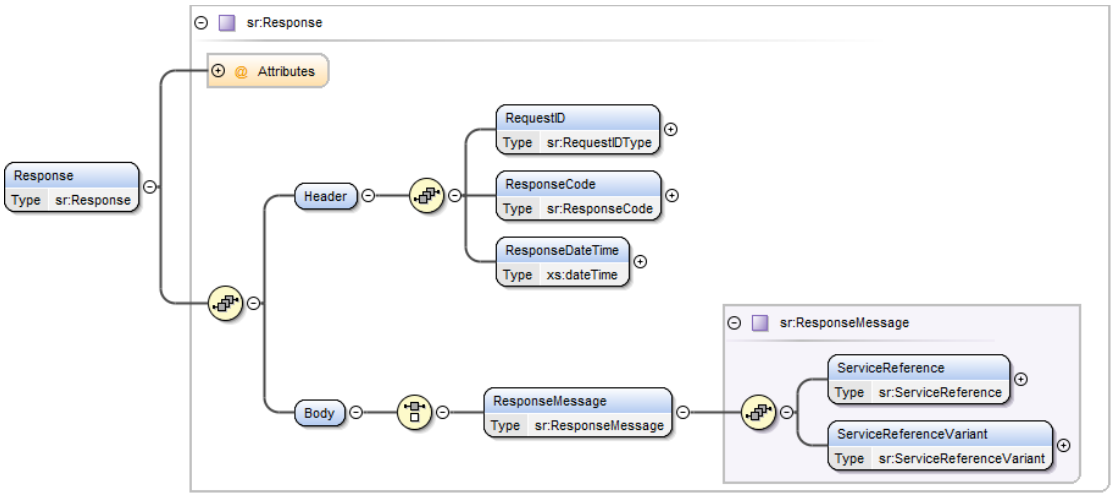


Figure 53 Response – Acknowledgement Message Structure

9.3.1.2 Service Response (from DCC) – DCCOnly Format

The DCCOnly format is applicable to Service Responses to DCC Only Service Requests.

The Service Response specific XML section depends on the actual Service Request. Where the Service Request requires data items to be returned in the response then it will contain a

Service Response specific element containing that data. See Annex for details of each such "DCC Only" Service Response.

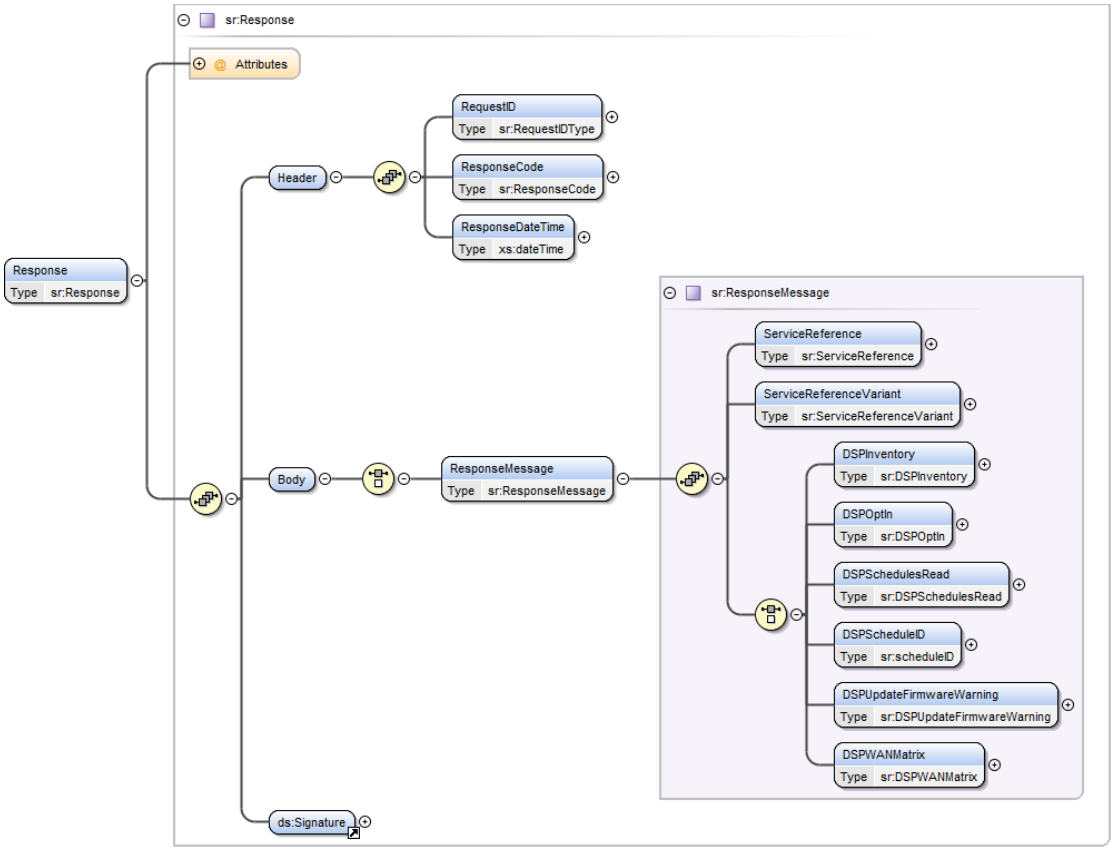


Figure 54 Response – Service Response – "DCC Only" Structure

Where the Service Request requires no data to be returned then an Acknowledgement Message is returned (see section 9.3.1.1), i.e. there is no Service Response specific element and the Response simply contains the Service Reference and Service Reference variant in the Body and the common items in the Header (including ResponseCode to indicate success (ResponseCode = I99) or failure).

9.3.1.3 Pre-command – PreCommand Format

The PreCommand format is applicable to responses to Service Requests that instruct the DCC to transform the request into a Pre-command.

The Service Response contains the GBCSPayload within the PreCommand i (see GBCS for details of how the GBCSPayload is constructed) and the version of the GBCS Use Case used to create the GBCSPayload (see section 9.5 for details on managing versions). Note that the GBCSPayload within the Pre-Command is a binary object which has been Base64 encoded and the binary object does not include a Message Authentication Code in either the MAC Header or ACB-SMD MAC as defined by GBCS Command structure. The binary object is constructed as per GBCS, and has the following structure;

Grouping Header || Command Payload || 0x00

Note that the 0x00 represents (in the DLMS COSEM ASN.1 schema) a signature of zero length.

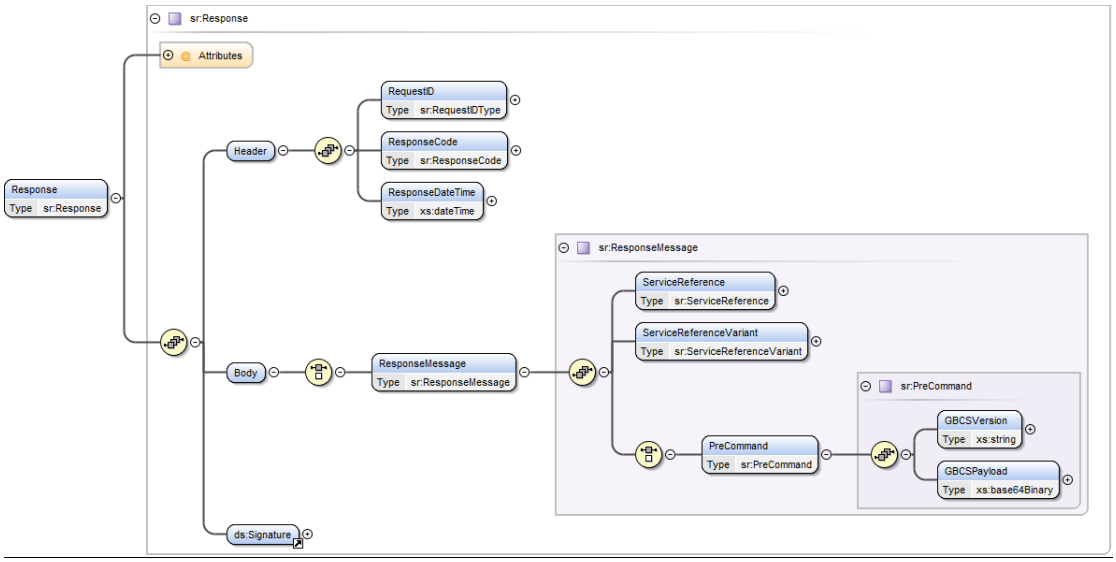


Figure 55 Response – Service Response – PreCommand Structure

The table below shows the data items returned.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
GBCSVersion	GBCS version number associated with the GBCS payload being returned. This is provided to allow the Correlate software to determine which version of GBCS command it should be checking. (See also section 9.5). The version number format will align with the CPL For example 1.0, 2.0	xs:string	Yes	None	N/A	Non-Sensitive
GBCSPayload	See GB Companion Specification for Details GBCSPayload is a binary object which has been Base64 encoded. The binary object is constructed as per GBCS, and has the following structure; Grouping Header || Command Payload || 0x00	xs:base64Binary	Yes	None	N/A	N/A

Table 26 Response – Pre-Command Data Items

9.3.1.4 Command for Local Delivery – LocalCommand Format

The LocalCommand format is applicable to responses to Service Requests or Signed Pre-Commands for which Local Command Services have been requested. A MAC is added to the associated Command generated by Transform and the Command is returned it to the DCC Service User for Local Delivery (see section 3). Its structure is similar to that of the PreCommand (see section 9.3.1.3), but the LocalCommand GBCSPayload includes the DSP

Access Control Broker MAC within the MAC Header and ACB-SMD MAC parts of the GBCS Payload.

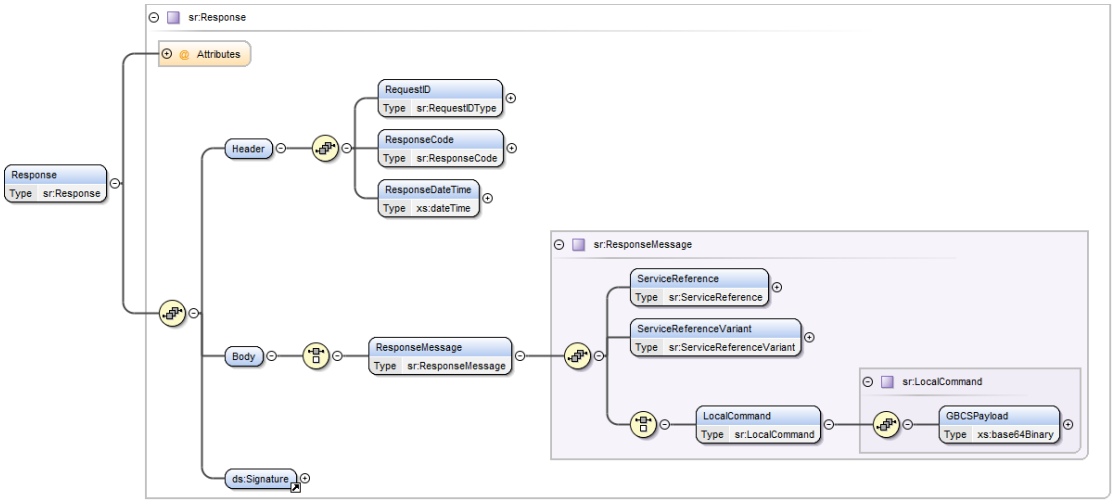


Figure 56 Response – Service Response – LocalCommand Structure

The table below shows the data items returned.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
GBCSPayload	See GB Companion Specification for Details GBCSPayload is a binary object which has been Base64 encoded. The binary object is constructed as per GBCS, and has the following structure; For Critical Commands: MAC Header || Grouping Header || Command Payload || 0x40 || KRP Signature || ACB-SMD MAC For Non-Critical Commands MAC Header || Grouping Header || Command Payload || 0x00 || ACB-SMD MAC	xs:base64Binary	Yes	None	N/A	N/A

Table 27 Response – LocalCommand Data Items

9.3.1.5 Service Response (from Device) – GBCSPayload Format

The GBCSPayload format is applicable to Service Responses from the Device to the DCC Service User. See Annex for details on the different Device Service Responses.

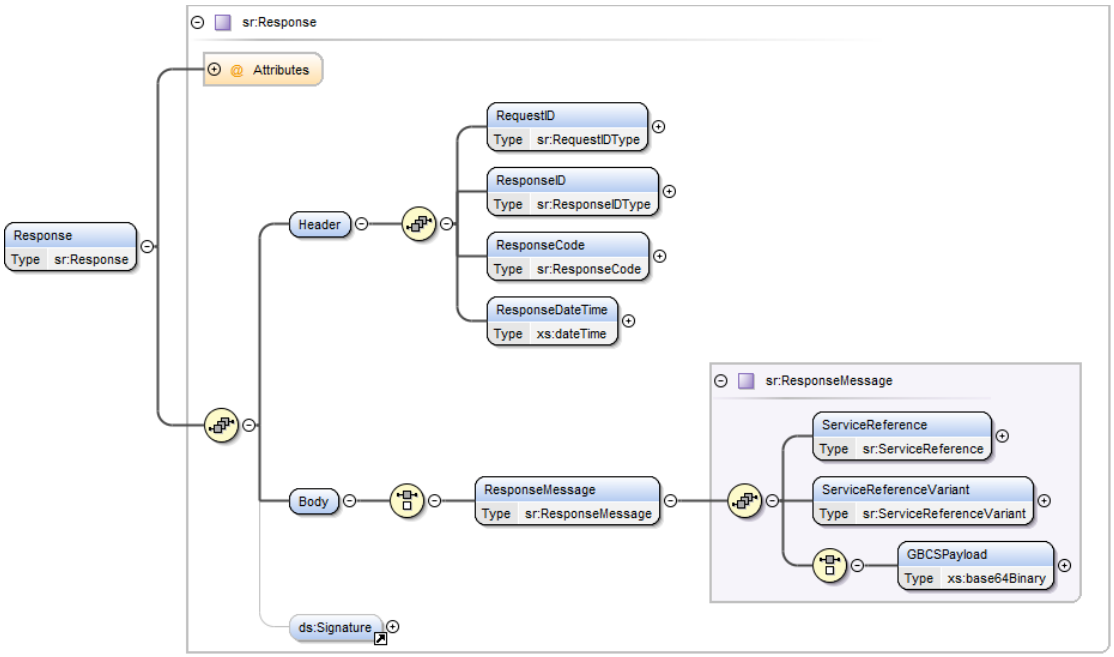


Figure 57 Response – Service Response – GBCSPayload Structure

The table below shows the data items returned.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
GBCSPayload	See GB Companion Specification for Details For Critical Responses: Grouping Header || Response Payload || 0x40 || SMD Signature For non-critical Responses: MAC Header || Grouping Header || Response Payload || 0x00 || SMD-KRP MAC	xs:base64Binary	Yes	None	N/A	N/A

Table 28 Response – GBCSPayload Data Items

9.3.1.6 Service Response (from Device) – CINMessage Format

The CINMessage format is applicable to successful Service Responses from the Device to the DCC Service User for which the DSP Access Control Broker has to add the CIN to the Device response, i.e. Service Request 9.1 Request Customer Identification Number. This message combines the GBCSPayload received from the Device with the Customer Identification Number generated by the DCC Data Systems. See Annex for details.

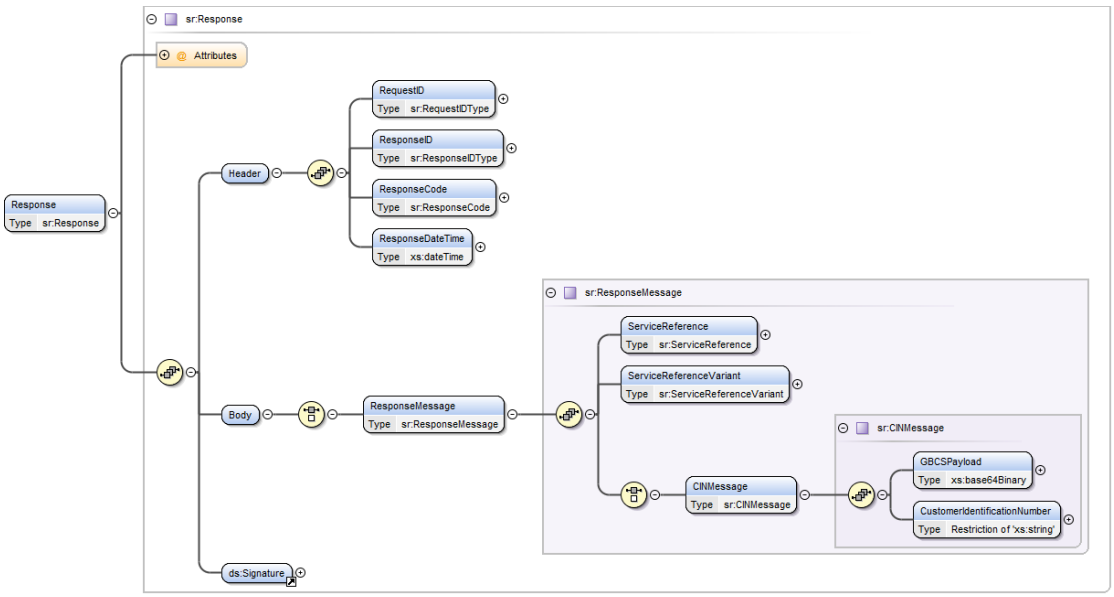


Figure 58 Response – Service Response – CINMessage Structure

The table below shows the data items returned.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
GBCSPayload	See GB Companion Specification for Details For non-critical Responses: MAC Header || Grouping Header || Response Payload || 0x00 || SMD-KRP MAC	xs:base64Binary	Yes	None	N/A	N/A
CustomerIdentificationNumbe	A number issued to Electricity Smart Meter / Gas Smart Meter for display on the User Interface	Restriction of xs:string (length = 4 pattern = "[0-9]{4}")	Yes	None	N/A	N/A

Table 29 Response – CINMessage Data Items

9.3.1.7 Service Response (from Device) – DSPScheduledMessage Format

For SMETS2 or later Devices, the DSPScheduledMessage format is applicable to Service Responses from the Device to the DCC Service User for which the DSP Access Control Broker has to add the DSP Schedule ID to the Device response, i.e. DSP Scheduled Device responses. This message combines the GBCSPayload received from the Device with the DSP Schedule ID. See Annex for details.

Note: For DSP Scheduled responses, the ServiceReference and ServiceReferenceVariant are those of the ServiceReferenceVariant being scheduled, e.g. if SR 5.1 Create Schedule includes DSPScheduledServiceReference = 4.8 and DSPScheduledServiceReferenceVariant = 4.8.1, each activation instance response will include ServiceReference = 4.8 and ServiceReferenceVariant = 4.8.1

For SMETS1 Devices, the format described in this section is not used, and responses corresponding to scheduled messages will be returned in the SMETS1ResponseMessage format described in section 9.3.4. Note that the DSP schedule ID included in the DSPScheduledMessage format for SMETS2 or later Devices is instead included in the SMETS1ResponseMessage format for SMETS1 Devices.

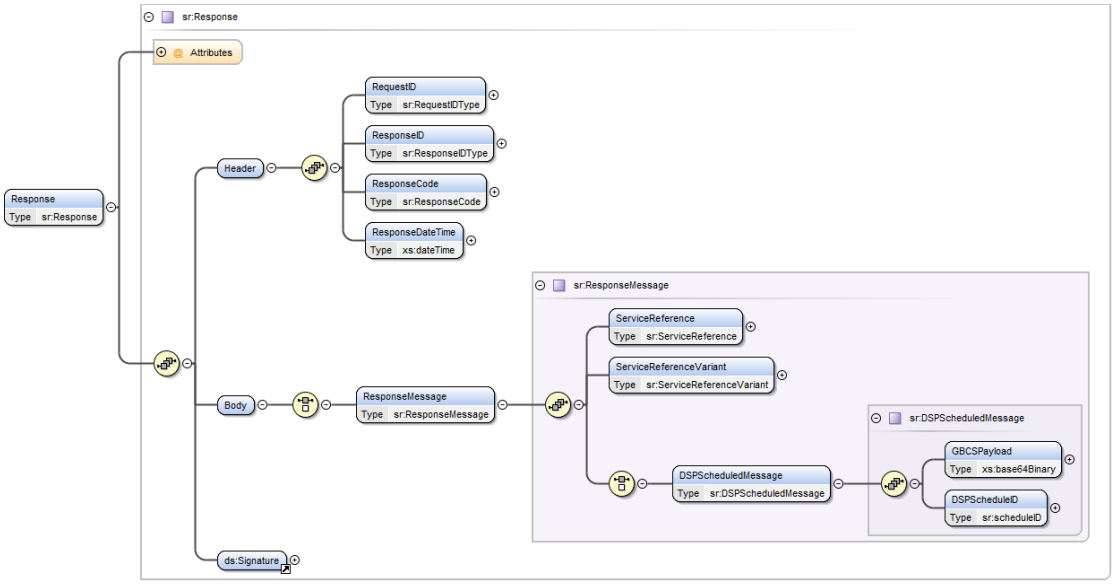


Figure 59 Response – Service Response – DSPScheduledMessage Structure

The table below shows the data items returned.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
GBCSPayload	See GB Companion Specification for Details For non-critical Responses: MAC Header || Grouping Header || Response Payload || 0x00 || SMD-KRP MAC Note that for all DSP Scheduled Responses the Known Remote Party will be the ACB (not the DCC Service User)	xs:base64Binary	Yes	None	N/A	N/A
DSPScheduleID	Schedule ID generated by the DCC Data Systems Valid Set: >= 0 and <= 1000000000000	sr:scheduleID (Restriction of xs:nonNegativeInteger) See Annex 17	Yes	None	N/A	N/A

Table 30 Response – DSPScheduledMessage Data Items

9.3.1.8 Service Response (from Device) – FutureDatedDeviceAlertMessage Format

The FutureDatedDeviceAlertMessage format is applicable to Alerts from the Device to the DCC Service User for Future Dated Command execution. This message structure is very similar to that of the Service Response GBCS Payload (see section 9.3.1.5), but in this case the GBCS Payload is actually an Alert (rather than a Response) and the Request ID, Service Reference and Service Reference Variant are those of the Request for which the Device Alert is the Response. The following is also added to the XML Response:

- FutureDatedAlertCode of the Device Alert
- InstructionNumber. Only relevant for multiple instruction Commands. Set to 1 for single instruction Commands
- TotalCommandInstructions. Only relevant for multiple instruction Commands. Set to 1 for single instruction Commands

For multiple instruction commands, the InstructionNumber in any given Response is simply a count of how many Alerts have been received so far by the DCC to indicate execution of the Command. The TotalCommandInstructions is always set to the total number of Alerts expected for the specific Command being executed (as defined in the relevant Annex and summarised in Annex 15 section 15.4.4.5). The two attributes thus provide a means to track the Responses as, for example, 1 of 3, 2 of 3 and finally 3 of 3 when all expected Device Alerts have been received.

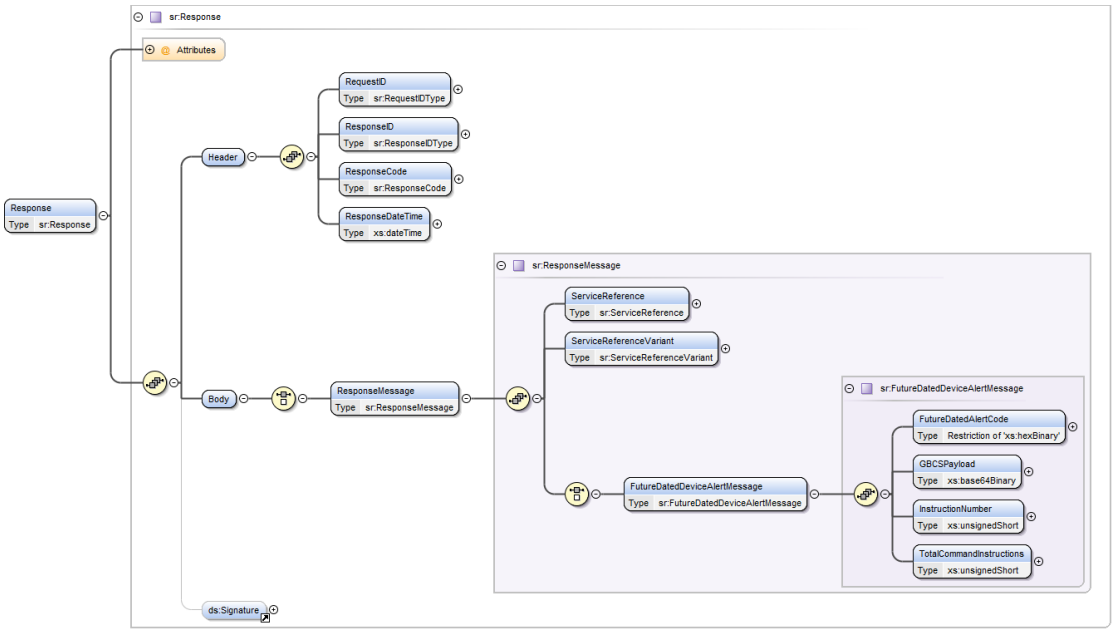


Figure 60 Response – Service Response – FutureDatedDeviceAlertMessage Structure

The following table details the data items in the Future Dated Device Alert Message:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
FutureDatedAlertCode	Code indicating the alert or reason for the alert to be generated Valid set: The FutureDatedAlertCode can only have a value of 8F66 for success and 8F67 for failure. See GBCS	xs:hexBinary	Yes	None	N/A	Non-Sensitive
GBCSPayload	See GB Companion Specification for Details For Critical Device Alerts: Grouping Header || Alert Payload || 0x40 || SMD Signature	xs:base64Binary	Yes	None	N/A	N/A

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
InstructionNumber	Indicates the number of Alerts received by the DCC (ie the number of activation date-time instructions executed) so far in respect of the Command for which the Future Dated Device Alert is a Response. Valid set: • 1. Single activation date-time Instruction Command • >= 1 and <= TotalCommandInstructions (as defined in the relevant Annex and summarised in Annex 15 section 15.4.4.5). Multiple activation date-time instruction Command	xs:unsignedShort	Yes	None	N/A	Non-Sensitive
TotalCommandInstructions	Indicates the total number of activation date-time instructions in the Command for which the Future Dated Device Alert is a Response. Valid set: • 1. Single activation date-time Instruction Command • m (GBCS Use Case dependent. See relevant Annex). Multiple activation date-time instruction Command	xs:unsignedShort	Yes	None	N/A	Non-Sensitive

Table 31 Response – Future Dated Device Alert Data Items

9.3.2 Device Alert – DeviceAlertMessage Format

The DeviceAlertMessage format is applicable to SMETS2 or later Device Alerts. This message combines the GBCSPayload received from the Device with the Alert Code extracted from the GBCSPayload.

If an Alert Code is subject to throttling, two optional data elements are included to show the count of consolidated Alerts and the sequence number of the passed through Alert.

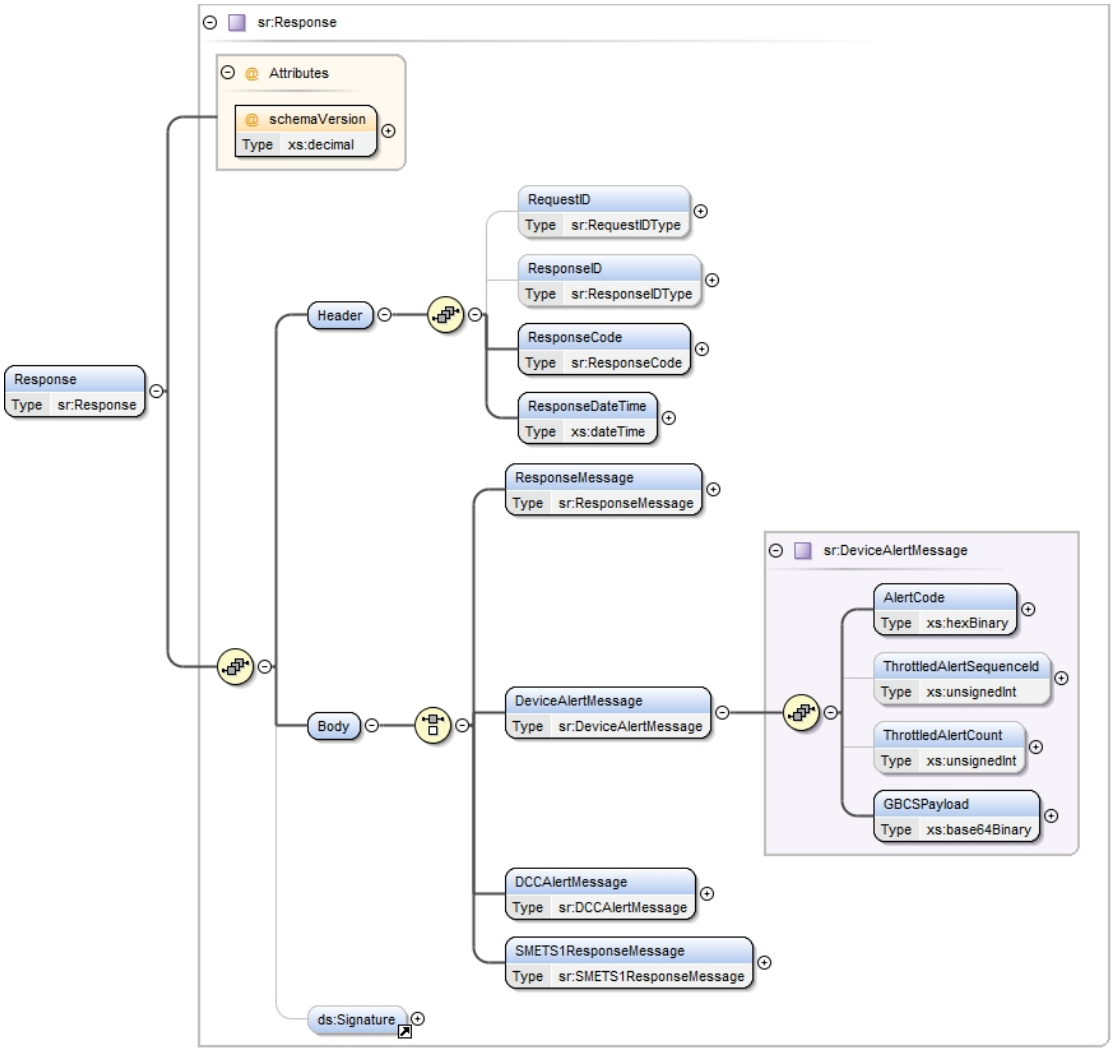


Figure 61 Response – DeviceAlertMessage Structure

The following table details the data items in the Device Alert Message:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
AlertCode	Code indicating the alert or reason for the alert to be generated GBCS includes '0x' at the start of such codes. This definition uses a hexBinary representation for valid values. Valid set: See GBCS for base list and apply hexBinary representation of these GBCS defined values	xs:hexBinary	Yes	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ThrottledAlertSequenceID	An optional data item that identifies that this Alert Code is currently subject to throttling by the DCC Data Systems. If this attribute is included in the Alert then it indicates the sequence number for this Alert message since Alert throttling began.	xs:unsignedInt	No	None	N/A	Non-Sensitive
ThrottledAlertCount	An optional data item used to indicate the number of Alerts that have been consolidated by DCC Data Systems since the last Alert was forwarded to the Service User.	xs:unsignedInt	No	None	N/A	Non-Sensitive
GBCSPayload	See GB Companion Specification for Details for message construction. For Critical Device Alerts: Grouping Header || Alert Payload || 0x40 || SMD Signature For Non-Critical Device Alerts: MAC Header || Grouping Header || Alert Payload || 0x00 || SMD-KRP MAC	xs:base64Binary	Yes	None	N/A	N/A

Table 32 Response – Device Alert Data Items

9.3.3 DCC Alert – DCCAlertMessage Format

The DCCAlertMessage format is applicable to DCC Alerts. This message is generated by the DCC Data Systems as a result of a trigger event. For DCC Alert details see Table 49~~Table 49~~ and Annex section 16.

If an Alert Code is subject to throttling, two optional data elements are included to show the count of consolidated Alerts and the sequence number of the passed through Alert.

