

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP260 ‘June 2024 SEC Release housekeeping’ Legal text – version 1.0

About this document

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

SEC Section A – Definitions and Interpretations

These changes have been redlined against SEC Section A version 37.0

Amend definition of 'SM WAN' as follows:

SM WAN Smart Metering Wide Area Network (SM WAN) means the SMETS1 SM WAN or the SMETS2+ SM WAN

SEC Section F – Smart Metering System Requirements

These changes have been redlined against SEC Section F version 16.0

Amend Section ‘Annex to Section F4’ (after F4.17) as follows:

Annex to Section F4 - Dual Band Communications Hub Configuration Tables

Each data item in the first column is to be configured in accordance with third column.

Where Pages are used, at least two channels must be configured per Page.

SEC Section G – Security

These changes have been redlined against SEC Section G version 21.0

Amend SEC Section G3. SYSTEM SECURITY: OBLIGATIONS ON USERS as follows:

Security Incident Management

- G3.4 Each User shall ensure that, on the detection of any unauthorised event of the type referred to at Sections G3.1 to G3.3, it takes all of the steps required by its User Information Security Management System.
- G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, ensure that the DCC, the Panel and the Security Sub-Committee are promptly notified.

G3.5AA User shall not be required to notify a Major Security Incident in accordance with Section G3.5 where it has reason to be satisfied that the DCC, the Panel and the Security Sub-Committee is already aware of the Major Security Incident that would otherwise be notified.

SEC Section G – Security

These changes have been redlined against SEC Section G version 21.0

Amend SEC Section G12 ‘Definitions’. as follows:

Triage System Interface	means a secure virtual private network <u>(VPN)</u>, encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a <u>remote</u> Triage Facility, which provides <u>mutual authentication</u>, confidentiality and integrity of communications. The Triage System Interface: • Must use either TLS or IPsec, and • If using TLS then must include client authentication.
-------------------------	---

Section H 'DCC Services'

These changes have been redlined against Section H version 21.0.

Amend Section H17 as follows:

H17. **MAP / MANUFACTURER REPORTS**

- H17.1 Subject to Section H17.2, the following entities shall be eligible to request and receive reports under this Section H17 in respect of Smart Meters: (a) the Manufacturer of the Smart Meter; and/or (b) the Meter Asset Provider of the Smart Meter.
- H17.2 The DCC shall only provide reports under this Section H17 to Meter Asset Providers and Manufacturers which are either: (a) a Party; or (b) party to an agreement in the form of the Specimen Enabling Services Agreement.
- H17.3 In order to receive reports in respect of a particular Smart Meter, the entity requesting the report will need to provide reasonable evidence to the DCC that such entity is the Manufacturer or Meter Asset Provider of the Smart Meter. The DCC shall not provide reports to an entity unless the DCC has obtained such reasonable evidence of such entity's status as Manufacturer or Meter Asset Provider.
- H17.4 Reports under this Section H17 can be requested quarterly, monthly or on an ad hoc basis (but not more than once each month). The DCC shall provide the reports in accordance with such requests.
- H17.5 Each report under this Section H17 will set out (as a minimum) for each and every Smart Meter for which the recipient is the Manufacturer or Meter Asset Provider:
- (a) Smart Meter ID or Global Unique Identifier (GUID);
 - (b) Smart Meter Type, Smart Meter Model and Manufacturer;
 - (c) firmware version;
 - (d) SMI Status;
 - (e) Region;
 - (f) the Registered Supplier(s) and its/their effective from date(s); and
 - (g) Communications Hub make, model and firmware version.
- H17.6 The DCC shall provide reports under this Section H17 via its preferred file sharing platform, and shall mark them as confidential and not to be shared with any third party apart from the Registered Supplier Party.
- H17.7 Each entity which obtains one or more reports pursuant to this Section H17 undertakes to:
- (a) only use the data contained in those reports for its internal business purposes;
 - (b) not sell or commercially exploit the data contained in those reports; and

- (c) keep the data contained in those reports confidential in accordance with Section M4 (Confidentiality).

SEC Section M – General

These changes have been redlined against SEC Section M version 10.0.

Amend SEC Section M10.2 Other Notices as follows:

M10.2 Save as referred to in Section M10.1, any notice or other communication to be made by one Party to another Party under or in connection with this Code or any Bilateral Agreement shall be in writing and shall be:

- (a) delivered personally or by courier;
- (b) sent by first class prepaid post; or
- (c) sent by ~~fax or~~ email.

