DCC Guidance Note

Communications Hubs Usage

Document Version:	**V1.7.2**
Date:	**21 February 2024**
Author:	**DCC**
Classification:	**DCC Controlled & for SECAS publication as a Design Note**

Table of Contents

1 Introduction 4

2 Behaviour observed in the Comms Hub 7

2.1 Guidance Point 1: CH Timing Management 7

2.1.1 CSP-N Comms Hub Time sync Overview 7

2.1.2 CSP-S&C Comms Hub Time sync Overview 11

2.1.3 Pre-assessment of clock drift 14

2.1.4 Method using SRV8.9 and Event Log Entry 18

2.2 Guidance Point 2: Improved usage of Synchronise Clock (SRV6.11 and SRV8.1.1) commands 20

2.3 Guidance Point 3: Billing Calendar Periodicity & Start Time 23

2.3.1 Start Date Recommendations in SR 6.8 23

2.3.2 The Expected Billing Calendar Sequence 24

2.4 Guidance Point 4: CoT Data Availability & Restrictions 26

2.4.1 CoT date processing of Future Dated CoT Commands 26

2.4.2 CoT and Data Restrictions 27

2.5 Guidance Point 5: Device Interoperability Guidance 28

2.5.1 Issue Definition 28

2.5.2 GSME Potential Interoperability issue 29

2.5.3 DCC Guidance 29

2.6 Guidance Point 6: GPF default values 30

2.6.1 Setting CommodityType on GPF 30

2.6.2 CF and CV default values for GSME & GPF 30

2.6.3 Additional Note on CV & CF 31

2.7 Guidance Point 7: GPF behaviours associated with GSME half hour push 32

2.7.1 Issue Definition 32

2.7.2 CH behaviour associated with Half Hour Profile Data log 33

2.7.3 CH behaviour associated with Daily Consumption Log (SR4.17) 41

2.7.4 CH behaviour associated with Historical Attributes 41

2.8 Guidance Point 8: Upgrade End Request status values 41

2.8.1 OTA Transfer Handling 41

2.8.2 OTA Transfer to ESME/GSME/HCALCS successfully 42

2.8.3 OTA Transfer to PPMID successfully 44

2.8.4 Incorrect FW Image Transferred to ESME/GSME/HCALCS 45

2.8.5 Incorrect FW Image Transferred to PPMID 46

2.8.6 OTA Transfer to Device Aborted 47

2.8.7 Different Behaviour between CHs: Handling a FW Image after Transfer ...47
2.9 Guidance Point 9: Triggers for 8F84 Alert Generation ...48
2.9.1 Issue Definition ...48
2.9.2 Comms Hubs scenarios and triggers...48
2.9.3 Conclusion ...55
2.10 Guidance Point 10: Comms Hub Last Communication with HAN devices (SRV8.9 & SSI Comms Hub Diagnostic) ...56
2.10.1 Issue Definition ...56
2.10.2 SSI Comms Hub Diagnostic & Display Interface ...56
2.10.3 Comms Hubs Handling of *last_communication_date-time* in SRV8.9 ReadDeviceLog (CCS06) Service Responses ...64
2.10.4 Mapping between SSI Comms Hub Diagnostic and SRV8.9 ReadDeviceLog (CCS06) Service Responses ...71
2.11 Guidance Point 11: GBCS 4.1 CH FW handling of GSME/PPMID/HCALCS OTA 71
2.11.1 Problem Statement ...71
2.11.2 Background...72
2.11.3 Upgrades taking place within 14 days of CH Firmware Download ...73
2.11.4 Retention of 14-Day Timer during Reboot ...75
2.12 Guidance Point 12: Usage of Alerts 819D and 819E targeting ACB ...77
2.12.1 Problem statement...77
2.12.2 Comms Hubs scenarios and triggers...77
2.12.3 Conclusions ...80
2.13 Guidance Point 13: Comms Hub behaviour for joining Devices in Sub GHz band during TCSO...81
2.13.1 Background...81
2.13.2 Comms Hub behaviours for Sub GHz device capacity detection ...83
2.13.3 Alert 8F2D Generation ...84
2.13.4 Scenario for Sub GHz band capacity limit after TCSO. ...84
2.13.5 DCC recommendation for industry. ...84
3 Recourse ...86
4 Appendix – Deprecated Guidance ...87
5 Appendix - Document Control...88
6 Appendix - Technical Specifications References ...89

1 Introduction

This Guidance Document has been created to provide information and direction on Comms Hub behaviours to DCC customers. It aims to provide a short, educational overview on key areas of functionality within the system, and forms part of DCC's goals for customer engagement by establishing repeatable, work package-based processes.

Items for inclusion are identified through multiple routes like testing, observation and items raised with Industry forums. Where clarification and increased understanding are felt needed on matters raised as a result of testing, DCC have created, through this document, a vehicle to highlight them to Testing Participants, in line with DCC's SEC obligations. This increased understanding of the subject area is then available to DCC's Industry partners and other interested parties.

In order for an item to be included, the following criteria is used for assessment:

- A particular aspect or feature of CH needs a concise explanation, to aid the DCC users in their operations, testing or evaluation.
- It provides information to Service Users to improve their use of the CHs.
- The subject should primarily address some facet of CH usage which needs highlighting (the format of this document follows the Use of DUIS DCC document).
- There are differences in the behaviour of the different CSPs or CHs which it is useful to share.

A summary of the guidance is provided here:

#	Guidance Point	Description
1	Timing Management	*This is migrated from DUIS-GP 46 (part).* Covers CH Timing Management with reference to the CSP mechanisms implemented.
2	Clock Synchronisation	*This is migrated from DUIS-GP 52 (part).* Improved usage of Synchronise Clock commands.
3	BillingCalendar snapshots	Setting and maintaining the Billing Calendar snapshot process.
4	CoT behaviour	*This is migrated from DUIS-GP 31 (part).* Outlining recommendations associated with Future Dated CoT commands, & covering aspects of overlapping data.
5	Device Interoperability Guidance	*This is migrated from DUIS-GP 22 (complete).* Covers Interoperability issues associated with Device Compatibility & Interworking.
6	GPF default values	Covers IRP584 Clarification on setting CommodityType on GPF and CRP620 CF and CV default values.