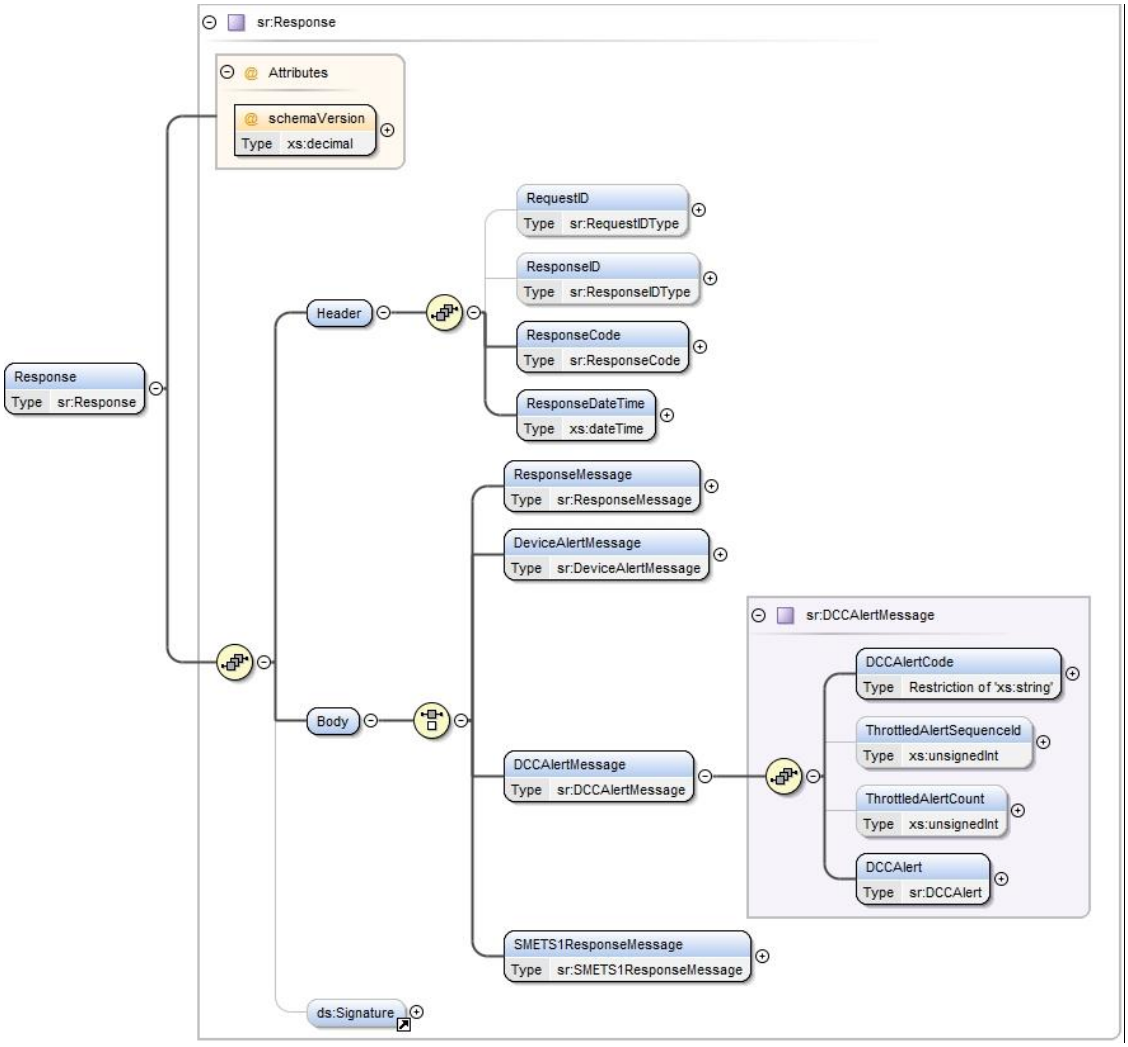


Figure 62 Response – DCCAlertMessage Structure

The following table details the data items in the DCC Alert Message:

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
DCCAlertCode	Code indicating the Alert or reason for the Alert to be generated by DCC Valid set: See Table 49~~Table 49~~	Restriction of xs:string (Enumeration)	Yes	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
ThrottledAlertSequenceID	An optional data item that identifies that this Alert Code is currently subject to throttling by the DCC Data Systems. If this attribute is included in the Alert then it indicates the sequence number for this Alert message since Alert throttling began.	xs:unsignedInt	No	None	N/A	Non-Sensitive
ThrottledAlertCount	An optional data item used to indicate the number of Alerts that have been consolidated by DCC Data Systems since the last Alert was forwarded to the Service User.	xs:unsignedInt	No	None	N/A	Non-Sensitive
DCCAlert	This is body specific content dependent on the DCCAlertCode being sent. See section 13 and Annex 16 for body specific format.	Sr:DCCAlert See section 13 and Annex 16	Yes	None	N/A	N/A

Table 33 Response – DCC Alert Data Items

9.3.4 Response – SMETS1 Response Message Format

The DUIS XML SMETS1ResponseMessage format defines:

- SMETS1 Responses from S1SPs, which when wrapped and signed by the DCC Data Systems become Countersigned SMETS1 Responses; and
- SMETS1 Alerts from S1SPs, which when wrapped and signed by the DCC Data Systems become Countersigned SMETS1 Alerts.

Annex section 19 describes the use of the DUIS XML Schema SMETS1 Response Message format. Schema fragments for individual SMETS1 Responses are described in sub-sections within the Service Request descriptions in the Service Request Definition annexes. Schema fragments for those SMETS1 Alerts that include specific payload are described in Annex 15.

Note that for SMETS1 Devices, scheduled requests do not have a dedicated response format, unlike for SMETS2 or later Devices; instead they are conveyed in Countersigned SMETS1 Responses and are indicated by the population of the DSP schedule ID within the message format.

9.3.5 Parse Output Format

The Parse Output format defines the output of the Parse function which is used to translate GBCS format device responses into a more accessible format. This format will use the DCC Service User Message Mapping Catalogue XML schema, which is very similar to the XML schema used for the other DCC responses.

Annex section 18 describes the use of the Message Mapping Catalogue XML Schema. Schema fragments for individual Service Responses are described in sub-sections within the Service Request descriptions in the Service Request Definition annexes.

9.3.6 Response Types and Command Variant Values

The following table describes the Response Types applicable to each Command Variant value:

CV	Response Type (SMETS2 or later)	Response Type (SMETS1)
1	Acknowledgement	Acknowledgement
	Service Response (from Device)[2]	SMETS1 Response[2]

CV	Response Type (SMETS2 or later)	Response Type (SMETS1)
	Parse Output	
2	Command for Local Delivery (synch)	Acknowledgement[3]
		DCC Alert containing the UTRN[3]
3	Acknowledgement	Acknowledgement[3]
	Service Response (from Device) [2]	SMETS1 Response[3]
	Command for Local Delivery (asynch) [2]	DCC Alert containing the UTRN[3]
	Parse Output	
4	Pre-command	Acknowledgement
		SMETS1 Response[2]
5	Acknowledgement	N/A
	Service Response (from Device) [2]	
	Parse Output	
6	Command for Local Delivery (synch)	N/A
7	Acknowledgement	N/A
	Service Response (from Device) [2]	
	Command for Local Delivery (asynch) [2]	
	Parse Output	
8	Service Response (from DCC)	Service Response (from DCC)
N/A	Device Alert[2]	SMETS1 Alert[2]
	Parse Output	
N/A	DCC Alert[2]	DCC Alert[2] (including S1SP Alerts)
9[1]	Service Response (from Device) [2]	SMETS1 Response[2]
	Parse Output	

Table 34 Response Types and Command Variant Values

[1] DSP Scheduled Command Response (CV is internal use only)

[2] Requires Ack to be returned to the DCC Data Systems (see Receive Response Service in Figure 9~~Figure 9~~)

[3] Only applicable to SRV2.2 for SMETS1 Devices

9.3.7 Device Responses and Future Dating

Where a Device is capable of Future Dating a Command at the Device, the message type(s) returned by the Device depend on whether the Command has been executed immediately, has been stored for future execution, has been executed at a future date or has been cancelled. This can be summarised as follows, where the possible values of 'n' (instructions in the Command) and 'm' (activation date-time instructions in the Command) are defined in the corresponding Service Request Reponses in the Annexes (in some cases 'n' and 'm' are fixed values and in others variable between a minimum and a maximum value. The value(s) of 'n' and 'm' can be the same or different for Electricity and Gas):

1. Service Response (from Device) – GBCSPayload. See section 9.3.1.5

a. On Demand

i. One Device Response (Command execution outcome)

ii. The GBCSPayload includes 'n' results corresponding to the execution of each of the 'n' instructions in the Command

b. Future Dated (Device) received by the Device before the required ExecutionDateTime

i. One Device Response (Command storage outcome)

ii. The GBCSPayload includes 'n' results corresponding to the storing of each of the 'n' instructions in the Command

c. Future Dated (Device) received by the Device on or after the required ExecutionDateTime

i. The Command is executed immediately, i.e. it is treated as if its Mode of Operation was "On Demand"

ii. One Device Response (Command execution outcome)

iii. The GBCSPayload includes 'n' results corresponding to the execution of each of the 'n' instructions in the Command

d. Future Dated (Device) Cancellation

i. One Device Response (Command execution outcome, which is the cancellation of a previously stored but not yet executed Command)

ii. The GBCSPayload includes 'm' results corresponding to the cancellation of each of the 'm' activation date-time instructions in the Command

2. Service Response (from Device) – FutureDatedDeviceAlertMessage. See section 9.3.1.8

a. Future Dated (Device)

i. 'm' Device Alerts (Command activation date-time instructions execution outcome). These Device Alerts are delivered wrapped as responses rather than as device alerts, since they are execution outcomes. See section 9.3.1.8

ii. The GBCSPayload of each Future Dated Device Alert includes 1 of the 'm' results corresponding to the execution of each of the 'm' activation date-time instructions in the Command previously stored on the Device

9.4 Service Request Matrix

This section defines the list of Service References supported by the DCC User Gateway.

In some cases Service Reference has been divided into Service Reference Variants to align to GBCS Use Cases.

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

- the Service Reference, e.g. 1.2
- the Service Reference Variant

- identical to the Service Reference where there is no Service Reference Variant, e.g. 1.2
- required to align to GBCS Use Cases. There is one Service Reference Variant per GBCS Use Case

- the Service Name, e.g. Update Price
- the security classification:
  - Critical – is the Service Request identified as a Critical Service Request.
    - For SMETS2 or later Devices this means the Service Request requires DCC Service User signing of the GBCS Command. (Note that some Critical Commands are signed by the Access Control Broker.)
    - For SMETS1 Devices there is no equivalent of GBCS signature so the Service Request will be subject to additional checks by the DCC Data Systems and S1SP, as defined in the Service Request Processing Document
  - Sensitive – does the Service Response contain sensitive data (see GBCS for sensitive data encryption details for SMETS2 or later Devices)
  - Protection Against Replay – does the Service Request require Protection Against Replay (see section 4.18 for an overview and GBCS for full details for SMETS2 or later Devices, and section 4.19.4 and SMETS1 Supporting Requirements Document for SMETS1 Devices)
- the Modes Of Operation applicable. See section 2.3
- the Eligible User Role(s) applicable:

DUIS User Role Reference	DUGIDS User Role Reference	User Role Description
IS	EIS	Electricity Import Supplier
ES	EES	Electricity Export Supplier
GS	GIS	Gas Import Supplier
RSA	SNA	Supplier Nominated Agent
ED	ENO	Electricity Network Operator
GT	GNO	Gas Network Operator
OU	OU	Other User

Table 35 DCC User Roles

- the Service Request's applicability to SMETS1, as defined in DUIS.

For those Service Requests that are applicable to SMETS1 please note the following differences:

- Security Classification
  - Critical. Critical Service Requests, though sent by the Service User with Command Variant 4, within DCC use the Non-Critical processing pattern, i.e. Command Variant 1
  - Sensitive. Sensitive Service Responses don't include encrypted data

    - Protection Against Replay. Anti-Replay protection is performed by the DCC Data Systems (including S1SPs) rather than the Device.

- Modes of Operation. See section 2.3, but please note Modes of Operation Transform and Future Dated (Device) are N/A to SMETS1.

    - Mode of Operation Future Dated (DSP) applies to Service Requests that are otherwise Future Dated (Device) for SMETS2 or later.

This section should be read in conjunction with:

- section 9, which describes the general formatting and Common Data Items for all Service Requests and Service Responses
- the Annex
- the DUIS XML Schema
- the MMC XML Schema

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
1.1	1.1.1	Update Import Tariff (Primary Element)	Yes	No	Yes	Yes	Device	No	No	EIS GIS	Yes
1.1	1.1.2	Update Import Tariff (Secondary Element)	Yes	No	Yes	Yes	Device	No	No	EIS	No
1.2	1.2.1	Update Price (Primary Element)	Yes	No	Yes	Yes	Device	No	No	EIS GIS	Yes
1.2	1.2.2	Update Price (Secondary Element)	Yes	No	Yes	Yes	Device	No	No	EIS	No
1.5	1.5	Update Meter Balance	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
1.6	1.6	Update Payment Mode	Yes	No	Yes	Yes	Device	No	No	EIS GIS	Yes
1.7	1.7	Reset Tariff Block Counter Matrix	Yes	No	Yes	Yes	No	No	No	EIS	No
2.1	2.1	Update Prepay Configuration	Yes	No	Yes	Yes	Device	No	No	EIS GIS	Yes
2.2	2.2	Top Up Device	No	No	Yes	Yes	No	No	No	EIS GIS	Yes
2.3	2.3	Update Debt	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
2.5	2.5	Activate Emergency Credit	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
3.1	3.1	Display Message	No	No	No	Yes	DSP	No	No	EIS GIS	No
3.2	3.2	Restrict Access For Change Of Tenancy	No	No	No	Yes	DSP	No	No	EIS GIS	Yes
3.3	3.3	Clear Event Log	No	No	No	Yes	No	No	No	EIS GIS	Yes
3.4	3.4	Update Supplier Name	No	No	No	Yes	DSP	No	No	EIS GIS	No
3.5	3.5	Disable Privacy PIN	No	No	Yes	Yes	No	No	No	EIS GIS	No
4.1	4.1.1[7]	Read Instantaneous Import Registers	No	Yes	No	Yes	DSP	No	No	EIS GIS ENO GNO	Yes
4.1	4.1.2[7]	Read Instantaneous Import TOU Matrices	No	Yes	No	Yes	DSP	No	No	EIS GIS ENO GNO	Yes
4.1	4.1.3	Read Instantaneous Import TOU With Blocks Matrices	No	Yes	No	Yes	DSP	No	No	EIS ENO	Yes
4.1	4.1.4[7]	Read Instantaneous Import Block Counters	No	Yes	No	Yes	DSP	No	No	GIS	Yes
4.2	4.2	Read Instantaneous Export Registers	No	No	No	Yes	DSP	No	No	EES ENO	Yes
4.3	4.3[7]	Read Instantaneous Prepay Values	No	Yes	No	Yes	DSP	No	No	EIS GIS	Yes

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
4.4	4.4.2[7]	Retrieve Change Of Mode / Tariff Triggered Billing Data Log	No	Yes	No	Yes	DSP	No	No	EIS[5] GIS[5]	Yes
4.4	4.4.3[7]	Retrieve Billing Calendar Triggered Billing Data Log	No	Yes	No	Yes	DSP	No	No	EIS[5] GIS[5]	Yes
4.4	4.4.4	Retrieve Billing Data Log (Payment Based Debt Payments)	No	No	No	Yes	DSP	No	No	EIS[5] GIS[5]	Yes
4.4	4.4.5	Retrieve Billing Data Log (Prepayment Credits)	No	No	No	Yes	DSP	No	No	EIS[5] GIS[5]	Yes
4.6	4.6.1[7]	Retrieve Import Daily Read Log	No	Yes	No	Yes	DSP	Yes	No	EIS[5] GIS[5]	Yes
4.6	4.6.2	Retrieve Export Daily Read Log	No	No	No	Yes	DSP	Yes	No	EES[5]	No
4.8	4.8.1[7]	Read Active Import Profile Data	No	Yes	No	Yes	DSP	Yes	No	EIS[5] GIS[5] ENO GNO OU	Yes
4.8	4.8.2	Read Reactive Import Profile Data	No	No	No	Yes	DSP	Yes	No	EIS[5] ENO OU	Yes
4.8	4.8.3	Read Export Profile Data	No	No	No	Yes	DSP	Yes	No	EES[5] ENO OU	Yes
4.10	4.10[7]	Read Network Data	No	Elec No, Gas Yes	No	Yes	DSP	Yes	No	EIS GIS ENO GNO	Yes
4.11	4.11.1	Read Tariff (Primary Element)	No	No	No	Yes	No	No	No	EIS GIS OU	Yes
4.11	4.11.2	Read Tariff (Secondary Element)	No	No	No	Yes	No	No	No	EIS OU	No
4.12	4.12.1	Read Maximum Demand Import Registers	No	No	No	Yes	DSP	Yes	No	EIS ENO	No
4.12	4.12.2	Read Maximum Demand Export Registers	No	No	No	Yes	DSP	Yes	No	EES ENO	No
4.13	4.13	Read Prepayment Configuration	No	No	No	Yes	DSP	No	No	EIS GIS	Yes
4.14	4.14[7]	Read Prepayment Daily Read Log	No	Yes	No	Yes	DSP	Yes	No	EIS[5] GIS[5]	No
4.15	4.15	Read Load Limit Data	No	No	No	Yes	DSP	Yes	No	EIS ENO	Yes
4.16	4.16	Read Active Power Import	No	No	No	Yes	No	Yes	No	EIS ENO	Yes
4.17	4.17[7]	Retrieve Daily Consumption Log	No	Yes	No	Yes	DSP	Yes	No	EIS[5] GIS[5] ENO GNO OU	No
4.18	4.18	Read Meter Balance	No	No	No	Yes	DSP	No	No	EIS GIS	Yes

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
5.1	5.1	Create Schedule	No	No	No	No	No	No	Yes	EIS EES GIS ENO GNO OU	Yes
5.2	5.2	Read Schedule	No	No	No	No	No	No	Yes	EIS EES GIS ENO GNO OU	Yes
5.3	5.3	Delete Schedule	No	No	No	No	No	No	Yes	EIS EES GIS ENO GNO OU	Yes
6.2	6.2.1	Read Device Configuration (Voltage)	No	No	No	Yes	No	No	No	EIS SNA ENO	Yes
6.2	6.2.2	Read Device Configuration (Randomisation)	No	No	No	Yes	No	No	No	EIS SNA ENO	No
6.2	6.2.3	Read Device Configuration (Billing Calendar)	No	No	No	Yes	No	No	No	EIS SNA GIS	Yes
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	No	No	No	Yes	No	No	No	EIS EES GIS SNA ENO GNO OU	Yes
6.2	6.2.5	Read Device Configuration (Instantaneous Power Thresholds)	No	No	No	Yes	No	No	No	EIS SNA	Yes
6.2	6.2.7	Read Device Configuration (MPxN)	No	No	No	Yes	No	No	No	EIS EES GIS SNA ENO GNO OU	No
6.2	6.2.8	Read Device Configuration (Gas)	No	No	No	Yes	No	No	No	GIS SNA GNO	Yes
6.2	6.2.9	Read Device Configuration (Payment Mode)	No	No	No	Yes	No	No	No	EIS GIS SNA	Yes
6.2	6.2.10	Read Device Configuration (Event and Alert Behaviours)	No	No	No	Yes	No	No	No	EIS GIS ENO	No
6.4	6.4.1	Update Device Configuration (Load Limiting General Settings)	Yes	No	Yes	Yes	Device	No	No	EIS	Yes
6.4	6.4.2	Update Device Configuration (Load Limiting Counter Reset)	No	No	Yes[9]	Yes	DSP	No	No	EIS	Yes
6.5	6.5	Update Device Configuration (Voltage)	No	No	Yes[9]	Yes	DSP	No	No	ENO	Yes

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
6.6	6.6	Update Device Configuration (Gas Conversion)	Yes	No	Yes	Yes	No	No	No	GIS	Yes
6.7	6.7	Update Device Configuration (Gas Flow)	Yes	No	Yes	Yes	No	No	No	GIS	Yes
6.8	6.8	Update Device Configuration (Billing Calendar)	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
6.11	6.11	Synchronise Clock	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
6.12	6.12	Update Device Configuration (Instantaneous Power Threshold)	No	No	No	Yes	DSP	No	No	EIS	Yes
6.13	6.13	Read Event Or Security Log	No	No	No	Yes	No	No	No	EIS[5] GIS[5] ENO GNO SNA	Yes
6.14	6.14.1	Update Device Configuration (Auxiliary Load Control Description)	Yes	No	No	Yes	No	No	No	EIS	No
6.14	6.14.2	Update Device Configuration (Auxiliary Load Control Scheduler)	Yes	No	Yes	Yes	Device	No	No	EIS	No
6.14	6.14.3	Update Device Configuration (Auxiliary Controller Scheduler)	Yes	No	Yes	Yes	Device	No	No	EIS	No
6.15	6.15.1	Update Security Credentials (KRP)	Yes	No	Yes	Yes	Device	No	No	EIS GIS ENO GNO	Yes
6.15	6.15.2	Update Security Credentials (Device)	Yes	No	Yes	Yes	No	No	No	EIS GIS	No
6.17	6.17	Issue Security Credentials	Yes	No	Yes	Yes	No	No	No	EIS GIS	No
6.18	6.18.1	Set Maximum Demand Configurable Time Period	No	No	Yes	Yes	DSP	No	No	ENO	No
6.18	6.18.2	Reset Maximum Demand Registers	No	No	No	Yes	DSP	No	No	ENO	No
6.20	6.20.1	Set Device Configuration (Import MPxN)	No	No	Yes	Yes	DSP	No	No	EIS GIS	No
6.20	6.20.2	Set Device Configuration (Export MPAN)	No	No	Yes	Yes	DSP	No	No	EES	No
6.21	6.21	Request Handover Of DCC Controlled Device	No	No	Yes[9]	Yes	DSP	No	No	EIS GIS	Yes
6.22	6.22	Configure Alert Behaviour	No	No	No	Yes	No	No	No	EIS GIS ENO	No
6.23	6.23	Update Security Credentials (CoS)	No	No	Yes	Yes	DSP + Device	No	No	EIS GIS	Yes
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	No	No	No	Yes	No	No	No	EIS GIS ENO GNO	Yes
6.24	6.24.2	Retrieve Device Security Credentials (Device)	Yes	No	No	Yes	No	No	No	EIS GIS	No
6.25	6.25	Set Electricity Supply Tamper State	Yes	No	Yes	Yes	No	No	No	EIS	Yes
6.26	6.26	Update Device Configuration (daily resetting of Tariff Block Counter Matrix)	Yes	No	Yes	Yes	No	No	No	EIS	No

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
6.27	6.27	Update Device Configuration (RMS Voltage Counter Reset)	No	No	Yes[9]	Yes	DSP	No	No	ENO	Yes
6.28	6.28	Set CHF Sub GHz Configuration	No	No	Yes	Yes	No	No	No	EIS GIS	No
6.29	6.29	Request CHF Sub GHz Channel Scan	No	No	Yes	Yes	No	No	No	EIS GIS	No
6.30	6.30	Read CHF Sub GHz Configuration	No	No	No	Yes	No	No	No	EIS GIS SNA	No
6.31	6.31	Read CHF Sub GHz Channel	No	No	No	Yes	No	No	No	EIS GIS SNA	No
6.32	6.32	Read CHF Sub GHz Channel Log	No	No	No	Yes	No	No	No	EIS GIS SNA	No
7.1	7.1	Enable Supply	Yes	No	Yes	Yes	No	No	No	EIS	Yes
7.2	7.2	Disable Supply	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
7.3	7.3	Arm Supply	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
7.4	7.4	Read Supply Status	No	No	No	Yes	No	No	No	EIS EES GIS SNA ENO GNO	Yes
7.5	7.5	Activate Auxiliary Load Control	Yes	No	Yes	Yes	No	No	No	EIS	No
7.6	7.6	Deactivate Auxiliary Load Control	Yes	No	Yes	Yes	No	No	No	EIS	No
7.7	7.7	Read Auxiliary Load Control Switch Data	No	No	No	Yes	DSP	No	No	EIS OU ENO	No
7.8	7.8	Reset Auxiliary Load	Yes	No	Yes	Yes	No	No	No	EIS	No
7.9	7.9	Add Auxiliary Load To Boost Button	No	No	Yes	Yes	DSP	No	No	EIS	No
7.10	7.10	Remove Auxiliary Load From Boost Button	No	No	Yes	Yes	DSP	No	No	EIS	No
7.11	7.11	Read Boost Button Details	No	No	No	Yes	DSP	No	No	EIS OU	No
7.12	7.12	Set Randomised Offset Limit	Yes	No	Yes	Yes	No	No	No	EIS	No
7.13	7.13	Set Auxiliary Controller State	Yes	No	Yes	Yes	No	No	No	EIS	No
7.14	7.14	Read Auxiliary Controller Configuration Data	No	No	No	Yes	DSP	No	No	EIS OU ENO	No
7.15	7.15	Read Auxiliary Controller Operational Data	No	No	No	Yes	DSP	No	No	EIS OU ENO	No
7.16	7.16	Limit APC Level	Yes	No	Yes	Yes	No	No	No	None	No
8.1	8.1.1	Commission Device	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
8.2	8.2	Read Inventory	No	No	No	No	No	No	Yes	EIS EES GIS SNA ENO GNO OU	Yes
8.3	8.3	Decommission Device	No	No	No	No	No	No	Yes	EIS GIS	Yes
8.4	8.4	Update Inventory	No	No	No	No	No	No	Yes	EIS EES GIS SNA ENO GNO OU	Yes
8.5	8.5	Service Opt Out	No	No	Yes	No	DSP	No	No	None	No
8.6	8.6	Service Opt In	No	No	No	No	No	No	Yes	None	No
8.7	8.7.1	Join Service (Critical)	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
8.7	8.7.2	Join Service (Non-Critical) [1]	No	No	Yes[9]	Yes	No	No	No	EIS GIS OU	Yes
8.8	8.8.1	Unjoin Service (Critical)	Yes	No	Yes	Yes	No	No	No	EIS GIS	Yes
8.8	8.8.2	Unjoin Service (Non-Critical) [1]	No	No	Yes[9]	Yes	No	No	No	EIS GIS OU	Yes
8.9	8.9	Read Device Log	No	No	No	Yes	DSP	No	No	EIS GIS OU	Yes
8.11	8.11	Update HAN Device Log[1]	No	No	Yes[9]	Yes	DSP	No	No	EIS GIS OU	Yes
8.12	8.12.1	Restore HAN Device Log	No	No	Yes	Yes	No	No	No	EIS GIS	No
8.12	8.12.2	Restore GPF Device Log	No	No	Yes	Yes	No	No	No	EIS GIS	No
8.13	8.13	Return Local Command Response	No	No	No	No	No	No	Yes	EIS GIS	No
8.14	8.14.1	Communications Hub Status Update-Install Success	No	No	No	No	No	No	Yes	EIS GIS	No
8.14	8.14.2	Communications Hub Status Update – Install No SM WAN	No	No	No	No	No	No	Yes	EIS GIS	No
8.14	8.14.3	Communications Hub Status Update. – Fault Return	No	No	No	No	No	No	Yes	EIS GIS SNA	No
8.14	8.14.4	Communications Hub Status Update – No Fault Return	No	No	No	No	No	No	Yes	EIS GIS SNA	No
9.1	9.1	Request Customer Identification Number	No	No	Yes	Yes	No	No	No	OU	No
11.1	11.1	Update Firmware	No	No	No	No	No	No	Yes[2]	EIS GIS	Yes

Service Reference	Service Reference Variant	Name	Critical	Sensitive Response	Protection Against Replay	On Demand	Future Dated	DSP Scheduled	DCC Only	Eligible User Role	SMETS1 Applicability
11.2	11.2	Read Firmware Version	No	No	No	Yes	DSP	No	No	EIS EES GIS SNA ENO GNO OU	Yes
11.3	11.3	Activate Firmware	Yes	No	No[8]	Yes	Device	No	No	EIS GIS	Yes
11.4	11.4	Update PPMID Firmware	No	No	No	No	No	No	Yes[2]	EIS GIS	No
12.1	12.1	Request WAN Matrix	No	No	No	No	No	No	Yes	EIS EES GIS SNA ENO GNO OU	No
12.2	12.2	Device Pre-notification	No	No	No	No	No	No	Yes	EIS EES GIS SNA ENO GNO OU	Yes
14.1	14.1	Record Network Data (GAS)	No	No	Yes	Yes	No	Yes	No	GNO	No

Table 36 Service Request Matrix

[1] Service Request available in relation to Type 2 Devices
[2] See section 2.3.10 for details on Firmware Distribution Mode of Operation
[5] Service Request also available to the 'Old' Registered Supplier
[7] Service Request can't be Sequenced for Gas, because the DCC can't read the encrypted status returned by the Device
[8] Yes for SMETS1 Devices
[9] No for SMETS1 Devices

9.4.1 Commands for Local Delivery

The Command Variant (see section 3) of a Request that sends a Command to a Device indicates if the Command is to be delivered via the SM WAN, returned to the DCC Service User for Local Delivery or both. A Command can be delivered locally:

- for all On Demand Requests available to DCC Service User Role EIS, EES or GIS, where Devices have a status in the Smart Metering Inventory of "Pending", "Installed Not Commissioned" or "Commissioned"
- and for all On Demand Requests available to the ENO, GNO, SNA or OU Service User Role where Devices have a status of "Installed Not Commissioned" or "Commissioned" in the Smart Metering Inventory

Please note that Service Request SR 8.1.1 – Commission Device cannot be requested for Local delivery to a Device as without SM WAN a Device cannot be Commissioned.

9.5 Managing Changes to Requests and Responses

It is inevitable that changes to Requests and Responses will be required in the future as a result of the introduction of new services or modifications to existing ones. This section describes the approach that will be used to allow the management of changes to the XML definitions supported on the DCC User Gateway.

9.5.1 DUIS XML Schema versions

When changes are made to the XML definitions a new version of the DUIS XML schema will be published. The schema version is identified by an additional attribute on the root elements, Request and Response, as shown below

```
<xs:element name="Request">
        <xs:complexType>
          …
        <xs:attribute name="schemaVersion" type="xs:decimal" use="required"/>
</xs:complexType>
```

The new schema will support new versions of individual Service Requests and Responses as required. This is described in section 9.5.2 and 9.5.3. New versions of Service Requests and Responses will be backwards compatible wherever possible with the previous versions.

In order to allow a phased transition to a new schema version across the DCC Service User community, the DCC Data Systems will support both the latest version of the DUIS XML schema and at least the immediately preceding version.

The principles of updates to schema versions, using 1.0 as an illustration but also applicable to later major versions, is as follows

- The schema version will be constructed of a major and minor version. In development of version 1.0, this schema version will always be 1.0 and a separate DUIS/MMC development version will be notified within the schema comments.
- Once version 1.0 is in use in the Production environment, the XML schema version will be updated with minor version increments (eg 1.1, 1.2 etc) for minor updates to the current baseline, whilst major version updates (eg 2.0) will be used for significant changes to the baseline.

9.5.1.1 Schema Versions in SMETS1 Responses and Alerts

As described in section 9.3.4, Responses and Alerts related to SMETS1 Devices carry embedded XML data from S1SPs, which is of XML type SMETS1SignedResponse (for Responses or SMETS1 Alerts) or S1SPAlert. The XML data signed by the S1SPs include a schema version, in addition to the schema version of the overall DUIS message.

SMETS1 Responses and Alerts were introduced in DUIS v3.0, and the schema version of the SMETS1SignedResponse XML data generated by S1SPs must be v3.0. If the DCC Service User is using a later version of the DUIS XML schema e.g. v3.1 or v4.0, then the SMETS1SignedResponse schema version generated by the S1SP will be different from the schema version of the outer Response XML structure.

