Data Communications Company

DCC Guidance Note

Use of DUIS

Document Version:	**V2.13**
Date:	**Nov. 2019**
Author:	**DCC**
Classification:	**DCC Controlled & for SECAS publication as a Design Note**

Table of Contents

1 Introduction

Version 2.10 is a major revision of content – 15 Guidance points have been deprecated for insertion into an updated DCC User Gateway Interface Design Specification (DUGIDS). There is only one functional change from 2.9 – to Guidance point 16, to revise timeout settings for certain ALCS SRs, and for SR 8.11.

Going forwards this Guidance Note will focus on:

a) Interoperability Issues;

b) Timeout and Retry settings;

c) Workaround.

DUGIDS and this Guidance Note will both be updated on a quarterly basis, if required.

DCC has identified a series of behaviours regarding the use of the DUIS that Users should be aware of. These are explained in this guidance note to ensure that all SEC parties and RDPs (Registration Data Providers) are aware of the issue and its implications in line with DCC's obligations under SEC section H14.39.

These issues have been raised as a result of testing and subsequently highlighted to Testing Participants as part of the DCC's SEC obligations. The limitations highlighted by this guidance note have been discussed internally at the DCC's Design Issues Board (DIB). This document reflects the outcome/decisions of this board and is supported by the DCC's Issue Resolution Board (IRB).

The following table identifies the impact areas of each guidance point.

Guidance Point Number	DUIS 1	DUIS 2	DUIS **3**	SMETS2	SMETS1
7	☑	☑	☑	☑	
8	☑	☑	☑	☑	
9	☑	R	R	☑	
11	☑	☑	☑	☑	
12	☑	☑	☑	☑	
14	☑	☑	☑	☑	
16	☑	☑	☑	☑	
17	☑	☑	☑	☑	
18	☑	☑	☑	☑	
20	☑	☑	☑	☑	
21	☑	☑	☑	☑	
22	☑	☑	☑	☑	
28	☑	☑	☑	☑	
29	☑	☑	☑	☑	
30	☑	☑	☑	☑	
31	☑	☑	☑	☑	
32	☑	☑	☑	☑	
33	☑	☑	☑	☑	☑

Please note, the table above only shows the active guidance notes and not including any deprecated guidance notes.

A summary of the guidance is provided here:

#	Guidance Point Title	Description
1	Time value to be set within Service Requests	*Deprecated. DUIS 2 contains correct text which applies to all DUIS Schemas.*
2	Reading BillingCalendar date time values and potential PARSE error	*Deprecated.* Not to READ BillingCalendar (SR6.2.3) from ESME or GSME prior to being SET using a DUIS Service Request (SR6.8).
3	Reading Tariff data and potential PARSE error	*Deprecated.* Not to READ the Tariff (SR4.11.1/SR4.11.2) from an ESME or GSME prior to a Tariff being SET using a DUIS Service Request (SR1.1.1).
4	*Critical Commands to Devices with an SMI status of "Pending" - HTTP 500 Response*	*Deprecated. This guidance on system behaviour is no longer required as an agreed change (N12 alert) has been implemented for all DUIS Schemas.*
5	Clarification regarding when "Additional DCC System Processing" occurs in relation to receipt of Service Responses	*Deprecated.* Where "Additional DCC System Processing" exists for a DUIS Service Request Variant, this guidance sets out whether this occurs before the relevant User receives the Service Response. If before, Customers know this processing has taken place when receiving the Service Response. If not, Additional DCC System Processing runs in a workoff queue alongside the Service Response.
6	Service Request Variant 8.1.1 - CommissionDevice - what is the definition of a successful Response from the Device?	*Deprecated.* DCC system checks the "MessageSuccess" attribute in the Response to determine a "successful Response" and not the individual ElecClockTimeStatus or GasClockTimeStatus values received from the device within the GBCS response.
7	Workaround to avoid the potential issues associated with GBCS IRP510 - CH behaviour on 2nd CCS01 when using Service Request Variant 8.11 - UpdateHANDeviceLog	For DCC release 1.x CH, Users should not send multiple SR8.11s and always wait for either N24 or N25 DCC alerts. Please read the guidance note in full.
8	Use of SRV8.14.3 - CommsHubStatusUpdate-FaultReturn where Communications Hub has not been installed	Workaround advice to populate the CHFConnectionMethod data item within SR8.14.3 with the existing "ESME" enumeration value where a Comms Hub was not/has never been installed.
9	Use of SRV6.2.4 ReadDeviceConfiguration(IdentityExcMPxN) and invoking the associated GBCS Use Case GCS21e - Read GSME/GPF Configuration Data Device Information (device identity)	DUIS 1 only, RESOLVED FOR DUIS 2 - Guidance on use of SR6.2.4 targeted at a GPF device.
10	Reading Prepayment Configuration values from devices and potential PARSE error	*Deprecated.* Not to READ the Prepayment Configuration from an ESME or GSME (4.13 - ReadPrepaymentConfiguration) prior to the DebtRecoveryRatePeriod values being SET using DUIS Service Request SRV2.3 – UpdateDebt. Recommends proposed SR ordering.

11	Handover of Security Credentials on GPF from ACB credentials added as part of the manufacturing process	Advice on use of Service Request 6.21, and Service Request 6.15.1 for managing Network Operator certificates on the GPF.
12	Use of SR4.4.4 and the "VALID" values that can be used for the EndDateTime value within the ReadLogPeriod XML data item	All Users are advised to read all logs prior to CoS dates - to ensure all the data they require is retrieved before the CoS event occurs. Details various observed implementations of 'read to the end of log'.
13	*Use of SRV1.1.1 and SRV1.2.1 and setting price values on GSME*	*Deprecated. Resolved for all DUIS Schemas.*
14	General guidance and handling failure scenarios when using Service Request Variant 8.11 - UpdateHANDeviceLog	Advice on Failure Scenario 1 – failure to establish communication, and Failure Scenario 2 – "lost" Alerts.
15	General guidance for how DCC Systems handles any Combined Devices	*Deprecated.* Combined devices should to comply with the security characteristics of the higher security classification, e.g. combined IHD/PPMID would be a Type 1 device (PPMID is Type 1, IHD is Type 2).
16	General guidance on DCC Retry and Timeouts for Service Request Processing	Explains principles and rules for retry and timeout, and also describes (a) how retry and timeout values are configured in DCC Data Systems, (b) retry and timeout for DCC Users, (c) for synchronous HTTP requests to DCC.
17	Resetting of Network Operator Anti Replay Counter/Remote Party Floor Sequence Number	Sets out options for Network Operators, one of these options is only available from DUIS 2.x onwards.
18	GSME/GPF Wildcard features workaround	Guidance on wildcard workaround for SRV 1.1.1 (Update Import Tariff) and SRV 2.1 (Update Prepayment Configuration) for GSME/GPF only.
19	DebtRecoveryRatePeriod in SR 2.3 Update Debt for ESME (GBCS Use Case ECS07)	*Deprecated.* DUIS 1 only, resolved for DUIS 2. Guidance on Service Request 2.3 Update Debt on ESME only.
20	Alert storms caused by 0x8F3E	Guidelines for Type 1 and Type 2 devices to seek to prevent avoidable 'alert storms' - relates to alert 0x8F3E only.
21	DNO's Communication to Meters	Advice to Network Operators on when to trigger SR 6.15.1 to update DNO credentials.
22	Device Interop Guidance	Guidance to upgrade the Comms Hub and GPF before the Device to reduce likelihood of interoperability issues.
23	UTRN counter cache reset	*Deprecated.* Guidance to Supplier to populate the SupplierPrepaymentTopUpFloorSeqNumber / RemotePartyPrepaymentTopUpFloorSeqNumber in 6.15.1, 6.21 and 6.23 Service Requests.
24	Prepayment Clarifications (agreed and aligned with IRP 560)	*Deprecated.* Guidance to Energy Supplier - Not to set the specified list of SMETS Configuration Data Items to a negative value. - Avoid the specified list of actions whilst Emergency Credit is 'available'. - To avoid inadvertent disconnection, do not automatically reset Meter Balance to zero.
25	Scheduled Service targeting GSME	*Deprecated.* Guidance to Service User to create the DSP Schedule for SR4.6.1/4.8.1/4.14 targeting GPF only.

26	GSME-PPMID re-join	*Deprecated.* Guidance to Service User to re-join the PPMID to the GSME via SR8.7.2 Join Service (Non-Critical) targeting PPMID following a successful execution of the SR6.15.2 Update Security Credentials (Device) targeting GSME.
27	End of time for GPF/GSME log/profile reading	*Deprecated.* Guidance to Service User to use 2 seconds before the endDateTime if they wish the log entry is exclusive.
28	Could non-mandated GBCS alerts be configured off	Explain to Service User that it is possible to disable the non-mandated GBCS alerts on the basis the alert is - an alert defined by GBCS so is included in GBCS table 16.2 - Supported by the DUIS schema Service User currently use - Supported by the SMETS2 device
29	How to interpret the high value of 16,777.215 m3 in the SR4.8.1 response	For SR4.8.1 gas response, DCC Service Users should treat the value of 16,777,215 m3 as an invalid value. This value should not be used as part of any calculations or estimations.
30	non-zero Disablement Thresholds	Customer are advised, that if a Disablement Thresholds are set at value other than zero then devices may not behave consistently as expected,
31	Future dated COTs	The restriction date in the Service Request may be in the future or in the past, and the Command will be executed on receipt. The restriction is applied as soon as the command is executed, which means that the current householder will be restricted from access to their own data if the restriction date is in the future. DCC Service Users are advised not to set an execution date prior to the restriction date if the restriction is not intended to apply to the current tenant.
32	What is the recommendation for setting up a schedule	• There is no real benefit for Users 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 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. • Service Users should expect to receive the device response between the scheduled time and 6am, however it is worth nothing that the DCC has a 24-hour SLA to deliver a schedule and, especially in times for unexpected outage, the delivery times may change during the day
33	what happen to a suspended device	After a device model/firmware is suspended from CPL - Not possible to I&C a device which is not yet fully I&Ced - Not possible to send any NON-critical command with exception of OTA and Change of Supplier

2 Behaviours observed in the use of the DUIS

2.1 Deprecated - Guidance Point 1

The issue identified with in this guidance point has been resolved within the DUIS 2 release, the contents of which apply to all DUIS schemas. The detail of this guidance point can be found in the appendix.

2.2 Deprecated - Guidance Point 2

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 6, SR6.2.3, Service Request Narrative, Point 2.

The detail of this guidance point can be found in the appendix.

2.3 Deprecated - Guidance Point 3

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 4,

- SR4.11.1 Service Request Narrative, Point 2, And
- SR4.11.2 Service Request Narrative, Point 2

The detail of this guidance point can be found in the appendix.

2.4 Deprecated - Guidance Point 4

The issue identified within this guidance point has been resolved through the use of an N12 alert for all versions of DUIS. This solution has been implemented by DSP and is in Production. The detail of this guidance point can be found in the appendix.

2.5 Deprecated - Guidance Point 5

The issue identified within this guidance point has been clarified within the Operational DUGIDS in the following annexes

- Annex 1, SR1.1.1, Service Request Narrative, Point 3 and Point 4
- Annex 3, SR3.2, Service Request Narrative, Point 3
- Annex 6,
  - SR6.15.1, Service Request Narrative, Point 6, 7 and 8
  - SR6.15.2, Service Request Narrative, Point 3
  - SR6.21, Service Request Narrative, Point 6, 7 and 8
  - SR6.23, Service Request Narrative, Point 7, 8, 9, 11 and 15
- Annex 8,
  - SR8.1.1, Service Request Narrative, Point 3
  - SR8.3, Service Request Narrative, Point 5
  - SR8.4, Service Request Narrative, Point 5

    - SR8.5, Service Request Narrative, Point 10
    - SR8.7.1, Service Request Narrative, Point 6
    - SR8.7.2, Service Request Narrative, Point 5
    - SR8.11, Service Request Narrative, Point 12
- Annex 11,
    - SR11.1, Service Request Narrative, Point 4
    - SR11.2, Service Request Narrative, Point 2d
    - SR11.3, Service Request Narrative, Point 3e
- Annex 12, SR12.2, Service Request Narrative, Point 5

The detail of this guidance point can be found in the appendix.

2.6 Deprecated - Guidance Point 6

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 8, SR8.1.1, Service Request Narrative, Point 3

The detail of this guidance point can be found in the appendix.

2.7 Guidance Point 7 – Workaround to avoid the potential issues associated with GBCS IRP510 - CH behaviour on 2nd CCS01 when using Service Request Variant *8.11 - UpdateHANDeviceLog*

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
7	☑	☑	☑	☑	

Guidance Type	Workaround
Functional Area	Install and Commission
Keywords	Install and Commission, CCS01, 8.11, IRP510, N24, N25

GBCS does not define the expected behaviour of the CH in the scenario where a 2nd GBCS Use Case CCS01 is sent (Add new Device ID to CHF Device Log to Whitelist the device and allow a connection of the device to the ZigBee HAN). As a result of this the subsequent Service Request Variant *8.11 – UpdateHANDeviceLog* definition in DUIS is silent on this as well.

Through testing activities, it has been confirmed that different CH device manufacturers have different implementations and this is causing some potential issues for the use of *SR8.11 – UpdateHANDeviceLog* for CHFs in the South and Central CSP regions.

If, subsequently a different CCS01 Command is received by the CH (generated by DCC on receipt of an SR8.11 from a User) for the same Device, the CH behaviour currently differs between manufacturers.

For Devices that have not begun the HAN joining process, this should not cause issues. However, for those that have completed CBKE (Certificate Based Key Exchange) and so joined the HAN, it would appear that communication between the Comms Hub and the Device would cease at the application layer (since they are no longer using the same Link Key). The Device would then eventually attempt to undertake Trust Centre Swap Out processing, but this would fail. Currently, there would seem to be no specified way of returning the affected Device to a state where it was possible to re-connect it to the HAN (or another HAN).

The sending of a new subsequent *SR8.11 – UpdateHANDeviceLog* for an already whitelisted Device should be relatively rare but could happen where, for example:

- a DCC User believes whitelisting has failed e.g.
  - because an N25 DCC Alert is received, but whitelisting has not failed (e.g. because the CS14 Alert was lost, for example because of communications issues);
  - because no SR8.11 Response is received; or
- a DCC User triggers a second SR8.11 in error.

2.7.1 Guidance / Workaround

In order to avoid the potential issues listed above of a Device being placed into a state where it is not possible to re-connect it to the HAN (or another HAN) DCC recommends the following guidance / workaround be adopted by Users.

- Users should not send multiple SR8.11s with a data item "*RequestType*" with a value of "*Add*" to add the same device Id to the same CHF device log without waiting for the end of the HAN joining process (ZigBee Join window). This ZigBee Join window is defined by DCC as the value of time (number of seconds) included in the 8.11 Service Request attribute "JoinTimePeriod" plus a configurable network transmission time (expected to be set at circa 30 seconds).

- Users will know when this HAN joining process (ZigBee Join window) activity has ended by the receipt of either one of the;

  – DCC Alert 24 - Successful Communications Hub Function Whitelist Update or

  – DCC Alert 25 - **Potentially** Unsuccessful Communications Hub Function Whitelist Update

- These determine that DCC has either received positive confirmation or has not received positive confirmation that the requested addition to the Communications Hub Function's whitelist was successful respectively.

- Users should always wait for one of these DCC Alerts to be received before sending any subsequent SR8.11 with a data item "*RequestType*" with a value of "*Add*" to add the same device Id to the same CHF device log.

- In the event that one of these DCC Alerts is not received, then the User should investigate the issue and **NOT re-send the original SR** in the hope that it will work as this could potentially cause the issue highlighted above of a Device being placed into a state where it is not possible to re-connect it to the HAN (or another HAN).

- It is important that the User first confirms the actual situation of whether or not the HAN joining process was completed, i.e. that the device Id was successfully written into the CHF Device log and CBKE completed, by sending an *SR8.9 – Read Device Log* to the Comms Hub.

  – If the requested device_id is returned from the CHF in the response but with a LastCommunicationsDateTime of either 2000-01-01 00:00:00 or 2136-02-07 06:28:15 (Both these dates are in effect, "null" values) then this indicates that communications has not been established with that device. In this instance the User should send an *SR8.11- UpdateHANDeviceLog* Service Request with a data item "*RequestType*" with a value of "*Remove*" to the same CH for the same Device prior to sending a subsequent *SR8.11- UpdateHANDeviceLog* Service Request with a data item "*RequestType*" with a value of "*Add*" to the same CH for the same Device. This will ensure that all details of the Device are removed from the CHF Device Log and will reset the HAN joining process (ZigBee Join window) activity ready for a clean start and

avoid any potential for confusion on the device of the same Device already being in the CHF Device Log.

– If the requested device_id is returned from the CHF in the response with a LastCommunicationsDateTime that is not one of the “null” values listed above then this indicates that communications were actually established with that device. In this instance the User should continue with the next steps in the commissioning process, as they would have done if success had been reported initially.

– If the requested device_id is not returned at all from the CHF in the response, it is confirmed that the command did not work and as a result a subsequent *SR8.11 – UpdateHANDeviceLog* can be sent to the CHF to re-attempt the addition to the CHF Device Log.

Please see attached GBCS IRP for further technical details and reference.

IRP510 CH behaviour on 2nd CC

2.7.2 Additional details to note

If this workaround is not followed and a Communications Hub Device does end up in a state whereby there is no specified way of returning the affected Device to a state where it is possible to re-connect it to the HAN (or another HAN) then this hub should be returned to the DCC in line with User obligations.

A query has been raised by a User as to which *CHFFaultReason* value should be used when Users send the associated SRV8.14.3 - CommsHubStatusUpdate-FaultReturn to DCC. In these scenarios, DCC would offer guidance that a value of “***SMHAN Interface Fault***” should be used.

2.7.3 Applicable to GBCS2.x or later devices

The issue identified within this guidance point has been largely resolved through the implementation of IRP510 within GBCS v2.x and later devices. However, this guidance point remains applicable to GBCS v1.x devices running DUIS 2.

2.8 Guidance Point 8 – Use of SRV8.14.3 - CommsHubStatusUpdate-FaultReturn where Communications Hub has not been installed

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
8	☑	☑	☑	☑	
Guidance Type	Workaround				
Functional Area	Install and Commission				
Keywords	Not-installed, Returns, 8.14.3				

It has been identified by Users that there is a missing enumeration value on the *CHFConnectionMethod* data item within *SRV8.14.3 - Communications Hub Status Update.* The scenario where this causes issue is when a Communication Hub has been identified as faulty but has never been installed.

In these scenarios none of the existing three enumeration values available (Hot-shoe, Cradle or ESME) are appropriate.

2.8.1 Proposed Workaround

The workaround required until a permanent fix to add a fourth enumeration value of "*not-installed*" will be for Users to **populate the *CHFConnectionMethod* data item within *SR8.14.3* with the existing "ESME"** enumeration value.

2.9 Guidance Point 9 – Use of SRV6.2.4 ReadDeviceConfiguration(IdentityExcMPxN) and invoking the associated GBCS Use Case GCS21e - Read GSME/GPF Configuration Data Device Information (device identity)

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
9	☑			☑	
Guidance Type	Optimising System behaviour				
Functional Area	Meter Reading				
Keywords	GCS21e, 6.2.4, IRP513, DeviceIdentifier, ModelType, ManufacturerIdentifier, SupplyTamperState, SupplyDepletionState				

Several issues with the use of *SRV6.2.4 ReadDeviceConfiguration(IdentityExcMPxN)* have been identified during DCC testing phases that require some guidance by DCC for its operational use.

2.9.1 Sending SRV6.2.4 to a GPF (Target ID within the SRV)

Following a series of testing issues being raised against SRV6.2.4 being sent to a Business Target ID of a GPF device, Users should note the following guidance.

DCC do not believe that for DCC R1.3 release there is value in sending a SRV6.2.4 to a GPF (*BusinessTargetID* within the SRV) due to the existence of design ambiguity issues with the GBCS Use Case *GCS21e - Read GSME/GPF Configuration Data Device Information (device identity)* and DCC is, on this basis, advising Users to either;

a) Not send this SRV to a GPF if possible, or

b) If the SRV is sent to a GPF, that the results returned are ignored as they are not valid and may be misleading.

If Users wish to return the *constant data* items of *DeviceIdentifier*, *ModelType* and *ManufacturerIdentifier* then DCC offers guidance that SRV6.2.4 should be sent to the CHF device instead (BusinessTargetID value). This will return the same values for the device (CHF and GPF have same constant data items as it is a single physical device).