M10.3 All notices and communications as described in Section M10.2 shall be sent to the physical address ~~fax number,~~ or email address specified for such purpose in the relevant Party's Party Details. Where no ~~fax or~~ email address is specified for a particular type of notice or communication, notice may not be given in that manner.

M10.4 Subject to Section M10.5, all notices and communications as described in Section M10.2 shall be deemed to be received by the recipient:

- (a) if delivered personally or by courier, when left at the address set out for such purpose in the relevant Party's Party Details;
- (b) if sent by first class prepaid post, two Working Days after the date of posting; and
- (c) ~~Not used if sent by fax, upon production by the sender's equipment of a transmission report indicating that the fax was sent to the fax number of the recipient in full without error; and~~
- (d) if sent by email, one hour after being sent, unless an error message is received by the sender in respect of that email before that hour has elapsed.

SEC Appendix P – SMKI Repository Code of Connection

These changes have been redlined against SEC Appendix P version 2.0.

Amend SEC Appendix 2.2 as follows:

- 2.2. SMKI Repository content access for users without a DCC Gateway Connection
- Parties, RDPs or representatives of the SMKI PMA, Panel or Code Administrator wishing to obtain information lodged in the SMKI Repository, other than via a DCC Gateway Connection, may do so by contacting the Service Desk as set out in the SMKI Repository User Guide, via personal visit, e-mail, ~~signed fax~~, signed letter or telephone for the purposes of viewing, and/or obtaining a copy of a document lodged in the SMKI Repository. Following such contact, the DCC shall ensure that the relevant requested copies of Certificates or other information is provided via optical media such as CD, DVD or, where appropriate, email.

SEC Appendix R – Common Test Scenarios document

These changes have been redlined against SEC Appendix R version 5.0

Amend SEC Section 8.1.26. Response Code Tests as follows:

8.1.26. Response Code Tests

The following table outlines the Response Code Tests required to be executed by User Role. The purpose of these tests is to prove that a party can receive a subset of Response Code messages based on the differing types of response codes that can be received.

New User

The following User Role tables reflect the test Response Codes that must be executed by a new Party seeking to undertake UEPT, unless the Testing Participant has descoped a subset of Service Requests and this have been agreed with DCC or, where referred to the Panel, has been determined by the Panel. The tests are those indicated as 'Mandatory, Mandatory SMETS1 and Mandatory SMETS2+ ' in the test scenario column, for which they must be executed for each specific User Role. Those indicated as 'Mandatory' must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as 'Mandatory SMETS1' must be executed in respect of a SMETS1 Device. Those indicated as 'Mandatory SMETS2+' must be executed in respect of a SMETS2+ Device. Where the Response Code Tests are indicated as N/A there is no requirement to test during execution of the test scenarios.

Reference	Name	Test Scenario	User Role
E11	Failed Validation - Invalid Service Request / Device Type combination	Mandatory	IS ES GS ED GT RSA MDR OU
E13	Failed Validation – Invalid Request Type for URL	Mandatory	IS ES GS ED GT RSA MDR OU
E19	Failed Validation – Device doesn't exist	Mandatory	IS ES GS ED GT RSA MDR OU
E60	Failed Validation – Invalid Service Request for SMETS1 Devices	Mandatory SMETS1	IS ES GS ED GT RSA MDR OU
E61	Failed Validation – Invalid Command Variant for SMETS1 Service Request	Mandatory SMETS1	IS ES GS ED GT RSA MDR OU

In cases where error is generated, the E4 error takes precedence. The E11 error does apply to the MDR role as the MDR role only communicates with an ESME which means the E11 cannot be generated.

Appendix AD ‘DCC User Interface Specification’

These changes have been redlined against Appendix AD version 5.2.

Amend Definitions as follows:

Transport Layer Security (TLS)	means a protocol that provides for the privacy and integrity of data transferred between communicating applications and their users as defined in SEC Section A.
---------------------------------------	---

Amend Section 1.3 as follows:

S1SP Alert	means a communication that complies with format specified in 3.6.3 and contains an S1SPAlert element populated according to Clause 3.9.15 <u>3.9.15.2</u> .
-------------------	--

Amend Section 2.2 as follows:

2.2 Establishment of Logical Connection

Logical connections between the Users and the DCC User Interface shall be subject to the establishment of cryptographic protection as detailed in the DCC Key Infrastructure (DCCKI) Document Set.

The DCC shall make the DCC User Interface available on an Internet Protocol version 4 address range.