9.5.2 Request versions

Where the change to the Request XML definition is driven solely by changes to the overall Request structure (eg changes to Header items) then these changes will be managed by use of the schema version only. That is, the new schema will contain the new definition of the Request, with an updated set of attributes as required. The previous definition will remain in the previous schema and will be supported if a DCC Service User is still using that schema, however once a DCC Service User moves to the new schema they will need to use the new definition.

Where a change to a Service Request specific XML definition is driven by a change to the underlying device protocol specification (eg a change to GBCS) then a different approach must be taken. This is necessary since in this case there is a dependency on the device firmware and the version of the device protocol specification supported by that device firmware. Since this is device specific and the DCC will need to support many variants of device firmware at any one time, the preferred approach to managing these changes will be to extend the Service Request XML definition so that it can support variations of the underlying GBCS Use Cases.

For example, if a change to GBCS required a change in the Update Supplier Name Service Request (SR 3.4) to provide an additional attribute then the UpdateSupplierName XML element definition would be extended to include this additional attribute as shown below.

```
DUIS Schema x.0
<xs:element name="UpdateSupplierName">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SupplierName" type="xs:string"/>
        <xs:element name="SupplierTelephoneNumber" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

DUIS Schema y.0
  <xs:element name="UpdateSupplierName">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SupplierName" type="xs:string"/>
        <xs:element name="SupplierTelephoneNumber" type="xs:string"/>
        <xs:element name="webURL" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
```

In this particular example, a DCC Service User using the earlier schema version (DUIS Schema x.0) can continue to send SR3.4 with the original attributes whilst a DCC Service User using the later schema (DUIS Schema y.0) can now use the extra attribute. The DCC Data Systems

will determine which GBCS Use Case to construct based on the Firmware Version (and hence GBCS version) supported by the target device as recorded within the DCC Data Systems Smart Metering Inventory.

As well as the above scenario of modifications to existing Service Request definitions there are a couple of other change scenarios to consider.

The first scenario is the simple case of adding a brand new Service Request. This is relatively straightforward and will result in a new XML definition being added to the new schema. This new Service Request will, of course, have a new Service Reference associated with it.

The second scenario is where there is a change to the underlying device protocol specification but this change does *not* affect the Service Request XML definition. In this case the DCC Transform Service will simply create the correct version of the underlying GBCS Command based on its knowledge of the device firmware for the device being addressed. Where this scenario occurs for a Critical Service Request then the Pre-Command returned by the Transform Service to the User will include a version indicator so that the Parse and Correlate software can determine which version of the GBCS Command it should be checking against.

The above scenarios are just examples of how a particular change to GBCS may be handled in later versions of the schema. The specifics of individual changes will be dependent on the precise nature of the change to the GBCS Specification and in particular to the level of backwards compatibility provided in the updated GBCS Use Cases. A mapping of GBCS Use Cases to Service Requests for all DUIS and MMC Schema versions is provided later in this document in Appendix 10. Specific details of any validation rules or backwards compatibility constraints are contained in the individual Service Request definitions in the relevant Annex.

Finally, consideration must be given to DCC Only Service Requests and how to manage changes to these Requests. For consistency, these will be handled in the same way as device based Service Requests, ie the Service Request XML element will be updated to contain additional attributes wherever possible otherwise a brand new Service Request will be created.

9.5.3 Response versions

The handling of changes to Response XML definitions needs to be applied to both the DUIS XML Schema and the MMC XML Schema.

For the DUIS XML Schema the approach is similar to that applied for Requests and is described below. For the MMC XML Schema the approach is described in Annex 18.

For the DUIS XML schema, where the change to the Response XML definition is driven solely by changes to the overall Response structure (eg changes to Header items) then these changes will be managed by use of the schema version only. That is, the new schema will contain the new definition of the Response, with an updated set of attributes as required. The previous definition will remain in the previous schema and will be supported if a DCC Service User is still using that schema, however once a DCC Service User moves to the new schema they will need to use the new definition. The DCC Data Systems will determine which version of the Response to return to the DCC Service User based on the schema version used in the corresponding Request.

Where a change to a DCC Only Service Response specific XML definition is driven by a change to the specific data items of that Service Response then a similar approach will be taken, ie the XML element definition will be updated in later versions of the schema whilst the previous definition will remain in the previous schema. The DCC Data Systems will determine which version of the Service Response to return to the DCC Service User based on the schema version used in the corresponding Service Request.

Where a change to the underlying device protocol changes the content of the GBCS Response then this has no impact on the DUIS XML Schema definition, but it will be handled by the MMC XML schema (see Annex 18).

9.5.4 Supported DUIS XML schema versions

For this version 5.21 of DUGIDS, the DCC Data Systems is expected to support the following XML Schema Versions:

- DCC User Interface Specification (DUIS) V5.2
  - DUIS XML Schema Version - Request - 5.2
  - DUIS XML Schema Version - Response - 5.2
  - DUIS XML Schema Version - SMETS1SignedResponse - 3.0
  - DUIS XML Schema Version – S1SPAlert - 3.0
- Message Mapping Catalogue (MMC) V5.2
  - MMC XML Schema Version – GBCSResponse – 5.2

The DCC Data Systems will also support previous Schema Versions as follows:

- DCC User Interface Specification (DUIS) V5.1
  - DUIS XML Schema Version - Request - 5.1
  - DUIS XML Schema Version - Response - 5.1
  - DUIS XML Schema Version - SMETS1SignedResponse - 3.0
  - DUIS XML Schema Version – S1SPAlert - 3.0
- Message Mapping Catalogue (MMC) V5.1
  - MMC XML Schema Version – GBCSResponse – 5.1

~~The DCC Data Systems will also support previous Schema Versions as follows:~~

- DCC User Interface Specification (DUIS) V5.0
  - DUIS XML Schema Version - Request - 5.0
  - DUIS XML Schema Version - Response - 5.0
  - DUIS XML Schema Version - SMETS1SignedResponse - 3.0
  - DUIS XML Schema Version – S1SPAlert - 3.0
- Message Mapping Catalogue (MMC) V5.0
  - MMC XML Schema Version – GBCSResponse – 5.0

- DCC User Interface Specification (DUIS) V4.0
  - DUIS XML Schema Version - Request - 4.0
  - DUIS XML Schema Version - Response -4.0
  - DUIS XML Schema Version - SMETS1SignedResponse -3.0
  - DUIS XML Schema Version – S1SPAlert -3.0

- Message Mapping Catalogue (MMC) V4.0
    - MMC XML Schema Version – GBCSResponse - 4.0

- DCC User Interface Specification (DUIS) V3.1
    - DUIS XML Schema Version - Request - 3.1
    - DUIS XML Schema Version - Response -3.1
    - DUIS XML Schema Version - SMETS1SignedResponse - 3.0
    - DUIS XML Schema Version – S1SPAlert - 3.0
- Message Mapping Catalogue (MMC) V3.1
    - MMC XML Schema Version – GBCSResponse - 3.1

- DCC User Interface Specification (DUIS) V3.0
    - DUIS XML Schema Version - Request - 3.0
    - DUIS XML Schema Version - Response -3.0
    - DUIS XML Schema Version - SMETS1SignedResponse -3.0
    - DUIS XML Schema Version – S1SPAlert -3.0
- Message Mapping Catalogue (MMC) V3.0
    - MMC XML Schema Version – GBCSResponse - 3.0

DUIS v1.0 and v2.0 will not be supported by DCC from November 2021 onwards. The URLs for versions v1.0 and v2.0 have not been removed, so it is still possible to send Service Requests to them, but Users should recognise that these are no longer supported versions. DCC Users are recommended to ensure that they use DUIS v3.0 or later.

- DCC User Interface Specification (DUIS) V2.0
    - DUIS XML Schema Version - Request - 2.0
    - DUIS XML Schema Version - Response - 2.0
- Message Mapping Catalogue (MMC) V2.0
    - MMC XML Schema Version – GBCSResponse - 2.0
- SEC APPENDIX AD - DCC User Interface Specification (DUIS) – Version AD 1.1
    - DUIS XML Schema Version - Request - 1.0
    - DUIS XML Schema Version - Response - 1.0
- SEC APPENDIX AF – Message Mapping Catalogue (MMC) – Version AF 1.0

- MMC XML Schema Version – GBCSResponse - 1.0

Details on how to access different versions of the interface are provided in section 10.2.

10 Web Services Implementation

10.1 Technical Implementation

The technical implementation of the DCC User Interface is provided by using "web services" to allow Requests and Responses to be sent between the DCC Data Systems and the systems of the DCC Service Users.

The DCC User Gateway accepts Service Requests or Signed Pre-Commands as XML documents submitted using an HTTP POST command. (Note this should not be confused with a SOAP based web service). Similarly, when data is pushed from the DCC User Gateway to a DCC Service User, the DCC Service User needs to provide a web server to accept POSTed data. The content of this POST command will be either a Service Response (from Device), a Command for Local Delivery (asynchronous), a Device Alert or a DCC Alert message.

The POST command is an HTTP protocol method to request that the addressed web server accepts the data enclosed in the message's body for processing. The web server responds with an HTTP response, which may also include data in the message body.

The contents of all the POSTed commands and any HTTP response data is XML, and is defined by the DUIS XML schema. The interface utilises HTTP status codes within the HTTP response to communicate the success or failure of the call.

To process Requests, there are three services provided by the DCC Data Systems as follows:

- Transform Service – a synchronous communication mechanism for transformation of Critical Service Requests into GBCS Format and the returning of a Pre-Command to the DCC Service User.
- DCC Only Service – a synchronous communication mechanism to process DCC Only Service Requests or a request for a Command to be returned by the DCC to the DCC Service User to be locally applied (via a Hand Held Terminal).
- Send Command Service – an asynchronous communication mechanism to which a DCC Service User must send any Non-Critical Service Request or Signed Pre-Command where the DCC Service User wishes the DCC only to send the associated Command to the Device specified in the message.

The Transform and DCC Only web services follow a synchronous processing pattern and return Service Response data to DCC Service Users within the HTTP response.

The Send Command web service also completes synchronously and returns an HTTP response, but this response simply provides an Acknowledgement to indicate acceptance of the Service Request by the DCC.

Figure 63~~Figure 63~~ illustrates the synchronous pattern. Note that the submitted request is defined by the XML object Request, The DCC Data Systems synchronously responds to the submission with an appropriate HTTP Status Code and XML Response content. The content of the synchronous Response is an Acknowledgement, a Pre-Command, a Command for Local Delivery or a Service Response (from DCC) as defined in section 9.3.1.

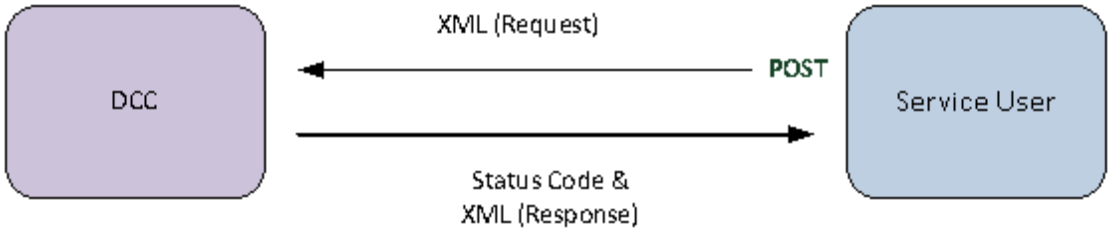


Figure 63 Service Request from Service User to the DCC

To receive asynchronous Service Responses and Alerts, the DCC Service User system must implement a web service as follows:

Receive Response Service – a service to receive Service Responses and Alerts from the DCC Data Systems.

To implement this service, the Service User is required to provide a URL for a web server that will accept the HTTP POSTed XML (HTTP version 1.1) from the DCC Data Systems. The URL details are to be defined by the Service User and provided to the DCC as described in the Code of Connection for the DCC User Interface. It is the Service User's responsibility to ensure that this URL is available to receive data from the DCC Data Systems.

Figure 64~~Figure 64~~ illustrates the asynchronous pattern. The structure of the POST command is defined by the Response XML object. The content of the asynchronous Response is a Service Response (from Device), a Command for Local Delivery, a Device Alert or a DCC Alert as defined in section 9.3.1. The Service User responds back to the DCC with an HTTP response containing the appropriate HTTP status code to indicate whether the call was successful or not. Failure to receive an HTTP response will invoke the DCC retry behaviour as described in section 11.6.

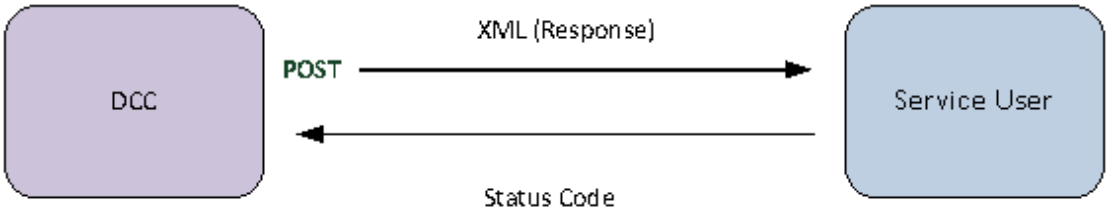


Figure 64 Service Response from the DCC to the Service User

10.2 URL Naming and API Versioning

URL names will be provided to DCC Service Users as part of the process of obtaining a connection to the DCC User Gateway.

Names used in this section are examples to help show the principles of API versioning. For the avoidance of doubt, the domain name used within the examples for api.mycorp.com is not a valid value and will be replaced with an actual value for service delivery as advised as part of the process of obtaining a connection to the DCC User Gateway.

The DCC User Interface provides a capability to manage the transition from one version of the interface definition to the next. DCC Service Users can choose to upgrade at a later date than at the point when the User Gateway components are cut over to a new version of the published API. Support for the old version of the API and for the new version will continue until customers have completed their upgrade and cut-over tasks.

The endpoints for the service are named as follows:

Web Service	URL for Message Gateway Request	Comment
DCC Only Service	http://api.mycorp.com/serviceD/	For services only requiring interaction with DCC Data Systems
Transform Service	http://api.mycorp.com/ServiceT/	For transformation of Critical Service Requests to Pre-commands

Web Service	URL for Message Gateway Request	Comment
		or for sending SMETS1 Critical Service Requests to SMETS1 devices via the SMETS1 Service provider
Send Command Service	http://api.mycorp.com/serviceS/	For sending a non-critical Service Request or signed Pre-command (for Critical Service Requests) to the device or for sending non-Critical SMETS1 Service Requests to SMETS1 devices via the SMETS1 Service provider

Table 37 URL Naming

The Message Gateway services are identified with a separate document root/sub-domain "api" because this approach allows digital certificates to be managed separately to those used for other parts of the DCC domain, and because it is compatible with recommendations on service design in the Government Service Design Manual.

To support the introduction of new versions of the DCC User Interface and to allow multiple versions to be supported, each major new version of the API will be given a new set of URLs that identify the web services to be called to access that version of the interface. Minor version changes will continue to use the same URLs as the previous major release, e.g. version 3.1 of the API uses the same URLs as version 3.0.

The URLs for versions v1.0 and v2.0 have not been removed, so it is still possible to send Service Requests to them, but Users should recognise that these are no longer supported versions. DCC Users are recommended to ensure that they use DUIS v3.0 or later.

```
http://api.mycorp.com/serviceD/   // The original v1.0 API
http://api.mycorp.com/serviceT/   // The original v1.0 API
http://api.mycorp.com/serviceS/   // The original v1.0 API
http://api.mycorp.com/serviceD/2.0/   // The previous v2.0 API
http://api.mycorp.com/serviceT/2.0/   // The previous v2.0 API
http://api.mycorp.com/serviceS/2.0/   // The previous v2.0 API
http://api.mycorp.com/serviceD/3.0/   // The v3.0 and v3.1 API
http://api.mycorp.com/serviceT/3.0/   // The v3.0 and v3.1  API
http://api.mycorp.com/serviceS/3.0/   // The v3.0 and v3.1 API
http://api.mycorp.com/serviceD/4.x/   // The v4.0 API
http://api.mycorp.com/serviceT/4.x/   // The v4.0 API
http://api.mycorp.com/serviceS/4.x/   // The v4.0 API
http://api.mycorp.com/serviceD/5.x   // The v5.0, and v5.1 and 5.2 API
http://api.mycorp.com/serviceT/5.x/   // The v5.0, and v5.1 and 5.2 API
http://api.mycorp.com/serviceS/5.x/   // The v5.0, and v5.1 and 5.2 API
```

It is assumed that a DCC Service User will only use one version of the interface at any point in time.

11 Error Handling

A submitted Service Request or Signed Pre-command may not be successfully processed by the DCC Data Systems due to a number of reasons. From the point that the Service Request or Signed Pre-command is accepted by the DCC Data Systems, the DCC Data Systems are responsible for (as applicable depending on its Command Variant – see section 3):

SMETS2 or later:

- sending the Command to the CSP
- returning the Command to the DCC Service User for Local Delivery
- returning the Pre-command to the DCC Service User
- returning the Service Response to the DCC Service User

SMETS1:

- sending the Service Request to the S1SP, which will (as appropriate) send SMETS1 format commands to the Device
- returning the Service Response to the DCC Service User
- sending an S1SP Alert related to the Service Request, where applicable

This section describes the Error Handling and Retry Strategy implemented in the DCC User Gateway. It shall be interpreted as applying to SMETS1 Devices (with appropriate terminology adjustments even if not explicitly stated) as well as SMETS2 or later Devices, unless indicated otherwise.

11.1 Error Handling

Errors encountered when processing a Service Request or Signed Pre-command, which cannot be resolved by the retry strategy, are passed back to the original DCC Service User who requested the service.

Errors may be caused by an incomplete or invalid Service Request or Signed Pre-command (see section 7), due to failure to deliver the GBCS message to the Device, or failures to process a request within the DCC Data System processing

The Response Code contained in the Acknowledgement or Service Response message will indicate the failure type. See section 12.3 for more details on DCC Data Systems Response Codes.

For SMETS1 Devices there may also be error conditions within the S1SP. Since S1SP processing takes place after initial validation and acknowledgement of Service Requests by the DCC Data Systems, a new type of error handling has been introduced. The new message type S1SP Alert enables an S1SP to generate a message to be sent to the Service User via the DCC Data Systems, e.g. to indicate that a Service Request failed validation checks within the S1SP.

Note that S1SP Alerts include S1SP Alert Codes used for other purposes, so S1SP Alerts do not always indicate error conditions.

11.2 Retry Strategy

For those Commands that are to be delivered to a Device via the CSP, the DCC Data Systems will at the point of execution attempt to deliver the GBCS Command to the device's communications hub via the appointed CSP provider.

Should it not be possible to deliver the Command (i.e. if there is an error reported during the delivery processing), then the DCC Data Systems shall attempt to redeliver the message at a

later time. The redelivery is controlled by an algorithm with a "back-off" period and a maximum number of retries before eventually failing. Should the delivery fail after the final attempt, then a failure message is returned to the DCC Service User via a DCC Alert with an appropriate Response Code as defined in section 12.3.

In a similar fashion, if the Command is delivered (i.e. there are no errors reported during delivery processing) but no response is received within a configurable timeout period then the DCC Data Systems will attempt to redeliver the message at a later time. Again, the redelivery is controlled by an algorithm with a "back-off" period and a maximum number of retries before eventually failing and returning a failure message to the DCC Service User via a DCC Alert with an appropriate Response Code as defined in section 12.3.

The retry approach for different Modes of Operation are described further in section 11.6.

Note that in all cases, the DCC Data Systems will re-send the Command with the same Request ID. This ensures that in the event that the Command is actually received by the Device then the anti-replay features of the GBCS will ensure that the Command is not executed twice.

11.3 Unfulfilled Requests

The DCC Data Systems shall monitor Service Requests and Signed Pre-Commands to ensure that a Service Response is received by DCC Service Users as expected.

For "On Demand" Service Requests or Signed Pre-Commands, if no response is received after a configurable period, a DCC Alert with an appropriate response code and the original Request ID for which there was no response from the device will be returned to the DCC Service User.

For "Future Dated (Device)" Service Requests or Signed Pre-Commands, if no response is received after a configurable period beyond the Execution Date Time, a DCC Alert with an appropriate response code and the original Request ID for which there was no response from the device will be returned to the DCC Service User.

For "Future Dated (DSP)" Service Requests, where a response to the future dated request is not received, then the retry strategy will be initiated. If there is no response after the retries, a DCC Alert with an appropriate response code and the original Request ID for which there was no response from the device will be returned to the DCC Service User.

For "DSP Scheduled" Service Requests, where a response to the scheduled request is not received, then the retry strategy will be initiated. If there is no response after the retries, a DCC Alert with an appropriate response code and the Schedule ID for which there was no response from the device will be returned to the DCC Service User. The lack of response to a "DSP Scheduled" Service Request doesn't affect the DSP Schedule, which will continue to run until its defined End Date or until it is deleted.

For the avoidance of doubt, no DCC Alerts with timeout response codes will be issued by the DCC Data Systems for "Transform" or "DCC Only" where the DCC Service User is expected to ensure that a Service Response is received from the DCC and take any appropriate remedial action required.

11.4 Failure to deliver Responses to DCC Service Users

If the DCC Data Systems has received a Service Response or Alert from a Device or generated a DCC Alert, but is unable to deliver that Service Response, Device Alert or DCC Alert to the DCC Service User (e.g. due to unavailability of the Service User's systems) then the DCC Data Systems will attempt to redeliver the message at a later time. The redelivery is controlled by an algorithm with a "back-off" period and a maximum number of retries before eventually failing.

Note that in this case the retry configuration will be such that the DCC Data Systems will retry for a significant period of time before ultimately recording a failure to deliver in the Service Audit Log.

11.5 Web Services Error Handling

All web service interactions between DCC Service Users and the DCC Data Systems follow a synchronous processing pattern for the individual web service call.

For the "Transform Service" and "DCC Only Service" web services, the synchronous completion of the web service call returns the Service Response to the DCC Service User. This Service Response will contain a response code (error code) if there have been any errors in processing the request.

For the "Send Command Service" web service, the synchronous completion of the web service call returns an Acknowledgement to the DCC Service User. This Acknowledgement will contain a response code (error code) if there have been any errors in processing the request (e.g. access control failure).

In a similar fashion the synchronous completion of the "Receive Response Service" web service call returns an http "acknowledgement" to the DCC Data Systems. This http acknowledgement will contain a response code (error code) if there have been any errors in processing the request (e.g. a data or validation failure).

In all cases, the web service client implementation should utilise an appropriate timeout to handle any failure to complete the service call.

See section 12 for more details on response codes returned by individual web services.

11.6 Service Request and Response Error Handling

The following sections describe the error handling and retry behaviour for each mode of operation of Service Request/Response processing (see section 2.3)

Note that all retry periods and timeout values are configurable items and may be subject to change as part of an agreed Service Management process. Some values are dependent on Mode of Operation and Target Response Times. These are described in Table 38~~Table 38~~. Other values are fixed in all cases and these have initial proposed values in square brackets within the following sections.

Mode of Operation	Initial Retry Period	Back-off period	Final Retry Period
On Demand	Configurable period based on the following factors: DCC Target Response Time HAN transfer time Device processing time Device wakeup time[1]	n/a	n/a
Future Dated (Device)	2 hours	2 hours	Future Dated (Device) Target Response Time + 60 mins
Future Dated (DSP)	2 hours	2 hours	Future Dated (DSP) Target Response Time + 60 mins
DSP Scheduled	2 hours	2 hours	DSP Scheduled Target Response Time + 60 mins

Table 38 Retry Periods

[1] Note that if a Command is sent to a Target ID that identifies the Gas Smart Meter (rather than the Gas Proxy Function), then the On Demand initial retry period will be extended by 30 minutes to allow time for the Gas Smart Meter to wake up and receive the Command

11.6.1 Transform and DCC Only

Error Scenario	Behaviour
DCC Service unavailable	The DCC shall notify DCC Service Users if the DCC Data Systems are unavailable using a HTTP Response Code of 503 – Service Unavailable (as defined in section 12.1). This notification may be before the DCC Service User notices that this is the case. In the absence of any such notification, where a DCC Service User is unable to access the DCC Services, the DCC Service User shall check connectivity of their own systems, check for known issues, and for notifications on the Self Service Interface (SSI) before investigation into DCC Data Systems is performed. If DCC Data Systems are persistently unavailable, the DCC Service User may raise an Incident with the DCC.
Invalid request or Access Control failure	Acknowledgement returned on synchronous web service completion with appropriate Response Code (reason for error). See section 12.3

Table 39 Error Handling – Transform and DCC Only

11.6.2 On Demand

Error Scenario	Behaviour
DCC Service unavailable	The DCC shall notify DCC Service Users if the DCC Data Systems are unavailable using a HTTP Response Code of 503 – Service Unavailable (as defined in section 12.1). This notification may be before the DCC Service User notices that this is the case. In the absence of any such notification, where a DCC Service User is unable to access the DCC Services, the DCC Service User shall check connectivity of their own systems, check for known issues, and for notifications on the Self Service Interface (SSI) before investigation into DCC Data Systems is performed. If DCC Data Systems are persistently unavailable, the DCC Service User may raise an Incident with the DCC.
Invalid request or Access Control failure	Acknowledgement returned on synchronous web service completion with appropriate Response Code (reason for error). See section 12.3
Failure to send command over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~)

Error Scenario	Behaviour
	If failed after further retries and expiry of initial retry period (see Table 38~~Table 38~~) then return DCC Alert N12 with appropriate Response code to requesting DCC Service User
Failure to receive response over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~) If nothing received after further retries and expiry of initial retry period (see Table 38~~Table 38~~) mark as failed and return DCC Alert N13 with appropriate Response code to requesting DCC Service User, If the response is received after the failure notification, it will be flagged as anomalous (since there is no outstanding request against it) and recorded within the DCC Data Systems Service Audit Trail and Event Log.
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once DCC Service User connection restored. Failed responses will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 40 Error Handling – On Demand

11.6.3 Future Dated (Device)

N/A to SMETS1 Devices.

Error Scenario	Behaviour
DCC Service unavailable	The DCC shall notify DCC Service Users if the DCC Data Systems are unavailable using a HTTP Response Code of 503 – Service Unavailable (as defined in section 12.1). This notification may be before the DCC Service User notices that this is the case. In the absence of any such notification, where a DCC Service User is unable to access the DCC Services, the DCC Service User shall check connectivity of their own systems, check for known issues, and for notifications on the Self Service Interface (SSI) before investigation into DCC Data Systems is performed. If DCC Data Systems are persistently unavailable, the DCC Service User may raise an Incident with the DCC.

Error Scenario	Behaviour
Invalid request or Access Control failure	Acknowledgement returned on synchronous web service completion with appropriate Response code to requesting DCC Service User.
Failure to send command over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~). If failed after further retries and expiry of initial retry period then place on "redelivery" queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) then return DCC Alert N12 with appropriate Response code to requesting DCC Service User.
Failure to receive Command Acknowledgement response over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~). If nothing received after further retries and expiry of initial retry period place on "redelivery" queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) then return DCC Alert N13 with appropriate Response code to requesting DCC Service User.
No Future Service Response received from Device	For all future dated commands acknowledged by the Device, if no response received from the specified Device within the Target Response Time after the execution date and time contained within the original Service Request then DCC to return DCC Alert N10 to the DCC Service User with a "Timeout" Response Code. If the response is received after the Timeout, it will be flagged as anomalous (since there is no outstanding request against it) and recorded within the DCC Data Systems Service Audit Trail and Event Log.

Error Scenario	Behaviour
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once DCC Service User connection restored. Failed responses will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 41 Error Handling – Future Dated (Device)

11.6.4 Future Dated (DSP)

Error Scenario	Behaviour
DCC Service unavailable	The DCC shall notify DCC Service Users if the DCC Data Systems are unavailable using a HTTP Response Code of 503 – Service Unavailable (as defined in section 12.1). This notification may be before the DCC Service User notices that this is the case. In the absence of any such notification, where a DCC Service User is unable to access the DCC Services, the DCC Service User shall check connectivity of their own systems, check for known issues, and for notifications on the Self Service Interface (SSI) before investigation into DCC Data Systems is performed. If DCC Data Systems are persistently unavailable, the DCC Service User may raise an Incident with the DCC.
Invalid request or Access Control failure	Acknowledgement returned on synchronous web service completion with appropriate Response code to requesting DCC Service User.
Access Control failure at Future Dated execution time	DCC Alert N7 returned with appropriate Response Code.
Failure to send Request over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~) from first delivery attempt . If failed after further retries and expiry of initial retry period then place on "redelivery" queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) from requested execution time then return

Error Scenario	Behaviour
	DCC Alert N11 to the DCC Service User with a "Timeout" Response Code.
Failure to receive response over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~) from first delivery attempt. If nothing received after further retries and expiry of initial retry period place on "redelivery" queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) from requested execution time then return DCC Alert N11 to the DCC Service User with a "Timeout" Response Code. If the response is received after the Timeout, it will be flagged as anomalous (since there is no outstanding request against it) and recorded within the DCC Data Systems Service Audit Trail and Event Log.
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once Service User connection restored. Failed responses will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 42 Error Handling – Future Dated (DSP)

11.6.5 DSP Scheduled

Error Scenario	Behaviour
Validation or Access Control failure at Scheduled execution time	DCC Alert N7 returned with appropriate Response Code.

Error Scenario	Behaviour
Failure to send Request over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~) from first delivery attempt . If failed after further retries and expiry of initial retry period then place on “redelivery” queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) from requested execution time then return DCC Alert N11 to the DCC Service User with a “Timeout” Response Code.
Failure to receive response over SM WAN	DCC retry at least once within initial retry period (see Table 38~~Table 38~~) from first delivery attempt .. If nothing received after further retries and expiry of initial retry period place on “redelivery” queue for subsequent re-send after back-off period (see Table 38~~Table 38~~). If failed after multiple re-delivery attempts up to expiry of final retry period (see Table 38~~Table 38~~) from requested execution time then return DCC Alert N11 to the DCC Service User with a “Timeout” Response Code. If the response is received after the Timeout, it will be flagged as anomalous (since there is no outstanding request against it) and recorded within the DCC Data Systems Service Audit Trail and Event Log.
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on “failed” queue for re-delivery once Service User connection restored. Failed responses will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 43 Error Handling – DSP Scheduled

11.6.6 Meter Scheduled

N/A to SMETS1 Devices.

Error Scenario	Behaviour
DCC Service User fails to receive response from DCC at scheduled time	This is a DCC Service User Responsibility. Suggestion – If nothing received after [24 hours] from expected receipt time DCC Service User to initiate Service Request to retrieve Billing Data OR initiate Service Request to read Smart Meter Device log
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once DCC Service User connection restored. Failed responses will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 44 Error Handling – Meter Scheduled

11.6.7 Device Alert

Error Scenario	Behaviour
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once DCC Service User connection restored. Failed Alerts will be held for [2 days] for re-sending once DCC Service User Connectivity is restored. The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 45 Error Handling – Device Alert

11.6.8 DCC Alert

Error Scenario	Behaviour
Unable to deliver response to Service User	DCC retry at regular intervals. If failed after [300 secs] from first DCC attempt to deliver response to Service User then place on "failed" queue for re-delivery once DCC Service User connection restored. Failed Alerts will be held for [2 days] for re-sending once DCC Service User Connectivity is restored.

Error Scenario	Behaviour
	The Service Management Framework will define the processes to be followed for long term unavailability of Service User connectivity, including how long data can be held for.

Table 46 Error Handling – DCC Alert

12 Response and Status Codes

This section defines the Response Codes and the HTTP status codes (see http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html) returned by the DCC Data Systems to the DCC Service User Systems in response to a Transform Service, DCC Only Service or Send Command Service web service call, and those to be returned by the DCC Service User Systems to the DCC Data Systems in response to a Receive Response web service call.

12.1 DCC Data Systems Web Service Status Codes

When the DCC Service Users call the DCC Data Systems web services, the DCC Data Systems return a response. Note that the DCC Data System utilises HTTP as a transport rather than application protocol, therefore all application related data is passed with a status code of 200.