If Users wish to return the *SupplyTamperState* or *SupplyDepletionState* values then DCC offers guidance that SRV6.2.4 should be sent to the Gas smart meter instead (BusinessTargetID value) in order to return the actual values of these data items.

GSME Supply Depletion State and GSME Supply Tamper State (which are in the existing GCS21e Use Case) don't have to be sent to the GPF by the GSME as part of the 'mirroring' function, and so can't reliably be read from the GPF, as noted in the existing GCS21e Use Case. These two data item values can only be reliably read from the GSME. DCC believes that there is still value in sending this Command to a Gas Smart Meter, where the data is accurate.

DCC recognise that there are wider issues associated with the Use Case GCS21e as defined in GBCS v1.0 that have been confirmed as not being fixed in later versions of GBCS (as the Use Case is intended to be removed during the next TSG2 specification set). As a result of this, DCC proposes to reduce the priority and severity of this DEFECT identified to low. Please note that there is a workaround available to Users to interrogate the device configuration from the GSME directly (using the same GBCS Command) and not send this Command to a GPF.

BEIS have raised GBCS IRP513 - Manufacturer and Model Values in Remote Party Responses raised for proposed inclusion in GBCS v2.0 to resolve this issue in the longer term.

2.10 Deprecated - Guidance Point 10

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 4, SR4.13, Service Request Narrative, by adding a new paragraph.

The detail of this guidance point can be found in the appendix.

.

2.11 Guidance Point 11 – Handover of Security Credentials on GPF from ACB credentials added as part of the manufacturing process

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
11	☑	☑	☑	☑	
Guidance Type	Optimising System Behaviour				
Functional Area	Install and Commission, Comms Hub Replacement				
Keywords	Certificate Updates, SR 6.21, Network Operator security credentials				

DCC has received a query from a User regarding the process that DCC supports for the Handover of Security Credentials on GPF (Gas Proxy Function) from ACB credentials added as part of the manufacturing process.

There are potentially two different options that an Import Supplier User Role could use in order to transfer control of the ACB security credentials held on the GPF as part of the manufacturing process to the correct Network Operator security credentials.

Potential Options available are as follows;

Option 1

- Suppliers may use a single Service Request process by sending *SR6.21 - Request Handover Of DCC Controlled Device* to change the default ACB certificates directly to the actual Network Operator certificates required for Business as Usual activities.

Option 2

- Suppliers may use a *two Service Request process* by sending *SR6.21 - Request Handover Of DCC Controlled Device* to change the default ACB certificates to their own Supplier certificates and then use a subsequent *SR6.15.1 - Update Security Credentials (KRP)* to change these certificates to the actual Network Operator certificates required for Business as Usual activities.

It is noted by DCC that the underlying GBCS Use Case and command *CS02b – Update Security Credentials technically* supports either option above equally.

DCC confirms that the design of the DCC Systems and associated DUIS v1.0 (DCC User Interface Specification), published by SECAS on 9 November 2016, does not currently support Option 2 as it is assumed that only the Network Operator User Role should be the Eligible User to change the Security Credentials associated with the Network Operator Credentials on the GPF.

This issue was discussed with Users at the BEIS led TSIRS (Technical Specification Issues Resolution subgroup) meeting on the 9th February 2017 and at a subsequent DCC DRF (Design Release forum) on the 21st February 2017 in order to gain information on Suppliers' assumptions to date regarding which approach has been chosen. The overwhelming majority of Suppliers confirmed that they were expecting to Use Option 1.

2.11.1 Guidance / Workaround

DCC confirms that Option 1 is the implementation that the DCC Systems support and is expecting Suppliers to operate in relation to this issue.

2.12 Guidance Point 12 – Use of SR4.4.4 and the "VALID" values that can be used for the EndDateTime value within the ReadLogPeriod XML data item

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
12	☑	☑	☑	☑	
Guidance Type	Optimising System Behaviour				
Functional Area	Prepayment				
Keywords	Billing Data Log, 4.4.4, IRP448				

The Service Request impacted by this issue is *SR4.4.4 - RetrieveBillingDataLog(PaymentBasedDebtPayments).*

During SIT for R1.3 DCC has identified an issue with different Party's implementations of GBCS Use Case GCS15d Retrieve Billing Data Log (Payment Based Debt Payments) and how it relates to IRP448 (DCC Testing Issue #3012).

The issue started with the identification that the DSP Systems are not sending the correct value for end of time specified for GCS15d. When the tester enters an EndDateTime value within the ReadLogPeriod XML data item of 3000-12-31T00:00:00Z it generates the GBCS payload with value, 0xFFFFFFFF, and some devices (GPFs and GSMEs) are rejecting this because they are expecting a value of 0xFFFFFFFE.

However, GBCS section 9.1.6 states the following,

> *9.1.6 Start of Time and End of Time values*
>
> *Where a date-time is specified as a 32 bit long unsigned integer:*
>
> *the Start of Time shall mean the value 0x00000000; and*
>
> *the End of Time shall mean the value 0xFFFFFFFF.*

This End of Time value is what DSP Systems use in all GBCS Use Cases to represent End of Time, so that is why the DSP TRANSFORM component is using 0xFFFFFFFF in the GCS15d command rather than 0xFFFFFFFE.

In fact, the GCS15d Use Case template in GBCS v1.0 is the only place in the whole of GBCS that suggests using 0xFFFFFFFE for End of Time; every other Use Case template dealing with logs is silent on the End of Time value and thus must follow section 9.1.6.

So, there is an ambiguity in GBCS regarding the exact value that should be used to represent "read to the end of log" for this GCS15d use case. Different GBCS implementers have interpreted this differently and this is causing alignment issues within the DCC ecosystem.

During SIT DCC has observed that different Device manufacturers (GPF and GSMEs) have implemented the GCS15d use case in different ways.

There are differences in whether or not each device supports or does not support the following functionality;

- variable “Latest End Time” field values
- fixed read to the end of log values of 0xFFFFFFFE or 0xFFFFFFFF.

Some devices support any date time value for "Latest End Time" field whilst others support only a fixed read to the end of log values of either 0xFFFFFFFE or 0xFFFFFFFF or accepts both values equally. There is no consistent implementation across devices or manufactures which causes the issues observed in SIT.

The table below summarises the current identification of device behaviours for GBCS v1.0 and pre any changes for IRP448. GSME device manufactures have been redacted for confidentiality purposes.

Device Type	CSP/ Manufacturer	Support for Variable End Dates?	Supported Value(s) for read to the end of log
GPF	CSP North	No	Yes, but 0xFFFFFFFE value only
GPF	CSP South/ Central - WNC	No	Yes, but 0xFFFFFFFE value only
GPF	CSP South/ Central - Toshiba	Yes	Yes, any value
GSME - Emulator	DCC	Yes	Yes, any value
GSME	[Redacted manufacturer A]	Yes	Yes, any value
GSME	[Redacted manufacturer B]	Yes	Yes, but 0xFFFFFFFE value only

Table 1. Device Support for Variable End Date & Read to the End of Log

DCC has a strong interest in getting this working for Users especially as the GPF device is part of the DCC’s responsibilities and so DCC recognises that it needs to have a consistent interpretation of GBCS across its Systems.

2.12.1 SIT Workaround used to progress SIT

When using Service Request *SR4.4.4 - RetrieveBillingDataLog(PaymentBasedDebtPayments),* a User (or simulated User) should ***always*** populate the DUIS Service Request with a *EndDateTime* value within the *ReadLogPeriod* XML data item of ‘2136-02-07T06:28:14Z’ to be interpreted by the DCC Systems as ‘read to the end of the log’.

DSP Systems shall then build a Command to the target device via the TRANSFORM component with an end time value of ‘0xFFFFFFFE’ as per the definition within GBCS v1.0 Use Case GCS15d Retrieve Billing Data Log (Payment Based Debt Payments).

Any other date value used for the *EndDateTime* value within the *ReadLogPeriod* XML data item may cause unexpected behaviours on a target device and potentially cause the

associated Command to fail on the device (this is dependent on the manufacture's implementation of the GBCS Use Case).

DCC recognises that using this workaround in Live will have a significant impact on Users so a secondary, more User friendly, workaround has been developed for use for R1.3 Live.

2.12.2 Proposed R1.3 DCC Live Workaround

DCC has implemented a small change to the DCC Systems to make the SIT workaround more robust and have less of an impact upon Users.

Under this change, the DCC systems have had a code change made specifically as a post processing step within the TRANSFORM component for GBCS v1.0 Use Case GCS15d Retrieve Billing Data Log (Payment Based Debt Payments). This change means that the DCC Systems shall build a Command to the target device via the TRANSFORM component with an end time value of '0xFFFFFFFE' for this specific use case in line with the GBCS use case definition to be interpreted by the device as 'read to the end of the log'.

This would mean less impact of the proposed workaround on Users as each User can continue to rely upon the existing DUIS definitions for values to use in the *EndDateTime* value within the *ReadLogPeriod* XML data item.

DUIS v1.0 currently states in section 3.10.1.14 for the *EndDateTime* value within the *ReadLogPeriod* XML data item the following,

An End Date of '3000-12-31T00:00:00Z' will be interpreted by the DCC Systems as 'read to the end of the log'.

With this relatively small DCC System change to the TRANSFORM component, **Users can continue to use an End Date value of '3000-12-31T00:00:00Z'** within all DUIS Service Requests rather than the pseudo end of log date '2136-02-07T06:28:14Z' that directly relates to the device expected value of '0xFFFFFFE'.

All other TRANSFORM rules within the DCC Systems will remain unchanged and an XML End Date value of '3000-12-31T00:00:00Z' within the DUIS Service Requests will continue to create a GBCS Command with a value of '0xFFFFFFF'.

Users should still note that specifying a more specific variable end date value that does not equal '3000-12-31T00:00:00Z' may still cause unexpected behaviours on the target device and potentially cause the associated Command to fail on the device (this is dependent on the manufacture's implementation of the GBCS Use Case).

Both Workaround options have been successfully tested by DCC during SIT.

2.12.3 Access Control Note

Users should be aware that an impact of this guidance is that consideration should be made of DCC Access Control rules when using a 'read to the end of the log' end date. As all of the Read log Service Requests are defined as Non Critical Service Requests, the DCC Systems performs Access Control to ensure that the Requestor is the Registered Supplier, Registered Network Operator or Registered Supplier Agent for the duration of the *ReadLogPeriod* data range.

In the event of a change of one of these Parties for a device, then there is a likelihood that a previously Registered Supplier, Registered Network Operator or Registered Supplier Agent may not be able to use this workaround.

DCC would therefore advise all Users to ensure that they read all logs prior to the CoS dates to ensure that Users have all the data they require before the CoS event occurs and they are no longer the Registered Supplier, Registered Network Operator or Registered Supplier Agent if using this 'read to the end of the log' workaround to obtain data form devices.

2.12.4 Summary

- Users should note that specifying a VARIABLE EndDateTime value within the ReadLogPeriod XML data item value that does not equal '3000-12-31T00:00:00Z' may cause unexpected behaviours on the target device and potentially cause the associated Command to fail on the device (this is dependent on the manufacture's implementation of the GBCS Use Case).

- Users are advised as part of this guidance to **only use a FIXED EndDateTime value within the ReadLogPeriod XML data item value of '3000-12-31T00:00:00Z' when sending SR4.4.4 - RetrieveBillingDataLog(PaymentBasedDebtPayments) to DCC.**

2.12.5 Applicable to GBCS2.x or later devices

The issue identified within this guidance point has been largely resolved through the implementation of IRP448 within GBCS v2.x and later devices. However, this guidance point remains applicable to GBCS v1.x devices running DUIS 2.

2.13 Deprecated - Guidance Point 13

The issues identified within this guidance point has been resolved by updating the DSP system and updating to DUIS 2. The detail of this guidance point has been moved to the appendix.

2.14 Guidance Point 14 – General guidance and handling failure scenarios when using Service Request Variant *8.11 - UpdateHANDeviceLog*

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
14	☑	☑	☑	☑	
Guidance Type	Optimising System Behaviour				
Functional Area	Install and Commission, Device Join/Unjoin				
Keywords	0x8F69, 0x8F12				

In order to improve experiences in User testing, it has been requested that guidance be provided by DCC on the steps to be taken when adding devices to the HAN, in particular around the use of *SR8.11 UpdateHANDeviceLog*. The following guidance applies equally to all Comms Hubs.

2.14.1 Success scenario

The scenario for successful installation and commissioning of a device on the HAN is summarised in the diagram below.

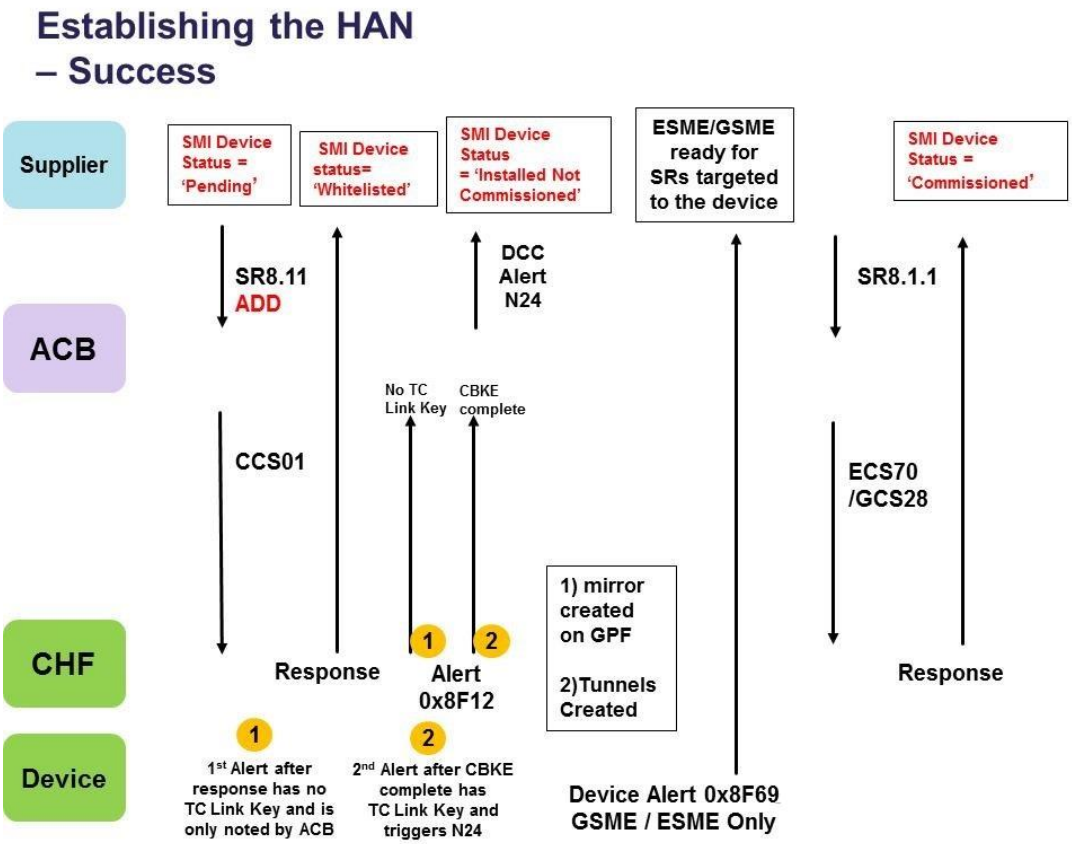

Figure 1. Establishing the HAN - Success

Service Request *8.11 UpdateHANDeviceLog* with a Request Type of "Add" is sent to the CHF to add the device to the Device Log (i.e. to Whitelist the device) and to allow a connection to be established between the CHF and the requested device on the ZigBee HAN. As part of this process, the CHF sends two Alerts with code 0x8F12 to the Access Control Broker (ACB = DSP) remote Party.

- The first Alert confirms the addition of the requested device to the Device Log and is simply noted by the ACB.
- The second Alert confirms completion of the exchange of Link Keys (Certificate Based Key Exchange) between the CHF and the requested device. The ACB informs the User of this event by sending *DCC Alert N24 Successful Communications Hub Function Whitelist Update.*

The CHF completes any further actions required for communications and the device (if it is an ESME or GSME) sends an Alert with code 0x8F69 to the Supplier*. At this point the device is now ready to receive SRs and complete the commissioning process. The time taken to produce the 0x8F69 Alert is device specific and therefore DCC cannot give specific guidance on how long to wait for the 0x8F69 Alert. It is suggested that Users determine an appropriate value based on their experience in device testing, noting that this value should also allow for up to 60 seconds for delivery across the SMWAN and DSP systems.

* Note that the Target ID for this Alert is derived from the identifier (ID) stored in the Supplier Trust Anchor Cell on the device as per GBCS definitions. If ACB certificates are installed and still present within the Supplier Trust Anchor Cell on a device then the Alert will not be sent by the device and will not be received by the User sending the SR8.11. This behaviour is aligned to the requirements of GBCS section 4.3.2.5 which states that;

> "*a Device shall not allow execution of any Remote Party Command other than an Update Security Credentials Command or a Provide Security Credentials Command**, nor issue any Remote Party Alerts, in relation to a Remote Party Role where the Remote Party Role stored in a Trust Anchor Cell is different than that of the Trust Anchor Cell itself**".*

If the User expects to be using ACB certificates and hence will not receive the 0x8F69 Alert then the only guidance DCC can provide is that the User should wait an appropriate amount of time after receipt of the N24 Alert before sending the next SR in the commissioning process. The amount of time to wait is device specific and therefore DCC cannot give specific guidance on what value to use. It is suggested that Users determine an appropriate value based on their experience in device testing.

Notwithstanding the above, following successful receipt of the I0 response for SR8.11 there are two possible scenarios in which the process of establishing communications on the HAN may fail to complete as described below and in these cases specific guidance is needed to ensure that the device may subsequently be connected to the HAN and commissioned successfully.

2.14.2 Failure Scenario 1 – failure to establish communications

Failure Scenario 1 occurs when the device and the CHF fail to complete CBKE and establish communications. It has been observed through testing that in this scenario the CHF does not send the second Alert 0x8F12, resulting in the Access Control Broker (DSP) ultimately timing out waiting for this expected Alert, and subsequently sending DCC Alert N25 to inform the User that no such Alert has been received.

The sequence of events for this Failure Scenario is shown in the diagram below.

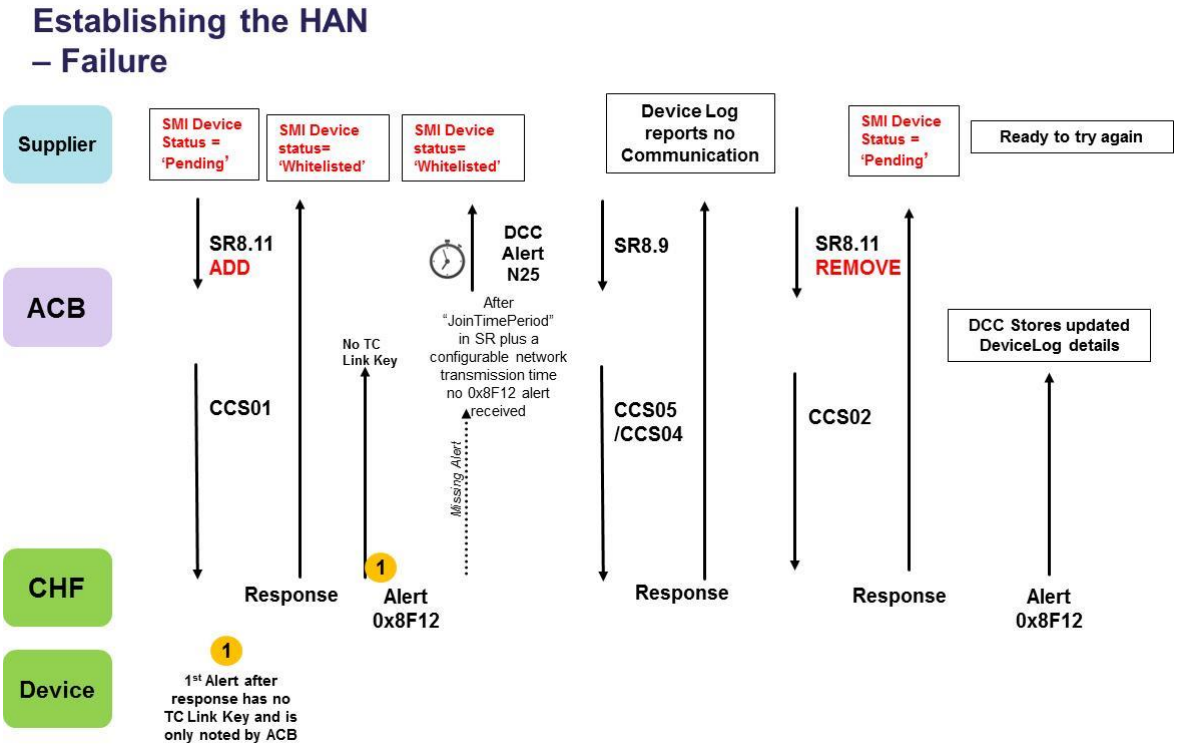

Figure 2. Establishing the HAN - Failure

The timeout used by the ACB (DSP) is equal to the value of time (number of seconds) included in the 8.11 Service Request attribute "JoinTimePeriod" plus a configurable network transmission time (expected to be set at circa 30 seconds). In the absence of a DCC Alert N24 confirming success, the User should always wait for at least this period of time for the ACB to send DCC Alert N25 before taking any further action*.