#	Guidance Point	Description
7	GPF behaviour associated with GSME half hour push	*This is migrated from DUIS-GP 40.* Service Users should be aware of scenarios which can lead to GPF and GSME data mismatch.
8	Upgrade End Request status values	As part of SECMOD 7 upgrades (PPMID / HCALCS OTA) guidance is provided on Upgrade End Request status values, received when the CH transfers the FW Image to the HAN Device.
9	8F84 alert 'Failure to Deliver Remote Party Message to ESME' triggers	There are differences in the generation of 8F84 alerts between the three Comms Hubs. This guidance point explains the various scenarios under which such alerts are triggered, covered in TS1376, such as: 1. the Comms Hub has a valid entry for the ESME in its neighbour table and also has an active tunnel for the same ESME 2. the Comms Hub does not have a valid entry for the ESME in its neighbour table and a previously requested tunnel is still active and yet to expire. 3. the Comms Hub does not have either a valid entry for the ESME in its neighbour table, nor does it have an active tunnel for this ESME (eg tunnel has expired).
10	Comms Hub last communication with HAN devices (SRV8.9 and SSI Comms Hub diagnostic)	There are differences in the information extracted from Comms Hubs through SRV8.9 ReadDeviceLog (CCS06) for the *last_communication_date-time* and in the Comms Hub diagnostic interface provided through SSI. This Guidance Point explains the usage and handling of information collected and mapped across these two data interfaces. 1. The last_communication_date-time in SRV8.9 ReadDeviceLog (CCS06) service responses to understand how Comms Hub populate such information for all HAN devices. This can be used to assess HAN connectivity. 2. Meaning of all data fields in the SSI Comms Hub Diagnostic user interface to have the ability to evaluate Comms Hub and devices HAN/WAN status, along with the differences across all three Comms Hubs. 3. SSI Comms Hub Diagnostic user interface errors for a clear understanding of what those errors mean. 4. How last_communication_date-time and SSI Comms Hub Diagnostic user interface relate to each other and can be used in conjunction to assess HAN connectivity.
11	GSME Slot Usage	As part of SECMOD 7 upgrades (PPMID / HCALCS OTA) guidance is provided on issues associated with the shared GSME Slot in relation to the 14 Day Retention timer.

#	Guidance Point	Description
12	Usage of Alerts 819D and 819E targeting Access Control Broker (ACB)	Addresses the potential gap between GBCS and DUIS on handling of the device alerts 819D (GSME Command Not Retrieved) and 819E (Tap Off Message Response or Alert Failure). There is no mechanism defined in DUIS to enable Access Control Broker (DSP) to pass above 2 devices alert to the Supplier or interested remote party. At this moment the alerts will be dropped by the DSP.
13	CH behaviour for joining Devices in Sub GHz band during TCSO	Covers capacity limits for the number of devices allowed on the Sub GHz channel during TCSO, both individual device limits and total devices allowed on the HAN. Identifies key differences in behaviour between the different CHs, in identifying and handling limits.

The layout of this document follows the pattern used in DCC Guidance Note 'Use of DUIS'.

2 Behaviour observed in the Comms Hub

2.1 Guidance Point 1: CH Timing Management

Guidance Point Number 1	GBCS 1.0	GBCS 2.0	
	x	x	
Guidance Type	Clarification on system behaviour, differences between CSPs, options to handle unexpected behaviour		
Functional Area	Timing, Time Drift		
Keywords	TS1405, TS1423, SRV6.11, SRV8.1.1, SRV6.13, 0x8154, SRV8.9, SRV11.2		

2.1.1 CSP-N Comms Hub Time sync Overview

2.1.1.1 Usage of GBCS defined Time Solutions

The EDMI Communications Hub has no functionality to query or correct its time via GBCS defined SRs. There is no 0x8F0C Alert 'Clock not adjusted (adjustment greater than 10 seconds)' or equivalent alert mechanism to indicate any CH time drift within the CSPN solution. At the present moment there is no provision for the Supplier to trigger time related query or update via the SSI.

Proposals for the energy supplier to ascertain remotely whether time drift in the meter or comms hub time has occurred is found in this document. This provides a methodology to derive CH time from sending a series of SRs, though it is recognised that factors such as NW latency, CH latency and NW congestion can impact calculations, and certain assumptions are made concerning unknown variables. As such the calculations can give an indication, rather than define definitive results. See section 2.1.3 below for supplier actions that can be performed to this end.

2.1.1.2 Need for Accurate Time

CH time accuracy is of critical importance for the CSPN SMWAN traffic encryption and decryption, as there is a time-based encryption on the NW packets. Usage of time-based encryption in the CH and Core system means that successful initiation relies on the CH receiving “Time Sync” from the Basestation.

Comms Hub time is therefore set to every 24hrs.