HTTP status codes are used to indicate success or failure of the web service call:

200: OK – The request has been accepted by the DCC. An XML response object is returned to the Service User, this contains a Response Code that indicates whether the request has passed or failed the business rules for the Service Request. See section 9.3.1.1 for the construction of this XML. Note that it is possible for a request to be syntactically correct, but fail business level validation. Successful Service Requests will return a Response Code with the prefix “I” (Information) or “W” (Warning). Failed Service Requests will return a Response Code with the prefix “E” (Error).

300: Multiple Choices – The recipient requires that the client redirect its request to the alternative URL provided in the Location header field.

400. Bad Request – Indicates that the syntax of the request is invalid and the DCC Data Systems are unable to parse the request.

500. Internal Server Error – Indicates that the DCC Data Systems are malfunctioning. The Service User should contact the DCC Helpdesk if this occurs.

503. Service Unavailable – The DCC Data Systems server is currently unavailable (because it is overloaded or down for maintenance). This is typically returned when there are no resources (routes, queues, etc.) to service the request. It is advised to wait for a period before resubmitting the request.

12.2 DCC Service User Web Service Status Codes

When DCC calls the DCC Service Users Receive Response web service, the DCC Service User returns an acknowledgement response. HTTP status codes are used to indicate success or failure of the web service call:

200: OK – The DCC Service User has accepted the message.

300: Multiple Choices – The recipient requires that the client redirect its request to the alternative URL provided in the Location header field.

400. Bad Request – Indicates that the syntax of the message is invalid and the DCC Service User system is unable to parse the message.

500. Internal Server Error – Indicates that a DCC Service User system is malfunctioning. The DCC shall contact the Service User’s Helpdesk should this occur.

503. Service Unavailable – The DCC Service User server is currently unavailable (because it is overloaded or down for maintenance). The DCC system shall wait for a configurable period (initially set to 15 minutes) before resubmitting the response.

12.3 DCC Data Systems Response Codes

This section specifies the meaning associated with the DCC Data Systems generic Response Codes within the response message. The Service Request specific Response Codes are included in the Annex.

All responses to the DCC Service User include a Response Code.

Error Response Codes are the result of:

- Access Control Second Step Authentication failures
- Access Control Authorisation failures
- Access Control Validation failures
- Failure to send a command to a Device or receive a response from it
- “Future Dated” and “DSP Scheduled” command time-outs
- Sequencing Failures

All Device Responses will include an ‘I0’ (success) Response Code, meaning that the DCC Data Systems have received a response from the Device. The error code (success / failure) of each GBCS Command in the Device response will be included in the GBCS payload message. These GBCS error codes are not documented here but they are documented in the GBCS itself.

A Response Code consists of a letter prefix (defining the type) followed by a number. Response Code Types:

- Information. Prefix ‘I’
- Error. Prefix ‘E’
- Warning. Prefix ‘W’

Please see Error Handling Strategy for details of the Error Handling Strategy Procedure.

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
I0	Success	Information	Request has had a successful outcome	All except Acknowledgement	N/A
I99	Acknowledgement	Information	Request received for sending to Device has been accepted and is correct Or DCC Only Service Request that doesn’t return data has had a successful outcome	Acknowledgement	N/A
E1	Failed Authorisation – Invalid User / User Role	Error	DCC Service User / User Role combination is not a valid SEC party / User Role	Acknowledgement and DCC Alerts	V2 Z1
E2	Failed Authorisation – Invalid User Role / Service Reference	Error	DCC Service User Role not allowed to call Service Reference	Acknowledgement	V4 Z1

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
E3	Failed Authorisation – Invalid User Status	Error	DCC Service User Status not allowed to call Service Reference	Acknowledgement and DCC Alerts	V3 Z1
E4	Failed Authorisation – Invalid User / User Role for Device	Error	DCC Service User Role not authorised party for Device and required date & time	Acknowledgement and DCC Alerts	V1 Z1
E5	Failed Authorisation – Invalid Device Status	Error	Device status incompatible with Service Reference	Acknowledgement and DCC Alerts	W6 Z1
E11[1]	Failed Validation – Invalid Service Request / device type combination	Error	Service Reference not compatible with the specified device	Acknowledgement	W7 Z1
E12	Failed Validation – Invalid Request / Command Variant combination	Error	Command Variant not applicable to the Request type	Acknowledgement	W1 Z1
E13	Failed Validation – Invalid Request Type for URL	Error	Request Type not valid for the URL, e.g. a “DCC Only” Service Request sent to the “Transform” URL	Acknowledgement	W2 Z1
E17	Failed Authorisation – Invalid DCC User Role / Device for locally delivered Commands	Error	DCC User Role / Device status combination doesn’t allow Request of Command for local delivery	Acknowledgement	W6 Z1
E19	Failed Authorisation – Device doesn’t exist[3]	Error	Device ID invalid	Acknowledgement and DCC Alerts	W3 Z1
E20	Communications Failure – Unable to Communicate with Device	Error	DCC Data Systems cannot establish communications with Device	DCC Alerts	X1
E21	Communications Failure – No Response Received from Device	Error	No response received from Device for an “On Demand” Command or a “Future Dated” Command Acknowledgement	DCC Alerts	X1
E30	Time-out – “Future Dated” Command	Error	DCC Data Systems don’t get response from Device on the expected date for “Future Dated” command	DCC Alerts	X2 X3
E31	Time-out – “DSP Schedule” /“Future Dated (DSP) Command	Error	DCC Data Systems cannot establish communications with or get response from Device for “DSP Scheduled” or “Future Dated (DSP) command	DCC Alerts	X2 X3
E40	Failed Sequenced Command – Invalid First Request	Error	DCC Data Systems fail sequenced Request because it includes the First In Sequence flag set to true and the Preceding RequestID is populated	Acknowledgement	Y1 Z1

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
E41	Failed Sequenced Command – Invalid Preceding Request ID	Error	DCC Data Systems fail sequenced Request, because its Preceding Request ID is also the Preceding RequestID of another Request in the same sequence	Acknowledgement	Y1 Z1
E42	Failed Sequenced Command – Circular Reference	Error	DCC Data Systems fail sequenced Request, because its Request ID is the same as its Preceding Request ID or the Preceding RequestID of its preceding request or of one of its preceding requests, e.g. request id 1 has request 2 as its preceding request and request 2 has request 1 as its preceding request	Acknowledgement	Y1 Z1
E43	Failed Sequenced Command – Previous Request(s) Failure	Error	DCC Data Systems fail sequenced Request, because previous Request (s) in the sequence failed	Acknowledgement and DCC Alerts	Y2 Z1
E44	Failed Sequenced Command – Previous Request(s) not received	Error	DCC Data Systems fail sequenced Request, because previous Request(s) in the sequence not received during “Wait Period”	Acknowledgement and DCC Alerts	Y2 Z1
E45	Failed Sequenced Command – Invalid Command Variant	Error	DCC Data Systems fail sequenced Request, because its Command Variant is not applicable to a sequenced Request	Acknowledgement	Y2 Z1
E46	Failed Sequenced Command – Request after Last In Sequence	Error	DCC Data Systems fail sequenced Request, because it is dependent on the Last In Sequence	Acknowledgement and DCC Alerts	Y2 Z1
E47	Failed Sequenced Command – Request failed because no response to “On Demand” Command received from device	Error	DCC Data Systems fail sequenced Request, because no response received from device to previous Command	Acknowledgement and DCC Alerts	Y2 Z1
E48	Failed Validation – Service Request Reference and Variant mismatch	Error	Invalid combination of Service Reference and Service Reference Variant	Acknowledgement	W4 Z1
E49	Failed Validation – Service Request Format and Service Reference Variant mismatch	Error	The Service Request format doesn’t match the Service Reference Variant in the message header	Acknowledgement	W5 Z1
E50	Local Command Services Not Returned	Error	The Service Request requesting a Command for Local Delivery has not returned a Command	Acknowledgement	W8 Z1

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
E51	Failed Validation – Signed Pre-Command Message Code and Service Reference Variant mismatch	Error	The GBCS Message Code in the Signed Pre-Command GBCS Payload doesn't map to the Service Reference Variant in the Signed Pre-Command XML header	Acknowledgement	W5 Z1
E52	Failed Validation – Unable to cancel Future Dated (DSP) Service Request	Error	The Service Request to cancel Future Dated (DSP) Service Request of the same type can't find a Service Request to cancel	Acknowledgement	Y1 Z1
E53	Failed Sequenced Command – Future Dated (DSP) not first in Sequence	Error	The sequenced Service Request is Future Dated (DSP) is not the first Request in the Sequence	Acknowledgement	Y2 Z1
E54	Failed Sequenced Command – Gas Service Request returns encrypted data	Error	The sequenced Gas Service Request returns encrypted data	Acknowledgement	Y2 Z1
E55	Failed Validation – Duplicate Request ID	Error	The Request's Request ID is the duplicate of another Request which is currently being processed by the DCC Data Systems	Acknowledgement	W5 Z1
E56	Failed Validation – Service Request no longer supported	Error	The requested Service Request is no longer supported by the DCC Data Systems. This error will only occur if a Service Request which exists in an older version of the DUIS schema can no longer be accepted by the DCC Data Systems on that version of the interface.	Acknowledgement and DCC Alerts	W9 Z1
E57[1]	Failed Validation – Invalid Service Request / GBCS version combination	Error	The Service Request is not compatible with the specified Device Firmware Version	Acknowledgement and DCC Alerts	W10 Z1
E58	Communications Failure – Command not delivered to ESME	Error	The CHF was unable to deliver the Command to the ESME The creation of this DCC Alert is in direct response to the receipt by the DCC of a Device Alert 0x8F84 - Failure to Deliver Remote Party Message to ESME (as defined by GBCS) from the CHF	DCC Alerts	X4 Z1

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
E59	Communications Failure – Dual Band CHF Sub GHz error	Error	The CHF sends one of the following Device Alerts to the DSP Access Control Broker to indicate a communications failure in the Sub GHz frequency range: Device Alerts without specific payload: • 0x8F22 - Critical Duty Cycle Action Taken • 0x8F24 - Regulated Duty Cycle Action Taken • 0x8F29 - Three Lost GSME Searches Failed • 0x8F2B - Sub GHz Channel not changed due to Frequency Agility Parameters Device Alerts with specific payload: • 0x8F20 - Limited Duty Cycle Action Taken • 0x8F2C - Message Discarded Due to Duty Cycle Management • 0x8F2D - No More Sub GHz Device Capacity The DCC Alert includes the Device Alert Code and, for those that contain specific payload, it also includes the corresponding information	DCC Alerts	X5 Z1
E60	Failed Validation – Invalid Service Request for SMETS1	Error	The Service Request is not applicable to SMETS1	Acknowledgement	W11 Z1
E61	Failed Validation – Invalid Command Variant for SMETS1 Service Request	Error	The Command Variant is N/A to SMETS1 Service Requests	Acknowledgement	W11 Z1
E62	Failed Validation – Service Request failed S1SP Validation	Error	The Service Request failed the S1SP validation	DCC Alerts	W12 Z1
E63	Failed Validation - DCC Data Systems anti-Replay Intercept	Error	Protection against Replay mechanisms within the DCC have rejected a SMETS1 Service Request.	Acknowledgement and DCC Alerts	W13 Z1

Response Code	Response Code Name	Response Code Type	Description	Applicable to Response Types	Error Handling Strategy Procedure
E64	Failed Validation – Originator ID is not the Notified Critical Supplier or Notified Critical Network Operator ID	Error	The SMETS1 Service Request was not originated by the Notified Critical Supplier or Notified Critical Network Operator	Acknowledgement	W13 Z1
E65[2]	Failed Validation – Invalid Certificate Role	Error	The Service Request is not signed using an XML Signing Certificate (Remote Party Role 'XMLSign')	Acknowledgement	U1
E66[3, 4, ~~5~~]	Failed delivery – Unable to deliver to CoS Party	Error	DCC Data Systems cannot establish communications with the CoS Party	DCC Alerts	X6 Z1~~TBD~~[~~6~~]
E67[3, 4, ~~5~~]	Timeout – No response received from CoS Party	Error	No response received from the CoS Party within the timeout period.	DCC Alerts	X6 Z1~~TBD~~[~~6~~]
E68[3, 4, ~~5~~]	Failed Validation – Service Request failed CoS Party Validation	Error	The Service Request failed validation checks performed by the CoS Party	DCC Alerts	W14 Z1~~TBD~~[~~6~~]
E69[3, 4, ~~5~~]	Failed Validation – CoS Service Request failed anti-replay checks	Error	Protection against Replay mechanisms within the DCC have rejected the Service Request.	DCC Alerts	W15 Z1~~TBD~~[~~6~~]
E70[3, ~~5~~]	Failed Validation – CoS Anomaly Detection Threshold Breach	Error	A CoS-specific Anomaly Detection volume threshold has been exceeded	DCC Alerts	W16 Z1~~TBD~~[~~6~~]
E71[3, 4, ~~5~~]	Failed Validation – Invalid Authorisation response from CoS Party	Error	Authorisation payload or Signed Pre-Command from the CoS Party is not consistent with the original Service Request	DCC Alerts	W17 Z1~~TBD~~[~~6~~]
E100	Failed Authentication	Error	Request failed Authentication (as per checks in section 7.3)	Acknowledgement	U1 Z1

Table 47 DCC Data Systems Response Codes

[1] Because E57 is not supported by DUIS Schema 1.0, if a Service Request received via DUIS Schema 1.0 is to be rejected and E57 returned to the DCC Service User, E11 will be returned instead

[2] Because E65 is not supported prior to DUIS Schema 5.1, if a Service Request received via a DUIS Schema prior to 5.1 is to be rejected and E65 returned to the DCC Service User, E100 will be returned instead.

[3] Applicable only to SRV6.23. Because these Response Codes are not supported prior to DUIS Schema 5.1, if a Service Request received via a DUIS Schema version prior to 5.1 is to be rejected and E66 – E71 included in a DCC Alert, E19 will be included instead

[4] Applicable only where request is passed to ECoS Party for authorisation.

~~[5] Please note these changes are only created by the DCC Systems alongside the Implementation of the new ECoS functionality, which is not part of the June 2022 Release (expected as part of June 2023 Release). Please see Appendix 16 – Changes for the ECoS Service for further details.~~

~~[6] The Error Handling Strategy procedure will be confirmed when the ECoS service goes live (expected in the June 2023 release). Please see Appendix 16 – Changes for the ECoS Service for further details.~~

12.4 S1SP Alert Codes

S1SP Alerts are generated by S1SPs and may be used by the DSP to determine behaviour.

S1SP Alerts which are sent to DCC Service Users will be in a DCC Alert which contains an S1SPAlert.

S1SP Alert Codes shall be defined in a document to be published by DCC that is not part of SEC and is subject to change.

The following categories of S1SP Alert Code shall be sent to the Service User which sent the corresponding Service Request:

- a code meaning the delivery of a pre-payment top-up UTRN generated by an S1SP;
- a code meaning that the S1SP will not process the request further. The DSP will close processing of the request accordingly and send the S1SP Alert to the Service User;
- a code meaning that the S1SP is delivering a notification to the Service User.

The following table summarises how the DCC Data Systems respond to S1SP Alert Codes that have been identified at the time of writing this document.

S1SP Alert Code	Error or Notification	Error or Notification Description	DCC Alert Code	Response Code
S1UT	UTRN delivery	Delivery of a prepayment top up UTRN, generated by an S1SP, to the Supplier which requested it	N56	I0
Any code indicating an unrecoverable error condition	Unrecoverable error condition	The S1SP cannot process the request and it will not be completed successfully	N55	E62
Any code indicating a notification	Notification	The S1SP is delivering a notification, e.g. indicating that a SMETS1 Smart Meter has been commissioned within the DCC by the Commissioning Party	N55	I0

Table 48 S1SP Alert Codes Delivered in DCC Alerts

12.5 ECoS Alert Codes

The ECoS Party can send messages to DSP for forwarding alerts/notifications to a specific Service User. The DSP will send them to the Service User as a DCC Alert of type ECoSAlert with the DCC Alert Code N63 and containing the ECoS Alert Code provided by the ECoS Party.

Where the Service User is using a version of DUIS prior to 5.1 then any ECoS Alert will be delivered using DCC Alert N999.

ECoS Alert Codes are as per the table below:

ECoS Alert Code	Meaning
N/A~~TBD~~ [1]	

[1] No ~~The~~ ECoS Alert Codes are currently defined for ~~will be confirmed when~~ the ECoS service. This table is retained as a placeholder in case the need arises in future ~~goes live (expected in the June 2023 release). Please see Appendix 16 – Changes for the ECoS Service for further details.~~

13 DCC Alerts

The list of DCC Alerts is as follows:

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
AD1	Power Outage Event	Power Outage Event received from CSP	CSP notification of loss of mains power as detected at the Communications Hub in the Consumer Premises for a time equal to or greater than three (3) minutes	Registered EIS[1] Registered ENO[1] Registered GIS[2] Registered GNO[2]	SMETS2 or later
N1	Electricity Smart Meter Decommission or withdrawal	Decommissioning or withdrawal of an Electricity Smart Meter Device	Upon successful completion of Service Request: • 8.3 Decommission Device • Or 8.5 Service Opt Out for an Electricity Smart Meter Device	Registered ENO and, if applicable, registered EES	All
N2	Gas Smart Meter Decommission or withdrawal	Decommissioning or withdrawal of Gas Smart Meter Device	Upon successful completion of Service Request: • 8.3 Decommission Device • Or 8.5 Service Opt Out for a Gas Smart Meter Device	Registered GNO	All
N3	Cancellation of "Future Dated (DSP)" requests because of CoT	Cancellation of "Other User" "Future Dated (DSP)" Services not yet submitted to the Devices in the Electricity or Gas Smart Metering System	Upon successful completion of Service Request 3.2 Restrict Access for Change of Tenancy	All applicable Future Dated (DSP) Request senders	All
N4	Schedule removal because of CoT	Removal of "Other User" "DSP Scheduled" schedules for Devices in the Electricity or Gas Smart Metering System	Upon successful completion of Service Request 3.2 Restrict Access for Change of Tenancy	All applicable Schedule "owners"	All
N5	Schedule removal because of Device withdrawal	"DSP Scheduled" schedule removal[6]	Upon successful completion of Service Request 8.5 Service Opt Out for a Device	All applicable Schedule "owners"	SMETS2 or later
N6	Schedule removal because of Device decommission	"DSP Scheduled" schedule removal	Upon successful completion of Service Request 8.3 Decommission Device for a Device	All applicable Schedule "owners"	All
N7	"DSP Scheduled" / "Future Dated (DSP)" access control failure	"DSP Scheduled" / "Future Dated (DSP)" access control failure (Authorisation, Device status, GBCS compatibility check)	"DSP Scheduled" / "Future Dated (DSP)" Command generation access control failure	Schedule "owner" / "Future Dated (DSP) request sender	All
N8	Device removed from Inventory- Pending Status expired	Removal of Device from Inventory	Device in a status of 'pending' for > 36 months	Original DCC Service User that requested addition of the Device to the DCC Inventory	All
N9	Communications Hub Decommission	Decommission of Communications Hub	Upon successful completion of Service Request 8.3 Decommission Device for a Communications Hub	All Responsible Import Suppliers for that CH function, other than the Responsible EIS / GIS that instigated the Decommissioning Registered ENO Registered GNO	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N10	"Future Dated (Device)" command time-out	"Future Dated(Device)" command time-out	"Future Dated (Device)" command response not received from the device within the Target Response Time from the ExecutionDateTime	"Future Dated (Device)" request sender	SMETS2 or later
N11	"DSP Scheduled" / "Future Dated (DSP)" command time-out	"DSP Scheduled" / "Future Dated (DSP)" command time-out	"DSP Scheduled" Schedule instance / "Future Dated (DSP)" command not sent to or response not received from the Device within the Target Response Time from the ExecutionDateTime	Schedule "owner" / "Future Dated (DSP) request sender	All
N12	Failure to deliver command to Device	Failure to deliver command to Device	Failure to receive an acknowledgement notification from a CSP / S1SP via the SM WAN for an "On Demand" or "Future Dated" Command	Request sender	All
N13	Failure to receive response from Device	Failure to receive response from Device	Failure to receive a response from a Device for an "On Demand" Command or "Future Dated" Command Acknowledgement	Request sender	All
N14	Sequenced Request Failure	Sequenced Request Failure	Previous Command in sequence failed or timed-out	Request sender	All
N15	Sequenced Request received Out of Order	Sequenced Request received Out of Order	Preceding Request not received during "Wait Period"	Request sender	All
N16	Device Identity Confirmation	Device Identity Confirmation by Registered Energy Supplier – either first setting or update to previous setting	Upon successful receipt of Service Response Code I0 from Service Request 8.11 Update HAN Device Log (initial setting) OR Upon successful processing of a Service Request 8.4 Update Inventory - Update MPxN	Registered ENO Registered GNO	All
N17	Schedule removal because of CoS	Previously registered Supplier "DSP Scheduled" schedule removal	Upon successful completion of Service Request 6.23 Update Security Credentials (CoS)	Previously registered EIS Previously registered GIS	All
N18	Firmware Version / Hash mismatch	Firmware Version / Hash mismatch	Firmware Hash calculated by CSP/S1SP doesn't match Firmware Version DSP raises this Alert based on the response from CSP or S1SP.	Update Firmware request sender	All
N19	Firmware Distribution Device ID identification failure	Firmware Distribution Device ID identification failure	CSP/S1SP unable to identify Communications Hub or Meter Device Id a Firmware Image is to be sent to DSP raises this Alert based on the response from CSP or S1SP.	Update Firmware request sender	All
N20	Firmware image provided is too large	Firmware image provided is too large	CSP/S1SP unable to process request, because the Firmware Image is too large for the SMETS version of the target Device DSP raises this Alert based on the response from CSP or S1SP.	Update Firmware request sender	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N21	Unknown Firmware Version	Unknown Firmware Version	CSP/S1SP unable to process request, because it doesn't recognise the Firmware Version DSP raises this Alert based on the response from CSP or S1SP.	Update Firmware request sender	All
N22	Failure to deliver Update Firmware Command to CSP / S1SP	Failure to deliver Update Firmware command to CSP / S1SP	Failure to receive an acknowledgement notification from a CSP / S1SP via the SM WAN for an Update Firmware Command	Update Firmware request sender	All
N23	Failure to receive Update Firmware Command Validation response from CSP / S1SP	Failure to receive Update Firmware Command Validation response from CSP / S1SP	Failure to receive Update Firmware Command Validation response from CSP / S1SP	Update Firmware request sender	All
N24	Successful Communications Hub Function Whitelist Update	Communications Hub Function Whitelist Update	The DSP has received positive confirmation that the requested addition to the Communications Hub Functions whitelist resulted in establishing communications with the Device See Service Request 8.11 Narrative for more details on when this Alert is generated	Update HAN Device Log request sender	All
N25	Potentially Unsuccessful Communications Hub Function Whitelist Update	Communications Hub Function Whitelist Update	The DSP has not received positive confirmation that the requested addition to the Communications Hub Functions whitelist resulted in establishing communications with the Device See Service Request 8.11 Narrative for more details on when this Alert is generated	Update HAN Device Log request sender	SMETS2 or later
N26	Update Security Credentials (CoS) – access control failure	Update Security Credentials (CoS) – access control failure	Request has failed CoS Party Access Control, processing within CoS Party, CoS specific anti-replay checks, CoS specific ADT checks or, for Future Dated Requests, DSP Access Control at the point the Request is to be sent to the CoS Party / S1SP	Update Security Credentials (CoS) request sender	All
N27	Device CoS	New Import Supplier for Device	Upon successful completion of Service Request 6.23 Update Security Credentials (CoS)	Previously registered EIS Previously registered GIS	All
N28	Device Suspended	Device Suspended	Suspension of Device	Registered EIS Registered GIS Registered ENO[3] Registered GNO[4]	All
N29	Device Restored from Suspension	Device Restored from Suspension	Restoration of Device following Previous Suspension	Registered EIS Registered GIS Registered ENO[3] Registered GNO[4]	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N30	CHF Device Log Restored	CHF Device Log Restored	Upon successful completion of Service Request 8.12.1 Restore HAN Device Log	All Responsible Import Suppliers for that CHF, other than the Responsible EIS / GIS that submitted the Request[5]	SMETS2 or later
N31	GPF Device Log Restored	GPF Device Log Restored	Upon successful completion of Service Request 8.12.2 Restore GPF Device Log[5]	All Responsible Import Suppliers for that CHF, other than the Responsible EIS / GIS that submitted the Request[5]	SMETS2 or later
N33	Cancellation of "Future Dated (DSP)" requests because of Device Decommission	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the Device	Upon successful completion of Service Request 8.3 Decommission Device for a Device	All applicable Future Dated (DSP) Request senders	All
N34	Cancellation of "Future Dated (DSP)" requests because of CHF Decommission	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the CHF and its associated GPF	Upon successful completion of Service Request 8.3 Decommission Device for a Device	All applicable Future Dated (DSP) Request senders	All
N35	Cancellation of "Future Dated (DSP)" requests because of Device Withdrawal	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the Device[6]	Upon successful completion of Service Request 8.5 Service Opt Out for a Device	All applicable Future Dated (DSP) Request senders	SMETS2 or later
N36	Cancellation of "Future Dated (DSP)" requests because of CHF Withdrawal	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the CHF and Devices in its Whitelist	Upon successful completion of Service Request 8.4 Update Inventory for a CHF Withdrawal	All applicable Future Dated (DSP) Request senders	SMETS2 or later
N37	Schedule removal because of CHF withdrawal	"DSP Scheduled" schedule removal for ESME, GSME and GPF in the Whitelist	Upon successful completion of Service Request 8.4 Update Inventory for a CHF Withdrawal	All applicable Schedule "owners"	SMETS2 or later
N38	Cancellation of "Future Dated (DSP)" requests because of CoS	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the Device from the previously registered Supplier	Upon successful completion of Service Request 6.23 Update Security Credentials (CoS)	Previously registered EIS Previously registered GIS	All
N39	PPMID Alert	A PPMID Device generates a Device Alert as defined by GBCS	PPMID Device Alert received by the DSP Access Control Broker	Registered EIS[7] Registered GIS[7]	SMETS2 or later
N40	Schedule removal because of Device suspension	"DSP Scheduled" schedule removal	Suspension of Device	All applicable Schedule "owners"	All
N41	Cancellation of "Future Dated (DSP)" requests because of Device suspension	Cancellation of all "Future Dated (DSP)" Services not yet submitted to the Device	Suspension of Device	All applicable Future Dated (DSP) Request senders	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N42	Security Credentials updated on device	Security Credentials updated on Device by Service Request 6.15.1 or 6.21	Success Response from Update Security Credentials where the Remote Party whose certificate has been placed on the Device (or certificate information stored in the S1SP for a Request for a SMETS1 Device) is not the sender of the Service Request	The Remote Party whose certificate has been placed on the Device	All
N43	PPMID Removal	A PPMID Device has been removed from the HAN via Service Request 8.11	Success Response from Update HAN Device Log (Remove) where the removed Device Type is a PPMID	All Responsible Import Suppliers for that CHF, other than the Responsible EIS / GIS that submitted the Request[8]	SMETS2 or later
N44[10]	SMKI Recovery Procedure Complete (Placing ACB Credentials on the Device)[9]	SMKI Recovery Procedure is complete - at least one of the KRP Certificates on the Device has been replaced with an ACB Certificate	SMKI Recovery Procedure is complete - all requested KRP Certificate(s) on the Device have been set to those of the ACB by the SMKI Recovery Process	Registered EIS Registered GIS	SMETS2 or later
N45[10]	SMKI Recovery Procedure Complete	SMKI Recovery Procedure is complete - all required Certificates on the Device have been recovered	SMKI Recovery Procedure is complete – all requested certificate(s) on the Device have been replaced by the SMKI Recovery Process	Registered EIS Registered GIS Registered ENO[3] Registered GNO[4]	SMETS2 or later
N46	Quarantined Request – Anomaly Detection User Threshold Breach	An Anomaly Detection User-specific volume threshold has been breached	Request quarantined, because an Anomaly Detection User-specific volume threshold has been breached	Request sender	All
N47	Quarantined Request – Anomaly Detection DCC Threshold Breach	An Anomaly Detection DCC system-wide volume threshold has been breached	Request quarantined, because an Anomaly Detection DCC system-wide volume threshold has been breached	Request sender	All
N48	Quarantined Request – Anomaly Detection Attribute Limits Breach	An Anomaly Detection Attribute Limit has been breached	Request quarantined, because an Anomaly Detection Attribute Limit has been breached	Request sender	SMETS2 or later
N49	Firmware Version Updated in the Smart Metering Inventory N49 is introduced in DUIS Version 2.0	Device's Firmware Version updated in the Smart Metering Inventory	Upon successful completion of Service Request 11.2 Read Firmware Version where the target Device is ESME, GSME, CHF, PPMID or HCALCS and the Firmware Version returned by the Device is different from that in the SMI and it matches an entry on the CPL with a status of "Current"	Responsible EIS[11] Responsible GIS[11]	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N50	Firmware Version no longer valid on the CPL N50 is introduced in DUIS Version 2.0	Device's Firmware Version updated in the Smart Metering Inventory, but Device Status not set to 'Suspended'	Upon successful completion of Service Request 11.2 Read Firmware Version where the target Device is ESME, GSME, HCALCS, PPMID or CHF and the Firmware Version returned by the Device is different from that in the SMI and it matches an entry on the CPL with a status of "Removed" OR Upon completion of Service Request 11.3 Activate Firmware where the Firmware Version returned by the Device is different from that in the SMI and it matches an entry on the CPL with a status of "Removed" OR Future Dated Firmware Activation Alert (Alert Code 0x8F66 or 0x8F67 and Message Code 0x00CA) received by the DCC Data Systems where the Firmware Version returned by the Device is different from that in the SMI and it matches an entry on the CPL with a status of "Removed" OR PPMID Firmware Activation Alert (Device Alert Code 0x8F8B) received by the DCC Systems where the Firmware Version returned by the Device is different from that in the SMI and it matches an entry on the CPL with a status of "Removed"	Responsible EIS Responsible GIS	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N51	Invalid Firmware Version N51 is introduced in DUIS Version 2.0	Device's Firmware Version is unknown (not in the CPL) Device's Firmware Version not updated in the Smart Metering Inventory	Upon successful completion of Service Request 11.2 Read Firmware Version where the target Device is ESME, GSME, HCALCS, PPMID or CHF and the Firmware Version returned by the Device is different from that in the SMI and it doesn't match an entry on the CPL OR Upon completion of Service Request 11.3 Activate Firmware where the Firmware Version returned by the Device is different from that in the SMI and it doesn't match an entry on the CPL OR Future Dated Firmware Activation Alert (Alert Code 0x8F66 or 0x8F67 and Message Code 0x00CA) received by the DCC Data Systems where the Firmware Version returned by the Device is different from that in the SMI and it doesn't match an entry on the CPL OR PPMID Firmware Activation Alert (Device Alert Code 0x8F8B) received by the DCC Systems where the Firmware Version returned by the Device is different from that in the SMI and it doesn't match an entry on the CPL	Responsible EIS Responsible GIS	All
N52	GSME Firmware Version Mismatch N52 is introduced in DUIS Version 2.0	GSME's Firmware Version returned by the GPF is different from that in the Smart Metering Inventory GSME's Firmware Version not updated 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	Responsible GIS	All
N53[12]	Command not delivered to ESME N53 is introduced in DUIS Version 2.0	CHF unable to deliver Command to ESME The creation of this DCC Alert is in direct response to the receipt by the DCC of a Device Alert 0x8F84 - Failure to Deliver Remote Party Message to ESME (as defined by GBCS) from the CHF	Failure to Deliver Command to ESME Alert (Alert Code 0x8F84, Message Code 0x00D5 and Request Id of the Command) received by the DCC Data Systems	Request sender	SMETS2 or later