(*Note that if neither DCC Alert N24 or N25 are received by the User after waiting for the timeout period to expire, then the User should proceed as if DCC Alert N25 had been received.)

After receiving DCC Alert N25 the User should confirm the Failure Scenario by checking the Device Log on the CHF. To do this, the User should send a Service Request *8.9 - Read Device Log* to the CHF and examine the response. If the response contains an entry for the relevant device with a LastCommunicationsDateTime of either 2000-01-01 00:00:00 or 2136-02-07 06:28:15 then this indicates a default "null" value and that communications have not been established with that device.

(If the response shows a valid time in LastCommunicationsDateTime for the relevant device then this indicates Failure Scenario 2 – see below.)

Where communications have not been established, the User should remove the device from the CHF's device log by sending SR8.11 with a RequestType of "Remove". Upon successful completion of this SR8.11, the device's status within the Smart Metering Inventory (SMI) will be returned to "Pending" and the User can start again, if appropriate, with adding the device to the HAN by sending SR8.11 with a RequestType of "Add".

2.14.3 Failure Scenario 2 – "lost" Alerts

Failure Scenario 2 occurs when the device and the CHF actually complete the CBKE process and establish communications, but the second Alert 0x8F12 is not delivered to the ACB (DSP). The ACB (DSP) ultimately times out waiting for this expected Alert, and therefore subsequently sending DCC Alert N25 to inform the User that no such Alert has been received.

The sequence of events for this Failure Scenario is shown in the diagram below.

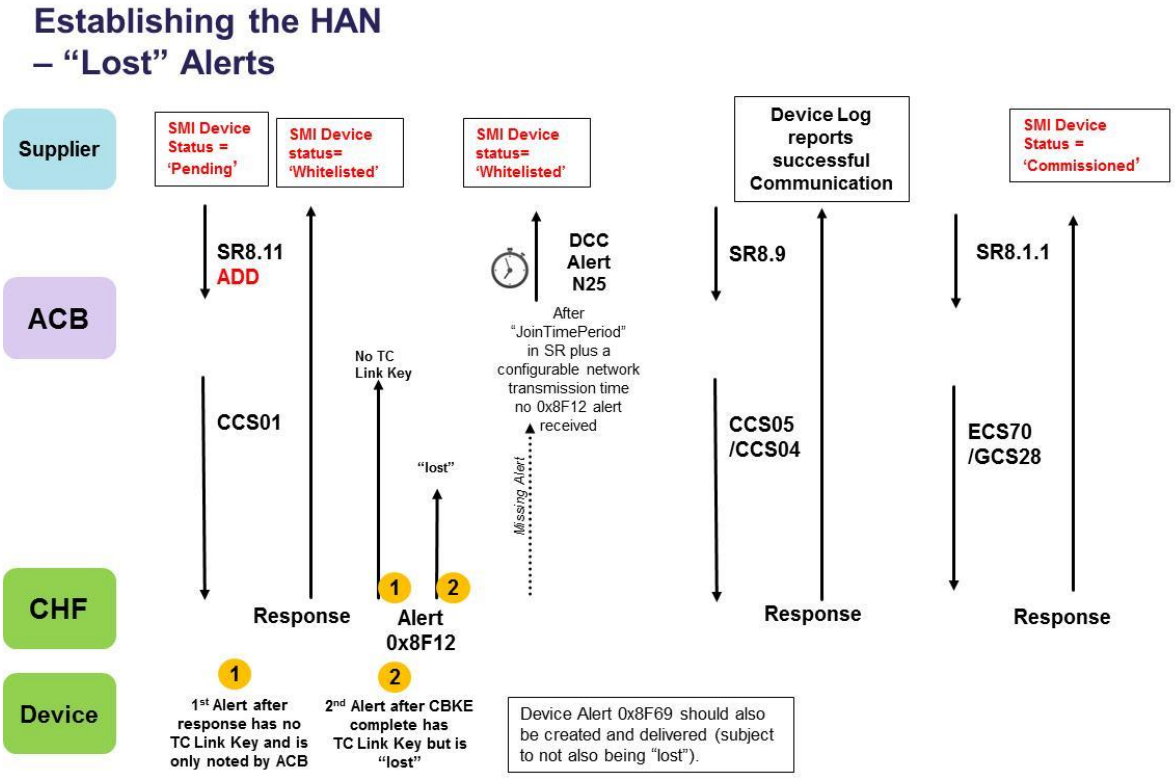

Figure 3. Establishing the HAN – "Lost" Alerts

Initial ACB (DSP) and User behaviour should be the same as for Failure Scenario 1 (since at this point the scenarios cannot be distinguished), so the User should wait for the timeout period to receive DCC Alert N25 before taking any further action and sending *SR8.9 - Read Device Log* to confirm the Failure Scenario.

If the SR8.9 response contains an entry for the relevant device with a valid time which is not one of the "null" values listed in Failure Scenario 1 then this indicates that communications has actually been established with that device.

In these circumstances the User should continue with the next steps to complete the commissioning of the device by sending *SR8.1.1 Commission Device*.

Note that in this scenario it is very important that a User does not send a SR8.11 with a RequestType value of "Remove" for a device that has successfully established communications with the CHF, since that device will not re-establish communications with the CHF without manual intervention.

2.15 Deprecated - Guidance Point 15

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 12, Service Request Narrative, Point 11.

The detail of this guidance point can be found in the appendix.

2.16 Guidance Point 16 – General guidance on DCC Retry and Timeouts for Service Request Processing

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
16	☑	☑	☑	☑	
Guidance Type	Guidance				
Functional Area	All				
Keywords	Retry and Timeout				

Several Users have asked for details on the retry and timeout approach for processing of Service Requests, in order to understand the expected behaviour of the DCC and thus how their own systems should operate.

The principles and rules for retry and timeout are contained in DUIS Section 2.10. This guidance note provides further explanation of this behaviour and also describes how retry and timeout values are configured in the DCC Data Systems.

2.16.1 Retry and timeout processing for requests to devices

The overall approach for retry and timeout for processing of a Service Request being sent to a device is summarised in the diagram below.

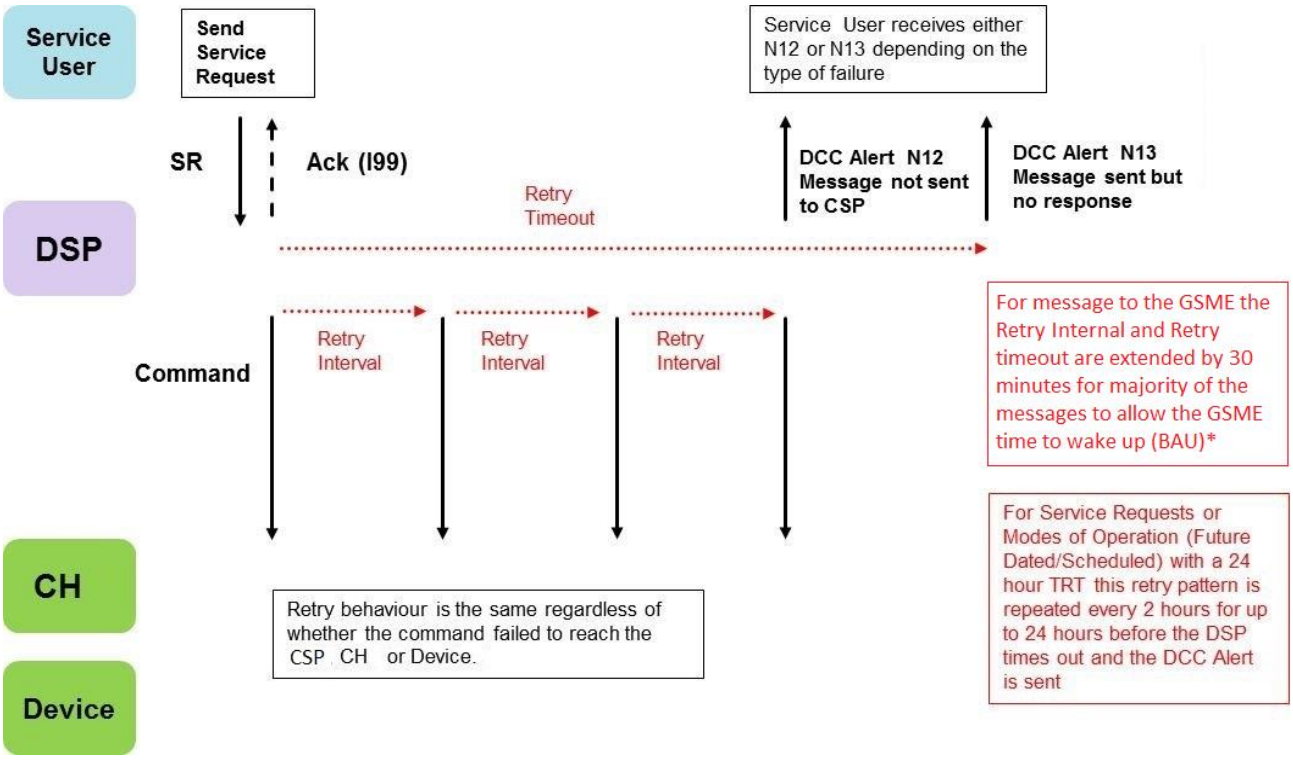

Figure 4. Retry and Timeout Processing of a Service Request

When a User sends a Service Request and receives a successful Acknowledgement (I99) the DSP solution starts a number of timers to handle retry behaviour for the processing of that Request:

- Retry Interval – this is the initial period that the DSP will wait for a Response from the device before re-sending the Request
- Retry Timeout – this is the total period that the DSP will wait for a Response before giving up and marking the Response as “Timed out”

The DSP will re-send the Request up to three times in most cases before finally timing out and at this point a DCC Alert N12 or N13 will be sent to the User. If the Request has failed because it has not been possible to send it to the CSP then DCC Alert N12 is returned as soon as the final attempt to send the Request has failed. If the Request was successfully sent to the CSP but no Response has been received then DCC Alert N13 is returned after the expiry of the Retry Timeout.

For messages sent to the GSME the Retry Interval and Retry Timeout are different to support both the business as usual processing and the I&C process.

- To support business as usual processing, the default GSME Retry Interval and Retry Timeout for the majority of messages are extended by 30 minutes to align to the GSME wake up period.

This 30 minute extension is applied to all retries so, for example, if the first request does not receive a response after 30 minutes (+ the retry interval) then a retry will be sent and will wait for a further 30 minutes (+ the retry interval) for a response to the first retry.

It should be noted that with a default configuration (with Retry Interval set as 1840 and Retry Timeout as 3780) this will mean there is only one retry for a request to a GSME, since the overall request timeout will have expired once the DCC has finished waiting for an answer to the first retry.

If more than one retry is required to a GSME then an SRV specific configuration will be required to extend the Retry Timeout to allow for multiple 30 minute retry intervals.

Please refer to the embedded word document at end of section 2.16.2 on the current settings for DCC Retry and Timeout configuration in the UIT and Production environments.

- **Applicable to CSP South and Central only (not required for CSP North).** To support 'on site' Install and Commission, many meter manufacturers have now implemented a shorter wakeup time. The DSP GSME Retry Interval and Retry Timeout for the CSP South and Central Regions only are changed and set up as below for those SRs identified as used by Suppliers for the 'on site' Install and Commission.

  Retry interval = 300:300:300:1840
  Retry timeout = 3780 e.g. approximately 63 minutes
  (purple text is new retry, green text is pre-existing retry, overall timeout period is unchanged).

It is assumed that the three 5-minute retries is sufficient to mitigate the particular concern that a message is not received first time by a GSME for any reason, (not required for CSP North). This is specifically selected to support the majority of the GSME fast wake up period during I&C.

The remaining retry at 1840 seconds and the overall timeout at 3780 seconds remain in place to support the existing "BAU" behaviour for GSME Retry which assumes a 30-minute wake up cycle.

Please note that the DSP cannot distinguish between an I&C scenario and a subsequent BAU scenario, therefore the 5-minute retry pattern will always be applied and will thus mean that in BAU the Command could be sent up to four times before the GSME wakes up on its 30-minute cycle.

As the result, during BAU

- For Commands which are subject to anti-replay protection, Customers should expect to see anti-replay alerts - likely 0x8F1E, but possibly 0x8F3D or 0x8F3E.
- For Commands which are not subject to anti-replay protection this will mean that all Commands are processed and multiple Responses are returned by the GSME, however current DSP processing behaviour will ensure that only the first Response is delivered to the Customer.

Please note that if the Request being processed has a 24-hour Target Response Time then at expiry of the Retry Timeout the DSP will place the Request on a "back off" queue and will try again in 2 hours' time. At that point, the same Retry Interval and Retry Timeout will be applied again for re-sending the Request.

The DSP will repeat this back off and retry process until the Request is successful or 24 hours has elapsed from either a) the receipt of the original On Demand or Device Future Dated Request, or b) the scheduled activation time of a DSP Scheduled or DSP Future Dated Request.

For Requests sent to Arqiva there is a delivery retry pattern which means the DSP will retry up to 3 times at 40-second intervals if it is unable to deliver the Request to the Arqiva central system. This delivery retry is common to all Requests sent to Arqiva and is controlled via a single configurable item. The SRV specific Retry Intervals defined in this document only apply once a Request has been successfully delivered to the Arqiva system, which means that overall Retry Timeout values must account for the circumstances where this delivery may take up to 120 seconds before it is successful.

2.16.2 Configuration of Retry Interval and Timeout values

DUIS section 2.10 states that "all retry periods and timeout values are configurable within the solution". This configuration is carried out by the DCC and allows the Retry Interval and Retry Timeout to be configured on a per Service Reference Variant basis.

There is a default set of values (which themselves are configurable) which are applied to all Service Reference Variants where no specific configuration is applied. As of writing this Guidance Note (02/11/18), the default set of values are as follows:

Retry Interval = 40:40:40 (seconds)
Retry Timeout = 320 (seconds)

Specific configuration can be applied to individual Service Reference Variants as required. The table overleaf shows some *examples* of individual SRV configuration that in place in the UIT (test) environment at the time of writing. Please note the configuration example at SRV 6.4.1 below applies in CSP (N) only.

SRV	Retry Interval	Retry Timeout	Retries	Notes
6.15.1	40:40:40 (Tef) 60:60:60 (Arq) (1840)	600 (3780)	3 (1)	This is a large GBT command message to the device and therefore extra time must be allowed before re-trying.
4.6.1	40:40:40 (GPF/ESME) 1840 (GSME)	600 (GPF/ESME) 3900 (GSME)	3 (GPF/ESME) 1 (GSME)	This is a large GBT response message from the device. The Timeout must be increased to allow the full response to arrive, but the

				Interval can remain as standard since the Interval timer will be reset as soon as the first GBT response block is received.
6.4.1	180:180:180 (ESME)	600	6	This configuration extends the retry processing to allow an extended time between retries. This is required in circumstances where the SRV is one that may be applied in parallel with other Service Requests.

Table 2. Configuration Example for CSP (N)

DCC shall make the current configuration settings in the UIT and Production environments available to Users on a regular basis.

Please see the attached document for details on the current settings for DCC Retry and Timeout configuration in the UIT and Production environments.

DCC Guidance - Retry and Timeout C

2.16.3 Retry and timeout processing for responses/alerts to Users

When a Response or Alert is being returned to a User, the DCC has a common retry and timeout pattern for delivery of the response/alert.

The DCC will retry up to three times at a configurable retry interval and if the message is not delivered then the DCC will place the message on a retry queue and try again in 2 hours' time (or as soon as the DCC detects that communication to that User is restored). The DCC will continue this process for up to 48 hours before it finally times out and the attempt to deliver the message is abandoned.

The default retry intervals are as follows (in seconds): 10 : 20 : 30.

To avoid Responses/Alerts flooding the User System at the point at which the DCC detects that communication to that User is restored, the User can use HTTP response code 503 in order to inform the DCC to back off and retry at a later point in time. This is detailed in the DUIS section 2.7 as below:

503 Service Unavailable – The User's web server is currently unavailable (because they are overloaded or down for maintenance). The DCC System shall wait for a set period of 15 minutes before resubmitting the response.

2.16.4 Retry and timeout processing for synchronous HTTP requests to DCC

The sending of Service Requests to the DCC is performed using HTTP requests with a synchronous response (i.e. the return of a DCC Acknowledgement for a request to a device or the return of a Service Response for a DCC Only request).

Retry and timeout behaviour for these interactions is the responsibility of the User but it is recommended that the User allow for a timeout of 60 seconds before attempting to send a retry for a particular HTTP request.

If a User sends a retry request while the DCC is still processing the previous instance of that request then the DCC will return an error response with error code E55.

2.17 Guidance Point 17 – Resetting of Network Operator Anti Replay Counter/Remote Party Floor Sequence Number

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
17	☑	☑	☑	☑	
Guidance Type	Guidance				
Functional Area	Install and Commission, Comms Hub Replacement				
Keywords	N42, Originator Counters, Network Operators, *UpdateSecurityCredentials,* RemotePartyFloorSequenceNumber				

2.17.1 Issue Definition

Many Commands defined within GBCS contain “Protection Against Replay” mechanisms in the form of Originator Counter values being stored on a Device for each Remote Party Role allowed to request execution of that type of Command (the ‘Execution Counter’). All these Execution Counters are initially set to zero on Devices at manufacture and are expected to increment over time as Commands are sent to Devices by each remote Party.

Within the DCC Service design, an option exists for installing Suppliers to populate the Network Operator security credential certificate slots (Trust Anchor cells) on Devices with transitional security credentials (either their own Supplier or the Access Control Broker security credentials) to complete the manufacturing, installation and commissioning process on Devices and then subsequently change these transitional security credentials to the correct desired longer term security credentials associated with the identity of the Network Operator for the location where the Device was installed.

In order to operate this option, a Supplier can send to the DCC either *SRV 6.15.1 – UpdateSecurityCredentials(KRP)* or *SRV 6.21 – RequestHandoverOfDCCControlledDevice* to complete this security credentials management process. These DUIS Service Requests allow for Suppliers to request the DCC to create Commands to Devices to change the Security Credentials associated with the Remote Party Role of Network Operator and this will set the Originator Counter value associated to this Remote Party Role to a particular value.

The value that is set by either *SRV 6.15.1 – UpdateSecurityCredentials(KRP)* or *SRV 6.21* for the Originator Counter for the new RemotePartyRole is important as the new Remote Party (e.g. Network Operator) will have no knowledge of the value set by these commands, but they need to be able to use this new Originator Counter value to increment from for all their Originator Counter values used in any subsequent SRV 6.15.1 they send to the Device. If the Network Operator does not know the Originator Counter value that has been set on the Device when the security credentials have been updated, there is a risk that any Originator Counter that they use in any subsequent Service Requests / Commands issued to a Device will be lower than the Originator Counter value currently set on the Device and as a result the Command will not be processed by the Device, as it would fail the Device’s Protection Against Replay mechanisms.

NOTE 1: The DUIS definition of SRV 6.15.1 and SRV 6.21 includes an attribute RemotePartyFloorSeqNumber which allows the Originator Counter to be set to a specific value but this attribute is only applicable to the Supplier Remote Party Role and is not available for use with the Network Operator Role (this is a GBCS constraint). So, the value of the Originator Counter after execution of SRV 6.15.1 or SRV 6.21 to replace the Network Operator security credentials will be the Originator Counter used by the command (either from the Supplier in the case of SRV 6.15.1 or the DCC in the case of SRV 6.21).