The DCC shall provide details of the IP addressing and network configuration to each User as part of the process for obtaining a connection to the DCC User Interface as described in the DCC User Interface Code of Connection.

Each User shall use Network Address Translation to remap internal Internet Protocol addresses to the published DCC provided Internet Protocol addresses at the User’s firewall prior to accessing the DCC User Interface.

Each User shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published Internet Protocol addresses at the User’s firewall to the reserved Internet Protocol addresses within their subnet.

Each User shall only access the DCC User Interface via a Transport Layer Security (TLS) session that has been established, between a non-DCC PEP and the DCC’s PEP

The DCC and each User shall implement TLS in a standard format:

1. conforming to TLS ~~1.2~~ as specified in RFC 5246
utilising the cipher suite TLS_RSA_WITH_AES_128_GCM_SHA256; and

2. using DCCKI Infrastructure Certificates for mutual client/server authentication.

Amend Section 3.5.10 as follows:

3.5.10 Service Response codes generated by DCC

The Response Codes consists of a letter prefix followed by a unique number (defining the specific procedure to be undertaken in response to the Response Code). The Response Code letter is either;

- Information - Prefix 'I'
- Error - Prefix 'E'
- Warning - Prefix 'W'

Please see the DCC's Error Handling Strategy for further details on error handling.

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 has passed access control Or In Response to a successful Non-Device Service Request where there is no specific XML data included in the Service Response	Acknowledgement	N/A
E1	Failed Authorisation – Invalid User / User Role	Error	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	User Role not permitted to send Service Reference	Acknowledgement	V4 Z1
E3	Failed Authorisation – Invalid User Status	Error	User Status not permitted to send Service Reference	Acknowledgement and DCC Alerts	V3 Z1
E4	Failed Authorisation – Invalid User / User Role for Device	Error	User Role not authorised for Device and required date & time	Acknowledgement and DCC Alerts	V1 Z1
E5	Failed Authorisation – Invalid Device Status	Error	Device SMI Status incompatible with Service Reference	Acknowledgement and DCC Alerts	W6 Z1

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
E11	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 “Non-Device” Service Request sent to the “Transform” URL	Acknowledgement	W2 Z1
E17	Failed Authorisation –Service Request or Signed Pre-Command is not available for Local Command Services	Error	User Role / Device status combination doesn’t permit Request of Command for local delivery	Acknowledgement	W6 Z1
E19	Failed Authorisation – Device doesn’t exist	Error	Device ID invalid	Acknowledgement	W3 Z1
E20	Communications Failure – Unable to Communicate with Device	Error	DCC 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	DCC Alerts	X1
E30	Time-out – “Future Dated” Command	Error	DCC Systems doesn’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 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 Systems fails a 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 Systems fails a 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 Systems fails a 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 Systems fails a 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 Systems fails a sequenced Request, because a Response has not been received for previous Request(s) in the sequence during the “Wait Period”	Acknowledgement and DCC Alerts	Y2 Z1
E45	Failed Sequenced Command – Invalid Command Variant	Error	DCC Systems fails a 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 Systems fails a 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 Systems fails a 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

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
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
E51	Failed Validation – Signed Pre-Command Message Code and Service Reference Variant mismatch	Error	The GB Companion Specification 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 is to cancel a Future Dated (DSP) Service Request of the same type but DCC 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) and 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 being processed by the DCC Systems	Acknowledgement	W5 Z1

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
E56	Failed Validation – Service Request no longer supported	Error	The requested Service Request is no longer supported by the DCC Systems. This error shall only occur if a Service Request which exists in an older version of the DUIS XML schema can no longer be accepted by the DCC Systems on that version of the DCC User Interface Please note this Response Code is not applicable to this version of DUIS	Acknowledgement and DCC Alerts	W9 Z1
E57	Failed Validation – Invalid Service Request / GBCS version combination	Error	The Service Request is not compatible with the specified target Device's Device Model according to the Device Model recorded in the Smart Metering Inventory for that Device and the version of GBCS that pertains to the entry for that Device Model in the Central Products List	Acknowledgement and DCC Alerts	W10 Z1
E58	Communications Failure – Command not delivered to ESME	Error	The Communications Hub Function 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 Systems of an Alert 0x8F84 - Failure to Deliver Remote Party Message to ESME (as defined by GBCS) from the Communications Hub Function	DCC Alerts	X4 Z1