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N54	Dual Band CH Alert N54 is introduced in DUIS Version 2.0	A Dual Band CH Device generates a Device Alert as defined by GBCS	Dual Band CH Device Alert received by the DSP Access Control Broker as defined by GBCS section 16.1, being one of: • Alert Type 1: ○ 0x8F21 (Duty Cycle fallen below Normal-Limited Duty Cycle Threshold) ○ 0x8F22 (Critical Duty Cycle Action Taken) ○ 0x8F23 (Duty Cycle fallen below Limited-Critical Duty Cycle Threshold) ○ 0x8F24 (Regulated Duty Cycle Action Taken) ○ 0x8F25 (Duty Cycle fallen below Critical-Regulated Duty Cycle Threshold) ○ 0x8F27 (Sub GHz Channel Scan initiated) ○ 0x8F29 (Three Lost GSME Searches Failed) ○ 0x8F2B (Sub GHz Channel not changed due to Frequency Agility Parameters) • Alert Type 2: ○ 0x8F20 (Limited Duty Cycle Action Taken) ○ 0x8F26 (Sub GHz Channel Changed) ○ 0x8F28 (Sub GHz Channel Scan Request Assessment Outcome) ○ 0x8F2A (Sub GHz Configuration Changed) ○ 0x8F2C (Message Discarded Due to Duty Cycle Management) ○ 0x8F2D (No More Sub GHz Device Capacity)	Responsible EIS[5] Responsible GIS[5]	SMETS2 or later

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N55	S1SP Service Request validation failure N55 is introduced in DUIS Version 3.0	DCC Alert indicating an error with a Service Request, initiated by an S1SP, or a notification by an S1SP	S1SP Service Request validation failure or notification. Additional information is provided in the S1SPAlert payload provided in the DCC Alert.	Service Request sender	SMETS1
N56	S1SP provision of a prepayment top-up UTRN N56 is introduced in DUIS Version 3.0	DCC Alert containing a prepayment top-up UTRN provided by an S1SP	The trigger is a User request for a prepayment top-up. Additional information is provided in the S1SPAlert payload provided in the DCC Alert.	Service Request sender	SMETS1
N57	SMETS1 CHF or SMETS1 PPMID Firmware notification N57 is introduced in DUIS Version 3.0	Notification of intended or successful Firmware version update of a SMETS1 CHF or SMETS1 PPMID	A valid request from the Lead Supplier to update the Firmware of a SMETS1 CHF/ SMETS1 PPMID, or successful activation of new SMETS1 CHF / SMETS1 PPMID Firmware	Gas Supplier associated with the SMETS1 CHF / SMETS1 PPMID	SMETS1
N58	Auxiliary Controller configuration change N58 is introduced in DUIS Version 3.1	APC / ALCS / HCALCS configuration changed on ESME	Upon successful completion of Service Request 6.14.1 Update Device Configuration (Auxiliary Load Control Descriptions) OR Upon successful completion of Service Request 6.14.2 Update Device Configuration (Auxiliary Load Control Scheduler) OR Upon successful completion of Service Request 6.14.3 Update Device Configuration (Auxiliary Control Scheduler)	Registered ENO	SMETS2 or later
N59	Firmware update in progress N59 is introduced in DUIS Version 5.0	Notification of a valid request from a Supplier to update the Firmware of a SMETS2 PPMID.	This is determined by DSP based on the notification received from CSPs, (which contains the list of devices that failed CSP validation checks).	All Responsible Import Suppliers for that Device, other than the Service Request sender	SMETS2 or later
N60	Failed to deliver Firmware image to Comms Hub N60 is introduced in DUIS Version 5.0	Failed to deliver Firmware image to Comms Hub	Notification from CSP indicating that the image could not be delivered to the Comms Hub.	Update Firmware request sender	SMETS2 or later
N61	Firmware image successfully delivered to Comms Hub N61 is introduced in DUIS Version 5.0	Firmware image successfully delivered to Comms Hub	Notification from CSP indicating that the image has been successfully delivered to the Comms Hub.	Update Firmware request sender	SMETS2 or later
N62	Comms Hub Alert N62 is introduced in DUIS Version 5.0	A Comms Hub generates a Device Alert as defined by GBCS	An Alert from a Comms Hub is received by the DSP Access Control Broker.	Responsible EIS Responsible GIS (For firmware delivery status the Alerts will be delivered to the sender of the Request)	SMETS2 or later
N63 ~~13~~	ECoS Alert N63 is introduced in DUIS Version 5.1	The ECoS Party sends a message to DSP for delivery to the relevant Service User	A notification from the ECoS Party is received by the DSP Access Control Broker	Responsible EIS Responsible GIS	All

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient	SMETS Version Applicability
N64	Comms Hub Firmware Activation N64 is introduced in DUIS Version 5.1	Successful Comms Hub Firmware Activation	Response from Comms Hub to the Activate Firmware request (CS06) sent by the CSP via DCC Data Systems.	All Responsible Suppliers	SMETS2 or later
N65 ~~13~~	CoS Certificate Alert N65 is introduced in DUIS Version 5.1	A Device is installed with an unsupported CoS Certificate in its CoS Party Trust Anchor Cell.	DSP detects that a newly installed Device holds an unsupported Certificate in its CoS Party Trust Anchor Cell.	Responsible EIS Responsible GIS	SMETS2 or later
N999	DUIS Version Mismatch N999 is introduced in DUIS Version 2.0	DCC Service User DUIS version incompatible with DCC Alert or Service Response to be sent	DCC Alert or Service Response is not compatible with the DUIS version used by the DCC Service User	Recipient of the incompatible DCC Alert or Service Response	All

Table 49 DCC Alerts

[1] DCC Service User ID with registered User Role EIS / ENO for an Electricity Smart Meter associated to the Communications Hub Function reporting the Power Outage

[2] DCC Service User ID with registered User Role GIS / GNO for a Gas Smart Meter associated to the Communications Hub Function reporting the Power Outage

[3] Only applicable to ESME

[4] Only applicable to GSME / GPF

[5] Alert is only sent if a Party is identified

[6] For GSME withdrawal, also applicable to GPF

[7] These DCC Service Users are identified by checking the Smart Metering Inventory to determine the Smart Metering System to which the PPMID is associated with. Once identified the Primary Import MPAN associated with the ESME and/or the MPRN associated with the GSME connected to the same Smart metering System are used to look up the Registered Suppliers. Alert is only sent if a Party is identified

[8] Alert only sent if the PPMID was joined to both Electricity and Gas equipment

[9] If Supplier Certificates have been replaced with ACB Certificates then the EIS / GIS has to replace them with their own by using Service Request 6.21 (Request Handover Of DCC Controlled Device) if the Digital Signing Certificate is one that has been replaced or by using Service Request 6.15.1 (Update Security Credentials (KRP)) if the Supplier's Digital Signing Certificate remains on the Device. In addition, if the Network Operator Certificates have been replaced with ACB Certificates then the EIS / GIS has to replace them with the Network Operator Certificates by using Service Request 6.21 (Request Handover Of DCC Controlled Device)

[10] Upon completion of the SMKI Recovery Procedure on a given Device, the Registered Supplier will receive N44 (if the ACB Credentials have been placed on the Device) or N45 (if the Service User's own Credentials have been placed on the Device). The Network Operator will receive N45 (if the Service User's own Credentials have been placed on the Device) or, in the case where ACB Credentials have been placed on the device, will subsequently receive an N42 Alert when the Registered Supplier replaces the ACB certificates with the Network Operator's certificates

[11] Only sent if the Responsible Supplier didn't submit the Service Request

[12] Please note that Alert N53 does not replace existing N12 or N13 Alerts from the DCC, which will continue to be produced to confirm the DCC processing of the relevant Service Request. Alert N53 is produced directly by the CHF and should be regarded as additional

information which may be used by the DCC Service User to adjust the frequency of requests being sent to the relevant ESME device. It is likely that after receipt of an Alert N53 a DCC Service User shall receive a subsequent Alert N13 at the end of the Final Retry Period for the Service Request sent if applicable

~~[13] Please note these changes are only created by the DCC Systems alongside the Implementation of the new ECoS functionality, which is not part of the June 2022 Release (expected as part of June 2023 Release). Please see Appendix 16 – Changes for the ECoS Service for further details.~~

14 Connection Mechanisms

14.1 Connection Overview

Physical connectivity to the DCC Data Centres is provided by a dedicated private network which is referred to as the DCC User Gateway Network.

The DCC is responsible for providing this network and for making available network services to allow DCC Service User organisations to obtain connectivity to the network.

A high level view of network connectivity is shown in Figure 65~~Figure 65~~.

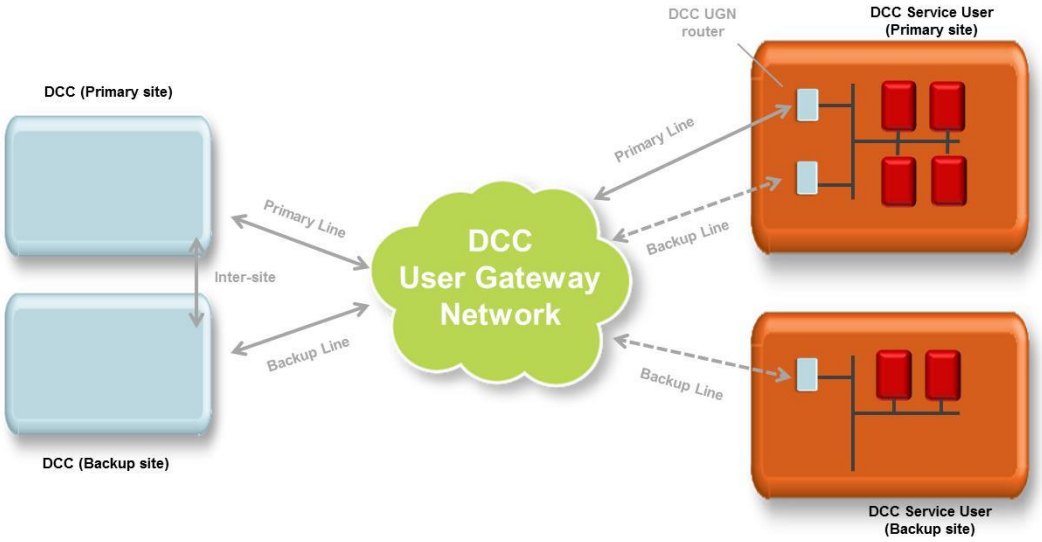


Figure 65 Physical Network Connections

Each DCC Service User shall be required to procure, from the DCC, as a minimum a Primary Line for connection to the DCC User Gateway Network. In addition, one or more Backup Lines may be procured to the same or alternate locations. The options available for physical connections are described in section 14.2.

As part of the connection to the DCC User Gateway Network, the DCC is responsible for providing the terminating network equipment within the DCC Service User's location(s). The obligations and responsibilities around this equipment are described in section 14.3.

For the avoidance of doubt, the DCC is responsible for maintaining its own connections to the DCC User Gateway Network.

14.2 Connection Options

As a minimum, the DCC will provide at least two "Means of Connection" options to the DCC User Gateway Network, as follows:

- a **High Volume Connection** for DCC Service Users who expect to carry out a large volume of Service Request processing; and
- a **Low Volume Connection** for DCC Service Users who expect to carry out a smaller volume of Service Request processing.

The technical solutions available for each of these means of connection are summarised below:

Connection Size / Type	Technology Solution	Bandwidth (download/upload)
High	Ethernet	100Mb (initially rated 10Mb)
Low	Superfast Broadband (FTTC)	40Mb/10Mb
Backup Only	Copper based backup link	20Mb/2.5Mb

Table 50 Connection Options

The table above shows the expected options which will be made available. The High Volume Connection is scalable and allows a DCC Service User to increase their bandwidth, up to 100Mb, when required without the need for additional site surveys or access to data centres. (The increase in bandwidth though would need to be agreed and managed via the DCC.) Additional options beyond 100Mb could be provisioned if required, however the DCC does not expect these to be required for the foreseeable future.

The Low Volume Connection (Superfast Broadband) is a business Fibre to the Cabinet (FTTC) option. Speeds will vary as per all DSL services but will be typically 10Mb upload and 40Mb download.

DCC Service Users may request and procure from the DCC as many DCC User Gateway Network connections from the options table above as they wish to meet their business needs for resilience and availability. Note that Backup lines may use any of the connection options described above i.e. they are not restricted to the Backup Only connection type. DCC Service Users may add further connections in the future or they may choose to upgrade from one option to another.

The DCC User Gateway Connections will be purchased by DCC Service Users via the DCC in accordance with the SEC charging arrangements.

14.3 DCC User Gateway Equipment

As part of the connection to the DCC User Gateway Network, the DCC is responsible for providing the terminating network equipment within the DCC Service User's location(s).

The table below provides technical details of the expected equipment requirements for each of the connection options.

Connection Size/Type	Technology Solution	Equipment
High	Ethernet	Cisco 3560-8PS Switch3560 Dimensions: 1.73 x 10.6 x 9.1 in. (4.4 x 27 x 23 cm) Max Power 204W
Low	Superfast Broadband (FTTC)	Cisco 3560-8PS Switch3560 Dimensions: 1.73 x 10.6 x 9.1 in. (4.4 x 27 x 23 cm) Max Power 204W
Backup	Copper based backup link	Cisco 887-M Router Dimensions: 1.75 x 12.8 x 9.8 in. (4.4 x 32.5 x 24.9 cm) Max Power 80W

Table 51 DCC User Gateway Equipment

This equipment will be provided by DCC. It should be noted that each Cisco 3560-8PS switch or Cisco 887-M router requires 1U of rack space and dual 240V UK power supplies.

The high level obligations and responsibilities around this equipment are described in SEC section H3 DCC User Gateway Equipment. More detailed obligations and responsibilities are contained in the DCC User Gateway Interface Code of Connection.

14.4 Maintenance

Maintenance of the DCC User Gateway equipment installed at customer premises is the responsibility of the DCC and wherever possible will be carried out remotely using the network connection itself to gain access to the equipment. Where this is not possible then the DCC Service User shall provide local access to the equipment as per the obligations and responsibilities described in the DCC User Gateway Interface Code of Connection.

14.5 Use of the Connection

The DCC User Gateway Network is used to provide access to many different DCC Services, not just the DCC User Gateway Interface for Service Request processing (which is the subject of this specific Design Specification).

The same physical connection to the DCC User Gateway Network may therefore be used by a DCC Service User to provide more than one “logical” connection to DCC Services. Each logical connection to DCC Services is governed by its own Code of Connection and is subject to its own authentication and security requirements to ensure separation of the services. Each logical connection will be set up as a separate VPN over the VPLS network.

In a similar fashion, there is a need to provide separate test connections for access to the DCC User Gateway Interface test services. Test connections can be provided over the same physical connection as the main services and will be subject to the same authentication and security requirements as described in the DCC User Gateway Code of Connection, albeit using separate test systems and security credentials to establish the test connection.

For DCC Service User Organisations operating with more than one SEC Party and Role it is possible to use the same physical connection for more than one role. The authentication mechanisms to support this are described in section 7 and section 15.

14.6 IP Addressing

Details of the IP addressing and network configuration will be provided to the DCC Service User as part of the process for obtaining a connection to the DCC User Gateway as described in the DCC User Gateway Connection.

15 Connection – Certificate and Key Management

Certificate and Key Management is described in the DCCKI SEC documentation set, including the following documents:

- DCCKI RAPP
- DCCKI Interface Specification
- DCCKI Code of Connection
- DCCKI Certificate Policy
- DCCKI Repository Interface Specification
- DCCKI Repository Code of Connection

16 Anomaly Detection

16.1 Overview

The DCC Data Systems are required to provide an anomaly detection service for Service Request and Response processing (including Alerts) in order to protect the overall DCC service from potential threats or malicious behaviour.

The anomaly detection service will perform anomaly detection on incoming Service Requests, Service Responses and Alerts. Where a Service Request is flagged as being anomalous then the message will be quarantined, pending an investigation and confirmation of validity from the relevant DCC Service User. Should the message(s) prove to be valid then the message shall be released from quarantine and delivered to the relevant device. Messages which are confirmed as not valid will be deleted.

There are two levels of operation for the anomaly detection service:

- DCC service wide anomaly detection which operates across all DCC Service Users to protect the overall DCC Service. This service is configured and managed by the DCC.

- DCC Service User specific anomaly detection which operates against the Service Request and Response processing for each DCC Service User. This is managed with each DCC Service User individually.

Volume threshold anomaly detection does not treat SMETS1 Service Requests differently to Service Requests for other Devices, i.e. numbers of Service Requests sent are counted towards volume thresholds irrespective of the SMETS versions of the associated Devices.

16.2 Approach

There are two patterns of usage for the anomaly detection service:

- Volume threshold checking against the rate of receipt of messages

- Attribute limit checking against specific values in each message

The basic approach for the volume threshold anomaly detection service is to check the volume of messages received against a set of agreed thresholds for the rate of receipt of messages. These thresholds are set for a given Service Reference Variant by configuration of one or more anomaly detection “rules”. See section 16.3 for more details.

For each volume threshold anomaly detection rule which is configured, there are two thresholds applied:

- a “Warning” threshold which if exceeded causes an event to be recorded and reported but which does not result in messages being stopped; and

- a “Quarantine” threshold which if exceeded causes an event to be recorded and reported but which also places the anomalous message and all subsequent requests of that type into quarantine.

For attribute limit checking, individual attributes within messages are checked against specific upper or lower limit values. These limits are set for a given Service Reference Variant by configuration of one or more anomaly detection “rules”. See section 16.4 for more details.

For either pattern of usage, when an anomaly detection rule is breached the relevant DCC Service User is informed via an out of band process, not via the DCC User Gateway.

The mechanism for notification of anomaly detection events is described in the Threshold Anomaly Detection Procedures document.

If messages have been quarantined then the DCC Service User is responsible for investigating the cause of the exception and confirming back to the DCC whether the messages were valid or not.

The mechanism for confirming validity of messages and subsequent release from quarantine is described in the Threshold Anomaly Detection Procedures document

Upon confirmation that the messages are valid then the DCC will release the messages from quarantine for onward delivery to the relevant device. If the messages are confirmed as not valid then they will be deleted from the DCC Data Systems.

If the DCC Service User does not notify the DCC of the decision to release or delete messages within [72] hours of the messages being placed in quarantine then the DCC will set these messages as "archived" and will delete these messages after a further [28] days have elapsed.

16.3 Volume Threshold Anomaly Detection Rules

The volume threshold anomaly detection rules to be applied for each DCC Service User are configurable items that can be changed over time. This section describes the available patterns and, where appropriate, related algorithms that are used for anomaly detection. The specific instances of volume threshold anomaly detection rules will be agreed with each DCC Service User and provided to the DCC. The mechanism for notification of anomaly detection rules is described in the Threshold Anomaly Detection Procedures document.

For Service Request processing the basic pattern for anomaly detection is to monitor the number of messages received over a given time period. The time period is a rolling window based on the total counts recorded for each recording interval, where the recording interval is calculated such that there are a fixed number of intervals (initially set at 30) within that period. So, for example, a time period of 30 minutes would use 30 recording intervals of 1 minute each, a time period of 60 minutes would use 30 recording intervals of 2 minutes each, and so on.

To avoid multiple, repeated notifications of thresholds being breached, a "quarantine event" will be started and notified at the first breach of the threshold and all subsequent messages placed in quarantine will be considered part of that quarantine event. The quarantine event will continue whilst the threshold is breached for consecutive recording intervals and will only be deemed complete at the end of the next recording interval at which the threshold is not breached.

The rules to be applied will be agreed with each DCC Service User. DCC Service Users are required to set anomaly detection rules for each Service Reference Variant that is classified as Critical and each Service Reference Variant that returns sensitive data. Rules may be set for other Service Reference Variants if desired.

The table below shows the template for defining the anomaly detection rules along with some examples (values are indicative and not intended to be taken as representative of actual values expected). The actual values will be agreed with DCC Service Users as described in the Threshold Anomaly Detection Procedures document.

Service Reference Variant	Warning threshold	Quarantine threshold	Time Period
SR1.1.1 Update Tariff	10	20	1440 minutes
SR7.2 Disable Supply	50	200	5 minutes
SR1.2.1 Update Price	25	50	30 minutes

Table 52: Example anomaly detection rules

For Service Responses there is less configurability on a per Service Request basis and in fact the only anomaly detection that is applied for Service Responses is to check that the Service Response has an associated unfulfilled Service Request. If it does not then that Service Response is considered anomalous. Information about anomalous Service Responses is recorded within the DCC Data Systems Service Audit Trail and event log and will be reported to the relevant DCC Service User. (The process for notifying the DCC Service User will be

agreed as part of the Service Management Framework.) Note, however, that anomalous Service Responses are not placed in quarantine but are discarded once they have been recorded in the Service Audit Trail, since there is no valid scenario in which these responses should be delivered to a DCC Service User.

For Alert processing it is expected that as a minimum there is at least one absolute rule which is applied for each Device to detect a "flood" of Alerts, for example receipt of 100 Alerts in 30 minutes. When such an anomaly detection threshold is breached then this is recorded in the DCC Data Systems event log and will be reported to the relevant DCC Service User. (The process for notifying the DCC Service User will be agreed as part of the Service Management Framework.)

16.4 Attribute Limit Anomaly Detection Rules

Attribute limit anomaly detection rules are set by the DCC and are applied to specific attributes on a pre-defined set of messages.

16.4.1 SMETS2 or later

Attribute limit checks are carried out against the values held in Signed Pre-Commands. A specific attribute may be subject to an upper or lower limit check, with a value which is above or below this limit being deemed anomalous.

An example of the configuration details held for an attribute limit anomaly detection rule is as follows

Service Reference Variant	Attribute	Limit Type	Value
SR1.1.1 Update Tariff	Standing Charge	Upper	100
SR1.6 Update Payment Mode	Disablement Threshold	Lower	0

Table 53: Example anomaly detection rules

If an attribute limit anomaly detection rule is breached then the message is placed in quarantine. The mechanism for notifying the affected Service User is exactly the same out of band mechanism as used for notification of breaches of volume threshold anomaly detection rules.

To avoid multiple, repeated notifications of the same limit check being breached, a "quarantine event" will be started and notified at the first breach of the limit and all subsequent messages that breach the same limit will be considered part of that quarantine event. The quarantine event will continue for a configurable maximum period of time after the first breach, after which that particular quarantine event will be deemed closed. Any subsequent messages that breach the same limit will start a new quarantine event.

The mechanisms for reporting and releasing messages from quarantine are exactly the same as for volume threshold anomaly detection quarantine events.

16.4.2 SMETS1

For SMETS1 Service Requests, Attribute Limit Anomaly Detection is carried out only by the S1SP, and on the XML values (whereas for SMETS2 or later Devices it is on GBCS attributes).

As described in the SEC Service Request Processing Document, any Service Request which breaches Attribute Limit Anomaly Detection shall be discarded by the S1SP. Release from Quarantine is not supported for SMETS1 Service Requests discarded due to Attribute Limit Anomaly Detection.

Appendices

Appendix 1 – Glossary

Acronym	Description
ACB	Access Control Broker
ALCS	Auxiliary Load Control Switch
APC	Auxiliary Proportional Controller
API	Application Programming Interface
BS	British Standard
CA	Certificate Authority
CAD	Consumer Access Device
CCS	Customer Consent Service
CESG	Communications Electronic Security Group, the UK Government's National Technical Authority for Information Assurance
CHECK	UK government IT Health Check Service
CHF	Communications Hub Function
CHTS	Communications Hub Technical Specifications
CIN	Customer Identification Number
CISO	Chief Information Security Officer
CMS	Customer Management Service
CoCo	Code of Connection
CoS	Change of Supplier
CoS Party	CoS Party is the general term to describe the Party that authorises CoS Service Requests. It may refer to an ECoS Party or the TCoS Party.
CoT	Change of Tenancy
Countersigned S1SP Alert	Asynchronous message sent by the DCC Data Systems to the DCC Service User. It is a DCC Alert with a DCC Alert Code that indicates it carries an S1SP Alert within it.
Countersigned SMETS1 Alert	Asynchronous message sent and signed by the DCC Data Systems to a DCC Service User. It incorporates a SMETS1 Alert provided by an S1SP, and contains data using MMC Device Alert formats.
Countersigned SMETS1 Response	Synchronous or Asynchronous message sent and signed by the DCC Data Systems to the DCC Service User, in response to a Service Request where the target is a SMETS1 Device. A Countersigned SMETS1 Response wraps a SMETS1 Response provided by an S1SP.
CPL	Central Products List
CR	Credit (Meter Payment Mode)
CREST	A not for profit organisation for the information security industry
CSP	Communications Services Provider

Acronym	Description
CSR	Certification Signing Request
CSS	Central Switching Service
CV	Command Variant
DCC	Data Communications Company
DCCKI	Data Communications Company Key Infrastructure
DECC	Department of Energy and Climate Change
DEMS	Device Estate Management Service
Device ID	Unique number by which an individual Device can be identified, as allocated to that Device in accordance with SMETS or CHTS (where applicable)
DMS	Device Management Service
DSP	Data Service Provider
DUGC	DCC User Gateway Catalogue
DUGIDS	DCC User Gateway Interface Design Specification (this document set)
DUIS	DCC User Interface Specification
DUIS Format	Format defined in this document set, i.e. the XML format defined in the XSD (DUIS XML Schema)
ECB	European Central Bank
ECDH	Elliptic Curve Diffie Helman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECoS Party	Enduring Change of Supplier Party SMETS2 or later: Performs authorisation checks on CoS Requests and creates a GBCS signed pre-command. SMETS1: Performs authorisation checks on CoS Requests.
EES	Electricity Export Supplier
EIS	Electricity Import Supplier
ENO	Electricity Network Operator
ENUM	ENUMeration
ESME	Electricity Smart Metering Equipment
FDEDA	Future Dated Execution Device Alert
FS	Firmware Service
GBCS	Great Britain Companion Specification
GBCS UC	Great Britain Companion Specification Use Case
GIS	Gas Import Supplier
GMAC	Galois Message Authentication Code
GNO	Gas Network Operator
GPF	Gas Proxy Function
GPG	CESG Good Practice Guide
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch

Acronym	Description
HHT	Hand Held Terminal
HMG	Her Majesty's Government
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
ICT	Information & Communications Technology
ID	Identifier
IHD	In Home Display
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KRP	Known Remote Party. SMETS2 or later: Definition as per GBCS. In the context of a specific Device, a Remote Party whose Security Credentials are stored on that Device in at least one Trust Anchor Cell SMETS1: In relation to a SMETS1 Device, shall mean a Party for which the Relevant S1SP holds either a current Notified Critical Supplier ID or a current Notified Critical Network Operator ID for the SMETS1 Device in question.
MAC	Message Authentication Code
MMC	Message Mapping Catalogue
MMC Format	Format defined in this document set for MMC, i.e. the XML format defined in the MMC XML Schema XSD (document 4 of this documentation set)
MPAN	Meter Point Administration Number (Electricity)
MPRN	Meter Point Reference Number (Gas)
M2M	Machine To Machine
N/A	Not Applicable
OU	Other User
PEP	Policy Enforcement Point Means, a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Data Systems and connecting systems, namely Service User Systems and RDP Systems. The PEP ensures that: (a) the policies in the applicable Code of Connection relevant to the applicable Party are being enforced; (b) there is appropriate separation of the DCC Data Systems from the connecting systems of the applicable Party; and (c) all the connections to the Service User Systems, RDP Systems, or DCC Data Systems are compliant with the same applicable Code of Connection.
PKCS	Public Key Cryptography Standards
PKR	Public Key Repository
PMS	Product Management Service

Acronym	Description
PP	PrePayment (Meter Payment Mode)
PPMID	PrePayment Interface Device
PS	Prepay Service DCC Systems
PTUT	Prepayment Top Up Token
RDP	Registration Data Provider
RNDS	Record Network Data Service
RS	Reading Service
S1SP	SMETS1 Service Provider; SMETS1 equivalent of CSP
S1SP Alert	An S1SP Alert is a message originated by an S1SP, containing information relevant to a SMETS1 Device, which is sent to the DSP for inclusion in a DCC Alert with a DCC Alert Code which indicates that it contains an S1SP Alert.
SAPC	Standalone Auxiliary Proportional Controller, a Device conforming to SMETS2 section 9 (SMETS2 v5.0 or later). SAPC Devices are implemented as Device Type ESME on the CPL and in DCC Data Systems,
SEC	Smart Energy Code
SECCo	Company established to facilitate the operation of the SEC
SLA	Service Level Agreement
SMETS1	Smart Metering Equipment Technical Specifications first version
SMETS1 Alert	SMETS1 Alerts are used to communicate Alert codes related to SMETS1 Devices which are (where applicable) the equivalent of Device Alerts. They include a subset of GBCS Device Alert codes which are deemed also applicable to SMETS1 Devices, and additional Alert codes for SMETS1 Devices. A SMETS1 Alert is sent by an S1SP to the DCC Data Systems and contains data using MMC Device Alert formats. The DCC Data Systems signs a SMETS1 Alert for sending to the appropriate Service User, incorporating it into a Countersigned SMETS1 Alert.
SMETS1 Response	A message from an S1SP to the DCC Data Systems, signed by the S1SP, in response to a Countersigned Service Request. The DCC Data Systems. A SMETS1 Response is sent by an S1SP to the DCC Data Systems and contains data using MMC Response formats. The DCC Data Systems signs a SMETS1 Response for sending to the appropriate Service User, incorporating it into a Countersigned SMETS1 Response.
SMETS2	Smart Metering Equipment Technical Specifications second version
SMKI	Smart Meter Key Infrastructure
SMS	Smart Metering Systems
SMS	Supply Management Service
SM WAN	Smart Meter Wide Area Network
SNA	Supplier Nominated Agent
SOAP	Simple Object Access Protocol
SS	Scheduling Service

Acronym	Description
SU	Service User
TBC	To Be Completed
TCoS Party	Transitional Change of Supplier Party SMETS2 or later: Performs authorisation checks on CoS Requests and creates a GBCS signed pre-command. SMETS1: Not applicable.
TLS	Transport Layer Security
TOU	Time Of Use
UC	Use Case
UKAS	United Kingdom Accreditation Service
UPRN	Unique Property Reference Number
URL	Uniform Resource Locator
URP	Unknown Remote Party. SMETS2 or later: Definition as per GBCS. In the context of a specific Device, a Remote Party whose Security Credentials are not stored on that Device SMETS1: In relation to a SMETS1 Device, shall mean a Party for which the Relevant S1SP does not hold either a current Notified Critical Supplier ID or a current Notified Critical Network Operator ID for the SMETS1 Device in question.
UTC	Coordinated Universal Time
UTRN	Unique Transaction Reference Number
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
WAN	Wide Area Network
WIP	Work In Progress
XML	eXtensible Markup Language
XML DSP Role Signing Private Key	A Private Key associated with a Public Key that is contained within an Organisation Certificate with a Remote Party Role of “dSPXmlSign”
XML User Role Signing Private Key	A Private Key associated with a Public Key that is contained within an Organisation Certificate with a Remote Party Role of “xmlSign”
XSD	XML Schema Definition

Table 54 Definitions

Appendix 2 – DUIS XML Schema Definition Instructions

The DUIS XML schema is compliant with the XML 1.1 standard and can be viewed using Internet Explorer. The DUIS XML schema contains 2 top level items that are used to define the messages passed between the DCC Service Users and the DCC Data Systems. These top level items are;

- Request – Defines the Service Requests and Signed Pre-Command for the DCC Data Systems
- Response – Defines the data that is returned by the DCC Data Systems to the DCC Service User. This covers Service Responses, Alerts and Acknowledgements.

For the avoidance of doubt, the DUIS/MMC XML Schema is provided as the authoritative source for data item definitions. Where any inconsistencies may exist between the definitions contained within the main text within this document and the DUIS/MMC XML Schema then the DUIS/MMC XML Schema shall take precedence.

The DUIS XML schema definition uses a small number of constructs to define the structure and formats of the data.

The key constructs used in the schema are;

- SimpleType – A basic data type for a data item for example an Integer or String. SimpleTypes may have a restriction to only allow certain data items to be entered, for example, EUI is defined as 8 pairs of hexadecimal strings separated by a colon.
- Element – An item within the XML, this may be a standard data type or be defined by a SimpleType.
- ComplexType – A collection on Elements that make up a structure
- Sequence – Within a ComplexType a Sequence specifies that the Elements must be included in a particular order. Elements within the Sequence may be optional or mandatory.
- Choice – Within a ComplexType there may be a choice between which Elements are allowable, this defined by a Choice.