NOTE2: The Network Operator only needs to send DCC a subsequent SRV 6.15.1 – UpdateSecurityCredentials(KRP) once the Device has already been handed over (via a Supplier SRV 6.15.1 or SRV 6.21) if they require to swap their own Network Operator security credential / certificates for another set of their own security credential / certificates. In this scenario though, the Originator Counter will again not be reset to the value specified within the RemotePartyFloorSeqNumber of the Network Operator's Service Request but will remain incrementing as they were previously. For avoidance of doubt, there is no way for the Originator Counter stored on a Device associated with the security credential /certificate held within the Network Operator Trust Anchor cell to be updated by the Network Operator via DUIS Service Requests.

Notwithstanding the above, the issue that remains is that the Network Operator needs to know the Originator Counter that is set on the device for the Network Operator Remote Party Role. There are a number of ways to address this as described in the following section.

2.17.2 DCC Guidance

There are 3 options available to address this issue.

i) Option 1: SR 6.24.1 method

The proposed workaround to be followed is for *SRV 6.24.1 - RetrieveDeviceSecurityCredentials(KRP)* to be sent to DCC to request the reading of the details associated with the NetworkOperator Public Security Credentials currently held on the specified Device.

As part of the response to this SRV, it includes the corresponding Originator Counter value ("RemotePartyFloorSeqNumber" data item). This value can then be stored and used by the Network Operator to determine the next Originator Counter value to be used in the next Service Request / Command sent to that Device from that remote Party so that Commands that are subject to "Protection Against Replay" mechanisms on Devices do not fail to process.

ii) Option 2:

Network Operators who are updating Certificates on a device are advised to use a value greater than 4,611,686,018,427,387,904 (0x4000000000000 in Hex) in the Originator Counter field for Service request 6.15.1 - Update Security Credentials (KRP). This number will be always greater than the Originator Counter number set on the Device by the DCC and it will prevent rejection due to the 'Protection Against Anti-replay' mechanism.

iii) Option 3:

The Network Operator currently receives an N42 Alert when the Security Credentials are changed on the device via a Supplier sending SRV6.15.1 or SRV 6.21. This N42 Alert contains an attribute indicating the RemotePartyFloorSequenceNumber (ie Originator Counter) now set on the Device. In DUIS v1.0, this value is however set to match the RemotePartyFloorSeqNumber which was included in the original SRV 6.15.1 or SRV6.21 and, as noted previously, this value is not applied when updating the Network Operator Role.

The RemotePartyFloorSequenceNumber in the N42 Alert has been populated with the Originator Counter used in the SRV6.15.1 or SRV 6.21 and this will therefore provide the correct details of the Originator Counter set on the Device. Network Operators can therefore use this value from the N42 Alert to set their own Originator Counter for use in subsequent SRV 6.15.1 requests.

2.18 Guidance Point 18 – GSME/GPF Wildcard features workaround

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
18	☑	☑	☑	☑	
Guidance Type	Guidance				
Functional Area	All				
Keywords	Gas and GPF Wildcard, 1.1.1, 2.1, IRP537, IRP538				

2.18.1 Issue Definition

TSIRS reference #31.3: DCC to add wildcard workaround to its DUIS MMC guidance note.

This issue only affects GSME and GPF as these use ZigBee interactions to perform data and configuration updates. Issues were found during SIT and UIT testing associated with the consistent execution of wildcard values within dates in two different service requests.

The impacted service requests are:

- SRV 1.1.1 Update Import Tariff: Season Start Date and Special Day Date in relation to the Tariff Switching Table and
- SRV 2.1 Update Prepayment Configuration: Season Start Date and Special Day Date in relation to the Non-Disablement Calendar

Energy Suppliers may be using these wildcard features to reduce the volume of configuration data being sent to devices. Energy Suppliers should also be aware that, whilst DUIS allows it, setting wildcards in Season Start Date or Special Day Date may be rejected by Devices or possibly lead to undefined behaviour. DCC have issued two separate IRPs on this subject (IRP537 and IRP538).

2.18.2 DCC Guidance

DCC Users/Customers should not use wildcard dates i.e. ‘FFFF’ in the impacted service requests data items. All the dates for these particular data items should be populated with explicit days, months and years in the service requests.

After implementation of IRP’s on GPF(IRP538) and GSME(IRP537), DCC Users/Customers will able to use wildcards in the impacted service requests data items where the business target id is GSME or GPF.

However, this guidance remains applicable to DUIS 2 since it continues to support GBCS v1.x devices.

2.19 Deprecated - Guidance Point 19

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 2, SR2.3, section 2.3.1.3, data Item for <DebtRecoveryRatePeriod>, additional description added in the table

The detail of this guidance point can be found in the appendix.

2.20 Guidance Point 20 – Alert storms caused by 0x8F3E

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
20	☑	☑	☑	☑	
Guidance Type	Guidance				
Functional Area	Install and Commission, Device Join/Unjoin, Decommission				
Keywords	Alert Storm, 8F3E, Join/Unjoin				

2.20.1 Overview

Alert 0x8F3E (Unauthorised Communication Access attempted) is raised by a device when it gets a request for data that is protected by Device Based Access Control (GBCS 13.7) from a device that is not authorised to communicate with it. Since alert 0x8F3E is raised for every unauthorised data request, testing has shown that an alert could be sent out as frequently as once every 30 seconds from one device. If multiple devices are simultaneously affected by the same issue, the number of alerts could become significant.

According to GBCS, alert 0x8F3E can be generated by CHF, GPF, ESME, GSME, PPMID and HCALCS.

This guidance point deals specifically with the scenarios that can lead to the generation of alert 0x8F3E. Other alerts are not considered in this guidance point.

2.20.2 General Guidelines

A 0x8F3E alert is raised by a device when that device believes that an unauthorised device on its HAN network is requesting data from it that is protected by Device Based Access Control. The alert storm is caused when the unauthorised device keeps on requesting data and the device from which the data is being requested keeps on raising these alerts. With this in mind, these are some general guidelines with which to adhere:

1. It is recommended that Type 1 and Type 2 devices follow BEIS guidelines on good network behaviour as set out in TS0793.

2. Devices should raise 0x8F3E alerts only on restricted attributes that are under Device Based Access Control (DBAC).

3. It is recommended that Type 1 and Type 2 devices are added to the logs of devices that they will be communicating with as soon as possible.

4. It is recommended that the PPMID is added to the GPF device log first before the GSME is added to the PPMID device log.

5. If a Type 1 device is to be unjoined from a meter or GPF then it must be both removed from the meter/GPF device log and sent an unjoin command.

2.20.3 Alert Scenarios

Several scenarios that can cause an excess of 0x8F3E alerts have been identified during testing. Recommendations on how to avoid 0x8F3E alerts in these different scenarios are set out below.

a) HAN device not in the GPF or meter device log

Scenario

In order for the GPF or the meter to accept requests from Type 1 or Type 2 devices on the same HAN, these Type 1/Type 2 devices must be in the meter or GPF device logs.

It was observed during testing that Type 1/Type 2 devices that were in the same HAN as the meter or GPF but not in their device log would request information from the GPF/ESME. In response, the GPF or ESME would raise an alert every time information was requested from a device that was not authorised to communicate with it.

Guidance

The HAN device should be added to the meter or GPF device log as soon as possible. The Type 1/Type 2 device will then be recognised when it is requesting DBAC data and no alerts should be raised by the GPF or meter.

BEIS has also introduced some guidance on the back-off behaviour that Type 1/Type 2 devices are advised to implement (reference TS0793). This paper recommends that devices should stop requesting data once they have been informed that they are not authorised to make the request, thus significantly reducing the number of alerts.

b) Unjoining a GSME from a GPF

Scenario

In one customer environment, a GSME was removed from the CHF device log by sending SR 8.11 to the CHF. The GSME was also sent SR 8.8.2 to unjoin it from the CHF, but this SR failed. The CHF then started sending alerts and carried on doing so even when the GSME was physically removed from the wall.

Guidance

There were no logs captured in this instance, therefore the informed assumption was made that the GSME kept trying to re-join the network (as it should) but because it was no longer in the CHF device log, the CHF responded by raising alerts.

It is recommended that when a GSME is removed from a network, that GSME should be removed from the radius of the network. If this is not done then alerts will continue to be raised.

c) Two different PPMIDs in a home (multi-supplier scenario)

Scenario

This scenario was set out by a customer in their test environment. In this scenario the starting configuration consists of a Type 1 device (A), an ESME and a GSME all on the same network. The Type 1 device is in the correct device logs and is fully functional.

A new supplier may provide a new Type 1 device (B) to use with the ESME and will add it to the ESME device log. Type 1 device (A) will be removed from the device log of the ESME, but it will remain on the premises.

Type 1 device (A) will continue to attempt to communicate to the ESME. In this case, the ESME will raise 0x8F3E alerts since Type 1 device (A) is no longer in the ESME device log.

Guidance

An unjoin command should be sent to Type 1 device (A) so that it is no longer joined to the ESME, this device will stop requesting data from the ESME and there will be no subsequent 0x8F3E alerts.

The unjoin command is only applicable to Type 1 devices, Type 2 devices cannot be sent this command. If a Type 2 device is removed from the meter or GPF device log and is left on the premises it will cause alerts to be sent from the meter or GPF every time it tries to communicate with the GPF or meter. In this situation it is recommended the Type 2 should be removed from the radius of the network.

d) Clarification of Device Based Control Access

Scenario

Section 13.7 of GBCS sets out the rules for DBAC and states that if an unauthorised HAN device tries to communicate, then the device from which the data is being requested should raise 0x8F3E alerts. However, during testing it was noted that some devices are raising 0x8F3E alerts when non-controlled data, such as the metering device type, is requested.

Guidance

Devices should ensure that they raise 0x8F3E alerts only when data that is under DBAC controls is requested. Entries in table 7.4 of GBCS which do not include references to SMETS attributes in either column H or I are not subject to DBAC. Device manufacturers need to ensure that they adhere to this. A more detailed explanation can be found in TS0832 issued by BEIS.

e) No response when Type 1/Type 2 devices request DBAC data

Scenario

Some Type 2 devices were not implementing the back-off behaviour that was recommended by BEIS in TS0793 because they were not receiving any response when they requested DBAC protected attributes from the GPF. They were expecting to receive a ‘NOT_AUTHORISED’ response before starting to implement this back-off behaviour.

Although this was only seen in GPFs, the same scenario could apply to different ESMEs sending ‘NOT_AUTHORISED’ while other ESMEs could simply not respond.

Guidance

The ‘Metering Device Type’ attribute on the GPF is not under DBAC control. If the Type 1/Type 2 device can read this attribute from the GPF, then it means that this device has successfully joined the HAN. If it is possible to read the ‘Metering Device Type’ but not possible to read data that is under DBAC control, this could indicate to the Type 1/Type 2 device that it is not allowed to access DBAC data and could be a signal to start the back-off behaviour that is advised in TS0793.

f) Devices acquired by customer

Scenario

It is possible for the customer to buy a device that does not adhere to BEIS guidelines issued in TS0793. In this case, the device could continuously interrogate the meter or GPF for attributes even though this device has no access to this data. This would cause the meter or GPF to raise many 0x8F3E alerts.

Guidance

If 0x8F3E alerts are being continually generated because of this device, then it is because this device is requesting DBAC protected data from a meter or GPF that does not have this device in their device log. The supplier could add this device into the device log of the meter or GPF so that it is authorised to access to this data and the 0x8F3E alerts will cease.

The supplier may also ask the consumer to turn the device off.

The supplier is also able to remove this device from the network. The issue in this case is that the device will still have the network key and will be able to communicate. This might cause noise on the network if the device keeps on sending data packets. These packets will have the correct encryption on the network layer but the application level encryption will be wrong. Therefore, it is advised that in device-meter interactions, the meter should not raise alerts when it receives a packet that it can understand on a network-layer level but not on application-layer level. Such a packet should simply be dropped by the meter. In device-GPF interactions these packets are dropped by the GPF.

In Release 4 the GPF will implement a rollover of the network key so that this device will no longer be able to communicate, even on a network-layer level.

g) GPF sets the notification flag before the GPF is in the GSME device log

A number of notification flags (including, but not limited to, "Push All Static Data - Metering Cluster", "Get Snapshot", and "Get Sampled Data") should not lead to the GSME sharing data with the GPF until the GPF has been added to the GSME Device Log. In the case of these flags, the GSME should only send the corresponding Command (e.g. "Get Notified Message") to the GPF once the GPF device ID has been added into the GSME device log.

Until the GSME has received and successfully processed a Remote Party Command

'joining' it to the GPF, it is not allowed to send any SMETS information to the GPF, as per GBCS Section 13.

The GPF does not know whether the GSME has successfully processed such a 'join' Command, and so is required to set various notification flags asking for the GSME to send information to it.

It is only the GSME that knows whether it has been authorised to respond to such GPF requests, where they relate to SMETS information. When the GSME knows that it has NOT YET been authorised to send SMETS information to the GPF (such as snapshots and sampled data), there would seem little point in the GSME asking the GPF to send it requests for such data (via Get Notified Messages sent to the GPF) – the GSME knows it is not authorised to respond. Thus, the GSME can avoid the GPF sending it requests for such unauthorised data by not asking for such requests. This will avoid the resulting unauthorised access Alerts.

Note: Some flags (e.g. "Tunnel Message Pending") need to be actioned by the GSME even before the GPF is in the Device Log. These are not in the scope of this guidance.

h) Join the GSME and the PPMID first before joining the PPMID and the GPF

Scenario

DCC was made aware during the TSIRS alert work shop on 23rd of May 2019, that majority of the PPMID manufacturers will not start requesting DBAC data from the GPF until SR8.7.2 was sent to PPMID adding the GSME into the PPMID device log, and will continue requesting data from the GPF until SR8.8.2 is send to PPMID to remove the GSME from the PPMID device log.

Guidance

It is recommended that

- During I&C of PPMID, the PPMID is added to the GPF device log first before the GSME is added to the PPMID device log as per Prepayment2.0 BPD.

SR	Description	Comment
8.11	Update HAN Log	Add PPMID to HAN Log
	Wait for Alert N24/N25	
8.7.2	Join Device (Non-Critical)	PPMID (Other Device)→GPF(Target Device)
8.7.2	Join Device (Non-Critical)	GSME (Other Device)→PPMID(Target Device)
8.7.1	Join Device (Critical)	PPMID (Other Device)→GSME(Target Device)

- During the PPMID removal, the GSME is removed from the PPMID device log first before the PPMID is removed from the GPF device log.

Please note, the recommended process will not work

- If a type 2 device is joined with the GPF OR

- If the PPMID manufacturer is requesting DBAC data from GPF as soon as it is successfully whitelisted in the CH via SR8.11 and joined ZigBee HAN.

2.21 Guidance Point 21 – DNO's Communication to Meters

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
21	☑	☑	☑	☑	
Guidance Type	Optimising System Behaviour				
Functional Area	Install and Commission, Comms Hub Replacement				
Keywords	Network Operators, N42, N16, 6.15.1				

2.21.1 Issue Definition

During the install and commission process energy suppliers will trigger SR 8.11 (Update HAN Log) to update the Comms Hub device log with the device details. After a successful receipt of Service Response Code I0 from SR 8.11 (Update HAN Device Log, initial setting), the DSP will trigger N16 (Device Identity Confirmation) to the Network Operators.

The N16 contains Import MPxN, Secondary Import MPAN, Export MPAN and ESME Variants.

At this point in time the Network Operator Trust Anchor Cell in ESME and GPF will not have been updated with the Network Operator certificates.

If a Network Operator triggers SR 6.15.1 to update their certificates in the Network Operator Trust Anchor Cell on ESME/GPF at this time then the command will be rejected because the Energy Suppliers have not yet updated the DNO's Certificates on ESME/GPF, hence the device will not recognise the command.

2.21.2 DCC Guidance

During their post installation activities, the energy suppliers will update the DNO's certificates in the Network Operator's Trust Anchor Cell using SR 6.21 (if the device was allocated ACB certificates during manufacture) or SR 6.15.1 (if the device was allocated supplier certificates during manufacture).

After a successful execution of the command, the DSP will send an N42 alert to the DNOs. At this point the ESME/GPF will have Network Operator credentials. Hence the ESME/GPF will recognise any service requests triggered by Network Operators.

Therefore, DNOs must wait for the N42 alert before they trigger SR 6.15.1 to update the DNO's credentials.

DNOs must not trigger SR 6.15.1 after receipt of an N16 alert because the device will not recognise the commands.

2.22 Guidance Point 22 – Device Interop Guidance

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
22	☑	☑	☑	☑	
Guidance Type	Clarification on System Behaviour				
Functional Area	All				
Keywords	Device Compatibility, Device Interoperability				

2.22.1 Issue Definition

DCC R2.0 will introduce the complexity of multiple versions of DUIS, Comms Hubs and Devices. The upgrade sequence of DUIS, Comms Hubs and Devices will result in different compatibility scenarios.

If service users upgrade the Devices before the Comms Hub then there will be a potential interoperability issue between the GSME and GPF, e.g. the Billing Frequency supported by the Comms Hub and the Meters may be different.

If the GPF is not operating in line with GBCS v2.0 (and is still operating to GBCS v1.0, whilst the GSME is operating to GBCS v2.0), then the GPF will not, by definition, support TOM Commands for Use Case GCS25a correctly. Interoperability issues may arise as the Gas Meter will support more billing periods than the GPF and the two devices will not support the same functionality.

2.22.2 DCC Guidance

Comms Hubs are designed to be backward compatible, hence it is recommended to upgrade the Comms Hub before the Device to avoid any interoperability issue.

If a GSME operating in line with GBCS v2.0 is installed within a HAN, then service users should ensure that the associated CH (GPF) is also operating to GBCS v2.0 to avoid any potential interoperability issues.

2.23 Deprecated - Guidance Point 23

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 6 for following Service Request by adding additional clarification for data item <RemotePartyPrepaymentTopUpFloorSeqNumber>

- SR6.15.1, Section 6.15.1.1.2, table 122,
- SR6.21, Section 6.21.1.2, table 170,
- SR6.23, Section 6.23.1.2, table 196,

The detail of this guidance point can be found in the appendix.

2.24 Deprecated - Guidance Point 24

The issue identified within this guidance point has been clarified within the Operational DUGIDS in the following annexes

- Annex 1
  - SR1.2,
    - table 54, data Item <StandingCharge>
    - table 59, data Item <BlockTariff> and <TOUTariff> within the <GasPriceElements>
  - SR1.5, Service Request Narrative, Point 7
- Annex 2
  - SR2.1,
    - Service Request Narrative, Point 4
    - table 5, data Item <EmergencyCreditLimit>, <EmergencyCreditThreshold>, <LowCreditThreshold>, <MaxMeterBalance>, <MaxCreditThreshold> within the <UpdatePrepayConfigElectricity>
    - table 6, data item <DebtRecoveryRateCap> within the <UpdatePrepayConfigGas>
  - SR2.3,
    - section 2.3.1.3 ElecDebtRecovery1 / ElecDebtRecovery2 Item definition, data Item <DebtRecoveryRate>
    - section 2.3.1.4 GasDebtRecovery1 / GasDebtRecovery2 Item definition, data Item <DebtRecoveryRate>

The detail of this guidance point can be found in the appendix.

2.25 Deprecated - Guidance Point 25

The issue identified within this guidance point has been clarified within the Operational DUGIDS in the following annex

- Annex 4
  - SR4.6.1, Service Request Narrative, Point 5
  - SR4.8.1, Service Request Narrative, Point 5

    - SR4.14, Service Request Narrative, Point 4
- Annex 5
    - SR5.1, Service Request Narrative, Point 6

2.26 Deprecated - Deprecated - Guidance Point 26

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 6, SR6.15.2, Service Request Narrative, Point 5

The detail of this guidance point can be found in the appendix.

2.27 Deprecated - Deprecated - Guidance Point 27

The issue identified within this guidance point has been clarified within the Operational DUGIDS Annex 4 for following Service Request

- SR4.4.2 Service Request Narrative, Point 8
- SR4.4.3 Service Request Narrative, Point 8
- SR4.4.4 Service Request Narrative, Point 4
- SR4.4.5 Service Request Narrative, Point 4
- SR4.6.1 Service Request Narrative, Point 9
- SR4.8.1 Service Request Narrative, Point 8
- SR4.14 Service Request Narrative, Point 8
- SR4.17 Service Request Narrative, Point 8

The detail of this guidance point can be found in the appendix.