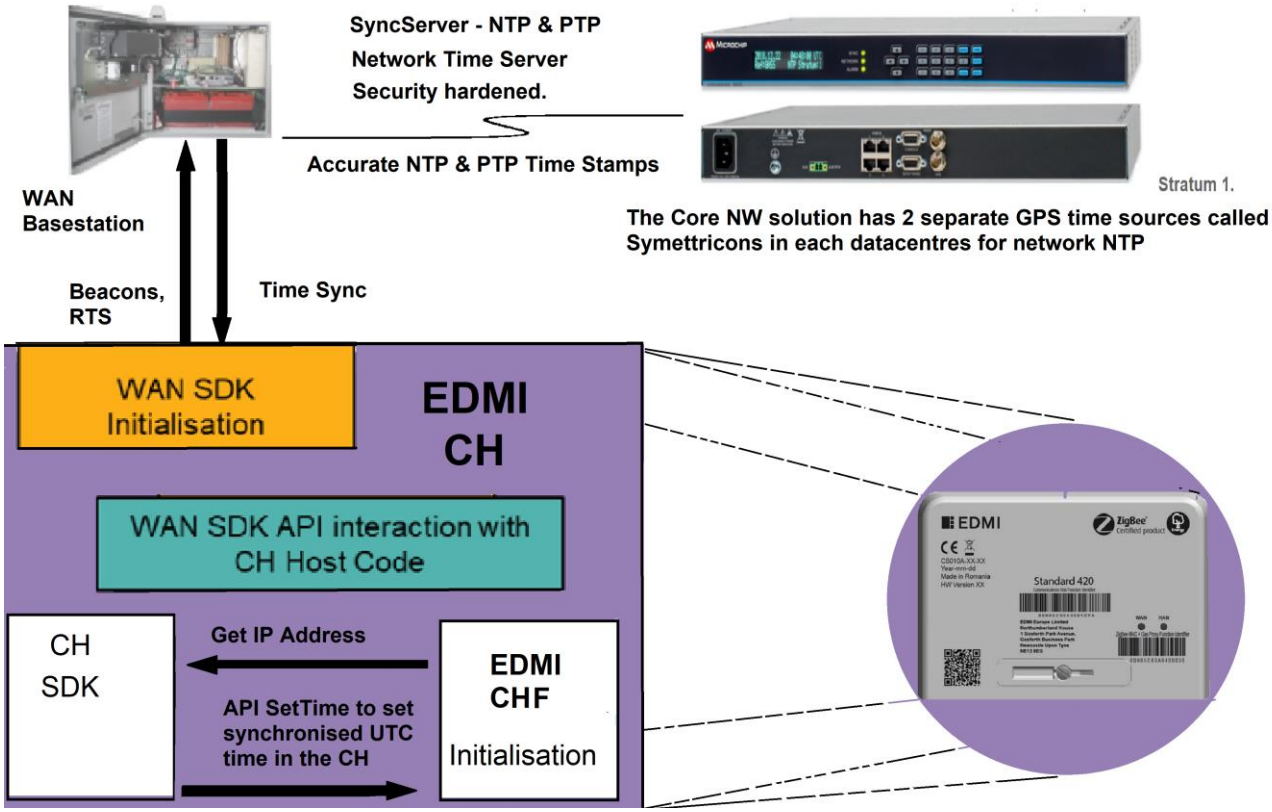
If for any reason the CH time drift occurs beyond a specific range the CH messages are likely to fail causing CSP-N systems to initiate alarms. The communication hub components are selected based on specification to ensure the comms hub time drift is not beyond few seconds in normal operating conditions of the components.

2.1.1.3 Time in CH Initialisation and WAN acquisition process.

The CSP-N CH at every bootup cycle - brand new install, CH reset (unplanned reboot) & CH FW upgrade (planned reboot) - will undergo an initialisation sequence. As part of this initialisation sequence the Basestation will provide a “Time Sync” every 90 seconds.

Once the hub achieves “Time Sync”, it acquires an IP address and initialises its other sub systems (see diagram). Therefore, at every boot up the CSP-N Comms Hub will function with accurate time; during initialisation it behaves as in a 'no WAN' state.