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
E59	Dual Band CHF Sub GHz event	Error	The CHF sends one of the following Alerts to the DCC Access Control Broker to indicate a communications event in the Sub GHz frequency range: 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 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 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 Devices	Error	The target device is a SMETS1 Device, but the Service Request is not a SMETS1 Service Request	Acknowledgement	TBC <u>W11</u>

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
E61	Failed Validation – Invalid Command Variant for SMETS1 Service Request	Error	The Command Variant is not valid for the SMETS1 Service Request	Acknowledgement	<u>TBC</u> <u>W11</u>
E62	SMETS1 Service Provider error or information	Error or information	Error condition or notification from a SMETS1 Service Provider, for example a Service Request failed validation within a SMETS1 Service Provider. Additional information shall be provided in the S1SPAlertCode within the DCC Alert payload	DCC Alerts	<u>TBC</u> <u>W12</u>
E63	DCC Data Systems anti-Replay Intercept	Error	Protection against Replay mechanisms within the DCC have rejected a SMETS1 Service Request.	Acknowledgement	<u>TBC</u> <u>W13</u> <u>Z1</u>
<u>E64</u>	<u>Failed Validation – Originator ID is not the Notified Critical Supplier or Notified Critical Network Operator ID</u>	<u>Error</u>	<u>Where the Service Request is a SMETS1 Critical Service Request or a ‘Top Up Device’ SMETS1 Service Request, the Request was not originated by the Notified Critical Supplier or Notified Critical Network Operator.</u>	<u>Acknowledgement</u>	<u>W13</u> <u>Z1</u>
E65	Failed Validation – Certificate Role Mismatch	Error	The Service Request or Signed Pre-Command is not signed using an Organisation Certificate with Remote Party Role ‘xmlSign’	Acknowledgement	<u>TBC</u> <u>U1</u> <u>Z1</u>
E66	Failed Delivery – Unable to deliver to CoS Party	Error	DCC Data Systems cannot establish communications with the CoS Party	DCC Alerts	<u>TBC</u> <u>X6</u> <u>Z1</u>
E67	Timeout – No response received from CoS Party	Error	No response received from the CoS Party within the timeout period.	DCC Alerts	<u>TBC</u> <u>X6</u> <u>Z1</u>
E68	Failed Validation – Service Request failed CoS Party Validation	Error	The Service Request failed validation checks performed by the CoS Party	DCC Alerts	<u>TBC</u> <u>W14</u> <u>Z1</u>
E69	Failed Validation – CoS Service Request failed anti-replay checks	Error	Protection against Replay mechanisms within the DCC have rejected the Service Request.	DCC Alerts	<u>TBC</u> <u>W15</u> <u>Z1</u>

Response Code	Response Code Name	Response code type	Description	Applicable to response types	Error Handling Strategy procedure
E70	Failed Validation – CoS Anomaly Detection Threshold Breach	Error	A CoS-specific Anomaly Detection volume threshold has been exceeded	DCC Alerts	TBC W16 Z1
E71	Failed Validation – Invalid 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	TBC W17 Z1
E100	Failed Authentication	Error	Request failed Authentication (as per checks in clause 3.2.3 Message Authentication)	Acknowledgement	U1 Z1

Table 1 : DCC Systems Response Codes

Amend Section 3.8.17 as follows:

3.8.17 Read Instantaneous Import Registers

3.8.17.1 Service Description

Service Request Name	• ReadInstantaneousImportRegisters
Service Reference	• 4.1
Service Reference Variant	• 4.1.1
Eligible Users	Import Supplier (IS) Gas Supplier (GS) Electricity Distributor (ED) Gas Transporter (GT) Meter Data Retriever (MDR) – Only for SMETS1 Devices
Security Classification	Non Critical
BusinessTargetID - Device applicable to this request	Electricity Smart Meter (ESME) Gas Smart Meter (GSME) Gas Proxy Function (GPF)
Can be future dated?	DSP
On Demand?	Yes
Capable of being DCC Scheduled?	No
Command Variants applicable to this Request (Only one populated)	1 - Send (Non-Critical) 2 - Return for local delivery (Non-Critical) 3 - Send and Return for local delivery (Non-Critical)
Common Header Data Items	See clause 3.4.1.1

Data Items Specific to this Service Request	See Specific Data Items Below	
Possible responses from this Service Request	These are the possible responses applicable to this Service Request. Please see clause 3.5 for more details on processing patterns - Acknowledgement - Service Response from Device – GBCSPayload - Response to a Command for Local Delivery Request - LocalCommand Format Also see Response Section below for details specific to this Request	
Response Codes possible from this Service Request	See clause 0 for Common Response Codes	
GBCS Cross Reference	Electricity	Gas
GBCS MessageCode	0x0027	0x0074
GBCS Use Case	ECS17b	GCS13a