2.28 Guidance Point 28 – Could non-mandated GBCS alerts be configured off

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
28	☑	☑	☑	☑	
Guidance Type	Clarification on System Behaviour				
Functional Area	All				
Keywords	SR6.22, alert storm, 8014, 8015, 81BB, TSIRS#52.15				

2.28.1 Issue Definition

The production data suggests that some devices send significant numbers of 0x8014(Power Factor Threshold Below) and 0x8015(Power Factor Threshold Ok) alerts to the Network Operator. Similarly, with 0x81BB (Reverse Current) alerts to the Supplier. All 3 alerts are defined as “Non-mandated” alerts by GBCS and so may not be supported by all device manufacturers.

Three questions were asked during TSIRS by DCC Service Users/Customers,

1. Could non-mandated GBCS alerts, such as 0x8014, 0x8015 and 0x81BB, be configured off by customer via SR6.22?

2. Should the meter reject the alert configuration if the meter does not support the “Non-mandated” GBCS alerts?

3. What about manufacture specific alerts not defined by GBCS?

2.28.2 Clarification on DCC behaviour for GBCS defined alerts

For any GBCS defined alerts, the DCC system supports alert configuration via SR6.22 - Configure Alert Behaviour for all alerts as defined by GBCS section 16.2 including both the Mandated and Non-mandated alerts. However, the following limitations should be noted

- Some Meters reject the alert configuration if the specific “Non-mandated” GBCS alerts are not supported by the Meter, as explained in TS1136 - Device configuration of non-mandated alerts.

- Customer could use SR6.22 to config the alert behaviour as defined by the DUIS Schema. The list of the alerts that can be configured are different across different versions of the DUIS. It is not possible for DCC Service User using an older version of DUIS to config an alert which is only supported by a later version of DUIS. The table below shows the different device alerts supported by different DUIS versions.

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x8002	Average RMS Voltage above Average RMS Over Voltage Threshold (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x8003	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 1 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x8004	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 2 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x8005	Average RMS Voltage above Average RMS Over Voltage Threshold on Phase 3 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x8006	Average RMS Voltage below Average RMS Under Voltage Threshold (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8007	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 1 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8008	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 2 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8009	Average RMS Voltage below Average RMS Under Voltage Threshold on Phase 3 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x810D	Combined Credit Below Low Credit Threshold (prepayment mode)	Supplier	ESME GSME	X	X	X
0x810E	Credit Added Locally	Supplier	ESME GSME	X	X	X
0x8119	Emergency Credit Has Become Available (prepayment mode)	Supplier	ESME GSME	X	X	X
0x8020	RMS Voltage above Extreme Over Voltage Threshold (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8021	RMS Voltage above Extreme Over Voltage Threshold on Phase 1 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8022	RMS Voltage above Extreme Over Voltage Threshold on Phase 2 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8023	RMS Voltage above Extreme Over Voltage Threshold on Phase 3 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8024	RMS Voltage above Voltage Swell Threshold (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x8025	RMS Voltage above Voltage Swell Threshold on Phase 1 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8026	RMS Voltage above Voltage Swell Threshold on Phase 2 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8027	RMS Voltage above Voltage Swell Threshold on Phase 3 (voltage rises above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8028	RMS Voltage below Extreme Under Voltage Threshold (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8029	RMS Voltage below Extreme Under Voltage Threshold on Phase 1 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802A	RMS Voltage below Extreme Under Voltage Threshold on Phase 2 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802B	RMS Voltage below Extreme Under Voltage Threshold on Phase 3 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802C	RMS Voltage below Voltage Sag Threshold (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802D	RMS Voltage below Voltage Sag Threshold on Phase 1 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802E	RMS Voltage below Voltage Sag Threshold on Phase 2 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x802F	RMS Voltage below Voltage Sag Threshold on Phase 3 (voltage falls below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8145	Clock adjusted (within tolerance)	Supplier	ESME GSME		X	X
0x8154	Immediate HAN Interface Command Received and Successfully Actioned	Supplier	ESME GSME		X	X
0x8155	Immediate HAN Interface Command Received but not Successfully Actioned	Supplier	ESME GSME		X	X
0x8161	User Interface Command Input and Successfully Actioned	Supplier	ESME GSME		X	X
0x8162	User Interface Command Input but not Successfully Actioned	Supplier	ESME GSME		X	X
0x8168	Supply Disabled then Armed - Activate Emergency Credit triggered	Supplier	ESME GSME		X	X
0x8183	Device joined SMHAN	Supplier	ESME GSME	X	X	X
0x8184	Valve tested	Supplier	GSME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x8085	Average RMS Voltage below Average RMS Over Voltage Threshold (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8086	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 1 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8087	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 2 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8088	Average RMS Voltage below Average RMS Over Voltage Threshold on Phase 3 (current value below threshold; previous value above threshold)	Network Operator	ESME	X	X	X
0x8089	Average RMS Voltage above Average RMS Under Voltage Threshold (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x808A	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 1 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x808B	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 2 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x808C	Average RMS Voltage above Average RMS Under Voltage Threshold on Phase 3 (current value above threshold; previous value below threshold)	Network Operator	ESME	X	X	X
0x808D	RMS Voltage above Extreme Over Voltage Threshold (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x808E	RMS Voltage above Extreme Over Voltage Threshold on Phase 1 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x808F	RMS Voltage above Extreme Over Voltage Threshold on Phase 2 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8090	RMS Voltage above Extreme Over Voltage Threshold on Phase 3 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8091	RMS Voltage above Voltage Swell Threshold (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8092	RMS Voltage above Voltage Swell Threshold on Phase 1 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x8093	RMS Voltage above Voltage Swell Threshold on Phase 2 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8094	RMS Voltage above Voltage Swell Threshold on Phase 3 (voltage returns below for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8095	RMS Voltage below Extreme Under Voltage Threshold (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8096	RMS Voltage below Extreme Under Voltage Threshold on Phase 1 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8097	RMS Voltage below Extreme Under Voltage Threshold on Phase 2 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8098	RMS Voltage below Extreme Under Voltage Threshold on Phase 3 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x8099	RMS Voltage below Voltage Sag Threshold (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x809A	RMS Voltage below Voltage Sag Threshold on Phase 1 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x809B	RMS Voltage below Voltage Sag Threshold on Phase 2 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x809C	RMS Voltage below Voltage Sag Threshold on Phase 3 (voltage returns above for longer than the configurable period)	Network Operator	ESME	X	X	X
0x81A1	Battery Cover Closed	Supplier	GSME	X	X	X
0x81A2	CH Connected to ESME	Supplier	ESME		X	X
0x81A3	CH Disconnected from ESME	Supplier	ESME		X	X
0x81A4	Close Tunnel Command Rejected	Supplier	ESME GSME	X	X	X
0x81A5	Communication From Local Port (e.g. Optical)	Supplier	ESME GSME	X	X	X
0x81A6	Customer Acknowledged Message on HAN Device	Supplier	ESME GSME	X	X	X
0x81A7	Debt Collection Completed - Time Debt 1	Supplier	ESME GSME	X	X	X
0x81A8	Debt Collection Completed - Time Debt 2	Supplier	ESME GSME	X	X	X
0x81A9	Debt Collection Completed - Payment Debt	Supplier	ESME GSME	X	X	X
0x81AA	Emergency Credit Exhausted	Supplier	ESME GSME	X	X	X
0x81AB	Emergency Credit Activated	Supplier	ESME GSME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x81AC	Error Measurement Fault	Supplier	ESME GSME	X	X	X
0x81AD	Error Metrology Firmware Verification Failure	Supplier	ESME GSME	X	X	X
0x81AE	Error Non Volatile Memory	Supplier	ESME GSME	X	X	X
0x81AF	Error Program Execution	Supplier	ESME GSME	X	X	X
0x81B0	Error Program Storage	Supplier	ESME GSME	X	X	X
0x81B1	Error RAM	Supplier	ESME GSME	X	X	X
0x81B2	Error Unexpected Hardware Reset	Supplier	ESME GSME	X	X	X
0x81B3	Error Watchdog	Supplier	ESME GSME	X	X	X
0x81B4	Excess Gas Flow Beyond Meter Capacity	Supplier	GSME	X	X	X
0x81B5	Flow Sensor Detects Air in Gas Flow	Supplier	GSME	X	X	X
0x81B6	Flow Sensor Detects Reverse Flow of Gas	Supplier	GSME	X	X	X
0x81B7	Incorrect phase sequencing	Supplier	ESME	X	X	X
0x81B8	Incorrect Polarity	Supplier	ESME	X	X	X
0x81B9	Meter Cover Closed	Supplier	ESME GSME	X	X	X
0x8010	Over Current	Network Operator	ESME	X	X	X
0x8011	Over Current L1	Network Operator	ESME	X	X	X
0x8016	Over Current L2	Network Operator	ESME	X	X	X
0x8013	Over Current L3	Network Operator	ESME	X	X	X
0x8014	Power Factor Threshold Below	Network Operator	ESME	X	X	X
0x8015	Power Factor Threshold Ok	Network Operator	ESME	X	X	X
0x81BA	Request Tunnel Command Rejected	Supplier	ESME GSME	X	X	X
0x81BB	Reverse Current	Supplier	ESME	X	X	X
0x81BC	Strong Magnetic Field Removed	Supplier	ESME GSME	X	X	X
0x81BD	Supply Connect Failure (Valve or Load Switch)	Supplier	ESME GSME	X	X	X
0x81BE	Supply Disabled Then Locked - Supply Tamper State Cause	Supplier	ESME GSME	X	X	X
0x81BF	Supply Disabled Then Armed - Uncontrolled Gas Flow Rate	Supplier	GSME	X	X	X
0x81C0	Supply Disconnect Failure (Valve or Load Switch)	Supplier	ESME	X	X	X
0x81C1	Terminal Cover Closed	Supplier	ESME	X	X	X
0x81C2	Tilt Tamper Ended	Supplier	ESME	X	X	X

Code	Meaning	Remote Party	Device	DUIS1	DUIS2	DUIS3
0x81C3	Tilt Tamper	Supplier	ESME	X	X	X
0x81C4	UTRN Manual Entry Suspended	Supplier	ESME	X	X	X
0x81C5	UTRN rejected as locked out	Supplier	ESME	X	X	X
0x81A0	Smart Meter Integrity Issue – Warning	Supplier	ESME GSME		X	X
0x81C6	Clock not adjusted (outside tolerance)	Supplier	ESME GSME			*

*0x81C6 are supported by GBCS3.2 and could be returned by the device. However the configuration of this alert is not yet supported by any version of DUIS schema. It is planned to be supported on or before Nov. 2020 release subject to approval of relevant SEC MOD.

2.28.3 Clarification provided for manufacture specific event/alerts not defined by GBCS

DCC system does not support configuration of any manufacture specific events/alerts that are not defined by GBCS.

On receipt of any manufacturer specific, non-GBCS device alerts, DSP will still forward to the DCC service user. The P&C parse will still populate the relevant field such as <AlertCode>, <GBCSHexAlertCode> according to device alert GBCS payload, however the <AlertDescription> will be populated as “UNKNOWN – not defined in GBCS”.

When using SR6.13 Read Event Or Security Log, DSP will still forward the device response including any manufacturer specific, non GBCS events/alerts to the DCC service user. The P&C parse will

- populate the data item <LogCode> and < OtherInformation> according to the device GBCS response payload,

- the < LogMeaning> will be populated as “UNKNOWN – not defined in GBCS” if present in the GBCS payload.

- The <OtherInformationLogMeaning> element is only populated for event codes 0x8161 and 0x8162. For these two codes (0x8161/0x8162), P&C will try to match ‘otherInformation’ value to the values from Table 16.4 of GBCS (User Interface Command Codes) and it will fail if it doesn’t match.

When using SR6.2.10 Read Configuration (Event and Alert Behaviours), DSP will still forward the device response including any manufacturer specific, non GBCS events/alerts to the DCC service user. However, the P&C parse result will ignore all such events/alerts in the parse result (The P&C will log to the application log the Unknown Alert Event code present in the response).

2.28.4 Guidance on disabling the GBCS defined alerts/events

If a Service User wishes to disable the device alerts/events, based on the clarification provided above, it is recommended that they:

- Step 1: check whether the specific alert/event is a GBCS defined alert or not, so is it included in GBCS Table 16.2;

- Step 2: check whether the specific alert/event is supported by the DUIS schema that the User is using

- Step 3: where the alert/event is marked as 'non-mandated' in GBCS Table 16.2, and supported by the DUIS schema that the User is using, read the alert/event configuration via SR6.2.10 to confirm whether or not the specific alert is supported by the device as detailed below which is aligned with TS1136 BEIS clarification:

    - ***Gas Suppliers*** should only configure, using SR6.22 (GCS20), GSME Event Codes that are supported by the GSME. If suppliers only configure those returned in SR6.2.10 (GCS20r) Responses from that GSME, they will meet this criteria.

    - ***Import Suppliers*** should only set, using SR6.22(ECS25a/1/2/3), for Event Codes that they know the ESME supports, so the corresponding code is in at least one of the following sets:
        - Mandated codes;
        - Included within the SR6.22 (ECS25r1) response at least once within data item <ElectricitySupplierAlerts>, <ElectricitySupplierHANAlertSettings>, <ElectricitySupplierAlarmSettings> or <ElectricitySupplierLoggingSettings>;
        - Codes which the Supplier knows via another route is supported by the ESME.

    - ***Network Operators*** should only set, using SR6.22 (ECS25b3), for Event Codes that they know the ESME supports, so the corresponding code is in at least one of the following sets:
        - Mandated codes;
        - Included within the SR6.22 (ECS25r2) response at least once within data item < NetworkOperatorESMECommon> or <ElectricityNetworkOperatorLoggingSettings >;
        - Codes which the Network Operators knows via another route is supported by the ESME

The above is regardless of whether the Supplier / Network Operator is configuring all alerts "off" or configuring some alerts "on" and others "off". Note that Network Operators are unknown to GSME and so cannot configure any GSME Alerts / Events.

2.29 Guidance Point 29 – How to interpret the high value of 16,777.215 m^3 in the SR4.8.1 response

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
28	☑	☑	☑	☑	
Guidance Type	Clarification on Device Behaviour				
Functional Area	Meter Reading				
Keywords	SR4.8.1, TSIRS#55.8				

2.29.1 Issue Definition

In rare cases, SR4.8.1 response may contain an exceptional high half hour measurement value of 16,777.215 m^3This guidance note provides explanation of how the 16,777.215 m^3 (0xFFFFFF in hex) half-hourly energy values by the GPF should be interpreted in the HAN and WAN. In summary, the 0xFFFFFF half-hourly energy value is used to specify missing data, not a literal value.

2.29.2 ZigBee Specified HAN Behaviour

On the HAN, when periodic information is transferred, invalid samples should be marked as 0xFFFFFF. (Ref: 07-5356-21-zse-zigbee-smart-energy-profile-specification_14June2017 section D.3.2.3.1.8 GetSampledDataResponse Command).

7379 **Samples (mandatory):** Series of data samples captured using the interval specified by the
7380 *SampleRequestInterval* field in the *StartSampling* command. Each sample contains the change in
7381 the relevant data since the previous sample, except for Instantaneous Demand where each (signed
7382 24-bit) sample is a snapshot of the current value. Data is organised in a chronological order, the
7383 oldest sample is transmitted first and the most recent sample is transmitted last. Invalid samples
7384 should be marked as 0xFFFFFF.

PPMID/IHDs shall not interpret 0xFFFFFF samples from a GetSampledDataResponse as valid data and shall not display such data on their screens.

2.29.3 GBCS and MMC schema specified WAN Behaviour

On the WAN, there is a reference in the SEC-Schedule-8-GBCS-V2.0-4 to refer to the ZigBee specification for the interpretation of the samples as shown highlighted below.

GCS17 Read GSME Profile Data Log
Normal response

Element	Meaning
Encrypted ZCL payload	
SampleID (UINT16)	*0 = Profile Data Log*
SampleStartTime (UTCTime)	*Sample Start Time*
SampleType (ENUM8)	*0 = Consumption Delivered*
SampleRequestInterval (UINT16)	*Time in seconds between samples*
NumberOfSamples (UINT16)	*1-19056*
Samples (Refer to ZigBee spec)	*Profile Data Log: Array of UINT24*

P&C will convert all samples (up to 19056) part of the SR4.8.1 (GCS17) response from binary format into a decimal format as defined by the MMC and its schema as below (extract from MMC 3.0 table 73).

PrimaryValue	The total gas imported in this 30 minute period. Multiplier (value of 1) and divisor (value of 1000) applied as defined in GBCS An invalid half-hourly sample may result in a 'high value' of 16,777,215 (0xFFFFFF)	xs:decimal	m3	Encrypted

2.29.4 DCC Guidance

For SR4.8.1 gas response, DCC Service Users should treat the value of 16,777.215 m^3 as an invalid value. This value should not be used as part of any calculations or estimations.

2.30 Guidance Point 30 – non-zero Disablement Thresholds

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
28	☑	☑	☑	☑	
Guidance Type	Note to Customer on Device Behaviour				
Functional Area	Prepayment				
Keywords	SR1.6, TSIRS#55.7				

2.30.1 Issue Definition

SMETS, GBCS and DUIS allows disablement thresholds to be set as negative, zero and positive values. The required behaviour in relation to the Disablement Threshold is the same regardless of whether its value is zero or not.

The supplier representatives at TSIRs have not yet identified a business scenario where they plan to use a value other than zero for Disablement Threshold. As a result device manufacturers have not had an opportunity to test all permutations.

This was discussed at TSIRS and, Manufacturers and Suppliers indicated there could be a range of unpredictable behaviour if the non-zero disablement threshold is set.

2.30.2 DCC Guidance

Customer are advised, that if a Disablement Thresholds are set at value other than zero then devices may not behave consistently as expected.

2.31 Guidance Point 31 – Future dated COTs

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
28	☑	☑	☑	☑	
Guidance Type	Clarification on System Behaviour				
Functional Area	All				
Keywords	SR3.2, TSIRS#56.1				

2.31.1 Issue Definition

The CHTS ‘Restrict GPF Data’ Command (SR 3.2 "Restrict Access For Change Of Tenancy") is to restrict access to all items of Personal Data stored in the GPF which have a UTC date and time

stamp prior to the date and time stamp specified in the Command (the date and time the new tenancy starts).

SR3.2 could be DSP future-dated but cannot be future-dated by the device. There are two timestamps which can be used within the SR3.2 command, namely:

SR3.2 Data Item associated with a Timestamp	**Usage**	**Comments / impact to supplier**
ExecutionDateTime	The UTC date and time the DCC Service User requires the command to be executed on the Device ID	Non-Mandatory value. This could be used where the Service Request is to be executed at a future date and time.
RestrictionDateTime	*The UTC date and time the DCC* Service *User requires the restriction to be applied from (so no personal data held in the device for a period prior to this date and time will be available over the HAN / via a User Interface)*	Mandatory. Key Point: The new tenants moving into the property won't see any historical data until the RestrictionDateTime is reached.

The *RestrictionDateTime* field within the Service Request 3.2 may be in the future or in the past, and the Command will be executed on receipt. The restriction is applied as soon as the command is executed, which means that the current householder will be restricted from access to their own data for a SRV3.2 delivered now even if the restriction date is in the future.

2.31.2 DCC Guidance

DCC Service Users are advised not to set an execution date prior to the restriction date if the restriction is not intended to apply to the current tenant.

There are 2 possible courses of action for the service user.

1. If the Supplier wants an immediate execution when the new tenancy has already started, it is recommended for the Supplier to build the SR3.2 without a specified *ExecutionDateTime*, and ensure *RestrictionDateTime* is in the past.

2. If the Supplier wants a future dated execution, because the new tenancy is starting at a future date, it is recommended for the Supplier to build SR3.2 with a specified *ExecutionDateTime* matching the *RestrictionDateTime* and both set to the selected future date for delivery of this Service Request.

The above Guidance is already included in the Operational DUGIDS 3.0 (July 2019) for SR3.2 as below

> The restriction date in the Service Request may be in the future or in the past, and the Command will be executed on receipt. The restriction is applied as soon as the command is executed, which means that the current householder will be restricted from access to their own data if the restriction date is in the future. DCC Service Users are advised not to set an execution date prior to the restriction date if the restriction is not intended to apply to the current tenant.