2.1.1.4 Method used for Accurate Time

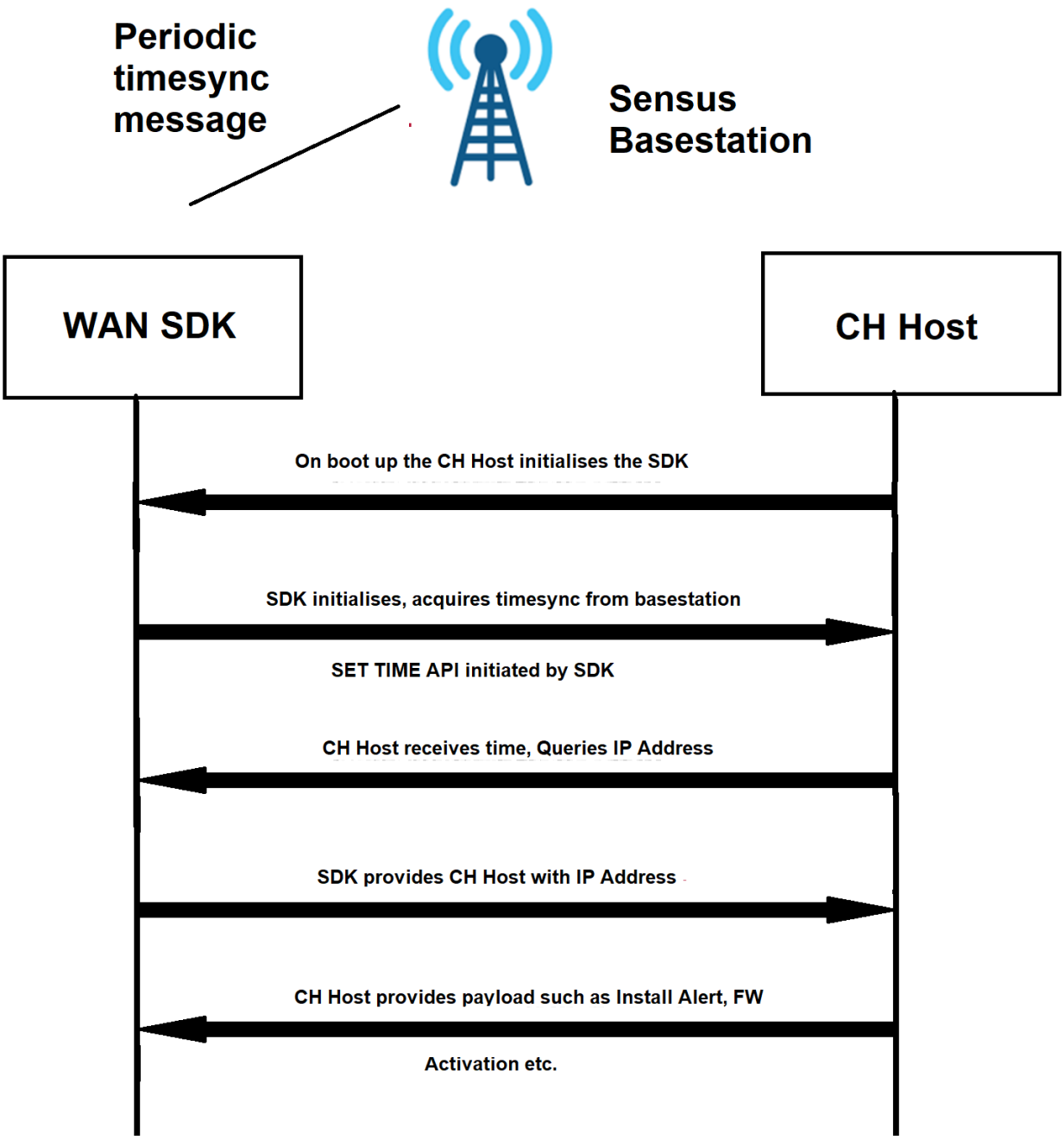


CH time is governed by the CH WAN SDK with the NW providing its 'Reliable' time source. The CH bootloader initiates the CH SDK, which during the initialisation goes through the steps of acquiring time.

2.1.1.5 Steps associated with getting Accurate Time

The CSP-N Basestation broadcasts a Time Sync message to each CH within its reach, at full power. The CH requires time and IP address to ensure it has connectivity to WAN and continue operation. The latency between the Basestation time and the CH time would be expected to be very minimal.

Upon initialisation the CH undergoes WAN joining tasks as shown in the follow diagram:



Upon initialisation the CH performs the following tasks:

- Getting a “Time Sync” from the Basestation
- Obtaining an IP address
- Pushing an Install Alert and WAN payload

CH which are installed will get a “Time Sync” message from the base station every 24 hours, from the time of first “Time Sync” received during time of install or from the time of a reboot.

2.1.1.6 Triggers for getting Accurate Time

Although the EDMI CH can flag its time as “invalid”, the CH does not attempt additional Time Syncs in addition to its normal operational daily synchronisation.

Time is only marked as “invalid” in the time between HAN starting and WAN Time Sync occurring, typically <90 seconds following any CH reboot.

2.1.1.7 Time Handling after Power Restoration when RF Reception is Impaired

After a power outage, the EDMI CH enters a managed power down protocol known as “Last Gasp”. This allows the last known time to be persisted and the UTC time in seconds will resume from that time when power was restored.

In the case where radio reception to the CH is impaired (ie no WAN), the absence of a subsequent Time Sync signal from the network results in the time remaining “invalid” and may be significantly behind “real” UTC time.

On re-establishment of WAN communications, time will be re-aligned automatically.

2.1.1.8 Time Handling after Reboot when RF Reception is Impaired

The EDMI CH may reboot on a critical software error or failure to communicate with an internal subsystem - e.g. the Zigbee Chipset.

When an unplanned reboot occurs, the EDMI CH is forced into an unmanaged re-start and its last known time is not persisted.

A change has been made to improve handling in this area, as shown in the following table

EDMI CH FW Version	EDMI CH Handling
Earlier version prior to GBCS 3.2	On boot-up the clock uses “seconds since power-up”.
GBCS 3.2 based releases (V3.x.x)	On boot-up the clock uses a back-up time reference to restore a better approximation of current UTC time

Note that in both cases, the CH clock time is marked as “invalid” until Time Sync has occurred.

2.1.1.9 Scheduling a CH Time Sync

For the EDMI CH, CH time is synchronised only once in every 24 hours starting with the first Time Sync after boot up.

The EDMI CH does not set its Time representation value to 0xFFFFFFFF, even in the event of a prolonged no-WAN incident. If there is not direct WAN access, the CH will attempt to obtain WAN Time Sync bursts indirectly through neighbouring CHs and time will be re-synchronised every 24 hours as normal.

Where no direct or indirect WAN access is available, the CH will continue to free-run its clock which has a nominal drift of <1 second per day until WAN access is re-acquired.

2.1.2 CSP-S&C Comms Hub Time sync Overview

2.1.2.1 Usage of GBCS defined Time Solutions

The Toshiba and WNC Communications Hubs have no functionality to query or correct its time via GBCS defined SRs, as they use SM2M instead. SM2M (smart m2m) is the trusted time server to the communication hubs in the CSP-C&S region. A communication hub sends a message to server when its clock needs to be synchronized. This message is queued to be sent out and is retried over the WAN.

Proposals for the energy supplier to ascertain remotely whether time drift in the meter or comms hub time has occurred is found in this document: Information to assist with the calculation can be found in section 2.1.3 below.

2.1.2.2 Need for Accurate Time

CSP-S&C comms hub design has a requirement on daily drift up to a maximum of 1 second per day, therefore every 9 days (for a maximum of 9 seconds drift) from the last Force Time Sync response, the CH will request the time from the server by sending a Push Time Sync command. The time is CH Time Management then synched, and the Force Time Sync response is received, ensuring the 9-day process begins again.

2.1.2.3 Time in CH Initialisation and WAN acquisition process

As part of the Birth Event process, a brand-new CH sends a Force Time Sync Command within the first hour of activation. This command Force Time Sync is normally retried over 8 days (with the exception on Birth Event when it is within 1 hour).

The server retry on Force Time Sync command is configurable and can be adjusted to improve performance and capacity. A persistent retry is performed during the initial hours, which is subsequently spaced up to 8 days.

The ForceTimeSync response stores the information to perform a very accurate drift assessment, only impacted by the time difference in the latency of two consecutive ForceTimeSync commands. Such difference would be small and very stable under normal operating conditions, hence having no impact synchronising the CH time).