Unless explicitly defined with the Type definitions, no restrictions are applied to the standard XSD Attributes and a User may use the full range of values as defined by that XML Type

The following is a simplified version of the section of the DUIS XML schema that defines the Response;

```
<xs:complexType name="Response">
  <xs:sequence>
    <xs:element name="Header">
      <xs:complexType>
        <xs:sequence>
          <xs:element maxOccurs="1" name="RequestID" type="sr:RequestIDType"
            minOccurs="0"/>
          <xs:element maxOccurs="1" name="ResponseID" type="sr:ResponseIDType"
            minOccurs="0"/>
          <xs:element name="ResponseCode" type="sr:ResponseCode"/>
          <xs:element name="ResponseDateTime" type="xs:dateTime"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="Body">
      <xs:complexType>
        <xs:choice minOccurs="1">
          <xs:element name="ResponseMessage" type="sr:ResponseMessage"> </xs:element>
          <xs:element name="DeviceAlertMessage" type="sr:DeviceAlertMessage"/>
```

```
            <xs:element name="DCCAlertMessage" type="sr:DCCAlertMessage"/>
          </xs:choice>
        </xs:complexType>
      </xs:element>
      <xs:element ref="ds:Signature" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
```

The structure is defined as a ComplexType and identified by the name "Response". It contains a Sequence of three Elements: Header, Body and ds:Signature. The four Elements of the Header have unique names, the first two are optional (minimum allowed occurrences is 0 and maximum is 1) and the last two are mandatory (minimum and maximum number of allowed occurrences is 1). The Body is a choice and so one of its three elements must be included in the XML. The ds:Signature is a reference to an external Schema and it is optional

The data types and restrictions are defined elsewhere in the schema, for example CommandVariant is defined as;

```
  <xs:simpleType name="CommandVariant">
    <xs:restriction base="xs:positiveInteger">
      <xs:enumeration value="1"/>
      <xs:enumeration value="2"/>
      <xs:enumeration value="3"/>
      <xs:enumeration value="4"/>
      <xs:enumeration value="5"/>
      <xs:enumeration value="6"/>
      <xs:enumeration value="7"/>
      <xs:enumeration value="8"/>
    </xs:restriction>
  </xs:simpleType>
```

That is a positive integer that must be between the values 1 and 8 inclusive.

Note that the education site w3schools.com provides a useful primer on XML schemas with many examples, see http://www.w3schools.com/schema/default.asp

Appendix 3 – MMC XML Schema Definition Instructions

The MMC XML schema can be viewed using Internet Explorer. The MMC XML schema contains 1 top level item that is used to define the data passed from the Parse software to DCC Service User's systems. This top level item is as follows;

- GBCSResponse – Defines the data that is returned by the Parse software to the DCC Service User. This covers Service Responses (from Device) and Device Alerts.

The MMC XML schema definition uses the same constructs as the DUIS XML schema (see Appendix 2) to define the structure and formats of the data.

For the avoidance of doubt, the DUIS/MMC XML Schema is provided as the authoritative source for data item definitions. Where any inconsistencies may exist between the definitions contained within the main text within this document and the DUIS/MMC XML Schema then the DUIS/MMC XML Schema shall take precedence.

The GBCSResponse also follows a similar approach to that defined in the DUIS XML schema, in that it is defined as a ComplexType and identified by the name "GBCSResponse". It contains a Sequence of two Elements: Header and Body.

A more detailed set of information on the MMC XML schema is contained in Annex 18.

Appendix 4 – XML Data Type Ranges

The following table summarises the minimum and maximum values for those numeric data types that have a range defined in XML and are used in the DUIS and / or the MMC XML Schema.

Datatype	Description	Minimum Value		Maximum Value	
xs:short	Signed 16-bit integer	-32,768	-2^{15}	32,767	$2^{15}-1$
xs:int	Signed 32-bit integer	-2,147,483,648	-2^{31}	2,147,483,647	$2^{31}-1$
xs:long	Signed 64-bit integer	−9,223,372,036,854,775,808	-2^{63}	9,223,372,036,854,775,807	$2^{63}-1$
xs:unsignedShort	Unsigned 16-bit integer	0		65,535	$2^{16}-1$
xs:unsignedInt	Unsigned 32-bit integer	0		4,294,967,295	$2^{32}-1$
xs:unsignedLong	Unsigned 64-bit integer	0		18,446,744,073,709,551,615	$2^{64}-1$

Table 55 XML Data Type Ranges

Appendix 5 – GBCS Assumptions – Requests

This version of DUGIDS documentation set includes the following GBCS assumptions:

ID	Description	Service Request / Use Case	GIST Ref / IRP / DECC Ref	DUGIDS Impact	Solution Impact	Action
A44	Although CRP412 states that Service Request 6.2.10 is applicable to the RSA (SNA) User Role, the GBCS UCs ECS25r1, ECS25r2 and GCS20r aren't applicable to the ACB role, so it is not possible for the RSA to run this Service Request. SR 6.2.10 will therefore not be allowed for the RSA role. DUGIDS conforms to SEC namely to permit use by Roles EIS, GIS and ENO.	6.2.10 / ECS25r1, ECS25r2, GCS20r	TBC	Request and Response	If the Command was generated by the ACB using the URP pattern it would be rejected by the Device	Build to assumption

Table 56 GBCS Assumptions

Appendix 6 – GBCS Assumptions – Responses

The Service Request Responses (Parse) are aligned to GBCS v2.0 Draft 5 The following is a list of outstanding GBCS assumptions / queries:

ID	Description	Service Request / Use Case	GIST Number	DUGIDS Impact	Solution Impact	Action
A44	Although CRP412 states that Service Request 6.2.10 is applicable to the RSA (SNA) User Role, the GBCS UCs ECS25r1, ECS25r2 and GCS20r aren't applicable to the ACB role, so it is not possible for the RSA to run this Service Request. SR 6.2.10 will therefore not be allowed for the RSA role.	6.2.10 / ECS25r1, ECS25r2, GCS20r	TBC	Request and Response	If the Command was generated by the ACB using the URP pattern it would be rejected by the Device	Build to assumption

Table 57 Response GBCS Assumptions

Appendix 7 – SEC and GBCS Version Assumptions

This version of DUGIDS documentation set includes the following SEC assumptions:

ID	Description	Service Request	DUGIDS Impact
A106	It is assumed that this DUGIDS document set is aligned to GBCS v4.2. Should there be any misalignment found then these will be documented here in a future version of this document.		

Table 58 SEC and GBCS Version Assumptions

Appendix 8 – SMI Device Status – Entity Lifecycle Diagrams

The following diagrams summarise the status lifecycle for each SMETS2 or later Device Type in the Smart Metering Inventory:

1. ESME (including SAPC)

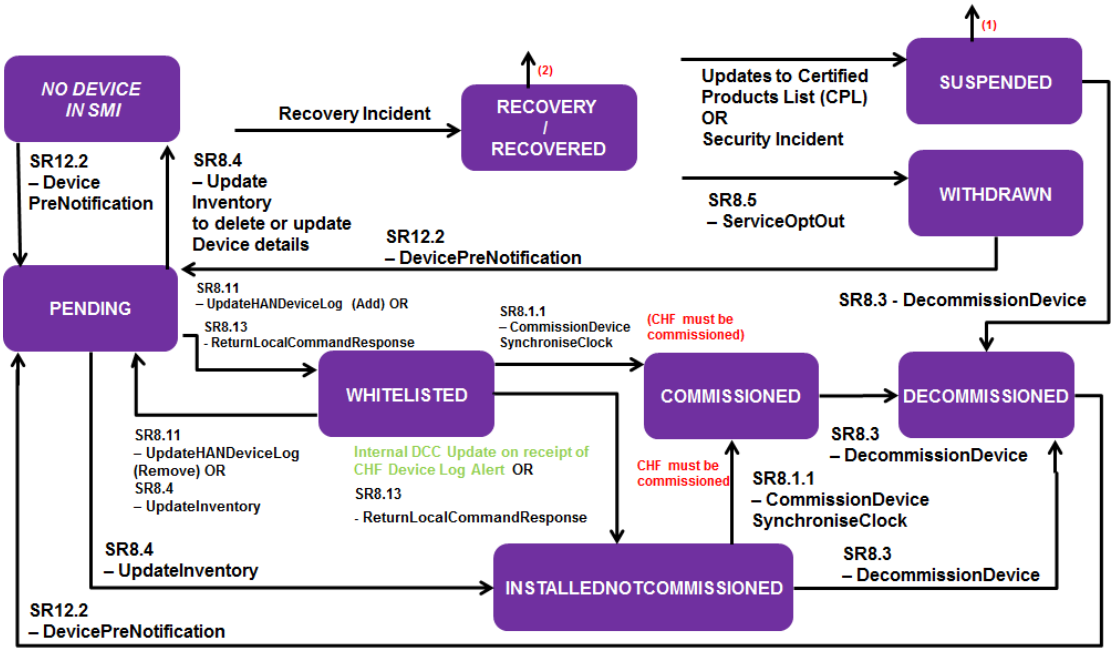


Figure 66 – Entity Lifecycle Diagram – ESME (including SAPC)

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(2) A Device may exit Recovery status after replacement of the Certificates has completed and ACB Certificates have not been used in the recovery process. If replacement uses ACB Certificates then the Device moves to Recovered status and it remains in Recovered status until those ACB Certificates have been replaced. Upon exiting Recovery or Recovered status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

2. GSME

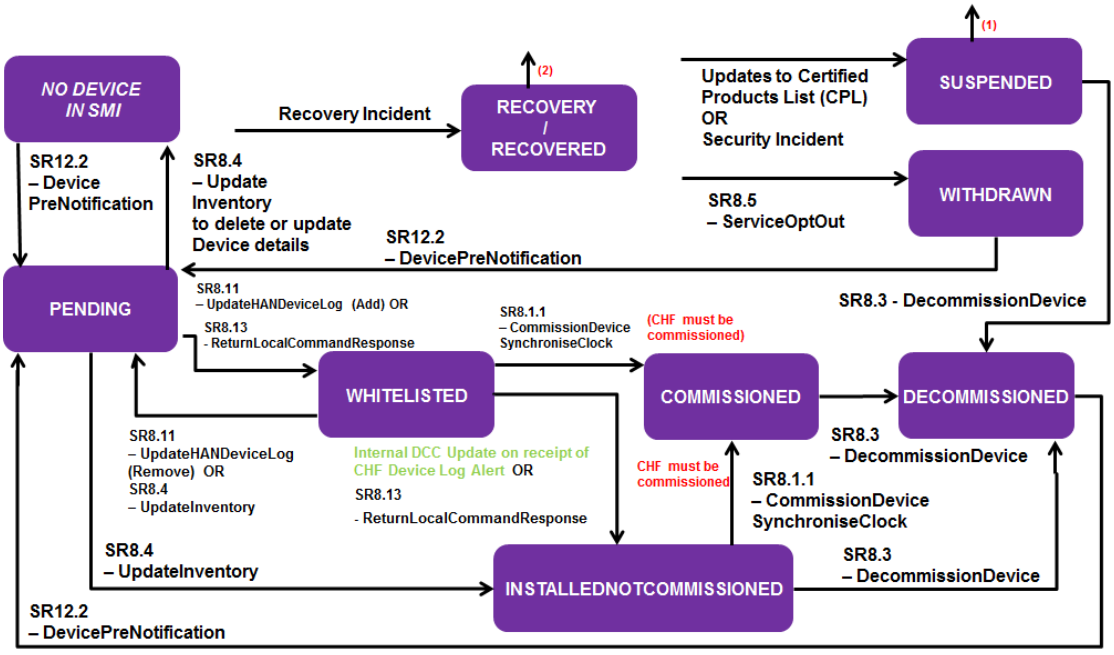


Figure 67 – Entity Lifecycle Diagram – GSME

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(2) A Device may exit Recovery status after replacement of the Certificates has completed and ACB Certificates have not been used in the recovery process. If replacement uses ACB Certificates then the Device moves to Recovered status and it remains in Recovered status until those ACB Certificates have been replaced. Upon exiting Recovery or Recovered status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

3. CHF

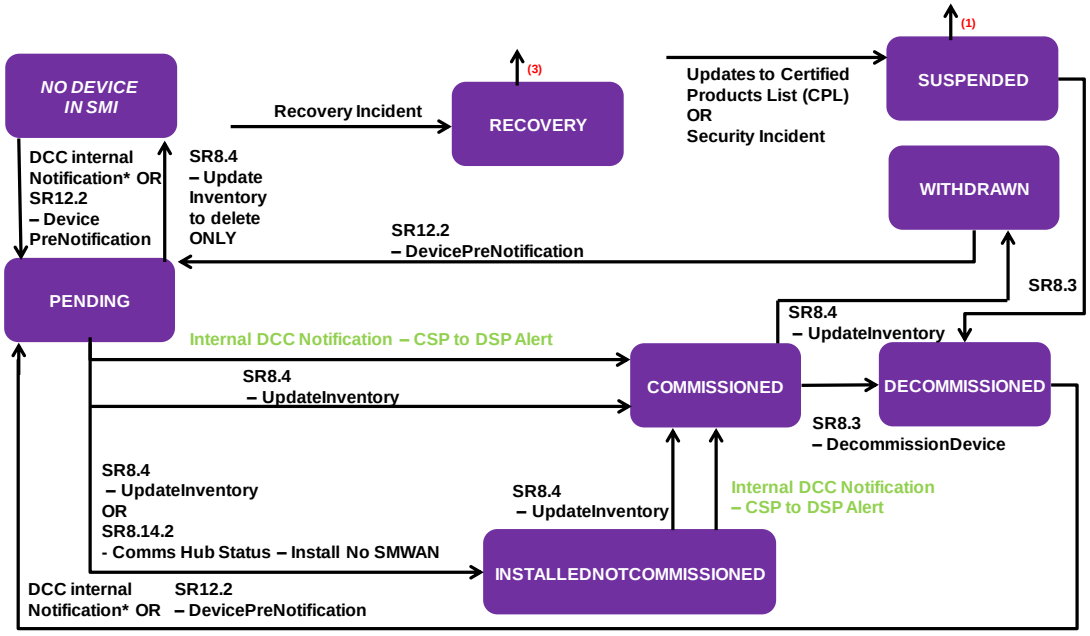


Figure 68 – Entity Lifecycle Diagram – CHF

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(3) A Device may exit Recovery status after replacement of the Certificates has completed. Upon exiting Recovery status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

4. GPF

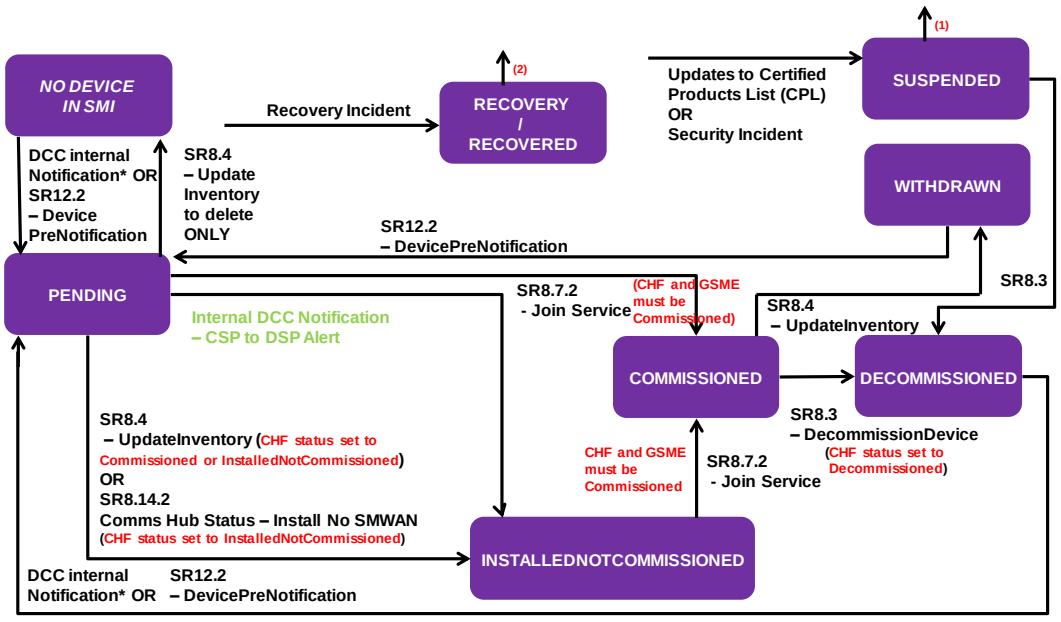


Figure 69 – Entity Lifecycle Diagram – GPF

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(2) A Device may exit Recovery status after replacement of the Certificates has completed and ACB Certificates have not been used in the recovery process. If replacement uses ACB Certificates then the Device moves to Recovered status and it remains in Recovered status until those ACB Certificates have been replaced. Upon exiting Recovery or Recovered status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

5. PPMID

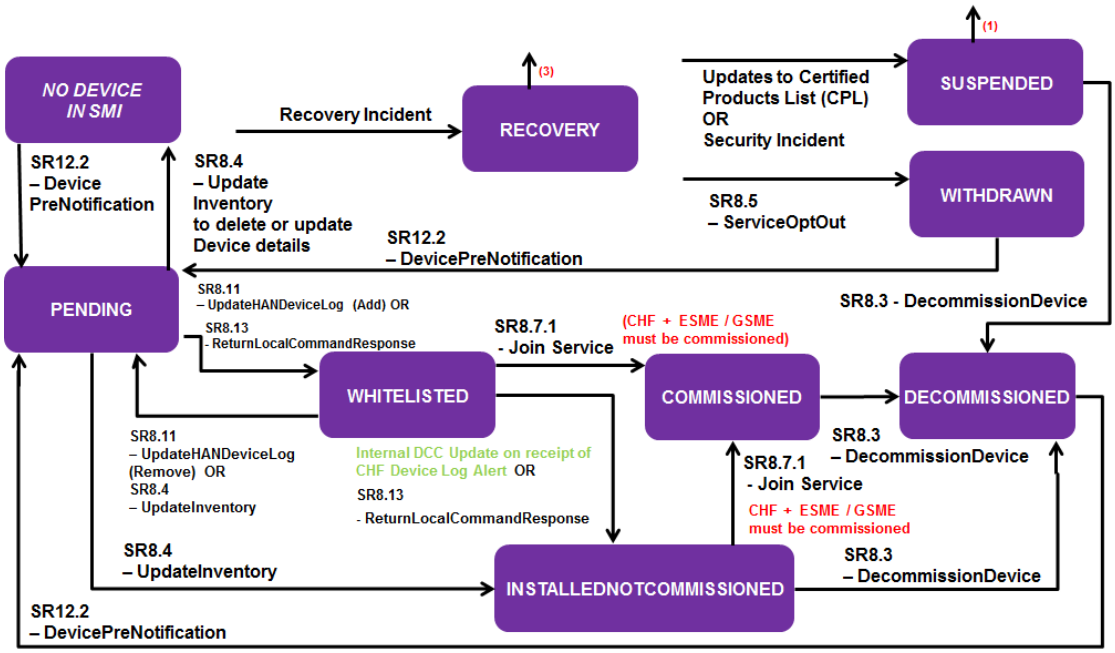


Figure 70 – Entity Lifecycle Diagram – PPMID

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(3) A Device may exit Recovery status after replacement of the Certificates has completed. Upon exiting Recovery status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

6. HCALCS

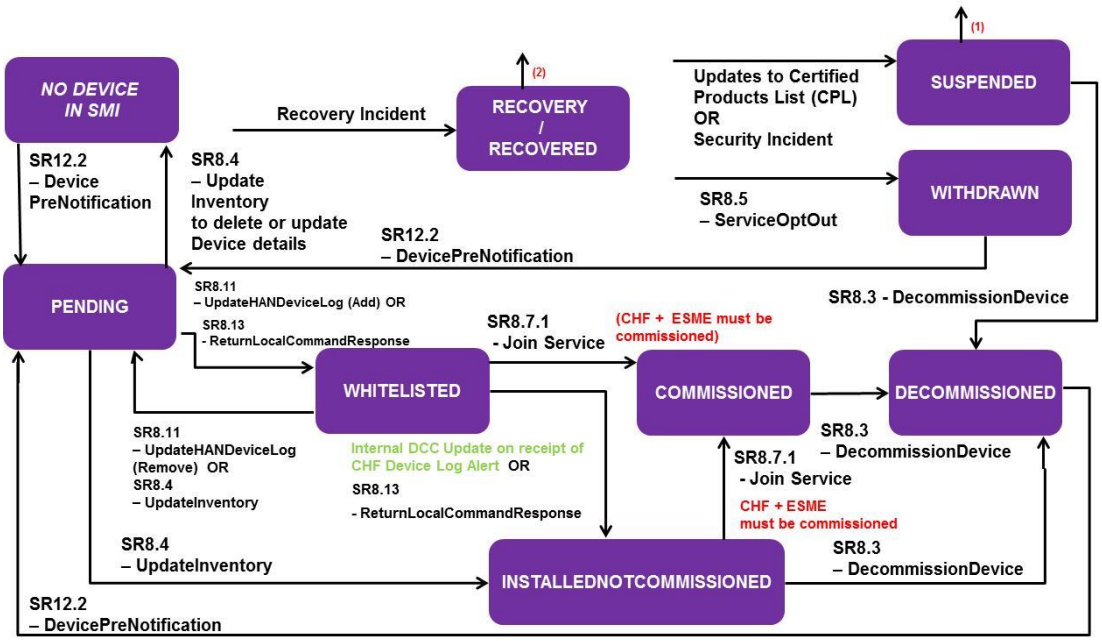


Figure 71 – Entity Lifecycle Diagram – HCALCS

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

(2) A Device may exit Recovery status after replacement of the Certificates has completed and ACB Certificates have not been used in the recovery process. If replacement uses ACB Certificates then the Device moves to Recovered status and it remains in Recovered status until those ACB Certificates have been replaced. Upon exiting Recovery or Recovered status the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its recovery. If a Device cannot be recovered, then it is possible to decommission that Device via Service Request 8.3

7. Type 2

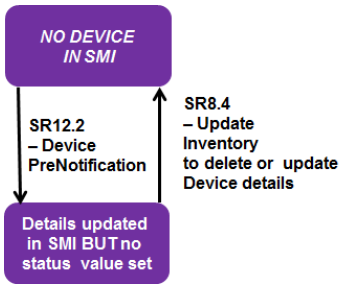


Figure 72 – Entity Lifecycle Diagram – Type 2

The following diagrams summarise the status lifecycle for each SMETS1 Device Type in the Smart Metering Inventory:

8. ESME

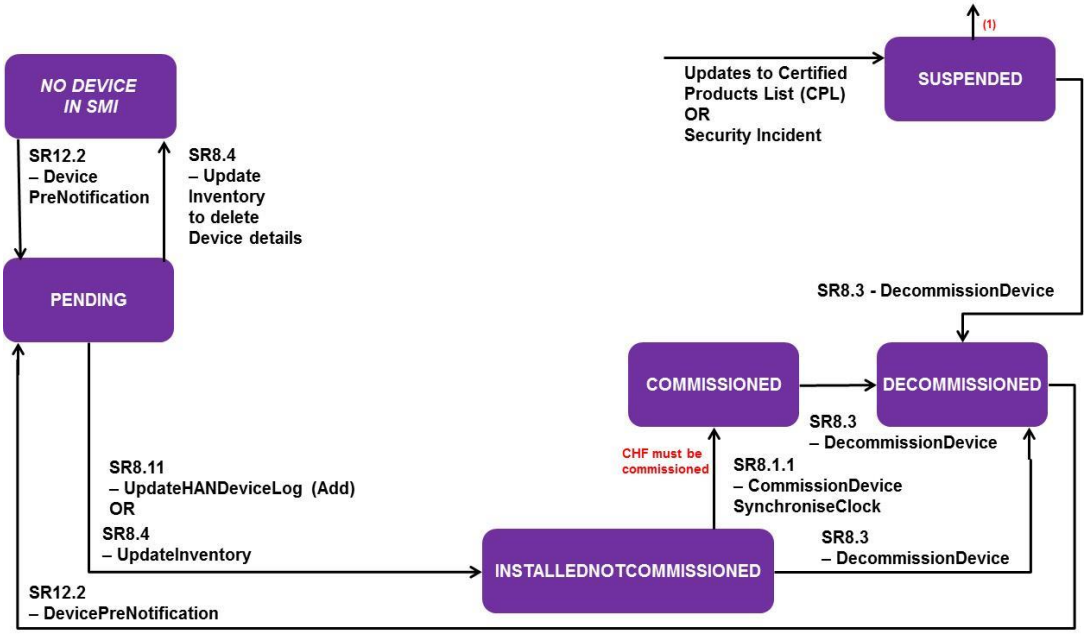


Figure 73 – SMETS1 Entity Lifecycle Diagram – ESME

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

9. GSME

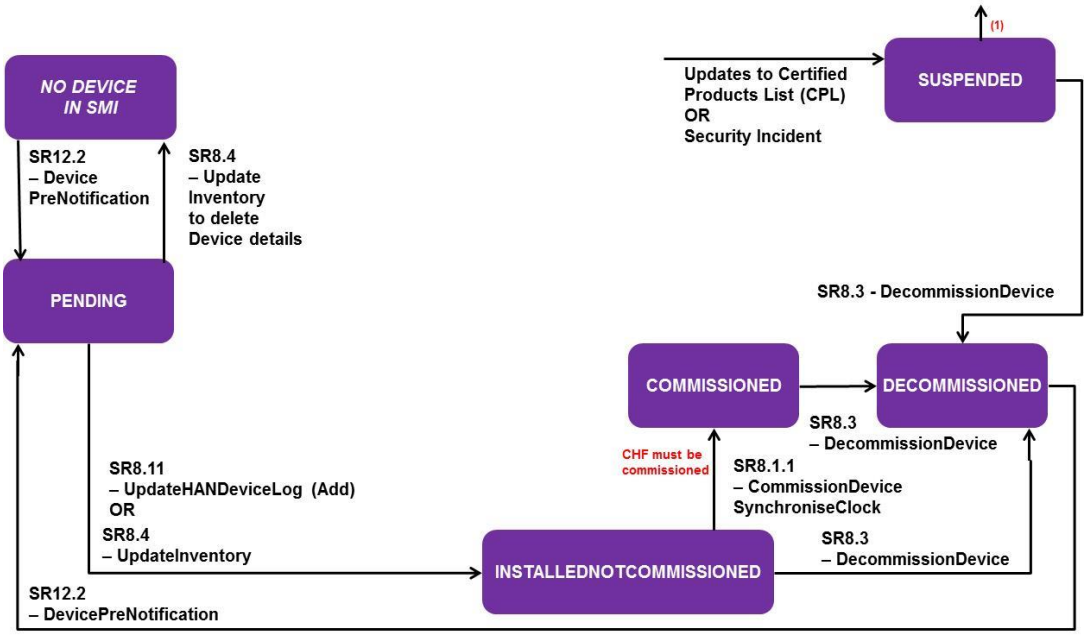


Figure 74 – SMETS1 Entity Lifecycle Diagram – GSME

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

10. CHF

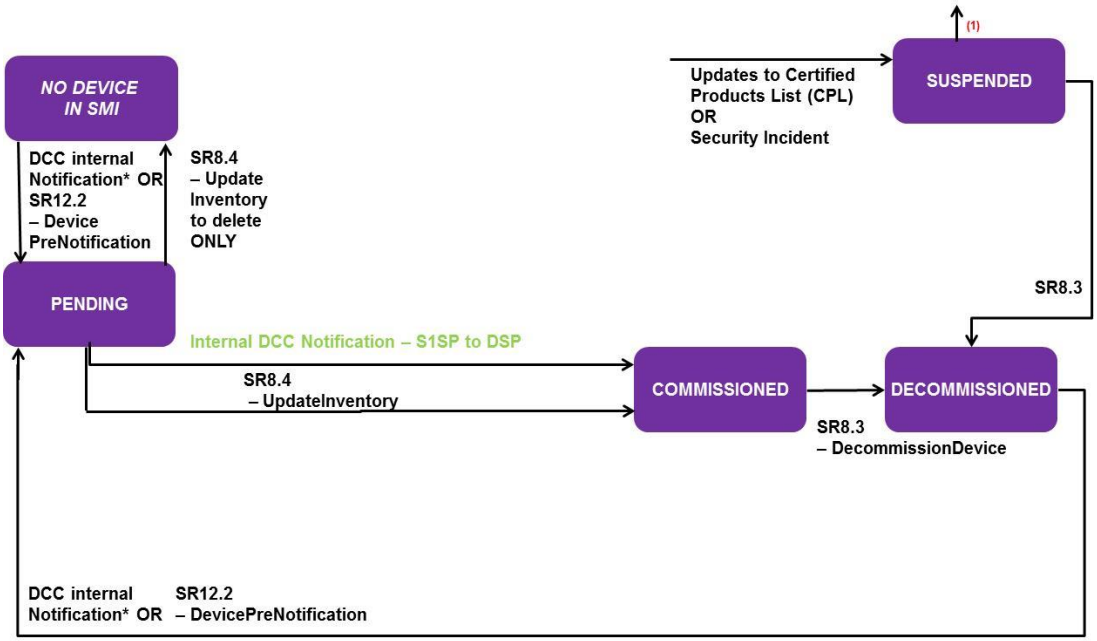


Figure 75 – SMETS1 Entity Lifecycle Diagram – CHF

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

11. GPF

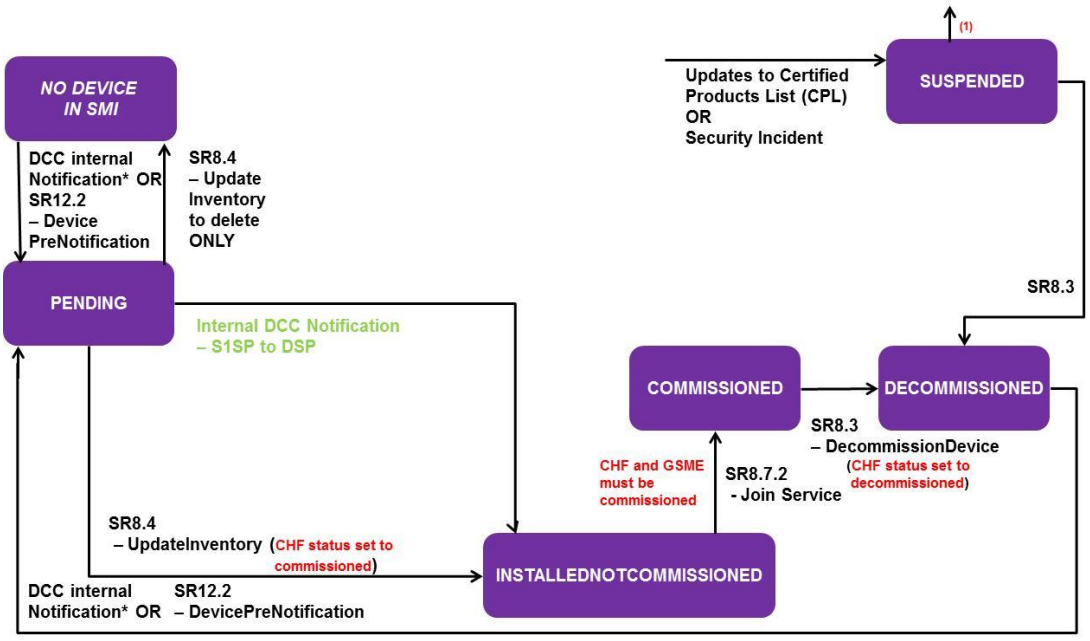


Figure 76 – SMETS1 Entity Lifecycle Diagram – GPF

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

12. PPMID

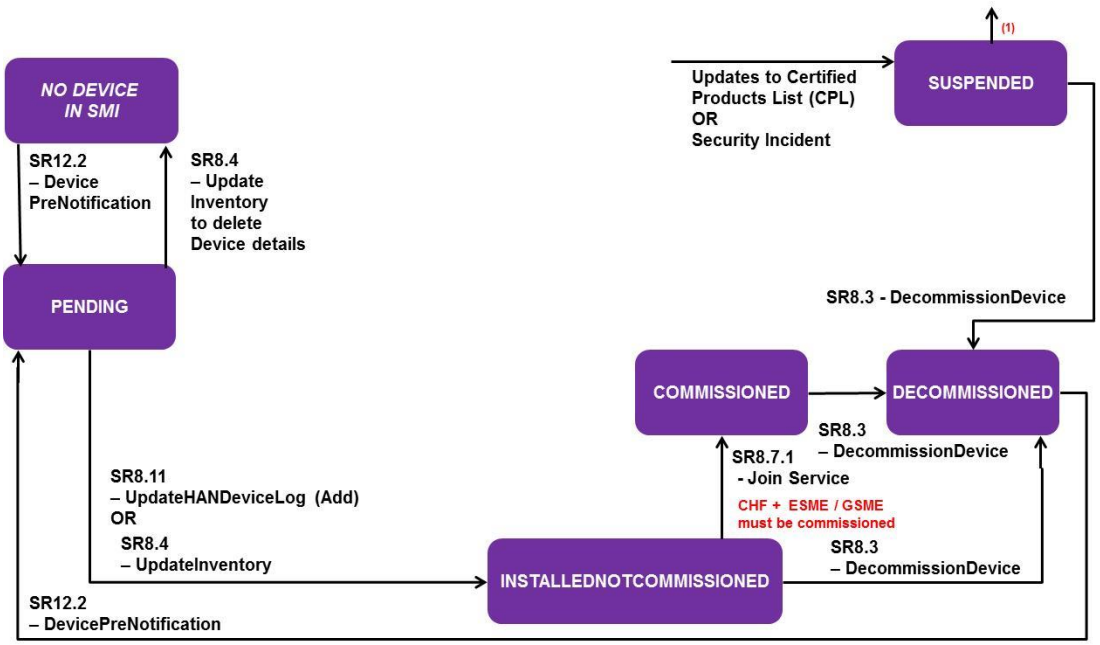


Figure 77 – SMETS1 Entity Lifecycle Diagram – PPMID

(1) If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Central Products List or of the Firmware Version being activated on the Device, the DCC Data Systems shall change the SMI Status of that Device to the status it held immediately prior to its Suspension

13. Type 2

As per SMETS 2 or later.