2.31.3 Impact if Guidance is not adopted

The current householder will be restricted from access to their own data from the delivery of a Service Request 3.2 onwards if the *RestrictionDateTime* is in the future.

2.32 Guidance Point 32 – What is the recommendation for setting up a schedule

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
32	☑	☑	☑	☑	
Guidance Type	Optimising System Behaviour				
Functional Area	Schedule Service				
Keywords	Schedule, 5.1				

2.32.1 Customer enquiry

A Customer has made an enquiry related to the Schedule Service (SR5.1) as below

- What is the DCC recommendation for setting up a Schedule Service?
- Is there any benefit for the customer staggering the population of the effective date/time?

2.32.2 Understanding the current DCC design

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

- DSP creates a worklist containing all the scheduled Service Request for each targeted device per service user with a run time (as specified by the SR5.1) against each of the work item
- DSP then works through the list, picking up any item from the list which has a run time in the past at an agreed rate.
- The agreed rate 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.
- The selection will not prioritise any SU over another, and are distributed across ALL service users
    - Select all records where execution time is in the past
    - Order by execution time
    - Select the N records with the earliest execution time
- On Demand message for any User will always take precedence and will affect the delivery profile of requests/responses.
- It is not guaranteed for any even spread across a particular service request or User.

2.32.3 DCC Guidance

Based on the above DCC design, the DCC recommendation is as below:

- There is no benefit for Users 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 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.
- Service Users should expect to receive the device response between the scheduled time and 6am, however it is worth noting that the DCC has a 24-hour SLA to deliver a schedule and, especially in times for unexpected outage, the delivery times may change during the day

2.33 Guidance Point 33 – what happen to a suspended device

Guidance Point Number	DUIS 1	DUIS 2	DUIS 3	SMETS2	SMETS1
33	☑	☑	☑	☑	☑
Guidance Type	Optimising System Behaviour				
Functional Area	Installation and Commission, OTA				
Keywords	I&C, OTA, SR12.2, CPL Suspended, SR8.11, SR6.21, SR8.1.1, SR11.1, SR11.2, SR11.3, SR6.23				

2.33.1 Customer enquiry

SSC has made a decision to remove some of the old device Models / Firmware Versions from the Certified Product List (CPL) after the CPA certification expired, this will mark the relevant CPL entry with a status of “Removed”.

As a result, the SMI device status which has a Device Model / Firmware Version associated with the “removed” CPL entry will change to be in a “Suspended” state and SR8.2 will respond the Device Status as “Suspended”.

Customers have made enquiries on whether they could still I&C, communicate with or perform OTA on those devices in a “Suspended” state.

2.33.2 Understanding the current DCC design

The response to the Customer enquiry will depend on the SMI Status the Device held immediately prior to its Suspension.

Not yet pre-notified

For those devices still in the supply chain (for example in the warehouse) and not yet pre-notified, after the Device Model / Firmware Version is removed from the CPL, it will not be possible to pre-notify those devices via SR12.2. SR12.2 will fail the CPL validation with error code “E120203” returned to service user, as specified by DUIS section 3.8.122.3 below

E120203	The Device Type / Manufacturer / Model / Firmware Version data specified by the User do not match the values contained on the Certified Products List (CPL) that have been approved for use.

In conclusion, it will not be possible to I&C a device with Device Model / Firmware Version removed from the CPL which are not yet pre-notified.

Pending

For those devices already pre-notified but still in the “Pending” state, after the Device Model / Firmware Version is removed from the CPL, the device status will become “Suspended”.

It will not be possible to whitelist those devices in the HAN via SR8.11 UpdateHANDeviceLog – add. SR8.11 will fail the status validation as the status is not "Pending" any more, and error code "E081105" will be returned to service user, as specified by DUIS section 3.8.109.3 below

E081105	The status of the Device being added to the Whitelist is not 'Pending' or 'Whitelisted'

In conclusion, it will not be possible to I&C a device with Device Model / Firmware Versions removed from the CPL which are still in the "Pending" stage.

Please note "Whitelisted" is a temporary stage, and the device status will either move to "InstalledNotCommissioned" for successful ZigBee join or revert back to "Pending" for failed ZigBee join after the join window timeout. It will be a very rare condition that a Device Model / Firmware Version is removed from the CPL while the device status is "Whitelisted". However, the same principle applies, SR8.11 will also fail the status validation and will be rejected by DSP with error code "E081105".

InstalledNotCommissioned & Commissioned

For those devices already in the "InstalledNotCommissioned" or "Commissioned" state, after the Device Model / Firmware Version is removed from the CPL, the device status will become "Suspended".

- All Non-Critical Command targeting "Suspended" device will be rejected by DSP for failing E5 check with exception of
    - 8.2 (Read Inventory) [1]
    - 12.1 (Request WAN Matrix)
    - 11.1 (Update Firmware)
    - 6.23 (Update Security Credentials (CoS))
- All Critical Command or Signed Pre-Commands will still be able to be send to a "Suspended" device

The detail of the E5 validation is defined in DUIS section 3.2.4 "Verify that the Service Request or Signed Pre-Command is applicable to the Device status".

Please note

- while the meter was in the "InstalledNotCommissioned" stage at the point of CPL suspension, if this meter still has the ACB certs in the trust anchor cell, as SR6.21 is also a non-critical command, it will not be possible to load the supplier certs onto meter via SR6.21 and it will fail the E5 validation. As a result all further service request will be rejected by the meter as it will fail the MAC and signature validation.
- SR11.2 is also a Non-Critical Command and will be blocked by the DSP E5 validation. This means following successful activation (SR11.3), if the activation result is not received by DSP for any reason, the device will remain in "Suspended" status, and there is no recovery method to move this device out from "Suspended" status until a further OTA of a newer version.

[1] E5 check does not apply to SR8.2 and SR12.1 regardless which device status it is

In conclusion, it will not be possible to send any non-Critical command to an "InstalledNotCommissioned" or "Commissioned" device after it becomes "Suspended" with the exception of OTA and Change of Supplier

Other notes on the DCC current design in relation to "Suspended" Device

1. If a Device ceases to be Suspended as a result of the Device Model / Firmware Version being added to the Certified Product List or of the Firmware Version being activated on the Device, the DCC Data Systems will change the SMI Status of that Device to the status it held immediately prior to its Suspension

2. For 6.23, and SR11.1 and SR11.3, As an exception, the Authorisation Check associated to E5 allows the Device Status to be 'Suspended', but successful completion of the Service Request doesn't change the Device Status in the Smart Metering Inventory

3. Following receiving response of SR11.2 reading of firmware version or successful firmware OTA activation (SR11.3) result, if the Firmware Version is no longer valid on the CPL, the SMI Firmware Version will be updated, but the Device Status will not be set to 'Suspended'. In this case DCC Alert N50 will be sent to the Responsible Import Supplier as a warning.

2.33.3 Summary of above note

	Meter status at point of Firmware CPL suspension	OTA capable?	notes
1#	Not yet pre-notified	NO	**can NOT** be pre-notified. SR12.2 will fail the CPL check, and error code "E120203" will be returned to service user
2#	Pending (already pre-notified)	NO	**can NOT** be whitelisted. SR8.11 will fail the status validation, and error code "E081105" will be returned to service user.
3#	"InstalledNotCommissioned" but ACB certs in the meter	No	**can NOT** load supplier certs onto meter, SR6.21 will fail the E5 validation for non-critical command
4#	"InstalledNotCommissioned" and supplier certs in the meter	YES	Will be able to commission with SR8.1.1, and then follows with SR11.1 and SR11.3 for OTA
5#	commissioned	YES	Will be able to issue SR11.1, SR11.3 for OTA and SR6.23 for Change of Supplier. However other non-critical command will be rejected by DCC/DSP system.

In conclusion, after a device model/firmware is suspended from CPL, it is not possible
- to I&C a device which is not yet fully I&Ced
- to send any NON-critical command with exception of OTA and Change of Supplier

3 Appendix – Deprecated Guidance

3.1 Guidance Point 1 – Time value to be set within Service Requests

The issues identified within this guidance have been resolved by DUIS 2.0.

Guidance Point Number	DUIS 1	DUIS 2
1	☑	
Guidance Type	Guidance	
Functional Area	All	
Keywords	Time, Second, DateTime	

A mismatch has been identified between the DUIS time definition and the GBCS time definition.

Mismatch

- *DUIS datetime allows precision of 100th of seconds, in the service request, the CurrentDateTime filed including 100ths of second [20160718152913.01Z]*
- *GBCS states that GeneralizedTime elements in GBCS (3.3.7) only has a resolution to the nearest second. [20160718152913.00Z],*

The issue that this causes is that the CORRELATE functionality within the DCC's Parse and Correlate software is failing because DUIS datetime allows precision of 100th of a second whilst GBCS limits the precision to seconds. This fails the "semantically the same" check and CORRELATE returns an error.

Some GBCS Commands, but not all depending on the underlying protocol being used (DLMS, ZigBee or ASN.1), have a restriction of whole seconds and so in these cases any value other than 00 in the 100ths of seconds will not be semantically the same and will fail correlate.

The full answer is that time definitions within GBCS depend upon the underlying protocol of the message sent to the device as it appears that each supports a different time granularity within their Commands.

***ZigBee timestamps:** ZigBee resolution is in whole seconds. ZigBee UTC Time is the number of seconds since 2000-01-01T00:00:00Z, so it has no precision for fractional seconds.*

- *DSP systems via the Transform component do not currently 'round' any 100th value provided up or down, the fractional values are truncated and ignored*
- *Correlate will ignore the 100th of the second's value in the DUIS Pre–Command and therefore there is no danger of correlation failure.*

***DLMS/COSEM timestamps:** DLMS/COSEM support 1000th of seconds, and DUIS time definition supports 100th of seconds, thus if time contains 1000th seconds, the remaining fraction of the COSEM value will be ignored.*

- *DSP systems via the Transform component will only populate the COSEM item down to 100th of seconds, thus no danger of correlation failure.*

ASN.1 timestamps: *ASN.1 supports GeneralizedTime in 100th seconds, however GBCS defines time as limited to whole seconds.*

- *DSP systems via the Transform component will truncate the time data item received in the DUIS Service Request to create a GBCS command with a resolution of one second, i.e. any time value using 100th seconds will be ignored.*

- *Correlate will currently fail if DUIS datetime contains fractions of seconds (issue ref #10157)*

- *Proposed solution to this ASN.1 issue identified - Users to ONLY submit time values in whole seconds and always set the 100th of second's values in the DUIS time format with a value of "00" within the DUIS Service Request, therefore allowing correlate to work successfully.*

3.1.1 *DCC Guidance (for all messages regardless of underlying message protocol)*

The workaround option is to issue guidance to all Users to ONLY submit time values in whole seconds and always set the 100th of second's values in the DUIS time format with a value of "00" within the DUIS Service Request and therefore allow Correlate to work successfully.

In reality, continuing to submit actual time values of 100ths of seconds for ASN.1 messages will be meaningless to Users as the DSP transform function will just round these value to whole seconds.

DCC recognises that strictly speaking this workaround is a bit more restrictive than required but it is also considered the easiest guidance that DCC can offer to Users for consistency across all Service Requests sent by Users and Commands created by the DCC, without getting too granular and making the proposed workaround more difficult for Uses.

- *Note – In reality, for full User information, only Service Requests associated with GBCS Use Cases that result in the creation of an ASN.1 Command as defined by GBCS, have the direct issue as described above and this is the scenario where using a single restricted value of 00 to represent whole seconds is important.*
  - *Users can therefore if they wish to continue to send time values within Service Requests representing 100th of a second precision for which the associated GBCS Use Case results in the creation of an 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.*

3.1.2 *DUIS 2.0 changes*

The following text is an extract from the DUIS v2.0 documentation. The proposed Updates to DUIS section 2.3 can be seen below in RED text.

2.3 Time

The DCC User Interface and DCC Systems shall use UTC (Coordinated Universal Time) for all Requests and Service Responses. All references to time or date and time in this DUIS are references to UTC. This shall be indicated to the DCC 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>09:30:10.12Z</Time>

xs:dateTime data types shall be formatted as

<DateTime>2015-12-25T09:30:10.12Z</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 populated by a User for the 100th of a second precision 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 an 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.

3.2 Guidance Point 2 – Reading BillingCalendar date time values and potential PARSE error

Guidance Point Number	DUIS 1	DUIS 2
2	☑	☑

Guidance Type	Optimising System Behaviour
Functional Area	Meter Reading
Keywords	Meter Read, BillingCalendar, Default Value, SR6.2.3

DUIS SR6.2.3 - ReadDeviceConfiguration(BillingCalendar) allows a User to read Device configuration of billing calendar data values that are currently held on Gas and Electricity meters. The Service Response to this SR includes the Billing Time, Billing period start date and time.

Evidence from testing the DCC solution with devices indicates that some ESME and GSME manufacturers hold default billing calendars that contain undefined wildcard values. The date and time values returned by ESME or GSME devices may contain undefined (FF) values for the date and time as wildcards, which is allowable as per DLMS but time in MMC is defined as per xs:time and doesn't accept the undefined values in the time. The result is that if wildcard dates are included within the GBCS Response, Parse fails with "Cannot convert time with undefined fields to XMLGregorianCalendarTime."

The BillingCalendar is set using DUIS SR6.8 - UpdateDeviceConfiguration(BillingCalendar). This does not support the use of wildcards within datetime to set the billing calendar and therefore the GBCS response expected from Devices is not expected to return wildcard datetime values.

DCC is not recommending any update to the DCC's Parse and Correlate software to cater for this error but instead a workaround solution is proposed.

3.2.1 *Proposed Guidance*

This scenario and potential error should only exist when no billing configuration has been set on an ESME or GSME device.

***Users are advised not to READ BillingCalendar from ESME or GSME prior to being SET using a DUIS Service Request**.*

Setting the BillingCalendar within and ESME or GSME should be one of the first Service Requests sent by a Supplier within the Install and Commissioning process so this is not expected to have a significant impact upon the User's business process.

3.2.2 *Impact if guidance is not adopted*

There is a risk that manufacture default values are returned by the Device which are not expected and not supported by the PARSE functionality within the DCC's Parse and Correlate software and an error is returned to the User.

3.3 Guidance Point 3 – Reading Tariff data and potential PARSE error

Guidance Point Number	DUIS 1	DUIS 2
3	☑	☑
Guidance Type	Optimising System Behaviour	
Functional Area	Tariff Update	
Keywords	ReadTariff, Default Value, SR4.11.1, SR4.11.2	

DUIS SR4.11.1 - ReadTariff(PrimaryElement) and DUIS SR4.11.2 - ReadTariff(SecondaryElement) allow a User to read the Tariff for the requested elements that are currently held on an ESME or GSME (as appropriate).

Evidence from testing the DCC solution with devices indicates that some ESME manufacturers hold a default season name within the device which is set during manufacture.

If this value is read by a DUIS Service Request, the Service Response to SR 4.11.1 returns an OCTET-STRING of [0x0000000000000001] for the season name, in hex code format. This hex code within an octet-string is not expected by the PARSE functionality within the DCC's Parse and Correlate software and as a result an error is returned to the User in this scenario.

DLMS Blue book 12 does not explicitly specify that an octet-string must be characters. The factory default value setting for the current season name is in hex code, but it also supports characters.

DCC is not recommending any update to the DCC's Parse and Correlate software to cater for this error but instead a workaround solution is proposed.

3.3.1 *Proposed Guidance*

This scenario and potential error should only exist when no tariff has been set on an ESME or GSME device.

Users are advised not to READ the Tariff from an ESME or GSME prior to a Tariff being SET using a DUIS Service Request.

Setting a Tariff on an ESME or GSME should be one of the first Service Requests sent by a Supplier within the Install and Commissioning process so this is not expected to have a significant impact the User's business process.

3.3.2 *Impact if guidance is not adopted*

There is a risk that manufacture default values are returned by the Device which are not expected and not supported by the PARSE functionality within the DCC's Parse and Correlate software and an error is returned to the User.

3.4 Guidance Point 4 – Critical Commands to Devices with an SMI status of "Pending" - HTTP 500 Response

The issue identified within this guidance point has been resolved through the use of an N12 alert for all versions of DUIS. This solution has been implemented by DSP and is in Production.

Guidance Point Number	DUIS 1	DUIS 2
4	☑	
Guidance Type	Clarification on System Behaviour	
Functional Area	Install and Commission	
Keywords	HTTP 500, Pending Status, Install, Commission, 8.1.1	

3.4.1 *Background and problem*

- *During User Testing a User's SR8.1.1 is being rejected with an HTTP 500 response.*
- *As per DUIS definition an HTTP 500 response implies "Internal Server Error – Indicates that the DCC Systems are malfunctioning."*
  - *This sets an expectation of ownership for issue resolution, that this is a DCC issue to resolve and not User resolvable.*
- *Target Device in the SR8.1.1 has a SMI status of "pending".*
- *Observation - If there is no device association with a CHF then SR8.1.1 cannot be routed to a CSP and hence cannot be processed. There is no specific error code in the design to trap this error and so the code defaults to a general rejection (currently with an HTTP 500 response).*
- *This HTTP 500 response is not giving the detail SU's require to understand the problem as it is an HTTP server-side generic error.*
- *This error generated an E5 Response Code in DUIS v0.8.2 but was changed in v0.8.2.1 as it was identified to be misaligned with DUGIDS in the DECC review process.*
- *The root cause of this is that there is no error trap for the condition where a User sends a critical command to a device with a status of "pending" as it's not a logical sending state. It is important to note that this sending state is not prohibited either and so if this is sent it should be trapped with a valid and appropriate Response Code and NOT an HTTP 500 response.*
- *General request is that any failure reason that requires User action needs to have an actual Response Code defined and NOT generate a default HTTP 500 response.*

3.4.2 *Proposed Guidance*

***For DCC Live - User should note that if a Service Request is sent to a Device with an SMI device status of "PENDING", this will result in an HTTP 500 response error being received by the User in Response to the Service Request and so this Service Request should not be sent to the DCC**. This is because a service request of this type cannot be routed to a Comms Hub by DCC as no device association has been created by the User for Devices in the SMI for devices with a SMI device status of "PENDING" (this is achieved by the User sending SR8.11).*

In the longer term DCC shall consider raising an Internal CR (Change Request) for inclusion in subsequent DCC releases. The possible changes for consideration are;

a) *reinstate the E5 Response Code OR*

b) *add a new, more precise, Error trap and Response Code specific to the failure reason. Suggestion is to use DCC Alert N12 - Failure to deliver Command to Device.*

3.5 Guidance Point 5 – Clarification regarding when "Additional DCC System Processing" occurs in relation to receipt of Service Responses

Guidance Point Number	DUIS 1	DUIS 2
5	☑	☑
Guidance Type	Clarification on System Behaviour	
Functional Area	Multi area	
Keywords	Service Response Processing, Additional DCC System Processing	

Section 3.8 of DUIS contains details of Service Request Definitions and within this section for some of the Service Request Variants an optional sub section exists to define any "Additional DCC System Processing".

A couple of Parties have queried these definitions and requested confirmation of whether or not this "Additional DCC System Processing" defined occurs before or after the relevant User receives the Service Response. They have queried whether there are any cases where the "Additional DCC System Processing" is asynchronous by nature and therefore a User cannot rely upon this processing to have been completed before they receive the Service Response. This guidance point is intended to clarify these queries for the benefit of all Parties.

3.5.1 *Guidance*

In summary, the only Service Requests with "Additional DCC System Processing" that will definitely occur before the Service Response is generated and sent to a User and therefore can be relied upon as having occurred are the SMI (Smart Metering Inventory) status updates defined within these sections. The rest are all post processing steps placed on a work off queue to action running alongside the Service Response sent to the Users. More details are included on each Service Request Variant in the table below.