Amend Section 3.8.21 as follows:

3.8.21 Read Instantaneous Export Registers

3.8.21.1 Service Description

Service Request Name	ReadInstantaneousExportRegisters	
Service Reference	4.2	
Service Reference Variant	4.2	
Eligible Users	Export Supplier (ES) Electricity Distributor (ED) Meter Data Retriever (MDR)	
Security Classification	Non Critical	
BusinessTargetID - Device applicable to this request	Electricity Smart Meter (ESME)	
Can be future dated?	DSP	
On Demand?	Yes	
Capable of being DCC Scheduled?	No Yes - SMETS1 Devices only	
Command Variants applicable to this Request (Only one populated)	1 - Send (Non-Critical) 2 - Return for local delivery (Non-Critical) 3 - Send and Return for local delivery (Non-Critical)	
Common Header Data Items	See clause 3.4.1.1	
Data Items Specific to this Service Request	See Specific Data Items Below	
Possible responses from this Service Request	These are the possible responses applicable to this Service Request. Please see clause 3.5 for more details on processing patterns	

	• Acknowledgement • Service Response from Device – GBCSPayload • Response to a Command for Local Delivery Request - LocalCommand Format Also see Response Section below for details specific to this Request	
Response Codes possible from this Service Request	See clause 0 for Common Response Codes	
GBCS Cross Reference	Electricity	Gas
GBCS MessageCode	0x0026	N/A
GBCS Use Case	ECS17a	N/A

Amend Section 3.8.117.2 as follows:

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

Service Request Responses
1.6 – Update Payment Mode
3.2 - Restrict Access For Change Of Tenancy
6.8 - Update Device Configuration (Billing Calendar)
6.14.1 - Update Device Configuration (Auxiliary Load Control Description)
6.14.2 - Update Device Configuration (Auxiliary Load Control Scheduler)
6.14.3 - Update Device Configuration (Auxiliary Controller Scheduler)
6.15.1 - Update Security Credentials (KRP)
6.15.2 - Update Security Credentials (Device)
6.21 - Request Handover of DCC Controlled Device
8.7.1 - Join Service (Critical)
8.7.2 - Join Service (Non-Critical)
8.8.1 - Unjoin Service (Critical)
8.8.2 - Unjoin Service (Non-Critical)
8.11 – Update HAN Device Log

Service Request Responses
8.12.1 - Restore HAN Device Log
8.12.2 - Restore Gas Proxy Function Device Log
11.2 – Read Firmware Version
11.3 - Activate Firmware

Amend Section 3.9.1 as follows:

3.9 DCC Alert Messages

3.9.1 Specific Data Items in the DCC Alert Message

Each Alert Code being reported as a DCC Alert shall conform to the DCC Alert format as defined in 3.6.3 DCC Alerts - DCCAlertMessage Format. The DCC shall ensure that the Body of each DCC Alert (DCCAlert XML element) conforms to one of the DCC Alert formats as defined in the table below:

DCCAlert Definition

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
PowerOutageEvent	The trigger event indicates that a device power has failed	sr:PowerOutageEvent See 3.9.2	AD1	None	N/A
DeviceStatusChangeEvent	The trigger event indicates that a Device's SMI Status has changed	sr:DeviceStatusChangeEvent See 3.9.3	N1, N2, N8, N9, N16, N28 and N29, N44, N45	None	N/A
DSPScheduleRemoval	The trigger event indicates that a DCC Schedule is to be deleted	sr:DSPScheduleRemoval See 3.9.4	N4, N5, N6, N17, N37 and N40	None	N/A
CommandFailure	The trigger event indicates that a Command has failed	sr:CommandFailure See 3.9.5	N3, N7, N10, N11, N12, N13, N14, N15, N33, N34, N35, N36, N38, N41 and N53	None	N/A