2.1.2.4 Method used for Accurate Time

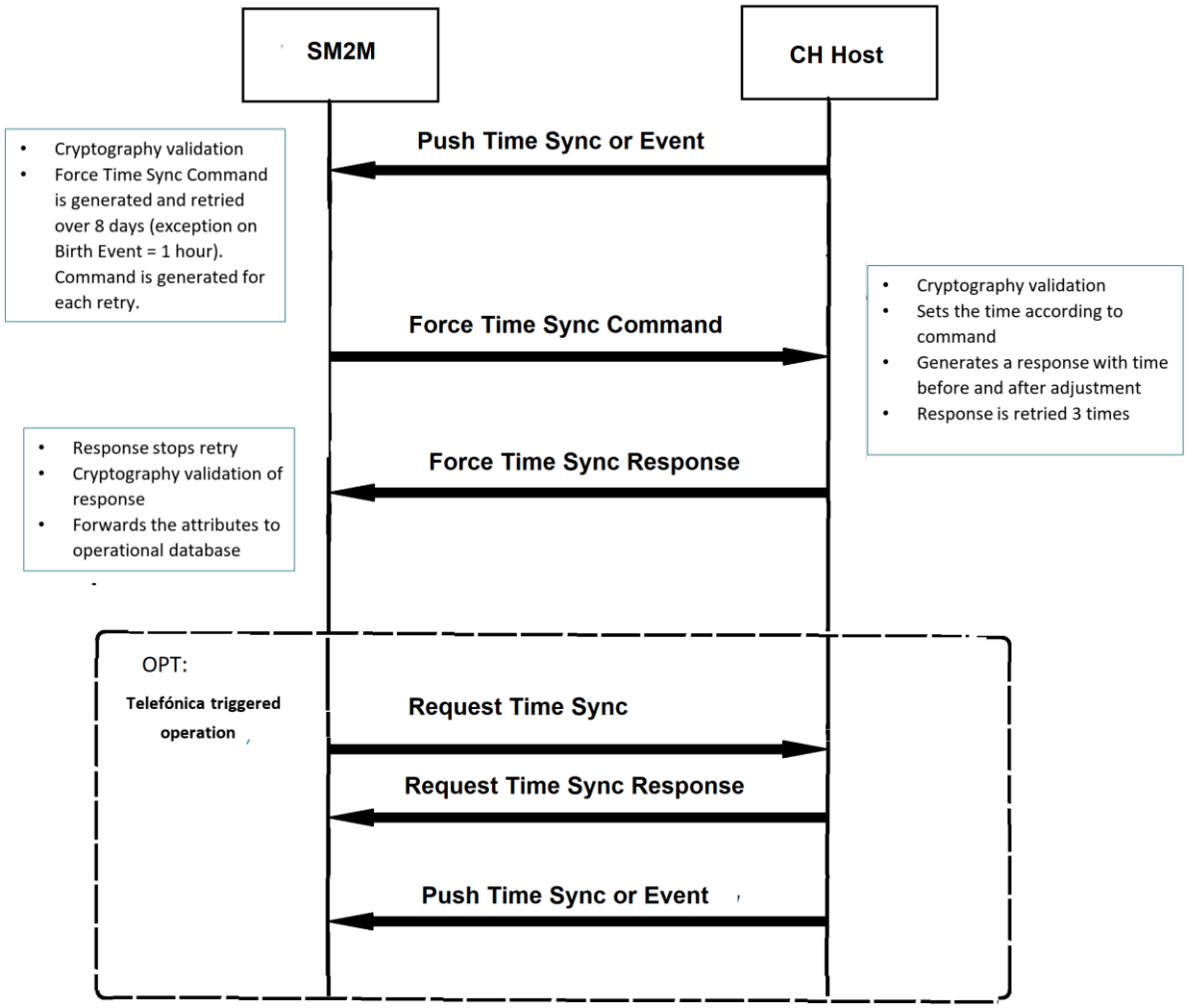
Within SM2M, the following Device Monitoring & Management (DMM) internal messages are used:

DMM Message Name	Comments / impact to supplier
ForceTimeSync	CSP-S&C CH design has a requirement on daily drift up to a maximum of 1 second per day, therefore every 9 days (for a maximum of 9 seconds drift) from the last Force Time Sync response, the CH will request the time from the server by sending a Push Time Sync command. The time is then synched, and the Force Time Sync response is received, ensuring the 9-day process begins again. Force Time Sync Response stores the Time Sync info from the CH into the SM2M operational database. Note that the SM2M operational database is only accessible by CSP-S&C.

DMM Message Name	Comments / impact to supplier
RequestTimeSync	Telefonica service desk and triage analysts can manually trigger an operation, whereby a Request Time Sync command is sent. This is performed as part of incidents, work orders and requests. This is localised analysis to target small groups of CH GUIDs (i.e. 8F0C investigation on a sample). This request is available via Telefonica Help Desk. A supplier cannot trigger a Time Synchronisation event for a given CH GUID via SSI, however they could ask CSP-S&C for a manual trigger event instead, after performing pre-assessment of clock drift.
PushTimeSync	In addition to events, there is a trigger message sent from hub to Sm2m designated PushTimeSync request which is used to maintain the clock drift within the allowed range by CHTS and GBCS.

SM2M (Smart m2m) is the trusted time server to the communication hubs in the CSP-C&S region. A communication hub sends a message to server when its clock needs to be synchronized. This message is queued to be sent out and is retried over the WAN.

2.1.2.5 Steps associated with getting Accurate Time



It is important to note, given the random nature of some of the events triggering the process, it is not easy to predict or align meters to the hub process.

2.1.2.6 Triggers for getting Accurate Time

There are several events which are intrinsic triggers, as time reliability is known to be impacted when they occur. Such events are:

-Birth Event

-New Firmware Activation Status

-Unplanned Reboot

-Supply Outage Restored

-Cold/ Warm Reboot

-Tamper

2.1.2.7 Time Handling after Power Restoration when RF Reception is Impaired

Both Toshiba and WNC CHs use the RTC as the time source on power up, however the time representation will always be 0xFFFFFFFF if Time Sync is not completed.

2.1.2.8 Time Handling after Reboot when RF Reception is Impaired

An unplanned reboot which results in the loss of Time Sync can occur when a CH needs to perform error recovery. Planned reboots will occur for example upon receipt of Device management (DMM) commands: Warm Reboot and Cold Reboot, or on Firmware activation after a CH firmware upgrade.

Additionally, Toshiba CH will perform a reboot as part of its WAN connectivity recovery mechanism (WAN self-heal) in Release 14.0 onwards.