Service Request Variant with Additional DCC System Processing	Processing Done Before Service Response Sent to User? Yes / No
SRV 1.1.1 Update Import Tariff	Yes – Additional processing relates to DCC System processing when creating the GBCS Command as part of the Transform

Service Request Variant with Additional DCC System Processing	Processing Done Before Service Response Sent to User? Yes / No
SRV 3.2 Restrict Access for Change of Tenancy	No – This is a subsequent action to delete all active DCC Schedules created by other Users and all Future Dated (DSP) requests created by Other Users
SRV 6.15.1 Update Security Credentials (KRP)	No – DCC Alert N42 is a subsequent action placed on to a work off processing queue running alongside the completion of the Service Response. This process updates the Device Status to the SMI Status it held immediately prior to the recovery process (SMI Status prior to the 'Recovery' SMI Status).
SRV 6.15.2 Update Security Credentials (Device)	No - DCC Systems are updated as a subsequent action to record which Device Certificates are currently in use by the Device. The design of the DCC Systems is that the update of the SMKI repository is an additional step on top of the request/response processing. This is why DUIS has this detailed in the section "Additional DCC System Processing" and is not included as part of the SR itself. This update is not actually part of the interface, its additional post processing results from the response, so the DCC system adds the action to a subsequent work queue.
SRV 6.21 Request Handover of DCC Controlled Device	No – DCC Alert N42 is a subsequent action placed on to a work off processing queue running alongside the completion of the Service Response. This process updates the Device Status to the SMI Status it held immediately prior to the recovery process (SMI Status prior to the 'Recovery' SMI Status).
SRV 6.23 Update Security Credentials (CoS)	No – All DCC Alerts N26, N27, N17 and other actions listed are subsequent actions placed on to a work off processing queue running alongside the completion of the Service Response.
SRV 8.1.1 Commission Device	Yes – SMI status update

Service Request Variant with Additional DCC System Processing	Processing Done Before Service Response Sent to User? Yes / No
SRV 8.3 Decommission Device	Yes – SMI status update No - All DCC Alerts N1, N2, N9, N6, N33, N34 and other actions listed are subsequent actions placed on to a work off processing queue running alongside the completion of the Service Response.
SRV 8.4 Update Inventory	Yes – SMI status update
SRV 8.5 Service Opt Out	Yes - SMI status update No - All DCC Alerts N1, N2 and other actions listed are subsequent actions placed on to a work off processing queue running alongside the completion of the Service Response.
SRV 8.7.1 Join Service (Critical)	Yes – addition of the Key Agreement Certificate to the Pre-Command to be sent back to the User Yes - SMI status update
SRV 8.7.2 Join Service (Non-Critical)	Yes – addition of the Key Agreement Certificate to the Pre-Command to be sent back to the User Yes - SMI status update
SRV 8.11 Update HAN Device Log	Yes - SMI status update No - All DCC Alerts N16, N24, N25 and other actions listed are subsequent actions placed on to a work off processing queue running alongside the completion of the Service Response.
SRV 11.1 Update Firmware	Yes – firmware hash calculation and comparison is part of the Request processing and occurs prior to response being sent
SRV 11.3 Activate Firmware	Yes - SMI status update

Service Request Variant with Additional DCC System Processing	Processing Done Before Service Response Sent to User? Yes / No
SRV 12.2 Device Pre-notification	Yes - SMI status update

Table 3. *Service Request Variants with "Additional DCC System Processing"*

3.6 Guidance Point 6 – Service Request Variant 8.1.1 - CommissionDevice - what is the definition of a successful Response from the Device?

Guidance Point Number	DUIS 1	DUIS 2
6	☑	☑
Guidance Type	Clarification on System Behaviour	
Functional Area	Install and Commission	
Keywords	Successful Response, 8.1.1	

Several parties have raised the following query through testing for confirmation. There is a query when determining a successful response to SR 8.1.1 when synchronising the clock to commission the device.

DUIS section 3.8.90.4 Additional DCC System Processing states that "Upon receipt of the successful Response from the Device, the DCC shall update the Smart Metering Inventory and set the Device's SMI Status of the Electricity Smart Meter or Gas Smart Meter DeviceId specified in the Signed PreCommand to 'Commissioned'." but this doesn't explain what constitutes a successful response.

For information, DUGIDS (DCC guidance status only) states "A successful completion of this Service Request results in the ESME / GSME Device Status being set to 'Commissioned' in the Smart Metering Inventory."

3.6.1 *Guidance*

DCC can confirm that both sets of words above confirm that the DCC system checks the "MessageSuccess" attribute in the Response to determine a "successful Response" and not the individual ElecClockTimeStatus or GasClockTimeStatus values received from the device within the GBCS response.

The DUIS was updated as part of the last consultation to state 'Upon receipt of the successful Response from the Device' within these words in order to clarify that it is the successful Device response that is used irrespective of the Time Status of the Device, but DCC accepts that given the queries this still might not be fully clear to all Parties hence the inclusion within this guidance paper.

3.7 Guidance Point 10 – Reading Prepayment Configuration values from devices and potential PARSE error

Guidance Point Number	DUIS 1	DUIS 2
10	☑	☑
Guidance Type	Optimising System Behaviour	
Functional Area	Prepayment Data	
Keywords	Hourly, Weekly, Monthly, Quarterly, 4.13, 3035, 2.3	

It has been noted during DCC testing (issue#3035) that the Parse and Correlate Software currently returns a Parse error: Invalid value for element - [DebtRecoveryRates[1]:periodCurrent] when an SRV4.13 – ReadPrepaymentConfiguration is sent to an ESME device before SRV2.3 Update Debt is sent to the target device.

- *For clarity, the MMC data item impacted by this guidance point is "DebtRecoveryRatePeriod" within the ra:ElecDebtRecovery XML type definition.*

The Parse component of the Parse and Correlate Software is currently only expecting one of five values [0x0E10, 0x015180, 0x093A80, 0x27FD80, 0x77F880] meaning [HOURLY, DAILY, WEEKLY, MONTHLY, QUARTERLY respectively as per MMC definitions] but in this test case the value returned was [0x00000000] assumed to mean [no debt value].

The MMC XML Schema forces Parse to translate the value in GBCS to one of the following XML values: HOURLY, DAILY, WEEKLY, MONTHLY and QUARTERLY. It is not clear how Parse would be expected to handle a value of 0x00000000 in GBCS.

*Note: it is likely that the same problem exists for the element [DebtRecoveryRates[**2**]:periodCurrent] but has not yet been identified due to the break-on-error nature of Parse, so this error scenario is never reached.*

The "DebtRecoveryRatePeriod" data item is set on a device via DUIS SRV2.3 – UpdateDebt.

3.7.1 *Proposed Guidance*

This scenario and potential error should only exist when no prepayment configuration settings have been set on an ESME device.

NB – It should be noted that SRV4.13 – ReadPrepaymentConfigurationServiceRequest reads data from Devices that has been set from a combination of both SRV2.1 – UpdatePrepayConfiguartion and SRV2.3 – UpdateDebt.

DCC has confirmed that the observation identified here for the [DebtRecoveryRates[1]:periodCurrent] and possibly the [DebtRecoveryRates[2]:periodCurrent] are ONLY set as part of SRV2.3 –UpdateDebt.

Users are advised not to READ the Prepayment Configuration from an ESME or GSME (4.13 - ReadPrepaymentConfiguration) prior to the** DebtRecoveryRatePeriod **values being SET using DUIS Service Request SRV2.3 – UpdateDebt).

*Setting DebtRecoveryRatePeriod **values** on an ESME or GSME should be one of the first Service Requests sent by a Supplier as part of the change of mode to prepayment process so this is not expected to have a significant impact Users business process.*

Proposed SR ordering,

- *Set - SRV2.1 - UpdatePrepayConfiguration*
- *Set - SRV2.3 - UpdateDebt*
- *Read - SRV4.13 - ReadPrepaymentConfiguration*

(Please note that the SR Reads both sets of Prepayment Configuration)

3.7.2 *Impact if guidance is not adopted*

There is a risk that manufacturer's default values are returned by the Device which are not expected and not supported by the PARSE functionality within the DCC's Parse and Correlate software and an error is returned to the User.

3.8 Guidance Point 13 – Use of SRV1.1.1 and SRV1.2.1 and setting price values on GSME

The issues identified within this guidance point has been resolved by updating the DSP system and updating to DUIS 2.

Please note that this guidance point has been further reviewed internally within DCC and further consideration has been made, via the DCC IRB (Issue Resolution Board), as to whether or not this issue can be resolved in time for R1.3 since first being documented in this document.

*Update provided at V2.3 (DCC Guidance Use of DUIS) – The DCC IRB recommended that **Option C** should be progressed as the final resolution for this issue and reversed the initial proposal as listed below. Wherever possible however, the original words have been left in the guidance document as they were prior to this updated decision to demonstrate transparency of decision-making process and issue tractability purposes.*

Subsequent updates are expected to the SEC subsidiary document DUIS (DCC User Interface Specification) in due course to reflect this Option C position.

Guidance Point Number	DUIS 1	DUIS 2
13		
Guidance Type	Optimising System Behaviour	
Functional Area	Install and Commission, Change of Supply, Tariff Update	
Keywords	Price and Tariff Update, 1.1.1, 1.2.1	

It has been noted during DCC testing (GBCSIssue#1487) that there is an ambiguity within the DUIS Version 1.0 definition that impacts the following two Service Requests;

- *Service Request 1.1.1 - UpdateImportTariff(PrimaryElement)*
- *Service Request 1.2.1 - UpdatePrice(Primary Element)*

*Whenever a User is looking to **add price data to a Gas Smart Meter** using either SRV1.1.1 or SRV1.2.1 then they should note the following DCC guidance to confirm the expected behaviours.*

GBCS Section 10.4.2.11 states the following,

> *"A GSME shall reject any PublishPriceMatrix command that does not contain four Price fields"*

This section of GBCS confirms that, there must be four prices in a Command that sets prices on a GSME if the GSME is not to reject the Command (so GCS01a and GCS01b Commands). Therefore each of the four values in TariffBlockPriceMatrixTOU: valueNext[1..4] must be populated if the GSME is to accept the Command. If no price has ever been set using a GBCS Command, then reading the GSME price matrix may resulting in fewer entries (depending on manufacturer set factory defaults).

3.8.1 *Issue definition*

*This has impacts for Users when populating **EITHER** of the data items BlockTariff and TOUTariff within the DUIS XML Schema within the GasPriceElements definition (Table 81 of DUIS Version 1.0).*

BlockTariff

- *Although the DUIS XML Schema definition for the BlockTariff data item within the GasPriceElements definition allowed for a minimum of one and a maximum of four prices to be populated as part of the sr:GasBlockPriceMatrix definition (Table 82 of DUIS Version 1.0), the underlying associated GBCS Use Cases (GCS01a - Set Tariff and Price on GSME and GCS01b - Set Price on GSME) defines that the Command must include values for all four prices in order for the Command to be considered valid by GBCS definitions.*

TOUTariff

- *Although the DUIS XML Schema definition for the TOUTariff data item within the GasPriceElements definition allowed for a minimum of one and a maximum of four prices to be populated as part of the sr:GasTOUPriceMatrix definition (Table 83 of DUIS Version 1.0), the underlying associated GBCS Use Cases (GCS01a - Set Tariff and Price on GSME and GCS01b - Set Price on GSME) defines that the Command must include values for all four prices in order for the Command to be considered valid by GBCS definitions.*

This means that one of the following options could be implemented;

a) *changes to current behaviour should be updated and reflected in DUIS and its associated XML schema (e.g. requiring all four entries of BlockTariff element to be present and remove the current minOccurs statement). This would be a DUIS XML Schema change and therefore impact DCC, Parse and Correlate Software and all Users.*

b) *Service Request has to be populated by the User to include values for all four prices for the DCC to Transform into the Command or*

c) *DCC could populate any "missing" price values with a zero value for those not included in the SRV up to the maximum of four price values. This would also impact the Parse and Correlate Software to reflect this rule. Further development work would be required by the DCC Systems (DSP and Parse and Correlate Software) to support these changes*

- *Similarly to the electricity use cases (ECS01a, ECS01b), a note can be added clarifying Transform action.*
  - *For electricity, DUIS refers: "Where a User does not provide a price value the DCC shall populate the associated GBCS Command with a value of zero to ensure that all 80 price values are set in the associated Command. Users are not obligated to populate all 80 price values."*
  - *Suggested addition - For Gas use cases (GCS01a, GCS01b), DUIS could state the following:*

    "Where a User does not provide a price value the DCC shall populate the associated GBCS Command with a value of zero to ensure that all four price values are set in the associated Command. Users are not obligated to populate all four price values."

3.8.2 *Impact on DCC Systems*

The DCC System does not currently populate the price matrix with any "missing" price fields for the gas use cases (GCS01a - Set Tariff and Price on GSME and GCS01b - Set Price on GSME).

Expected current behaviours observed

- *If a User only supplies a single price value with the XML, then that single value is the only value that is included within the transformed GBCS Command.*

- *If a User supplies two price values with the XML, then those two values are the only values that are included within the transformed GBCS Command.*

- *If a User supplies three price values with the XML, then those three values are the only values that are included within the transformed GBCS Command.*

- *If a User supplies all four price values with the XML, then all four values are the values that are included within the transformed GBCS Command.*

3.8.3 *Impact on Parse and Correlate Software*

Correlate's purpose is to guarantee that the information contained in DUIS message is equivalent to the message contained in Payload returned by Transform.

The current version of Parse and Correlate software does not require all four Prices to be defined for both GCS01a and GCS01b commands. It is only correlating the defined prices within the SRV XML.

- *if only one Price is defined in DUIS, Correlate will expect only one entry in the GBCS command.*
- *if only two price entries are defined in DUIS, Correlate will expect two Sub-payload entries.*
- *if only three price entries are defined in DUIS, Correlate will expect three Sub-payload entries.*
- *if all four price entries are defined in DUIS, Correlate will expect four Sub-payload entries.*

3.8.4 *Impact on GSME*

It is expected that if a GBCS Command does not include all four price values then the target Gas Smart Meter will not process the Command successfully.

3.8.5 *Initial Guidance – (in line with b above)*

*DCC notes this system behaviour and recommends that **option b** is the preferred option for this point in time to limit impact on all Parties and this guidance notes recommends this is the noted system behaviour for Users.*

When sending SRV1.1.1 to a Gas Smart Meter

- *When a User populates the GasPriceElements definition for either a BlockTariff or a TOUTariff within the Service Request 1.1.1 - UpdateImportTariff(PrimaryElement), they must ensure that they supply BlockPrice / TOUPrice values (as appropriate) for all four prices within the XML(defined in DUIS v1.0 Tables 1, 82 and 83).*

When sending SRV1.2.1 to a Gas Smart Meter

- *When a User populates the GasPriceElements definition for either a BlockTariff or a TOUTariff within the Service Request 1.1.1 - UpdateImportTariff(PrimaryElement), they must ensure that they supply BlockPrice / TOUPrice values (as appropriate) for all four prices within the XML(defined in DUIS v1.0 Tables 2, 82 and 83).*

DUGIDS for GBCS version 2.0 shall be been updated with a guidance note in line with this guidance to advise Users that they need to supply all four prices when populating the GasPriceElements definition for either a BlockTariff or a TOUTariff for Gas Smart Meters.

3.8.6 *Final Guidance – (in line with c above)*

*Update for version 2.3 – The DCC IRB recommended that **Option C** should be progressed as the final resolution for this issue and reversed the initial proposal as listed above. The original words have been left in the guidance document as they were prior to this updated decision to demonstrate transparency of decision-making process and issue tractability purposes.*

Subsequent updates are expected to the SEC subsidiary document DUIS (DCC User Interface Specification) in due course to reflect this Option C position. To confirm that the DCC Systems shall populate any "missing" price values with a zero value for those not included in the SRV up to the maximum of four price values.

3.9 Guidance Point 15 – General guidance for how DCC Systems handle any Combined Devices

Guidance Point Number	DUIS 1	DUIS 2
15	☑	☑
Guidance Type	Clarification on System Behaviour	
Functional Area	Device Join/Unjoin	
Keywords	PPMID and IHD, 12.2, CAD	

Several Parties have raised the following query through various Industry forums for confirmation.

There is a query circulating amongst Parties regarding how DCC will handle any potential "Combined Devices" that may potentially be designed and released to the market by some Device manufacturers e.g. PPMIDs and IHDs.

Note - A Combined Device is considered by DCC to be a single physical Device that supports a functionality set that relates to more than one of the Device types listed within SMETS.

In particular the queries being raised with DCC are with respect to device pre-notification, device joining and the ongoing identification and operation within the Smart Metering Inventory and wider DCC Systems for combined Devices

This will be of particular importance to Users when using Service Request Variant 12.2 – Device Prenotification to inform DCC of Devices that they are looking to install at

consumers premises and for DCC to record within the Smart Metering Inventory (SMI) and its subsequent playback to any requesting Users.

Service Request Variant 12.2 – Device Prenotification contains a mandatory data item "DeviceType" which must be a single enumeration value to define the Device Type that is being prenotified to the DCC.

If a single physical Device id is designed to cover functionality of multiple Device definitions then how should a User refer to this Device and hence prenotify this Device to the DCC using a single Device Type value?

3.9.1 *Guidance*

DCC can confirm the following design assumption with respect to this query,

> *"DCC is of the opinion that it is permissible for an IHD and a PPMID functionality to be combined into a single device. This single device would be expected to have a single Device ID and this device would be expected to comply with the security characteristics of the higher security classification, so in this case it would be a type 1 device (e.g. PPMID). As it is a single device we would only expect it to be certified once as a type 1 device. This device would need to be pre-notified onto the Smart Metering Inventory (SMI) as a type 1 device (e.g. PPMID) and hence it would be displayed to all parties as a type 1 device (e.g. PPMID).Any joining of this device to other Devices on the HAN should also follow the standard process for a device of this type to match the DeviceType that is prenotified."*
>
> *DCC further has made the assumption that this Device will be presented (or not presented as appropriate) on the Certified Products List (CPL) in accordance with the same criteria of the Combined Device having to comply with the security characteristics of the higher of the individual security classification of each of the functionality sets that relates to each Device within the Combined Device.*
>
> *Note – The DCC Systems do not contain any validation for this assumption and the information that the User provides within the SR12.2 will be considered to be accurate and definitive.*

DCC further believes that this statement would also naturally extend if a Device was also designed to include CAD (Consumer Access Device) functionality. DCC is aware that it is possible that this may be a potential future possibility for some Device manufacturers to design, build and provide to the market a single Device supporting PPMID, IHD and CAD functionality within a single physical Device. The final guidance on this point though will depend on how the current wider CAD security policy conversations conclude and if this combination is permissible. However, the current DCC working assumption is that DCC currently does not see anything to prevent this; hence the guidance above would be generic for all Type 2 Devices (e.g. IHD and/or CAD).

3.10 Guidance Point 19 – DebtRecoveryRatePeriod in SR 2.3 Update Debt for ESME (GBCS Use Case ECS07)

Guidance Point Number	DUIS 1	DUIS 2
19	☑	
Guidance Type	Guidance	
Functional Area	Prepayment	
Keywords	Update Debt, 2.3, IRP 275	

3.10.1 *Issue Definition*

DebtRecoveryRatePeriod in the service request 2.3 Update Debt for ESME (GBCS Use Case ECS07).

At present, IRP 275 is not implemented at the same version number across the DCC Solution. (IRP 275 v0.4 and IRP 275 v0.3 apply)

DUIS states that the ESME DebtRecoveryRatePeriod allowable values are 'Hourly', 'Daily', 'Weekly', 'Monthly' and 'Quarterly'.

However v0.4 of IRP275 modified the electricity GBCS use caseECS07 to allow only 'Hourly' and 'Daily' values in DebtRecoveryRatePeriod data element.

Thus, at the current time, if Users/Customers send Update Debt command to ESME with Debt recovery payment period of 'Weekly', 'Monthly' or 'Quarterly' as per current DUIS XML, the Update Debt command will be rejected by P&C because P&C will not expect any values other than 'Hourly' and 'Daily' in the service request.

3.10.2 *DCC Guidance:*

DCC Users/Customers should not use 'Weekly', 'Monthly' or 'Quarterly' period when they trigger service requests 2.3 Update Debt on ESME.

IRP275 v0.4 implementation will be updated to restrict ESME DebtRecoveryRatePeriod to 'Hourly' and 'Daily' and the DUIS schema will then represent aligned ESME DebtRecoveryRatePeriod processing.

The debt recovery rate period of 'Weekly', 'Monthly' and 'Quarterly' is now deleted from the DUIS XML from DUIS2.0.