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
FirmwareDistributionFailure	The trigger event indicates that a Firmware Distribution Command to the CSP has failed, at least for some of the Devices	sr:FirmwareDistributionFailure See 3.9.6	N18, N19, N20, N21, N22 and N23	None	N/A
UpdateHANDeviceLogResult	The trigger event indicates if a Command to Update a Communications Hub Whitelist Update. (addition ONLY) has succeeded or no Alert has been received by the DCC. .	sr:UpdateHANDeviceLogResult See 3.9.7	N24 and N25	None	N/A
ChangeOfSupplier	The trigger event indicates if an Update Security Credentials (CoS) has succeeded or has failed the CoS Party access control	sr:ChangeOfSupplier See 3.9.8	N26 and N27	None	N/A
DeviceLogRestored	The trigger event indicates that the CHF or GPF Device Log has been restored	sr:DeviceLogRestored (See clause 3.9.9)	N30, N31	None	N/A

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
PPMIDAlert	The trigger event indicates an Alert has been generated by the PPMID Device	sr:PPMIDAlert (See clause 3.9.10)	N39	None	N/A
SecurityCredentialsUpdated	The trigger event indicates receipt of a success Response from Update Security Credentials where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request	sr:SecurityCredentialsUpdated (see clause 3.9.11)	N42	None	N/A
PPMID Removal	The trigger event is receipt of a successful Response from Update HAN Device Log (Removal) where the removed Device is a PPMID that was joined to both an ESME and the GSME	sr:PPMIDRemoval (See clause 3.9.12)	N43	None	N/A
QuarantinedRequest	The trigger event indicates that the Service Request has been quarantined, because an Anomaly Detection volume threshold or attribute limit has been breached	sr:QuarantinedRequest (See clause 3.9.17)	N46, N47, N48	None	N/A

FirmwareVersionMismatch	N49. The trigger event indicates there is a mismatch between the Device's Firmware Version in SMI and that returned by the Read Firmware Version Service Request and that the version returned by the Device matches an entry on the CPL with a status of "Current" N50. The trigger event indicates there is a mismatch between the Device's Firmware Version in SMI and that returned by the Read Firmware Version Service Request, the Activate Firmware Service Request or the Future Dated Firmware Activation Alert and that the version returned by the Device matches an entry on the CPL with a status of "Removed" N51. The trigger event indicates there is a mismatch between the Device's Firmware Version in SMI and that returned by the Read Firmware Version Service Request, the Activate Firmware Service Request or the Future Dated Firmware Activation Alert and the version returned by the Device doesn't match an entry on the CPL N52. The trigger event indicates there is a mismatch between the	sr:FirmwareVersionMismatch (See clause 3.9.13)	N49, N50, N51, N52.	None	N/A
-------------------------	--	---	---------------------	------	-----

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
	GSME's Firmware Version in SMI and that returned by the Read Firmware Version Service Request where the target Device is GPF				

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
DualBandCHAlert	The trigger event indicates an Alert has been generated by the Dual Band CHF Device	sr:DualBandCHAlert (See clause 3.9.14)	N54	None	N/A
S1SPAlertDSP	Used for conveying an S1SP Alert N55: The trigger event indicates that a SMETS1 Service Provider reports a Service Request validation error or other notification. N56: The trigger event is the provision of a prepayment top-up UTRN in response to a Service Request where SRV is 2.2	sr:S1SPAlertDSP (See clause 3.9.15)	N55, N56	None	N/A
SMETS1CHFirmwareNotification	See Clauses 1.4.7.13 and 1.4.7.14.	sr:SMETS1CHFirmwareNotification (See clause 3.9.18)	N57	None	N/A
ALCSHCALCSCConfigurationChange	The trigger event indicates the ESME's ALCS/HCALCS/APC configuration has changed	sr:ALCSHCALCSCConfigurationChange (See clause 3.9.19)	N58	None	N/A
FirmwareUpgradeRequested	This Alert is used to share the list of Devices that have been approved by CSPs for firmware update.	sr:FirmwareUpgradeRequested (See clause 3.9.20)	N59	None	N/A
CSPFirmwareDeliveryStatus	The trigger event indicates a notification has been generated by the CSP in relation to the transfer of a firmware image to a Comms Hub.	sr:CSPFirmwareDeliveryStatus (See clause 3.9.21)	N60, N61	None	N/A
CommsHubAlert	The trigger event indicates an Alert has been generated by the Comms Hub	sr:CommsHubAlert (See clause 3.9.22)	N62	None	N/A