Both Toshiba and WNC CHs use the RTC as the time source on reboot, however the time representation will always be 0xFFFFFFFF if Time Sync is not completed. The only time a CH has 'Unreliable' time is immediately after its reboot, for a short window, while awaiting its Time Sync.

2.1.2.9 Scheduling a CH Time Sync

The Toshiba CH calculates its time drift over a 9-day period as being typically around approximately 5 seconds.

The WNC CH calculates its daily time drift as less than 0.259 seconds (i.e. not more than 86400 / 1,000,000 * 3). The maximum time drift over a 9-day period will not be over 2.33 seconds.

The WNC and Toshiba CH generate a Push Time Sync (Internal DMM Command) on expiry of the 9 days countdown timer from when the previous Push Time Sync is sent. It is possible that there may be some drift as the countdown timer is not managed by the RTC. As it is timed from the 9 days timer, there is no set time of day for the Time Sync.

After a WNC CH has completed a Force Time Sync, its time representation will NOT become 0xFFFFFFFF even if the WAN connection is dropped unless the CH reboots during the WAN incident. The 0xFFFFFFFF is only used when the WNC CH reboots following a No WAN scenario.

For the Toshiba CH, if Time Sync does not happen successfully (due to loss of WAN) on the 9th day, it will continue to operate with its clock. In this situation its time representation is not marked as 'Unreliable' or set to 0xFFFFFFFF.

2.1.3 Pre-assessment of clock drift

There are two methods for an energy supplier to ascertain remotely whether either the meter time, the comms hub time or both have drifted where a meter fails to synchronise its time with the comms hub, are proposed below.

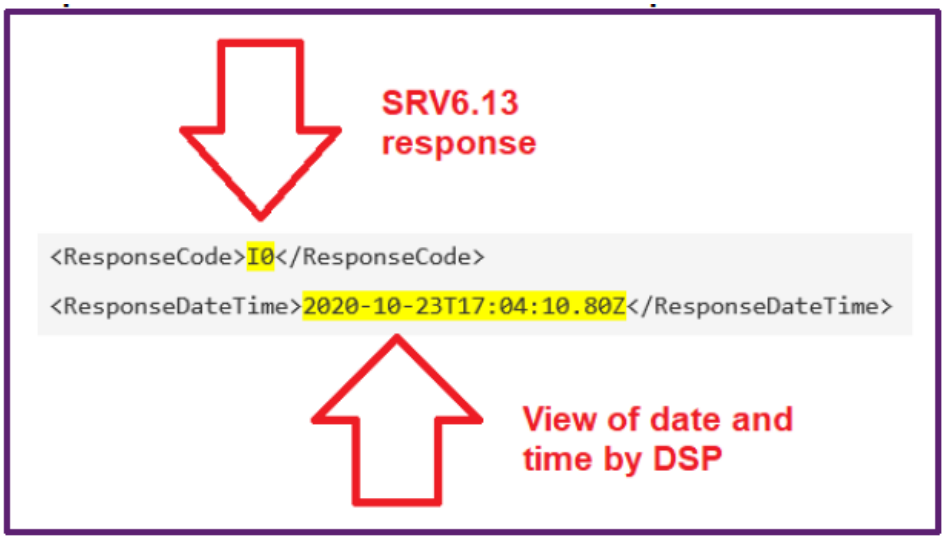
To perform this assessment, CSP-S&C suggests the use of 2 service requests which they trust are widely used by Industry.

In a situation a supplier may suspect of a hub time problem, there are a few steps available for a pre-assessment of clock drift, which may help with a decision on whether to raise an incident for a Telefonica assessment and provide details of the suspected drift. These methods rely on certain assumptions associated with message processing and throughput and provide a useful indicator to flag up a potential timing problem.

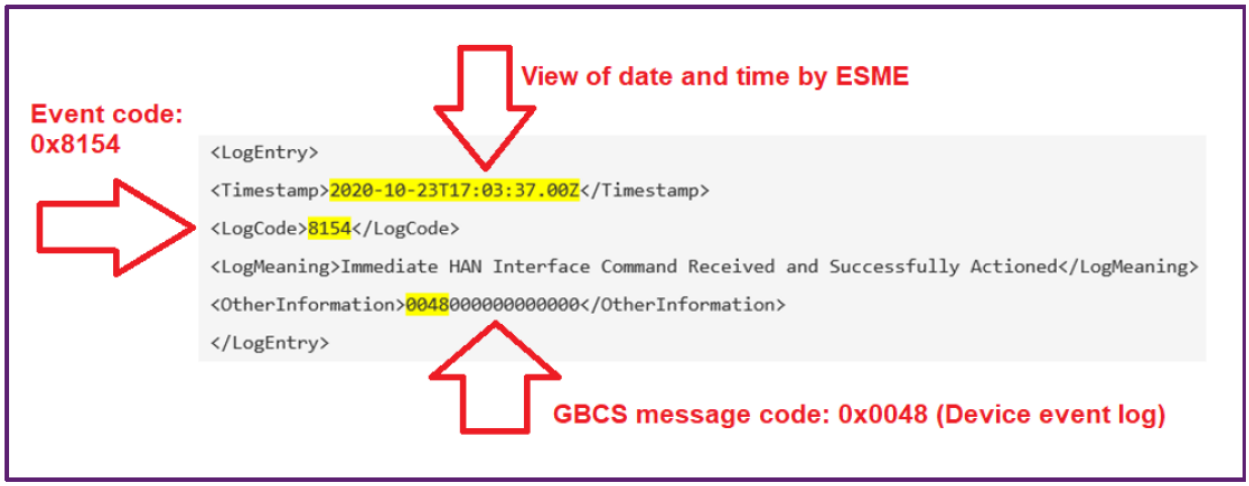
2.1.3.1 Method using information in SRV6.13 Read Event Log command

The approximate time drift can be calculated based on two-time references contained within the SRV6.13 Read Event Or Security Log service request response.

1) T1: DSP time which is stored in the “ResponseDateTime” XML field. This is the DSP time for when it processed the Device Response for SRV6.13.