Appendix 9 – Error Handling and DCC Alerts

The following diagrams outline the main Error Handling scenarios as described in section 11.6, including the DCC Alerts generated in each scenario.

Some aspects of messaging to SMETS1 Devices require different error handling strategies. This section includes separate sets of diagrams for SMETS1 Devices and SMETS2 or later Devices.

SMETS2 or Later Devices

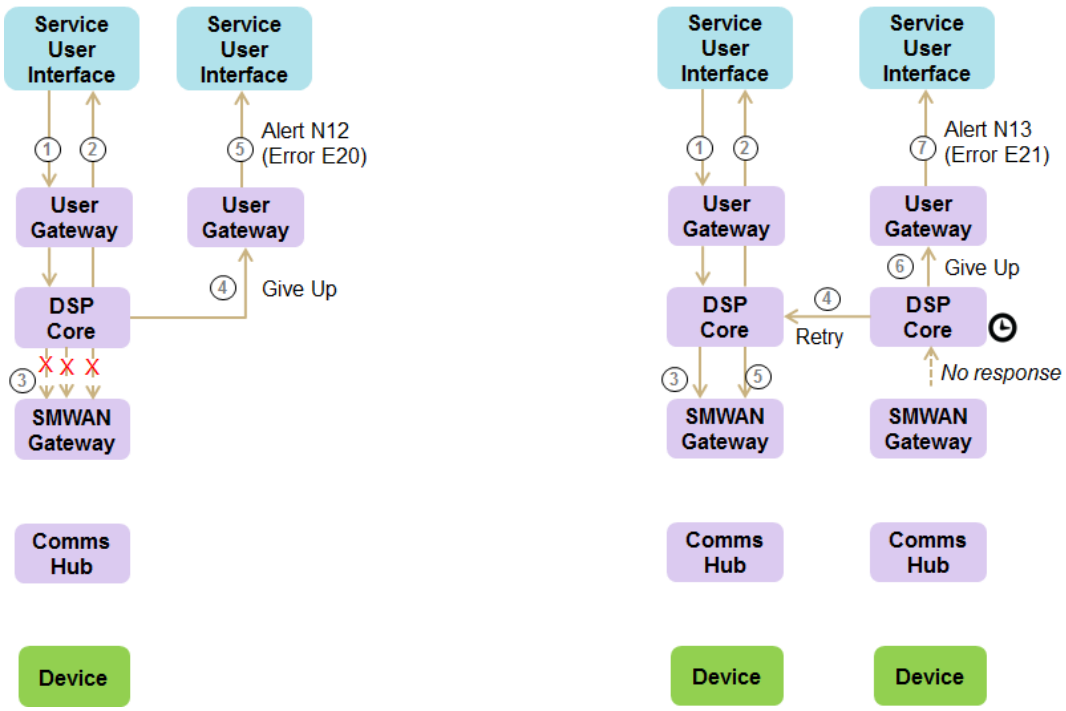


Figure 78 – Error Handling – On Demand

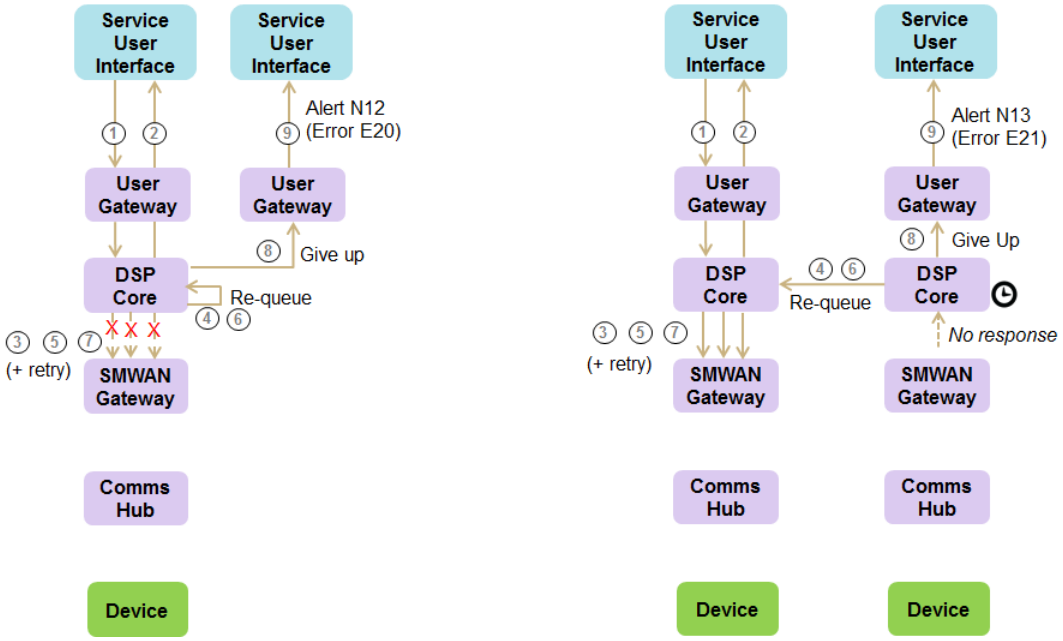


Figure 79 – Error Handling – Future Dated (Device) – Command Acknowledgement

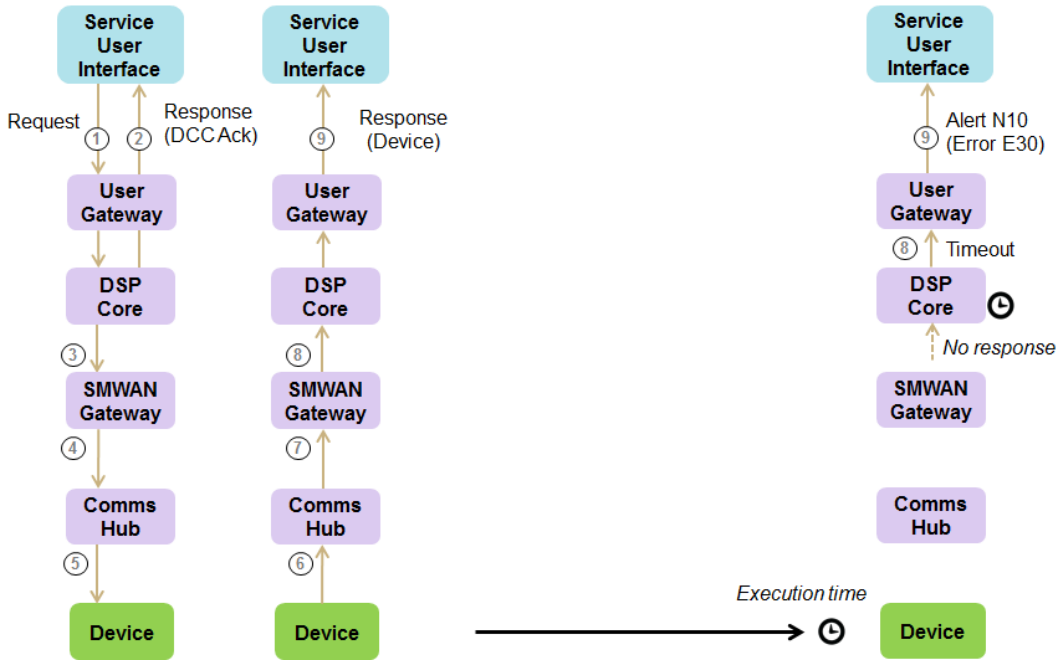


Figure 80 – Error Handling – Future Dated (Device) – Command Execution

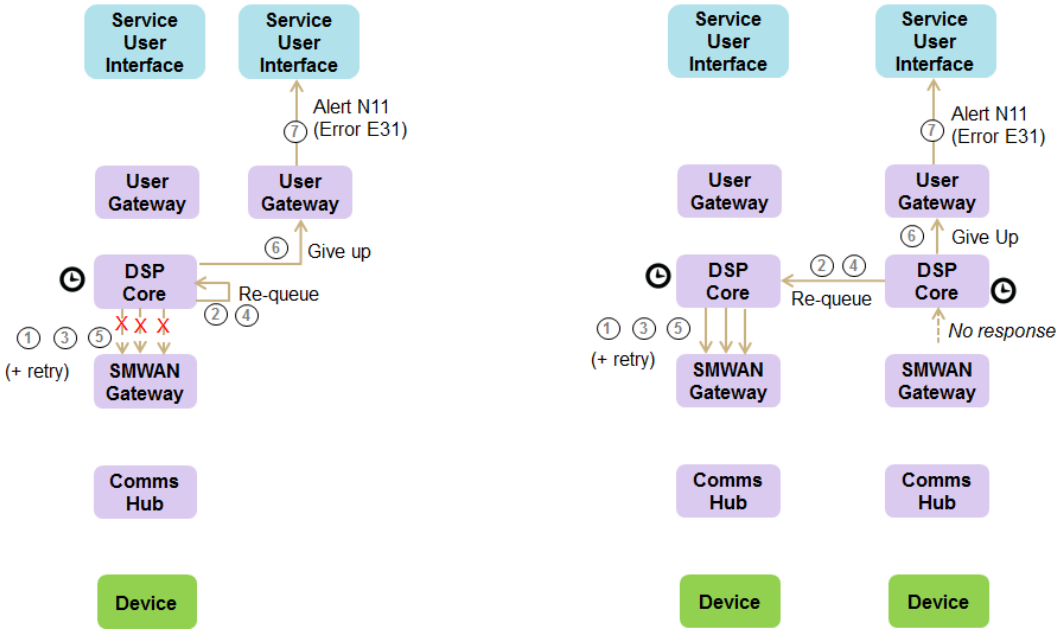


Figure 81 – Error Handling – DSP Scheduled / Future Dated (DSP)

SMETS1 Devices

Error Handling for SMETS1 Devices follows similar patterns to SMETS2 or later devices with the following variations:

- Validation errors may also be reported asynchronously by the S1SP via a DCC Alert.
- Retries when no response is received will be carried out by the S1SP rather than the DSP (note this only applies to the "short" retry strategy; where applicable the DSP will continue to use the "long" retry strategy and place requests on a back off queue for retry every 2 hours.)

The following diagrams show these variations for SMETS1 devices.

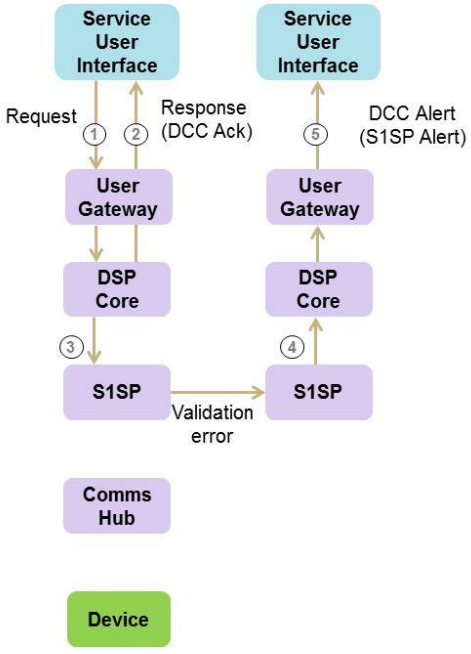


Figure 82 – Error Handling – S1SP Validation Error

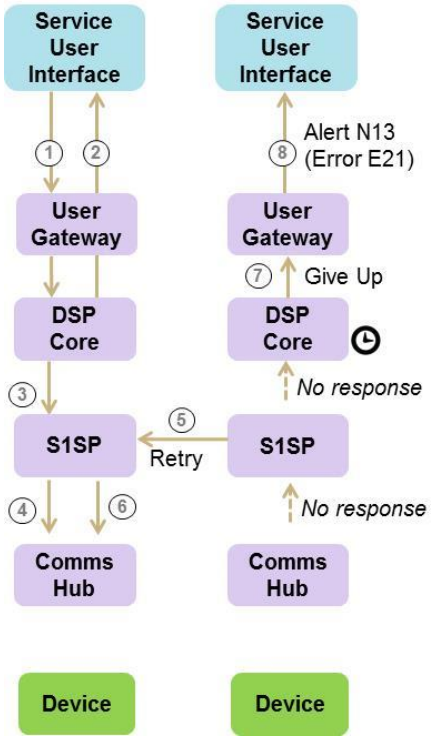


Figure 83 – Error Handling – S1SP Retry

Appendix 10 – Service Request Variant – GBCS UC Mapping Versioning

The following table summarises the Service Request Variant – GBCS UC mapping applicable to the different DUIS XSD, MMC XSD and GBCS versions:

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
1.1.1	>= 1.0	N/A	>= 1.0	N/A	ECS01a, GCS01a	ECS01a, GCS01a	ECS01a, GCS01a	ECS01a, GCS01a	ECS01a, GCS01a	ECS01a, GCS01a
1.1.2	>= 1.0	N/A	>= 1.0	N/A	ECS01c	ECS01c	ECS01c	ECS01c	ECS01c	ECS01c
1.2.1	>= 1.0	N/A	>= 1.0	N/A	ECS01b, GCS01b	ECS01b, GCS01b	ECS01b, GCS01b	ECS01b, GCS01b	ECS01b, GCS01b	ECS01b, GCS01b
1.2.2	>= 1.0	N/A	>= 1.0	N/A	ECS01d	ECS01d	ECS01d	ECS01d	ECS01d	ECS01d
1.5	>= 1.0	N/A	>= 1.0	N/A	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d	ECS04a, ECS04b, GCS40a, GCS40b, GCS40c, GCS40d
1.6	>= 1.0	N/A	>= 1.0	N/A	ECS02, ECS03, GCS02, GCS03	ECS02, ECS03, GCS02, GCS03	ECS02, ECS03, GCS02, GCS03	ECS02, ECS03, GCS02, GCS03	ECS02, ECS03, GCS02, GCS03	ECS02, ECS03, GCS02, GCS03
1.7	>= 1.0	N/A	>= 1.0	N/A	ECS05	ECS05	ECS05	ECS05	ECS05	ECS05
2.1	>= 1.0	2.0	>= 1.0	2.0	ECS08, GCS05	**ECS08a**, GCS05	ECS08a, GCS05	ECS08a, GCS05	ECS08a, GCS05	ECS08a, GCS05
2.2	>= 1.0	N/A	>= 1.0	N/A	CS01a, CS01b	CS01a, CS01b	CS01a, CS01b	CS01a, CS01b	CS01a, CS01b	CS01a, CS01b
2.3	>= 1.0	N/A	>= 1.0	N/A	ECS07, GCS04	ECS07, GCS04	ECS07, GCS04	ECS07, GCS04	ECS07, GCS04	ECS07, GCS04
2.5	>= 1.0	N/A	>= 1.0	N/A	ECS09, GCS06	ECS09, GCS06	ECS09, GCS06	ECS09, GCS06	ECS09, GCS06	ECS09, GCS06
3.1	>= 1.0	N/A	>= 1.0	N/A	ECS10, GCS07	ECS10, GCS07	ECS10, GCS07	ECS10, GCS07	ECS10, GCS07	ECS10, GCS07
3.2	>= 1.0	N/A	>= 1.0	N/A	ECS12, GCS09	ECS12, GCS09	ECS12, GCS09	ECS12, GCS09	ECS12, GCS09	ECS12, GCS09
3.3	>= 1.0	N/A	>= 1.0	N/A	ECS15a, ECS15c, CS11	ECS15a, ECS15c, CS11	ECS15a, ECS15c, CS11	ECS15a, ECS15c, CS11	ECS15a, ECS15c, CS11	ECS15a, ECS15c, CS11
3.4	>= 1.0	N/A	>= 1.0	N/A	ECS16, GCS44	ECS16, GCS44	ECS16, GCS44	ECS16, GCS44	ECS16, GCS44	ECS16, GCS44
3.5	>= 1.0	N/A	>= 1.0	N/A	ECS14, GCS11	ECS14, GCS11	ECS14, GCS11	ECS14, GCS11	ECS14, GCS11	ECS14, GCS11
4.1.1	>= 1.0	N/A	>= 1.0	N/A	ECS17b, GCS13a	ECS17b, GCS13a	ECS17b, GCS13a	ECS17b, GCS13a	ECS17b, GCS13a	ECS17b, GCS13a
4.1.2	>= 1.0	N/A	>= 1.0	N/A	ECS17d, GCS13c	ECS17d, GCS13c	ECS17d, GCS13c	ECS17d, GCS13c	ECS17d, GCS13c	ECS17d, GCS13c
4.1.3	>= 1.0	N/A	>= 1.0	N/A	ECS17e	ECS17e	ECS17e	ECS17e	ECS17e	ECS17e

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
4.1.4	>= 1.0	N/A	>= 1.0	N/A	GCS13b	GCS13b	GCS13b	GCS13b	GCS13b	GCS13b
4.2	>= 1.0	N/A	>= 1.0	N/A	ECS17a	ECS17a	ECS17a	ECS17a	ECS17a	ECS17a
4.3	>= 1.0	N/A	>= 1.0	N/A	ECS19, GCS14	ECS19, GCS14	ECS19, GCS14	ECS19, GCS14	ECS19, GCS14	ECS19, GCS14
4.4.2	>= 1.0	N/A	>= 1.0	N/A	ECS20b, GCS15b	ECS20b, GCS15b	ECS20b, GCS15b	ECS20b, GCS15b	ECS20b, GCS15b	ECS20b, GCS15b
4.4.3	>= 1.0	N/A	>= 1.0	N/A	ECS20c, GCS15c	ECS20c, GCS15c	ECS20c, GCS15c	ECS20c, GCS15c	ECS20c, GCS15c	ECS20c, GCS15c
4.4.4	>= 1.0	N/A	>= 1.0	N/A	ECS20a, GCS15d	ECS20a, GCS15d	ECS20a, GCS15d	ECS20a, GCS15d	ECS20a, GCS15d	ECS20a, GCS15d
4.4.5	>= 1.0	N/A	>= 1.0	N/A	ECS20d, GCS15e	ECS20d, GCS15e	ECS20d, GCS15e	ECS20d, GCS15e	ECS20d, GCS15e	ECS20d, GCS15e
4.6.1	>= 1.0	N/A	>= 1.0	N/A	ECS21a, GCS16a	ECS21a, GCS16a	ECS21a, GCS16a	ECS21a, GCS16a	ECS21a, GCS16a	ECS21a, GCS16a
4.6.2	>= 1.0	N/A	>= 1.0	N/A	ECS21c	ECS21c	ECS21c	ECS21c	ECS21c	ECS21c
4.8.1	>= 1.0	N/A	>= 1.0	N/A	ECS22b, GCS17	ECS22b, GCS17	ECS22b, GCS17	ECS22b, GCS17	ECS22b, GCS17	ECS22b, GCS17
4.8.2	>= 1.0	N/A	>= 1.0	N/A	ECS22c	ECS22c	ECS22c	ECS22c	ECS22c	ECS22c
4.8.3	>= 1.0	N/A	>= 1.0	N/A	ECS22a	ECS22a	ECS22a	ECS22a	ECS22a	ECS22a
4.10	>= 1.0	N/A	>= 1.0	N/A	ECS23, ECS23b, GCS18	ECS23, ECS23b, GCS18	ECS23, ECS23b, GCS18	ECS23, ECS23b, GCS18	ECS23, ECS23b, GCS18	ECS23, ECS23b, GCS18
4.11.1	>= 1.0	N/A	>= 1.0	N/A	ECS24, GCS21f	ECS24, GCS21f	ECS24, GCS21f	ECS24, GCS21f	ECS24, GCS21f	ECS24, GCS21f
4.11.2	>= 1.0	N/A	>= 1.0	N/A	ECS24b	ECS24b	ECS24b	ECS24b	ECS24b	ECS24b
4.12.1	>= 1.0	N/A	>= 1.0	N/A	ECS18b	ECS18b	ECS18b	ECS18b	ECS18b	ECS18b
4.12.2	>= 1.0	N/A	>= 1.0	N/A	ECS18a	ECS18a	ECS18a	ECS18a	ECS18a	ECS18a
4.13	>= 1.0	N/A	>= 1.0	N/A	ECS26a, GCS21b	ECS26a, GCS21b	ECS26a, GCS21b	ECS26a, GCS21b	ECS26a, GCS21b	ECS26a, GCS21b
4.14	>= 1.0	N/A	>= 1.0	N/A	ECS21b, GCS16b	ECS21b, GCS16b	ECS21b, GCS16b	ECS21b, GCS16b	ECS21b, GCS16b	ECS21b, GCS16b
4.15	>= 1.0	N/A	>= 1.0	N/A	ECS27	ECS27	ECS27	ECS27	ECS27	ECS27
4.16	>= 1.0	N/A	>= 1.0	N/A	ECS17c	ECS17c	ECS17c	ECS17c	ECS17c	ECS17c
4.17	>= 1.0	N/A	>= 1.0	N/A	ECS66, GCS61	ECS66, GCS61	ECS66, GCS61	ECS66, GCS61	ECS66, GCS61	ECS66, GCS61
4.18	>= 1.0	N/A	>= 1.0	N/A	ECS82, GCS60	ECS82, GCS60	ECS82, GCS60	ECS82, GCS60	ECS82, GCS60	ECS82, GCS60a
5.1	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5.2	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5.3	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
6.2.1	>= 1.0	N/A	>= 1.0	N/A	ECS26b, ECS26k	ECS26b, ECS26k	ECS26b, ECS26k	ECS26b, ECS26k	ECS26b, ECS26k	ECS26b, ECS26k
6.2.2	>= 1.0	N/A	>= 1.0	N/A	ECS26c	ECS26c	ECS26c	ECS26c	ECS26c	ECS26c
6.2.3	>= 1.0	2.0	>= 1.0	2.0	ECS26d, GCS21d	**ECS26l, GCS21k**	ECS26l, GCS21k	ECS26l, GCS21k	ECS26l, GCS21k	ECS26l, GCS21k
6.2.4	>= 1.0	2.0	>= 1.0	2.0	ECS26e, ECS26i, GCS21e	**ECS26m, ECS26n, GCS21m**	ECS26m, ECS26n, GCS21m	ECS26m, ECS26n, GCS21m	ECS26m, ECS26n, GCS21m	ECS26m, ECS26n, GCS21m
6.2.5	>= 1.0	N/A	>= 1.0	N/A	ECS26f	ECS26f	ECS26f	ECS26f	ECS26f	ECS26f
6.2.7	>= 1.0	N/A	>= 1.0	N/A	ECS40, GCS46	ECS40, GCS46	ECS40, GCS46	ECS40, GCS46	ECS40, GCS46	ECS40, GCS46
6.2.8	>= 1.0	N/A	>= 1.0	N/A	GCS21a	GCS21a	GCS21a	GCS21a	GCS21a	GCS21a
6.2.9	>= 1.0	N/A	>= 1.0	N/A	ECS26j, GCS21j	ECS26j, GCS21j	ECS26j, GCS21j	ECS26j, GCS21j	ECS26j, GCS21j	ECS26j, GCS21j
6.2.10	>= 2.0	2.0	>= 2.0	2.0	N/A	**ECS25r1, ECS25r2, GCS20r**	ECS25r1, ECS25r2, GCS20r	ECS25r1, ECS25r2, GCS20r	ECS25r1, ECS25r2, GCS20r	ECS25r1, ECS25r2, GCS20r
6.4.1	>= 1.0	N/A	>= 1.0	N/A	ECS28a	ECS28a	ECS28a	ECS28a	ECS28a	ECS28a
6.4.2	>= 1.0	N/A	>= 1.0	N/A	ECS28b	ECS28b	ECS28b	ECS28b	ECS28b	ECS28b
6.5	>= 1.0	2.0	>= 1.0	2.0	ECS29a, ECS29b	ECS29a, ECS29b, **ECS29c, ECS29d**	ECS29a, ECS29b, ECS29c, ECS29d	ECS29a, ECS29b, ECS29c, ECS29d	ECS29a, ECS29b, ECS29c, ECS29d	ECS29a, ECS29b, ECS29c, ECS29d
6.6	>= 1.0	N/A	>= 1.0	N/A	GCS23	GCS23	GCS23	GCS23	GCS23	GCS23
6.7	>= 1.0	3.1	>= 1.0	N/A	GCS24	GCS24	**GCS24a**	GCS24a	GCS24a	GCS24a
6.8	>= 1.0	2.0	>= 1.0	2.0	ECS30, GCS25	**ECS30a, GCS25a**	ECS30a, GCS25a	ECS30a, GCS25a	ECS30a, GCS25a	ECS30a, GCS25a
6.11	>= 1.0	N/A	>= 1.0	N/A	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28
6.12	>= 1.0	N/A	>= 1.0	N/A	ECS34	ECS34	ECS34	ECS34	ECS34	ECS34
6.13	>= 1.0	3.1	>= 1.0	4.0	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, ECS35f, CS10a, CS10b	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, ECS35f, CS10a, CS10b	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, **ECS35g**, CS10a, CS10b	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, **ECS35g**, CS10a, CS10b	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, ECS35g, CS10a, CS10b	ECS35a, ECS35b, ECS35c, ECS35d, ECS35e, ECS35g, CS10a, CS10b
6.14.1	>= 1.0	N/A	>= 1.0	N/A	ECS46a	ECS46a	ECS46a	ECS46a	ECS46a	ECS46a
6.14.2	>= 1.0	N/A	>= 1.0	N/A	ECS46c	ECS46c	ECS46c	N/A	N/A	N/A
6.14.3	>= 4.0	N/A	>= 4.0	N/A	N/A	N/A	N/A	ECS46d	ECS46d	ECS46d
6.15.1	>= 1.0	4.0	>= 1.0	2.0, 4.0	CS02b	CS02b	CS02b	CS02b **CS02g**	CS02b CS02g	CS02b CS02g

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
6.15.2	>= 1.0	N/A	>= 1.0	N/A	CS02d	CS02d	CS02d	CS02d	CS02d	CS02d
6.17	>= 1.0	N/A	>= 1.0	N/A	CS02c	CS02c	CS02c	CS02c	CS02c	CS02c
6.18.1	>= 1.0	N/A	>= 1.0	N/A	ECS37	ECS37	ECS37	ECS37	ECS37	ECS37
6.18.2	>= 1.0	N/A	>= 1.0	N/A	ECS57	ECS57	ECS57	ECS57	ECS57	ECS57
6.20.1	>= 1.0	N/A	>= 1.0	N/A	ECS39a, GCS41	ECS39a, GCS41	ECS39a, GCS41	ECS39a, GCS41	ECS39a, GCS41	ECS39a, GCS41
6.20.2	>= 1.0	N/A	>= 1.0	N/A	ECS39b	ECS39b	ECS39b	ECS39b	ECS39b	ECS39b
6.21	>= 1.0	N/A	>= 1.0	2.0	CS02b	CS02b	CS02b	CS02b	CS02b	CS02b
6.22	>= 1.0	2.0	>= 1.0	2.0	ECS25a, ECS25b, GCS20 (WAN Alerts only)	ECS25a, ECS25b, GCS20 (WAN Alerts only), **ECS25a1, ECS25a2, ECS25a3, ECS25b3, GCS20**	ECS25a, ECS25b, GCS20 (WAN Alerts only), ECS25a1, ECS25a2, ECS25a3, ECS25b3, GCS20	ECS25a, ECS25b, GCS20 (WAN Alerts only), ECS25a1, ECS25a2, ECS25a3, ECS25b3, GCS20	ECS25a, ECS25b, GCS20 (WAN Alerts only), ECS25a1, ECS25a2, ECS25a3, ECS25b3, GCS20	ECS25a, ECS25b, GCS20 (WAN Alerts only), ECS25a1, ECS25a2, ECS25a3, ECS25b3, GCS20
6.23	>= 1.0	N/A	>= 1.0	2.0	CS02b	CS02b	CS02b	CS02b	CS02b	CS02b
6.24.1	>= 1.0	4.0	>= 1.0	4.0	CS02a	CS02a	CS02a	CS02a **CS02f**	CS02a CS02f	CS02a CS02f
6.24.2	>= 1.0	N/A	>= 1.0	N/A	CS02e	CS02e	CS02e	CS02e	CS02e	CS02e
6.25	>= 1.0	N/A	>= 1.0	N/A	ECS81	ECS81	ECS81	ECS81	ECS81	ECS81
6.26	>= 2.0	2.0	>= 2.0	2.0	N/A	**ECS48**	ECS48	ECS48	ECS48	ECS48
6.27	>= 2.0	2.0	>= 2.0	2.0	N/A	**ECS29e, ECS29f**	ECS29e, ECS29f	ECS29e, ECS29f	ECS29e, ECS29f	ECS29e, ECS29f
6.28	>= 2.0	2.0	>= 2.0	2.0	N/A	**DBCH04**	DBCH04	DBCH04	DBCH04	DBCH04
6.29	>= 2.0	2.0	>= 2.0	2.0	N/A	**DBCH05**	DBCH05	DBCH05	DBCH05	DBCH05
6.30	>= 2.0	2.0	>= 2.0	2.0	N/A	**DBCH03**	DBCH03	DBCH03	DBCH03	DBCH03
6.31	>= 2.0	2.0	>= 2.0	2.0	N/A	**DBCH01**	DBCH01	DBCH01	DBCH01	DBCH01
6.32	>= 2.0	2.0	>= 2.0	2.0	N/A	**DBCH02**	DBCH02	DBCH02	DBCH02	DBCH02
7.1	>= 1.0	N/A	>= 1.0	N/A	ECS42	ECS42	ECS42	ECS42	ECS42	ECS42
7.2	>= 1.0	N/A	>= 1.0	N/A	ECS43, GCS32	ECS43, GCS32	ECS43, GCS32	ECS43, GCS32	ECS43, GCS32	ECS43, GCS32
7.3	>= 1.0	N/A	>= 1.0	N/A	ECS44, GCS39	ECS44, GCS39	ECS44, GCS39	ECS44, GCS39	ECS44, GCS39	ECS44, GCS39
7.4	>= 1.0	N/A	>= 1.0	N/A	ECS45, GCS33	ECS45, GCS33	ECS45, GCS33	ECS45, GCS33	ECS45, GCS33	ECS45, GCS33
7.5	>= 1.0	N/A	>= 1.0	N/A	ECS47	ECS47	ECS47	N/A	N/A	N/A