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
ECoSAlert	The trigger event indicates that the ECoS Party has generated an ECoS Alert.	sr:ECoSAlert (See clause 3.9.23)	N63	None	N/A
CoSCertificateAlert	The trigger event indicates that a Device has been installed with a CoSCertificate in its CoS Trust Anchor Cell that does not align with an active CoS Party.	sr:CosCertificateAlert (See clause 3.9.24)	N65	None	N/A
CommsHubFirmwareActivation	The trigger event indicates that a new version of Firmware has been activated on a SMETS2+ Comms Hub.	sr:FirmwareVersionActivationUpdate (See clause 3.9.25)	N64	None	N/A
DUISVersionMismatch	The trigger event indicates that the DCC Alert or Service Response to be sent to the User is not compatible with their DUIS XSD version	sr:DUISVersionMismatch (See clause 3.9.16)	N999	None	N/A

Table 2 : DCCAlert (sr:DCCAlert) data items

Amend Section 3.8.82 as follows:

3.8.82.2 Specific Data Items for this Request

SetCHFSubGHzConfiguration Definition

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
LowerBandSubGHzChannels0To26	Sets the configuration of the Sub GHz Channel Masks for the data item “Page 28 Mask” as defined by GBCS (each page equates to a set of channels that could be used in a specific frequency range) Sets list of channels 0 to 26 in the Lower Band Sub GHz (863 to 876 MHz) frequency range. See Response Code E062801 - By including a Channel number within the SR this shall mean ‘channel can be used by the Communications Hub’ - By NOT including a Channel number within the SR this shall mean	sr:Channels0To26 (Sequence of Channel0 sr:NoType to Channel26 sr:NoType, all optional, but a minimum of 2 Channels must be set)	LowerBandSubGHzChannels0To26	None	N/A

Managed by

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
	‘channel cannot be used by the CH’ At least 2 Channels must be set within this data item. Please see Annex to SEC Section F4 – where Pages are used, at least two channels must be configured per Page. See Response Code E062802				
LowerBandSubGHzChannels27To34	Sets the configuration of the Sub GHz Channel Masks for the data item “Page 29 Mask” as defined by GBCS (each page equates to a set of channels that could be used in a specific frequency range) Sets list of channels 27 to 34 in the Lower Band Sub GHz (863 to 876 MHz) frequency range. See Response Code E062801 By including a Channel number within the SR this shall mean	sr:Channels27To34 (Sequence of Channel27 sr:NoType to Channel34 sr:NoType, all optional, but a minimum of 2 Channels must be set)	Yes	None	N/A

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
	‘channel can be used by the Communications Hub’ By NOT including a Channel number within the SR this shall mean ‘channel cannot be used by the CH’ At least 2 Channels must be set within this data item. Please see Annex to SEC Section F4 - where Pages are used, at least two channels must be configured per Page. See Response Code E062802				
LowerBandSubGHzChannels35To61	Sets the configuration of the Sub GHz Channel Masks for the data item “Page 30 Mask” as defined by GBCS (each page equates to a set of channels that could be used in a specific frequency range) Sets list of channels 35 to 61 in the Lower Band Sub GHz (863 to 876 MHz) frequency	sr:Channels35To61 (Sequence of Channel35 sr:NoType to Channel61 sr:NoType, all optional, but a minimum of 2 Channels must be set)	Yes	None	N/A

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
	range. See Response Code E062801 - By including a Channel number within the SR this shall mean 'channel can be used by the Communications Hub' - By NOT including a Channel number within the SR this shall mean 'channel cannot be used by the CH'. At least 2 Channels must be set within this data item. <u>Please see Annex to SEC Section F4 - where Pages are used, at least two channels must be configured per Page.</u> See Response Code E062802				
UpperBandSubGHzChannel s0To26	Sets the configuration of the Sub GHz Channel Masks for the data item "Page 31 Mask" as defined by GBCS (each page equates to a set of channels	sr:Channels0To26 (Sequence of Channel0 sr:NoType to Channel26 sr:NoType, all optional)	Yes	None	N/A

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
	that could be used in a specific frequency range) List of channels 0 to 26 in the Upper Band Sub GHz (915 to 921 MHz) frequency range. See Response Code E062801 • By including a Channel number within the SR this shall mean 'channel can be used by the Communications Hub' • By NOT including a Channel number within the SR this shall mean 'channel cannot be used by the CH'. If the CH is used in the Central or South Regions This data item should be empty, but this is not validated by the DCC.				