2) T2: Device Time which is the timestamp against the “Event / Alert Code 0x8154” in the event log for processing SRV6.13 command (the MMC ‘LogCode’ is 8154).



a. For CH: **MMC ‘OtherInformation’ is 0x0093**. The otherInformation should be 0x0093 which is the GBCS Message Code for SRV6.13 (ECS35c) Read CHF Event Log Command.

b. For ESME: **MMC ‘OtherInformation’ is 0048.** The otherInformation should be 0x0048 which is the Message Code for the SRV6.13 (ECS35a) Read ESME Event Log.

c. For GSME: **MMC ‘OtherInformation’ is 0014.** The otherInformation should be 0x0014 which is the Message Codes for the SRV6.13 (CS10a) Read ZigBee Device Event Log Command.

FORMULA: Device time drift = T1 – T2

The above calculation is an approximation based on the following assumptions (negligible time)

1) The DSP time is always accurate, and any DSP time drift can be ignored

2) The DSP processing time (SRV6.13 device response) can be ignored

3) The WAN latency (and, for the meter, HAN latency) can be ignored

4) The device processing time (for adding the event into event log and sending the response out) can be ignored.

Please note for that for the GSME, the calculation may not work for some gas meters if the GSME is attempting to conserve power (by turning of its radio before sending a Response, so delaying the Response send to the next wake up). In this case, there can be a gap of around 30 minutes. The calculation may factor this 30 minute gap into the equation.

Ensure the SR6.13 response includes the event entry required

Evidence from production devices shows that most devices appear to response to the SR6.13 command first and then log an entry in the Event Log afterwards. This means that a single SRV6.13 command would not be enough to calculate the time drift for a given device, as it will miss the Event Log entry for such SRV6.13 command. A second SRV6.13 would be required.

When using SR6.13 to read the event log, it is important to ensure the required event entry is included within the time window specified by the StartDateTime and EndDateTime as per the options shown below in order of preference being option 1 the preferred option depend on adapter limitations.

	StartDateTime	EndDateTime	example
1	*Now* – 1 day*	*today's midnight*	<ReadEventOrSecurityLog> <ReadLogPeriod> <StartDateTime>2021-02-01T15:30:00.00Z</StartDateTime> <EndDateTime>2021-02-02T23:59:59.00Z</EndDateTime> </ReadLogPeriod> <LogToRead>Event</LogToRead> </ReadEventOrSecurityLog>
2		Now*	<ReadEventOrSecurityLog> <ReadLogPeriod> <StartDateTime>2021-02-01T15:30:00.00Z</StartDateTime> <EndDateTime>2021-02-02T15:30:00.00Z</EndDateTime> </ReadLogPeriod> <LogToRead>Event</LogToRead> </ReadEventOrSecurityLog>
3		Last midnight	<ReadEventOrSecurityLog> <ReadLogPeriod> <StartDateTime>2021-02-01T15:30:00.00Z</StartDateTime> <EndDateTime>2021-02-01T23:59:59.00Z</EndDateTime> </ReadLogPeriod> <LogToRead>Event</LogToRead> </ReadEventOrSecurityLog>

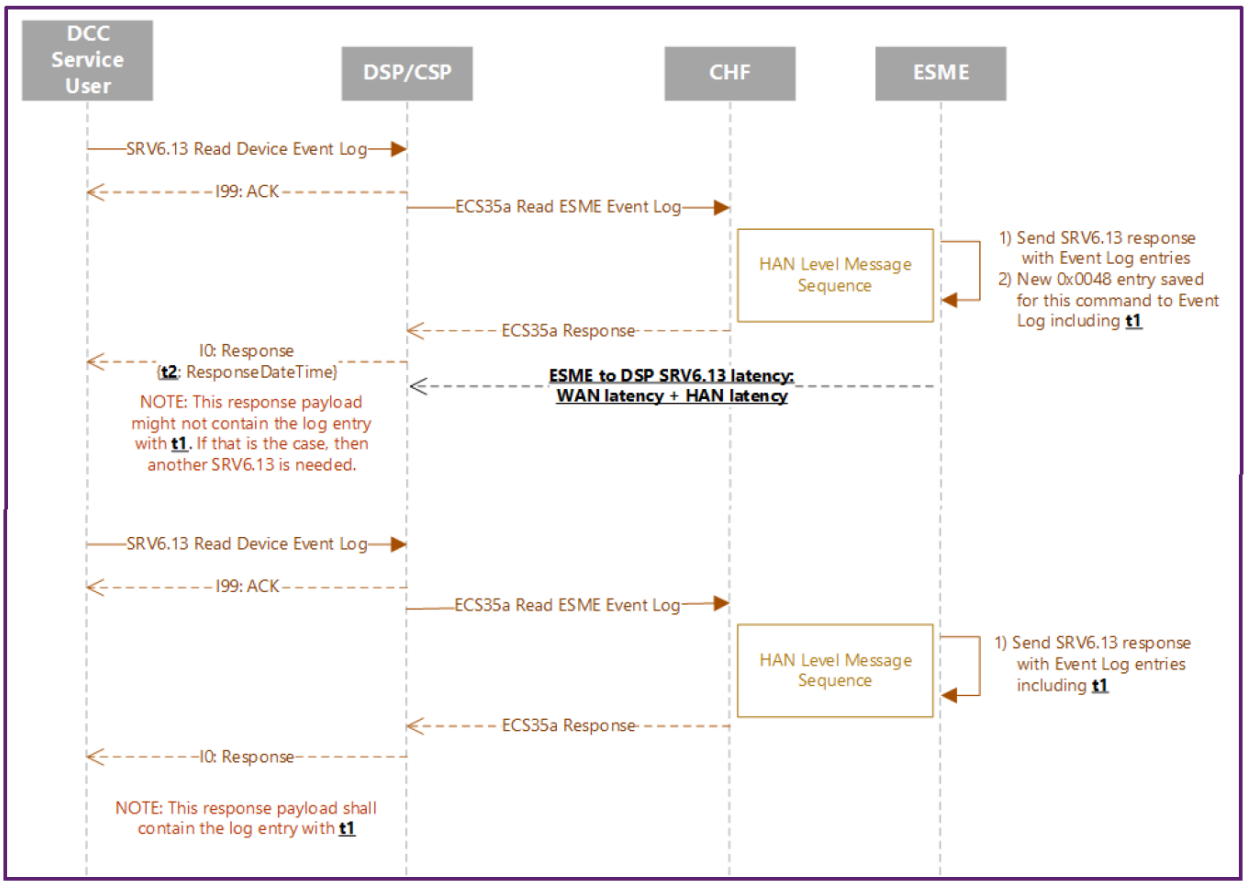
*where NOW datetime refers to the date and time at the moment of the execution of this SR6.13 command.