3.11 Guidance Point 23 – UTRN counter cache reset

Guidance Point Number	DUIS 1	DUIS 2
23	☑	☑
Guidance Type	Clarification on System Behaviour	

Guidance Point Number	DUIS 1	DUIS 2
Functional Area	Prepayment	
Keywords	IRP564, IRP477, UTRN counter cache, 6.21, 6.15.1, 6.23, change of supplier, PrepaymentTopUpFloorSeqNumber	

3.11.1 *Issue Definition*

IRP564 provided clarification required on GBCS 13.3.5.10:

- *When there is a Change of Supplier the Smart Meter's cache of UTRN counters will be cleared by the GSME and ESME*
- *The new Supplier should specify the floor counter explicitly in the:*
  - *SupplierPrepaymentTopUpFloorSeqNumber parameter of each 6.23 Update Security Credentials (CoS) Service Request,*
  - *RemotePartyPrepaymentTopUpFloorSeqNumber parameter of each:*
    - *6.15.1 Update Security Credentials (KRP).*
    - *6.21 Request Handover of DCC Controlled Device Service Request.*
- *The DCC will then include the value provided by the Supplier in the newRemotePartySpecialistFloorSeqNumber field in the resulting CS02b Command to the Smart Meter.*
- *The GSME and ESME will then be able to clear the URTN counter cache and use the new value provided by the supplier as the starting value for anti-reply.*

However, the SupplierPrepaymentTopUpFloorSeqNumber / RemotePartyPrepaymentTopUpFloorSeqNumber parameter is optional in DUIS and so the newRemotePartySpecialistFloorSeqNumber field in the Command would be absent if the Supplier did not provide this counter value. In this case the GBCS provides for a fall-back, which is to use the more general anti-replay counter value. For 6.15.1 Update Security Credentials (KRP) / 6.21 Request Handover of DCC Controlled Device Service Request Service Requests, the DUIS parameter is RemotePartyFloorSeqNumber which is mandatory on change of supplier, and maps to the newRemotePartyFloorSeqNumber parameter in the resulting GBCS Command. Thus, the fall-back functions as expected for these two Service Requests.

In the case of the 6.23 Update Security Credentials (CoS) Service Request, RemotePartyFloorSeqNumber is not used. An equivalent DUIS parameter (SupplierFloorSeqNumber) is present, although this maps to a differently named CS02b Command parameter, namely otherRemotePartyFloorSeqNumber. This difference in naming prevents the fall-back from functioning.

3.11.2 *DCC Guidance*

- *Suppliers should populate the SupplierPrepaymentTopUpFloorSeqNumber / RemotePartyPrepaymentTopUpFloorSeqNumber in 6.15.1, 6.21 and 6.23 Service Requests; and*

- *If suppliers do not do so in a 6.23 Service Request, this leads to UTRN counter floor value being wrongly set. However, this can be corrected by the Supplier sending a subsequent 6.15.1 Service Request containing the same details as in the 6.23 Service Request.*

3.11.3 *Impact if guidance is not adopted*

The issues that may arise if the guidance above is not followed are either that (1) previously used UTRNs may be accepted by a Smart Meter or that (2) valid, unused UTRNs are not accepted.

3.12 Guidance Point 24 – Prepayment Clarifications (agreed and aligned with IRP 560[2])

Guidance Point Number	DUIS 1	DUIS 2
24	☑	☑
Guidance Type	Clarification on System Behaviour	
Functional Area	Prepayment; Energy Suppliers, Negative Values; Emergency Credit 'available'; reset Meter Balance to zero;	
Keywords	IRP560, SR2.1; SR2.3; SR1.1.1; SR1.2.1; SR1.6; SR1.5; SR2.1;SR6.2.9;SR4.14; SR4.14;	

3.12.1 *Issue Definition*

DCC agreed to publish Guidance Point 24 following recent BEIS/Industry clarifications relating to prepayment capability for SMETS 2. This covers scenarios where Customers should avoid use of negative values. There is an additional point on avoiding inadvertent disconnection, resetting Meter Balance to zero.

3.12.2 *Negative values: do not use these when submitting prepayment configuration Service Requests for SR 2.1, SR 2.3, SR1.1.1., SR1.2.1*

When submitting prepayment configuration Service Requests, Energy Suppliers should not set any of the following values for the following SMETS Configuration Data Items to a negative value. Negative values will lead to undefined Device behaviour:

SR2.1 Update Prepay Configuration

[2] An IRP is an Technical Specification Issue Resolution Proposal, published by BEIS and issued via the Technical Specification Issue Resolution Subgroup (TSIRs). IRP 560 was approved by TSIRs on 30th Aug 2018.

- *Debt Recovery Rate Cap*
- *Emergency Credit Limit*
- *Emergency Credit Threshold*
- *Low Credit Threshold*
- *Maximum Meter Balance Threshold*
- *Maximum Credit Threshold*

SR2.3 Update Debt

- *Debt Recovery Rates [1 … 2]*

SR1.1.1 Update Import Tariff (Primary Element) / SR1.2.1 Update Price (Primary Element)

- *Standing Charge*

3.12.3 *To avoid inadvertent disconnection, do not automatically reset Meter Balance to zero*

In SMETS1, there is no 'Reset Meter Balance' functionality, therefore the energy suppliers may be unfamiliar with its consequences.

Energy Suppliers are reminded that, as per SMETS2, resetting the Meter Balance via SR1.5 Update Meter Balance with the parameter "ResetMeterBalance" sets it to £0.00 and this would cause supply to be disabled if:

1. *The Meter is in Prepayment Mode; AND*
2. *The Meter is NOT currently in a period of non-disablement; AND*
3. *The Disablement Threshold is £0.00 or greater.*

If Energy Suppliers do not wish to disable supply when resetting the Meter Balance, they should ensure that one of the above conditions is NOT true BEFORE resetting the Meter Balance (e.g. the Meter is in Credit Mode; the Meter is currently in a period of non-disablement).

3.12.4 *Impact if guidance is not adopted*

If this Guidance is not followed, undefined Device behaviour will result for ESME and GSME devices.

3.13 Guidance Point 25 – Don't target GSME for Scheduled Reading

Guidance Point Number	DUIS 1	DUIS 2
25	☑	☑

Guidance Point Number	DUIS 1	DUIS 2
Guidance Type	DUIS/GBCS Clarification	
Functional Area	Scheduling Service, daily read log, prepayment daily read log, profile log	
Keywords	SR5.1, SR4.6.1, SR4.8.1, SR4.14	

3.13.1 *Issue Definition*

Following GBCS clarification with BEIS, we wish to confirm that GSME does not allow the ACB role to execute the commands that have been identified as available for DSP Scheduling,

These commands can therefore only be DSP Scheduled via SR5.1 on the GPF.

Whilst the following SRs may also be scheduled via SR5.1, targeting either the GSME or GPF, they are NOT impacted by this issue:

- *4.10, GCS18 Read Network Data (GSME only)*
- *4.17, GCS61, Retrieve Daily Consumption Log (GPF only)*
- *14.1, GCS31, Record Network Data (Gas) (GSME only)*

3.13.2 *Proposed Guidance*

DCC Users/Customers should target the GPF only when creating the DSP Scheduled reading via SR5.1 for SR4.6.1, SR4.8.1 and SR4.14.

3.13.3 *Impact if guidance is not adopted*

The GSME will reject the request with a security alert if the DSP Scheduled reading for SR4.6.1, SR4.8.1 and SR4.14 is created via SR5.1 targeting the GSME.

DSP cannot match the Alert to the Request (by GBCS design), so since it is a Scheduled Request with a 24 hour SLA, if the GSME is targeted, retry will take place at 2 hour intervals until the 24 hour SLA expires, at which point we will send an N11 Alert for No response.

3.14 Guidance Point 26 – GSME-PPMID re-join following a device certificate change

Guidance Point Number	DUIS 1	DUIS 2
26	☑	☑
Guidance Type	Clarification on System Behaviour	

Guidance Point Number	DUIS 1	DUIS 2
Functional Area	PPMID – Join/Unjoin Function	
Keywords	SR8.7.1 Join Service (Critical), SR8.7.2 Join Service (Non-Critical), SR 8.8.2 Unjoin Service (Non-Critical),	

3.14.1 *Issue Definition*

Some DCC Customers are not performing the GSME/PPMID re-join following a device certificate change. This means the PPMID can no longer successfully send activate emergency credit and add credit commands to a GSME

.

3.14.2 *Proposed Guidance*

For a PPMID to successfully send activate emergency credit and add credit commands to a GSME, the PPMID needs to hold a copy of the GSME's Key Agreement certificate. Such certificates are sent to a PPMID as a result of the SR8.7.2 Join Service (Non-Critical) service request, where the target is the PPMID.

The SEC requires that installing suppliers instruct the GSME to change its Key Agreement certificate within 7 days of installation.

When this has been done on the GSME and there is an installed PPMID, the supplier also needs to trigger the sending of the new GSME Key Agreement certificate to the PPMID.

Following the successful execution of a SR6.15.2 Update Security Credentials (Device) targeting the GSME and containing the GSME's new Key Agreement certificate, if there is a PPMID which has previously been joined to the GSME, the supplier should send a SR8.7.2 Join Service (Non-Critical) targeting the PPMID. As per DUIS 3.8.97.4, the DCC will then place the GSME's new Key Agreement certificate in the resulting command sent to the PPMID, so allowing the PPMID to continue working with the GSME.

It is not necessary to send a SR8.8.2 Unjoin Service (Non-Critical) to the PPMID before sending the SR8.7.2, but the end result would be the same (assuming both were successful).

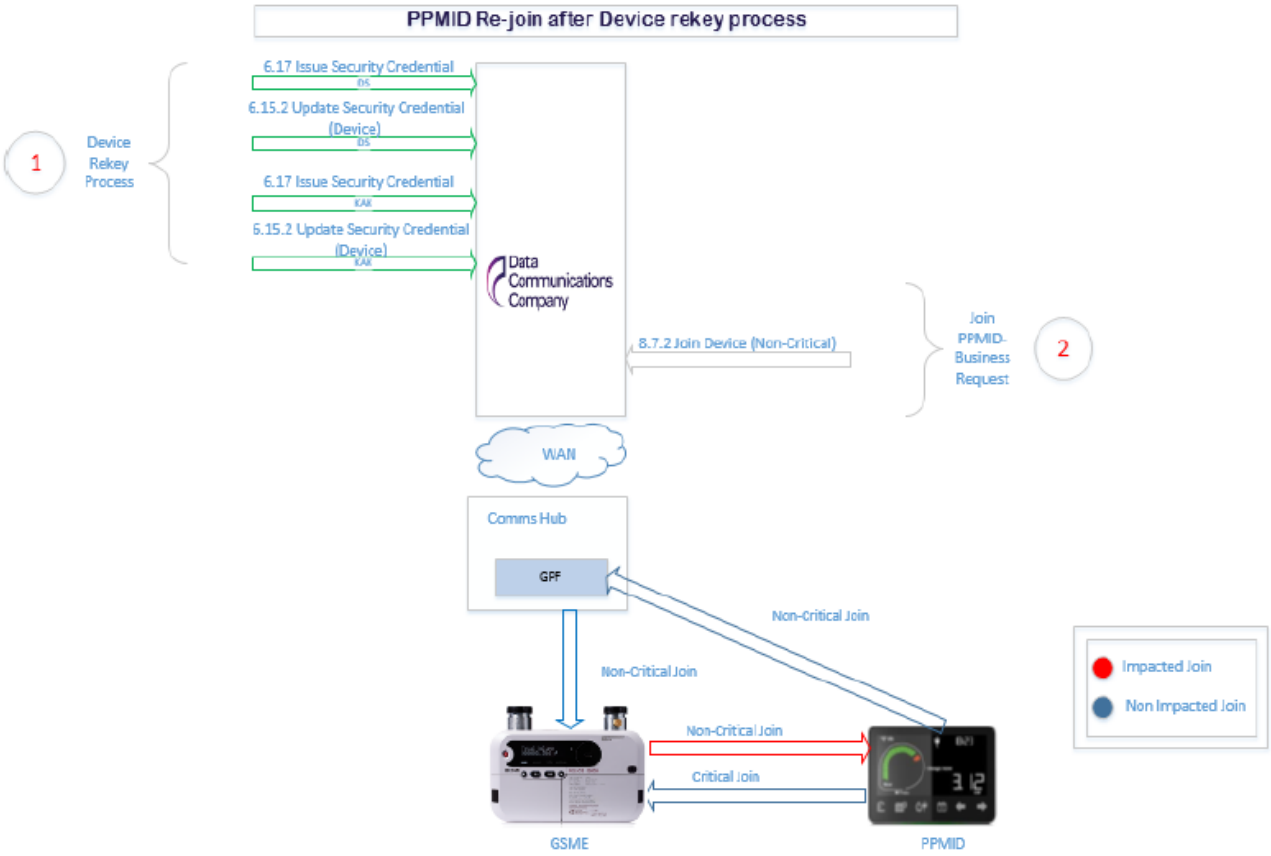

Figure 1: Schematic showing sequence required

3.14.3 *Impact if guidance is not adopted*

Gas Consumers will not be able to use their PPMID to

- *Activate Emergency Credit on GSME (PCS02)*
- *Apply Prepayment Top Up to a GSME (PCS01)*

3.15 Guidance Point 27 – End of time for GPF/GSME log/profile reading

Guidance Point Number	*DUIS 1*	*DUIS 2*
27	☑	☑
Guidance Type	*Clarification on System Behaviour*	
Functional Area	*Meter Read*	
Keywords	*4.6.1, 4.8.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.14, 4.17*	

3.15.1 *Issue Definition*

Some DCC Customers set up a daily schedule to read the previous day's half hour profile via SR4.8.1 targeting GPF. The schedule was set up using StartDateTime as 00:00:00 and endDateTime as 23:59:59. This should return 48 half hour entry of the previous day however one of the CH returns 49 entry with an additional entry of 00:00:00 for the current day, 1 second beyond the endDateTime specified by the customer in the SR XML.

3.15.2 *Root Cause and history of the Issue*

This is because DSP adds 1 second at endDateTime when reading the log entry from GPF.

During Aug 2017 E2E testing, DCC noticed different implementation within CH and GSME manufactures for end time when reading the logs. Some of the device manufactures implemented end time as inclusive and some as exclusive. From Specification point of view, DIUS and COSEM is inclusive of end time, however ZigBee is not always inclusive, and GBCS contains conflict requirements in different part regarding inclusive and exclusive of the endDateTime.

BEIS stated intention of the specification is that, when reading logs, all entries between StartDateTime and endDateTime inclusive are returned. And advice the most pragmatic way forward for consideration should be, given specifically to Change of Supplier (and reading of any closing read by the old supplier at midnight / any other half hour), add a second / DSP implementation of such adjustment.

*All service providers and 9 GSME manufactures were consulted on the options moving forward. The IRB decision (**20170829**) was made to*

- *as interim solution, update DSP to add one second to EndDateTime values sent in the GBCS command to ensure inclusive of EndDateTime for those device manufacture implemented exclude.*

- *as an enduring solution, update GBCS to modify the Use Cases so that ESME and GSME/GPF devices behave in the same way to ensure inclusive of EndDateTime (IRP586 still in draft)*

Follow this decision, DSP change of add one second to EndDateTime was deployed into production at Q3 2017. The undesired side affect of this change is that an extra log entry maybe included.

This issue impact follow log related service request targeting GPF and GSME

- *4.6.1, Retrieve Import Daily Read Log*
- *4.8.1, Read Active Import Profile Data*
- *4.4.2 Retrieve Change Of Mode / Tariff Triggered Billing Data Log*
- *4.4.3 Retrieve Billing Calendar Triggered Billing Data Log*
- *4.4.4 Retrieve Billing Data Log (Payment Based Debt Payments)*
- *4.4.5 Retrieve Billing Data Log (Prepayment Credits)*
- *4.14 Read Prepayment Daily Read Log*
- *4.17 Retrieve Daily Consumption Log*

3.15.3 *Proposed Guidance*

SU are recommended to use 2 seconds before the endDateTime if they wish the entry is exclusive, for example, endDateTime for end of day entry,

- *To ensure inclusive, 20/11/2018 00:00:00,*
- *To ensure exclusive, 19/11/2018 23:59:58*

The impacted SRs are 4.6.1/4.8.1/4.4.2/4.4.3/4.4.4/4.4.5/4.14/4.17

3.15.4 *Impact if guidance is not adopted*

Additional log entry beyond the endDateTime requested in the SR XML maybe returned.

4 Appendix –Document Control

Revision History

Revision Date	Summary of Changes	Version Number
05/08/16	Initial Version Created	D0.1
25/08/16	Document issued to Users following internal review	1.0
07/09/16	Updated for some typos	1.1
23/09/16	Updates made to guidance point 1 details to add specific details of time impacts on each GBCS underlying protocol as requested from DCC's Sept 2016 Design Release forum	1.2
03/10/16	Clarifications made to guidance point 1 to confirm what DSP Transform actually does with ASN.1 as previous version was incorrect.	1.3
08/11/16	Updated with two new guidance points 5 and 6 and base-lined for alignment to DCC Live milestone.	2.0
13/01/17	Updated with one new guidance point 7.	2.1
14/03/17	Updated with one new guidance point 8 to cover R1.2 known workarounds Updated with four new guidance points 9, 10, 11, 12 and 13 arising from observations from DCC testing phases.	2.2
16/05/17	Update made to guidance point 10 to confirm which SRV is the trigger point for the issue identified. Updated with new guidance point 14 arising from observations from DCC testing phases.	2.3
24/05/17	Formatting changes only on v2.3, no material changes	2.4
16/06/17	Update following RFC 056 DUIS/MMC BEIS Consultation	2.5
08/07/17	Updated with one new guidance point 15.	2.6
December 2017	Updated with 4 changes: • General guidance on DCC Retry and Timeouts for Service Request Processing point 16; • Resetting of Network Operator Anti Replay Counter/Remote Party Floor Sequence Number point 17; • GSME/GPF Wildcard features workaround point 18; • DebtRecoveryRatePeriod in SR 2.3 Update Debt for ESME (GBCS Use Case ECS07) point 19.	2.6
June 2018	• Update to rename alert 0x8F69 (point 14) • Update to DSP retry and timeout (point 16) • Update to DNO's originator counters (point 17) • Alert storm (point 20)	2.7

Revision Date	Summary of Changes	Version Number
	• DNO's communication to meters (point 21) • Device interop guidance (point 22) • Add in a guidance summary	
Aug 2018	• Add guidance 23 for IRP564 UTRN counter cache reset when 6.23 • Add guidance 24 for IRP560, prepayment clarification • Update the Guidance 16 for GSME retry • Update the Guidance 20 for the alert storm	2.8
Nov 2018	• Add guidance 25 Scheduled Service targeting GSME • Add guidance 26 GSME-PPMID re-join follows device certification change • Update the Guidance 16 for Arqiva retry and parallel processing • Update the Guidance 24 for reset meter balance	2.9
Feb 2019	Deprecate following guidance notes follow uplift of Operational DUGIDS 2.0e • Guidance Point 2 • Guidance Point 3 • Guidance Point 5 • Guidance Point 6 • Guidance Point 10 • Guidance Point 15 • Guidance Point 19 • Guidance Point 23 • Guidance Point 24 • Guidance Point 25 • Guidance Point 26 • Guidance Point 27 V1.10 Retry and Timeout configuration embedded for • Correcting an error related to SR8.11 timeout • DIB 201, change the SLA for ALCS SRs (SR6.14.1, SR6.14.2 and SR7.9) to be 30s, as the result, the timeout and retry for those 3 SRs reversed back to use the default configurations	2.10
June 2019	• Guidance 20 updated to provide sequence detail of PPMID join with GPF as defined by BPD	2.11
Sept 2019	• Guidance 20 updated to correct a mistake related to type 1 device • Guidance 28 added for configuration of non-mandated GBCS alert • Update applicable table to include DUIS3/SMETS1 for all active Guidance	2.12
Nov 2019	• Added Guidance 29, How to interpret the high value of 16,777.215 m3 in the SR4.8.1 response • Added Guidance 30, non-zero Disablement Thresholds • Added Guidance 31, Future dated COTs • Added Guidance 32, What is the recommendation for setting up a schedule	2.13

Revision Date	Summary of Changes	Version Number
	• Added Guidance 33, what happen to a suspended device	

Reviewers

Each individual guidance is reviewed internally followed by industry review via TSIRS before adding into this guidance document.

All versions, before release to industry, are reviewed internally by DCC Design Authority including both DCC and DSP.

5 Recourse

If SEC Parties have concerns with any of the information documented within this guidance note then they should raise these concerns with DCC in accordance with the SEC defined Testing Issue Resolution Process.