Table 3 : SetCHSubGHzConfiguration (sr: SubGHzConfiguration) data items

Amend Section 3.8.43 as follows:

3.8.43.2 *Specific Data Items for this Request*

CreateSchedule Definition

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
-----------	-------------------------	------	-----------	---------	-------

ScheduleFrequency	The frequency of which the required service reference is executed Valid set • Daily • Weekly (The specified Service Request will be scheduled once a week, on the Schedule Start Date day of the week.) • Monthly (The specified Service Request will be scheduled once a month, on the Schedule Start Date day of the month, where possible. For those months where the Schedule Start Date day of the month doesn't exist, the Service Request will be scheduled on the last day of that month.) • Quarterly (The specified Service Request will be scheduled once every three months, with Scheduled Start Date as for Monthly.) • Half-Yearly (The specified Service Request will be scheduled once every six months, with Scheduled Start Date as for Monthly.) • Yearly (The specified Service Request will be scheduled once every 12 months, with Scheduled Start Date as for Monthly.)	sr:ScheduleFrequency (Restriction of xs:string (Enumeration))	Yes	None	N/A
-------------------	--	--	-----	------	-----

ScheduleStartDate	The UTC date that the scheduled repeating request is required to commence from Valid date in the future	xs:date	Yes	None	UTC Date
ScheduleEndDate	The UTC date that the scheduled repeating request is required to cease, or if not present then the repeating schedule shall remain in force until deleted by the User or by the DCC Systems, e.g. because of Device Decommission Valid date in the future >= ScheduleStartDate	xs:date	User Role IS, GS, ES, ED, GT, <u>MDR</u> : No User Role OU: Yes	None	UTC Date
ScheduleExecutionStart Time	The UTC start time after which a scheduled Command (invoked by the schedule) may be run Valid Time	xs:time	No	00:01:00	UTC Time
KAPublicSecurityCredential	The Key Agreement Public Security Credentials, associated with the User submitting the Request that will be relied upon for Sensitive data Responses. Only applicable to those Scheduled Service Requests that can be submitted by User Roles for which the Device doesn't hold Security Credentials.	sr:Certificate (xs:base64Binary)	User Role IS, ES, ED: N/A User Role GT (where Response includes sensitive data and Device Type = Gas Smart Meter): Yes User Role OU (where Response includes sensitive data): Yes	None	N/A

DSPScheduledServiceReference	Reference of the Service Request to be Scheduled. Valid Set: see clause 3.1, where DCC Scheduled column in table is set to "Yes"	sr:DSP ScheduledServiceReference (Restriction of xs:string (Enumeration))	Yes	None	N/A
DSPScheduledServiceReferenceVariant	Reference Variant of the Service Request to be Scheduled. Valid Set: see clause Error! Reference source not found. 3.1, where DCC Scheduled column in table is set to "Yes"	sr:DSP ScheduledServiceReferenceVariant (Restriction of xs:string (Enumeration))	Yes	None	N/A
DeviceID	This is the Device ID to which the DCC Schedule is targeted.	sr:EUI (See clause 3.10.1.3)	Yes	None	N/A

Choice of Service Request XML Element to be Scheduled	Name and Request Data Items corresponding to DSPScheduledServiceReferenceVariant to be Scheduled, choice of:		Yes	None	N/A
	DSPRetrieveImportDailyReadLog	sr:ReadLogPeriodOffset			
	DSPRetrieveExportDailyReadLog				
	DSPReadActiveImportProfileData				
	DSPReadReactiveImportProfileData				
	DSPReadExportProfileData				
	DSPReadNetworkData				
	DSPReadPrepaymentDailyReadLog				
	DSPRetrieveDailyConsumptionLog				
	DSPReadMaximumDemandImportRegisters	sr:DSPReadData			
	DSPReadMaximumDemandExportRegisters				
	DSPReadLoadLimitData				
	DSPReadActivePowerImport				
	DSPRecordNetworkDataGAS	sr:RecordNetworkDataGAS			

Table 4 : CreateSchedule (sr:DSPSchedule) data items

(*this change relates to MP162 legal text)

SEC Appendix AG – Incident Management Policy

These changes have been redlined against SEC Appendix AG version 6.0

Amend SEC Appendix AG 2.1.3 and 2.10 as follows:

Incident Parties other than Registration Data Providers

2.1.3 ~~Except where section 2.10.10 (Major Security Incidents) applies, for~~ for the purposes of this clause 2.1.3 and clause 2.1.4, references to “Incident Party” do not include Registration Data Providers.

2.10. DCC Major Incidents and DCC Major Security Incidents

Amend heading after 2.10.9 ‘(NOT USED)’as follows:

All Major Security Incidents

2.10.10 Clauses 2.10.11 and 2.10.12 shall apply for a Major Security Incident.