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
7.6	>= 1.0	N/A	>= 1.0	N/A	ECS47	ECS47	ECS47	N/A	N/A	N/A
7.7	>= 1.0	N/A	>= 1.0	N/A	ECS61a	ECS61a	ECS61a	N/A	N/A	N/A
7.8	>= 1.0	N/A	>= 1.0	N/A	ECS47	ECS47	ECS47	N/A	N/A	N/A
7.9	>= 1.0	N/A	>= 1.0	N/A	ECS62	ECS62	ECS62	ECS62	ECS62	ECS62
7.10	>= 1.0	N/A	>= 1.0	N/A	ECS62	ECS62	ECS62	ECS62	ECS62	ECS62
7.11	>= 1.0	N/A	>= 1.0	N/A	ECS61c	ECS61c	ECS61c	ECS61c	ECS61c	ECS61c
7.12	>= 1.0	N/A	>= 1.0	N/A	ECS38	ECS38	ECS38	ECS38	ECS38	ECS38
7.13	>= 4.0	N/A	>= 4.0	N/A	N/A	N/A	N/A	ECS47a	ECS47a	ECS47a
7.14	>= 4.0	N/A	>= 4.0	N/A	N/A	N/A	N/A	ECS61d	ECS61d	ECS61d
7.15	>= 4.0	N/A	>= 4.0	N/A	N/A	N/A	N/A	ECS61e	ECS61e	ECS61e
7.16	>= 4.0	N/A	>= 4.0	N/A	N/A	N/A	N/A	ECS47e	ECS47e	ECS47e
8.1.1	>= 1.0	N/A	>= 1.0	N/A	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28	ECS70, GCS28
8.2	>= 1.0	2.0 (Response only)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.3	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.4	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.5	>= 1.0	N/A	>= 1.0	2.0	CS02b	CS02b	CS02b	CS02b	CS02b	CS02b
8.6	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.7.1	>= 1.0	N/A	>= 1.0	N/A	CS03a1, CS03a2, CS03c	CS03a1, CS03a2, CS03c	CS03a1, CS03a2, CS03c	CS03a1, CS03a2, CS03c	CS03a1, CS03a2, CS03c	CS03a1, CS03a2, CS03c
8.7.2	>= 1.0	N/A	>= 1.0	N/A	CS03a2, CS03b, CS03c	CS03a2, CS03b, CS03c	CS03a2, CS03b, CS03c	CS03a2, CS03b, CS03c	CS03a2, CS03b, CS03c	CS03a2, CS03b, CS03c
8.8.1	>= 1.0	N/A	>= 1.0	N/A	CS04ac	CS04ac	CS04ac	CS04ac	CS04ac	CS04ac
8.8.2	>= 1.0	N/A	>= 1.0	N/A	CS04ac, CS04b	CS04ac, CS04b	CS04ac, CS04b	CS04ac, CS04b	CS04ac, CS04b	CS04ac, CS04b
8.9	>= 1.0	2.0	>= 1.0	2.0	CCS05/CCS04, CS07	**CCS06**, CS07	CCS06, CS07	CCS06, CS07	CCS06, CS07	CCS06, CS07
8.11	>= 1.0	N/A	>= 1.0	N/A	CCS01, CCS02	CCS01, CCS02	CCS01, CCS02	CCS01, CCS02	CCS01, CCS02	CCS01, CCS02
8.12.1	>= 1.0	N/A	>= 1.0	N/A	CCS03	CCS03	CCS03	CCS03	CCS03	CCS03
8.12.2	>= 1.0	N/A	>= 1.0	N/A	GCS59	GCS59	GCS59	GCS59	GCS59	GCS59
8.13	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.14.1	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Service Request Variant					GBCS Use Cases					
ID	DUIS XSD version	Modified in DUIS versions	MMC XSD version	Modified in MMC versions	GBCS version 1.0/1.1	GBCS version 2.0/2.1	GBCS version 3.2/3.3	GBCS version 4.0	GBCS version 4.1	GBCS version 4.2
8.14.2	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.14.3	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8.14.4	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9.1	>= 1.0	N/A	>= 1.0	N/A	ECS50, GCS36	ECS50, GCS36	ECS50, GCS36	ECS50, GCS36	ECS50, GCS36	ECS50, GCS36
11.1	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11.2	>= 1.0	N/A	>= 1.0	N/A	ECS52, GCS38	ECS52, GCS38	ECS52, GCS38	ECS52, GCS38	ECS52, GCS38, **CS08**	ECS52, GCS38, **CS08**
11.3	>= 1.0	N/A	>= 1.0	N/A	CS06	CS06	CS06	CS06	CS06	CS06
11.4	>= 5.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12.1	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12.2	>= 1.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14.1	>= 1.0	N/A	>= 1.0	2.0 (doc only)	GCS31	GCS31	GCS31	GCS31	GCS31	GCS31

Table 59 Service Request Variant mapping to GBCS UC – Mapping Versioning

Appendix 11 – Use of Multiple EUI64 IDs

In accordance with the requirements of SEC Clause H1.5, a Service User may use more than one EUI64 ID for a given SEC Party and Role combination.

A Service User may use any of their EUI64 IDs to communicate over the DCC User Interface, provided that EUI64 ID has been notified to the DCC for use for this purpose and that the Service User has completed all the necessary steps (in particular those relating to security) that are required in order to use that EUI64 ID.

Where a Service User has more than one EUI64 ID. the behaviour of the DCC Data Systems with respect to Registration data will depend on how those EUI64 IDs are mapped to Market Participant IDs. There are two possible scenarios as outlined below.

DCC Service User

SEC Party ID	SEC Role	User ID
SEC001	EIS	1234
SEC001	EIS	2345

Party Participant Role Mapping

User ID	Energy Participant Code	Energy Role Code
1234	MPIDA	X
2345	MPIDB	X

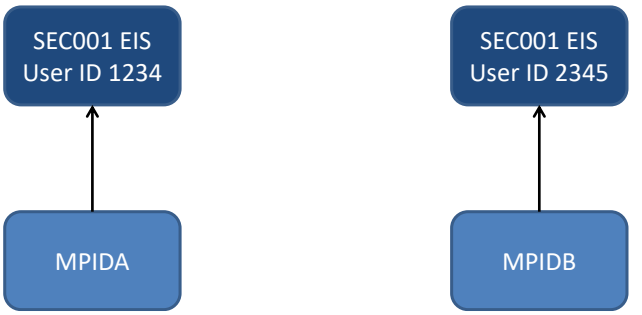


Figure 84 – EUI64 IDs mapped to different MPIDs

DCC Service User

SEC Party ID	SEC Role	User ID
SEC001	EIS	1234
SEC001	EIS	2345

Party Participant Role Mapping

User ID	Energy Participant Code	Energy Role Code
1234	MPIDA	X
2345	MPIDA	X

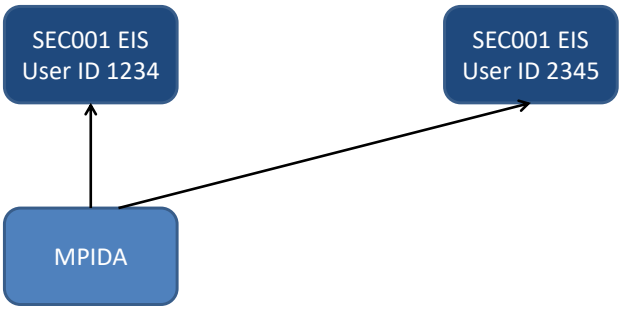


Figure 85 – EUI64 IDs mapped to same MPID

In the first scenario, the two User IDs operate independently and the relevant User ID must be used in order to pass any Registration Data checks associated with MPIDA or MPIDB.

In the second scenario, either User ID will pass the Registration Data checks associated with MPIDA however the Service User is responsible for ensuring they use the correct User ID that is associated with the SMKI security credentials held on the target device. If the wrong User ID is used then the GBCS Command will be rejected by the device.

Additionally, where Registration Data is used to determine a Responsible or Interested Party in order to deliver DCC Alerts then if an MPID maps to more than one User ID then the DCC Data Systems shall use its knowledge of which SMKI security credentials are held on the device in order to determine which User ID should be used. Where this cannot be done then the User ID that was notified first to the DCC for that MPID will be used.

Appendix 12 – Firmware Version Alerts

Support for multiple versions of GBCS relies on Firmware Version information in the Smart Metering Inventory (SMI) being accurate. With this in mind, the DCC Data Systems will monitor all Read Firmware Service Requests (see Annex 11) and will update the details held in the Smart Metering Inventory if this is necessary.

The following diagrams describe the logic for determining whether an update should be made and which DCC Alert is generated (see section 13).

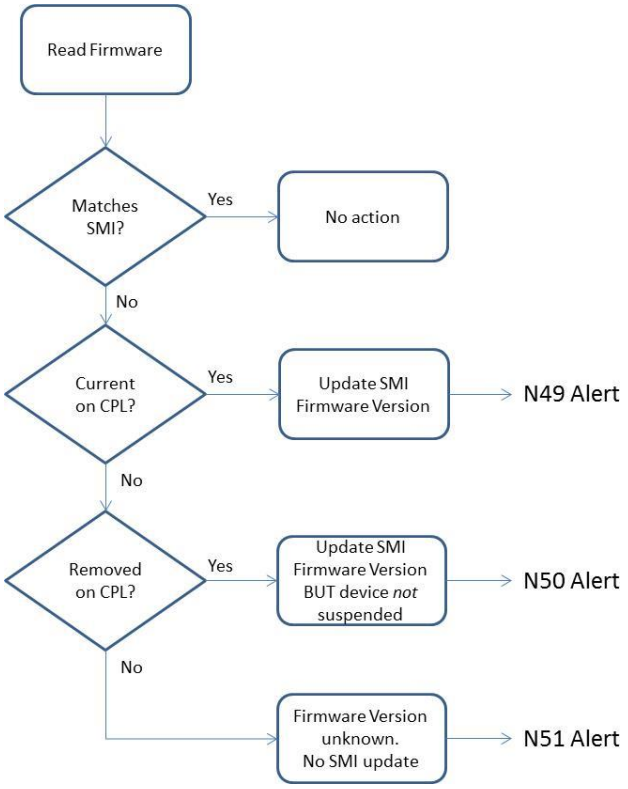


Figure 86 – Read Firmware (ESME, GSME, CHF, HCALCS, PPMID)

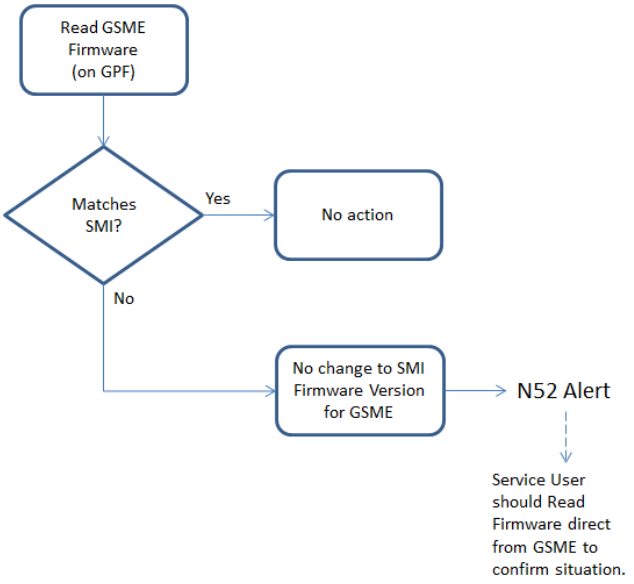


Figure 87 – Read GSME Firmware (on GPF)

Appendix 13 – Non-Critical Configurable Events / Alerts

The following tables summarise the non-critical Events / Alerts that are configurable by the Supplier on the ESME or GSME (Event / Alert Code in the 0x81 range) or by the Network Operator (Event / Alert Code in the 0x80 range) via Service Request 6.22 (Configure Alert Behaviour) – See Annex 6. See GBCS v2.0 Draft 5 section 16.2 for master data.

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
0x810D	Combined Credit Below Low Credit Threshold (prepayment mode)	x	x			
0x810E	Credit Added Locally	x	x			
0x8119	Emergency Credit Has Become Available (prepayment mode)	x	x			
0x8145	Clock adjusted (within tolerance)	x	x			
0x8154	Immediate HAN Interface Command Received and Successfully Actioned	x	x			
0x8155	Immediate HAN Interface Command Received but not Successfully Actioned	x	x			
0x8161	User Interface Command Input and Successfully Actioned	x	x			
0x8162	User Interface Command Input but not Successfully Actioned	x	x			
0x8168	Supply Disabled then Armed - Activate Emergency Credit triggered	x	x			
0x8183	Device joined SMHAN	x	x			
0x8184	Valve tested	x				
0x81A1	Battery Cover Closed	x	x			
0x81A2	CH Connected to ESME		x			
0x81A3	CH Disconnected from ESME		x			
0x81A4	Close Tunnel Command Rejected	x	x			
0x81A5	Communication From Local Port (e.g. Optical)	x	x			
0x81A6	Customer Acknowledged Message on HAN Device	x	x			
0x81A7	Debt Collection Completed - Time Debt 1	x	x			
0x81A8	Debt Collection Completed - Time Debt 2	x	x			
0x81A9	Debt Collection Completed - Payment Debt	x	x			
0x81AA	Emergency Credit Exhausted	x	x			
0x81AB	Emergency Credit Activated	x	x			
0x81AC	Error Measurement Fault	x	x			

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
0x81AD	Error Metrology Firmware Verification Failure	x	x			
0x81AE	Error Non Volatile Memory	x	x			
0x81AF	Error Program Execution	x	x			
0x81B0	Error Program Storage	x	x			
0x81B1	Error RAM	x	x			
0x81B2	Error Unexpected Hardware Reset	x	x			
0x81B3	Error Watchdog	x	x			
0x81B4	Excess Gas Flow Beyond Meter Capacity	x				
0x81B5	Flow Sensor Detects Air in Gas Flow	x				
0x81B6	Flow Sensor Detects Reverse Flow of Gas	x				
0x81B7	Incorrect phase sequencing				x	
0x81B8	Incorrect Polarity		x			
0x81B9	Meter Cover Closed	x	x			
0x81BA	Request Tunnel Command Rejected	x	x			
0x81BB	Reverse Current		x			
0x81BC	Strong Magnetic Field Removed	x	x			
0x81BD	Supply Connect Failure (Valve or Load Switch)	x	x			
0x81BE	Supply Disabled Then Locked - Supply Tamper State Cause	x	x			
0x81BF	Supply Disabled Then Armed - Uncontrolled Gas Flow Rate	x				
0x81C0	Supply Disconnect Failure (Valve or Load Switch)	x	x			
0x81C1	Terminal Cover Closed		x			
0x81C2	Tilt Tamper Ended	x				
0x81C3	Tilt Tamper	x				
0x81C4	UTRN Manual Entry Suspended	x	x			
0x81C5	UTRN rejected as locked out	x	x			
0x81A0	Smart Meter Integrity Issue – Warning	x	x			

Table 60 Non-critical Events / Alerts configurable by the Supplier

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
0x8002	Average RMS Voltage above Average RMS Over Voltage Threshold (current value above threshold; previous value below threshold)			x		
0x8003	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 1 (current value above threshold; previous value below threshold)				x	
0x8004	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 2 (current value above threshold; previous value below threshold)				x	
0x8005	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 3 (current value above threshold; previous value below threshold)				x	
0x8006	Average RMS Voltage below Average RMS Under Voltage Threshold (current value below threshold; previous value above threshold)			x		
0x8007	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 1 (current value below threshold; previous value above threshold)				x	
0x8008	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 2 (current value below threshold; previous value above threshold)				x	
0x8009	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 3 (current value below threshold; previous value above threshold)				x	
0x8020	RMS Voltage above Extreme Over Voltage Threshold (voltage rises above for longer than the configurable period)			x		
0x8021	RMS Voltage above Extreme Over Voltage Threshold on Phase 1 (voltage rises above for longer than the configurable period)				x	
0x8022	RMS Voltage above Extreme Over Voltage Threshold on Phase 2 (voltage rises above for longer than the configurable period)				x	
0x8023	RMS Voltage above Extreme Over Voltage Threshold on Phase 3				x	

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
	(voltage rises above for longer than the configurable period)					
0x8024	RMS Voltage above Voltage Swell Threshold (voltage rises above for longer than the configurable period)			x		
0x8025	RMS Voltage above Voltage Swell Threshold on Phase 1 (voltage rises above for longer than the configurable period)				x	
0x8026	RMS Voltage above Voltage Swell Threshold on Phase 2 (voltage rises above for longer than the configurable period)				x	
0x8027	RMS Voltage above Voltage Swell Threshold on Phase 3 (voltage rises above for longer than the configurable period)				x	
0x8028	RMS Voltage below Extreme Under Voltage Threshold (voltage falls below for longer than the configurable period)			x		
0x8029	RMS Voltage below Extreme Under Voltage Threshold on Phase 1 (voltage falls below for longer than the configurable period)				x	
0x802A	RMS Voltage below Extreme Under Voltage Threshold on Phase 2 (voltage falls below for longer than the configurable period)				x	
0x802B	RMS Voltage below Extreme Under Voltage Threshold on Phase 3 (voltage falls below for longer than the configurable period)				x	
0x802C	RMS Voltage below Voltage Sag Threshold (voltage falls below for longer than the configurable period)			x		
0x802D	RMS Voltage below Voltage Sag Threshold on Phase 1 (voltage falls below for longer than the configurable period)				x	
0x802E	RMS Voltage below Voltage Sag Threshold on Phase 2 (voltage falls below for longer than the configurable period)				x	
0x802F	RMS Voltage below Voltage Sag Threshold on Phase 3 (voltage falls below for longer than the configurable period)				x	
0x8085	Average RMS Voltage below Average RMS Over Voltage Threshold (current value below threshold; previous value above threshold)			x		

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
0x8086	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 1 (current value below threshold; previous value above threshold)				x	
0x8087	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 2 (current value below threshold; previous value above threshold)				x	
0x8088	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 3 (current value below threshold; previous value above threshold)				x	
0x8089	Average RMS Voltage above Average RMS Under Voltage Threshold (current value above threshold; previous value below threshold)			x		
0x808A	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 1 (current value above threshold; previous value below threshold)				x	
0x808B	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 2 (current value above threshold; previous value below threshold)				x	
0x808C	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 3 (current value above threshold; previous value below threshold)				x	
0x808D	RMS Voltage above Extreme Over Voltage Threshold (voltage returns below for longer than the configurable period)			x		
0x808E	RMS Voltage above Extreme Over Voltage Threshold on Phase 1 (voltage returns below for longer than the configurable period)				x	
0x808F	RMS Voltage above Extreme Over Voltage Threshold on Phase 2 (voltage returns below for longer than the configurable period)				x	
0x8090	RMS Voltage above Extreme Over Voltage Threshold on Phase 3 (voltage returns below for longer than the configurable period)				x	
0x8091	RMS Voltage above Voltage Swell Threshold (voltage returns below for longer than the configurable period)			x		

Event / Alert Code	Alert Name	GSME	ESME (All)	ESME (excl multi-phase)	ESME (multi-phase only)	ESME (twin element only)
0x8092	RMS Voltage above Voltage Swell Threshold on Phase 1 (voltage returns below for longer than the configurable period)				x	
0x8093	RMS Voltage above Voltage Swell Threshold on Phase 2 (voltage returns below for longer than the configurable period)				x	
0x8094	RMS Voltage above Voltage Swell Threshold on Phase 3 (voltage returns below for longer than the configurable period)				x	
0x8095	RMS Voltage below Extreme Under Voltage Threshold (voltage returns above for longer than the configurable period)			x		
0x8096	RMS Voltage below Extreme Under Voltage Threshold on Phase 1 (voltage returns above for longer than the configurable period)				x	
0x8097	RMS Voltage below Extreme Under Voltage Threshold on Phase 2 (voltage returns above for longer than the configurable period)				x	
0x8098	RMS Voltage below Extreme Under Voltage Threshold on Phase 3 (voltage returns above for longer than the configurable period)				x	
0x8099	RMS Voltage below Voltage Sag Threshold (voltage returns above for longer than the configurable period)			x		
0x809A	RMS Voltage below Voltage Sag Threshold on Phase 1 (voltage returns above for longer than the configurable period)				x	
0x809B	RMS Voltage below Voltage Sag Threshold on Phase 2 (voltage returns above for longer than the configurable period)				x	
0x809C	RMS Voltage below Voltage Sag Threshold on Phase 3 (voltage returns above for longer than the configurable period)				x	
0x8010	Over Current			x		
0x8011	Over Current L1				x	
0x8016	Over Current L2				x	
0x8013	Over Current L3				x	
0x8014	Power Factor Threshold Below		x			
0x8015	Power Factor Threshold Ok		x			

Table 61 Non-critical Events / Alerts configurable by the Network Operator

Appendix 14 – Combined Supplier User Role

Where a DCC Service User notifies the DCC that it is using the same unique identifier (DCC Service User ID) for all three supplier roles (EIS, EES, GIS) then the DCC Data Systems shall record this single DCC Service User ID within the DCC database DCC_SERVICE_USER entity against a role identified as Combined Supplier (CS).

For the purposes of Role Based Access Control (RBAC), this Combined Supplier role will allow the DCC Service User to access any Service Request which is applicable to any one of the constituent supplier roles (EIS, EES or GIS) as defined in section 9.4.

So, for example, a DCC Service User identified as using the Combined Supplier Role will have access to, amongst others, all of the following Service requests:

- SR 4.6.1 Retrieve Import Daily Read Log (accessible to EIS and GIS)
- SR4.6.2 Retrieve Export Daily Read Log (accessible to EES)
- SR6.2.1 Read Device Configuration Voltage (accessible to EIS)
- SR6.2.8 Read Device Configuration Gas (accessible to GIS)

For avoidance of doubt, subsequent to any RBAC checks on Service Requests the DCC Data Systems will, where applicable as defined in section 7.4, carry out a check based on Registration data to confirm that the DCC Service User is a Registered Supplier for the Device being communicated with.

Appendix 15 – Firmware Distribution Tracking State Diagram

The diagram below illustrates the possible states for tracking of a Firmware Distribution to a device. Firmware Distribution Tracking is introduced in DUIS 5.0. See Table 3.1 in section 2.3.10 for state definitions.

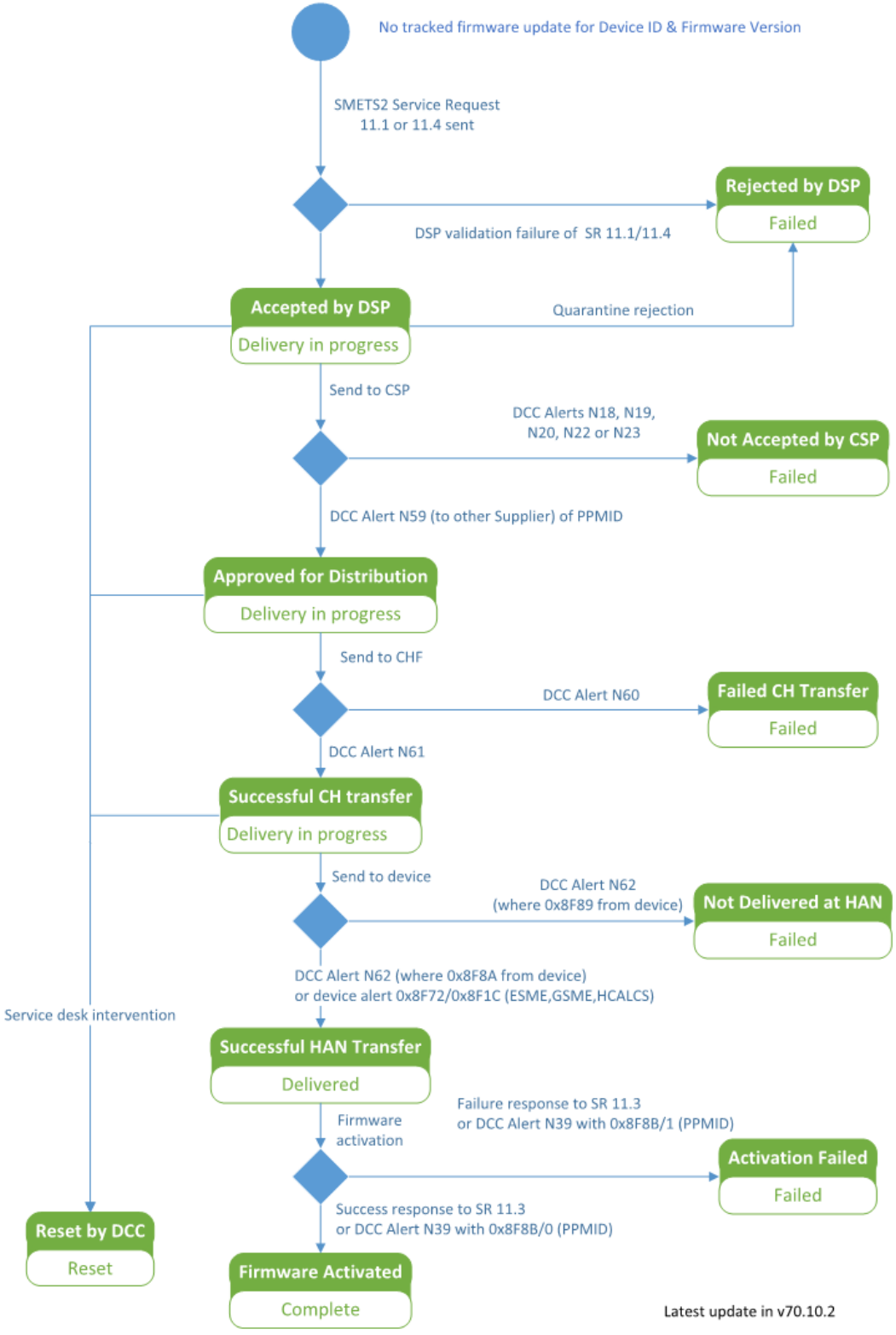


Figure 88 Firmware distribution tracking state diagram

Appendix 16 – Changes for the ECoS Service

The scope of the June 2022 release originally included changes made for the Enduring Change of Supplier (ECoS) service, including additional validation steps and new and updated DCC Alert definitions.

Due to replanning, the ECoS service wasis not longer part of the June 2022 release; however, it has beenwas decided that some of the new features would be made available as part of the June 2022 release, but others had to be postponed. Details of the impact of changes are described in a DUIS release guidance document which has been shared with the industry, and is embedded below for convenience.

Release Guidance Notes -DUIS v5.1 - F

The ECoS service is implemented as part of the June 2023 SEC Release.

Appendix 17 – Permitted Activities with Suspended Devices

Where a Device Model / Firmware Version is marked as Removed on the Central Products List (CPL), meaning that it is no longer valid for use via DCC, many operations for affected Devices are restricted by DCC.

Where a Device has a Device Model / Firmware Version associated with the Removed CPL entry, DCC will change the Device Status to Suspended.

The following table provides guidance on restrictions on Service Users for Devices where the Device Status is Suspended.

There is also information in this document regarding Device Status Suspended in footnote 3 in section 7.4 Table 14~~Table 14~~, and in the Device lifecycle diagrams in Appendix 8.

	Device Status at point of Firmware CPL suspension	OTA Firmware update permitted?	Notes
1	Not yet pre-notified	No	Cannot be pre-notified. SRV 12.2 will fail the CPL check, and error code "E120203" will be returned to Service User
2	Pending (already pre-notified)	No	Cannot be whitelisted. SRV 8.11 will fail the status validation, and error code "E081105" will be returned to Service User
3	"InstalledNotCommissioned" but ACB certificates in the Device for SMETS2 Devices (SMETS1 equivalent: Supplier certificates not associated with the Device)	No	Cannot allocate Supplier certificates to the Device because SRV 6.21 will fail the E5 validation for a non-Critical command
4	"InstalledNotCommissioned" and supplier certificates in the Device for SMETS2 Devices (SMETS1 equivalent: Supplier certificates have been associated with the Device)	Yes	Will be able to commission with SRV 8.1.1, and then follow with SRV 11.1 and SRV 11.3 for OTA Firmware update
5	Commissioned	Yes	Will be able to issue SRV 11.1, SRV 11.3 for OTA and SRV 6.23 for Change of Supplier.

Table 62 Permitted Activities for Suspended Devices

Revision History

Revision Date	Summary of Changes	Version
22/11/2013	Initial Draft for Internal Review	0.1
29/11/2013	Draft for Review	0.2
18/12/2013	Draft for Review	0.3
23/12/2013	Draft for Review	0.4
07/01/2014	Published for Service User consultation	0.5
28/02/2014	Consultation response. DCC assured product.	0.6
27/06/2014	Interim updates to support GBCS proving and DCC design activities. DCC internal version.	0.7
12/09/2014	Updated to align to GBCS v0.8	0.8
03/10/2014	Updated to include changes to Service Requests 5.1 – 5.3 and addition of Service Requests 8.14.1 – 8.14.4	0.8 rev 1
10/12/2014	Updated to include corrections and clarifications to version 0.8	0.8 rev A
06/03/2015	Updated to align to GBCS v0.8.1	0.8.1
27/03/2015	Updated to align to DUIS v0.8.1	0.8.1a
29/05/2015	Updated to align to DUIS Consultation response	0.8.1b
28/08/2015	Updated to align to DUIS Consultation response	0.8.1c
11/11/2015	Updated to align to GBCS 0.8.1 plus IRPs in Appendix 9 GBCS IRPs in scope	0.8.2
26/02/2016	Aligned to DCC Release 1.3	0.8.2.1
30/06/2016	Aligned to DCC Release 1.3.1	0.8.2.2
01/02/2017	Aligned to GBCS v2.0 Draft 2	2.0
19/05/2017	Aligned to GBCS v2.0 Draft 5	2.0b
30/06/2017	Aligned to DUIS and MMC v2.0 draft 2	2.0c
09/03/2018	Aligned to DUIS v2.0d	2.0d
31/01/2019	Included information from DCC DUIS guidance documents, clarifications to include information for users of DUIS 1 as well as DUIS 2 in order to make an operational DUGIDS covering all live versions of DUIS, and some corrections to descriptions of behaviour	2.0e
26/01/2018	Updated to include SMETS1 support	3.0a
16/03/2018	Updated to align to updated DUIS 3.0 and related SEC documents	3.0b
18/12/2018	Updated to align to TMAD v0.2	3.0b
17/05/2019	Updated to align to “operational DUGIDS” principles including changes from v2.0e.	3.0c
16/08/2019	Updated for DUIS v3.1a	3.1a

April 2020	Updated for internal DUIS v3.1b baseline. Only this document and Annexes 11 and 16 have been uplifted to DUGIDS v3.1b, and the DUGIDS v3.1a versions remain valid for the rest of the DUGIDS document set, including the XML schemas.	3.1b
April 2020	Updated for DUIS v4.0, including support for Auxiliary Proportional Controllers.	4.0a
November 2020	Update regarding schema versions applicable to SMETS1 Response and Alerts. Clarifications in Annexes 4 and 8. Updated for publication as operational DUGIDS.	4.0b
May 2021	Updated for DUIS v5.0, including support for firmware distribution to SMETS2 PPMIDs and HCALCS	5.0a
November 2021	Inclusion of DUIS guidance items. Published as operational DUGIDS.	5.0
June 2022	Updated for June 2022 SEC release alignment, including DUIS 5.1. This version of DUGIDS documents changes for Enduring Change of Supplier (ECoS), but the implementation is subject to limitations as noted in Appendix 16 – Changes for the ECoS Service~~Appendix 16 – Changes for the ECoS Service~~.	5.1a
November 2022	Update for November 22 SEC release alignment including MMC v5.1, GBCS v3.3 and GBCS v4.2, and guidance introduced based on items from the DCC Guidance Use of DUIS document.	5.1b
June 2023	June 2023 release changes include SEC modifications MP102, MP125 and MP220. This version corresponds to the full implementation of the ECoS programme, and includes further information about ECoS in addition to the information provided in advance in v5.1a. Guidance introduced based on items from the DCC Guidance Use of DUIS document.	5.2a