Calculation of meter time drift from DSP time

The message sequence chart below offers a view into the two time references needed to calculate the time drift for an ESME (same approach is also applied to a GSME), and those are,

- t1: Timestamp in the Event Log entry

• t2: Timestamp in the DSP XML I0 Response



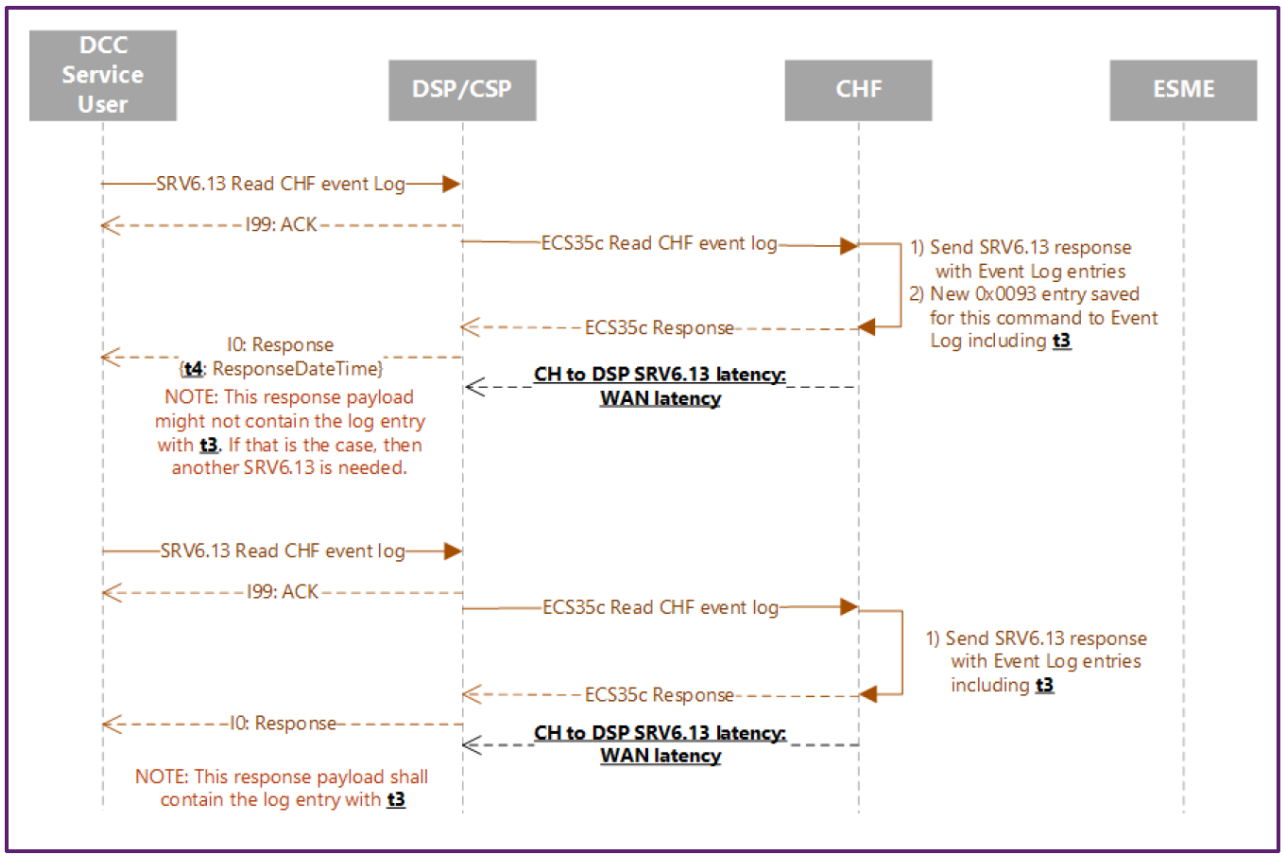
- $\boldsymbol{meter\ to\ DSP\ time\ drift \sim t2 - t1}$

Calculation of Communications Hub time drift from DSP time

The message sequence chart below offers a view into the two time references needed to calculate the time drift for a Communications Hub, and those are,

• t3: Timestamp in the Event Log entry

• t4: Timestamp in the DSP XML I0 Response



- $CH\ to\ DSP\ time\ drift \sim t4 - t3$

It would be possible to estimate the time drift between a Communications Hub and a meter, by using their individual time drift calculations from the DSP time and combining them.

- $meter\ to\ CH\ time\ drift \sim meter\ to\ DSP\ time\ drift - CH\ to\ DSP\ time\ drift$

2.1.4 Method using SRV8.9 and Event Log Entry

In a situation a supplier may alternatively use a method based on writing a separate entry in the event log prior to reading the log.

To perform this assessment, it is recommended to use 2 service requests widely used by Industry. The first command is a Read Command which will log and time-stamp an entry in CHF event log. The second command will retrieve the event log to read the time stamp from the first service request.

For the first command, send SR 8.9 (Read Device Log) to the CHF, or optionally SR 11.2 (Read Firmware Version). We will give the example of SR 8.9 CHF below. Please note the SR8.9 response includes only the last communications time of any HAN devices, and is therefore not a reliable method to determine the CH time drift alone.

If a CH clock drift is suspected the supplier should follow the approach below and then raise an incident via the BAU process.

Send SR 8.9 to obtain T4 and T4a, record the ResponseDateTime from I99 and I0 (as per the example below):

```
<sr:ResponseCode>I99</sr:ResponseCode>
T4a: <sr:ResponseDateTime>2021-03-17T13:56:25.97Z</sr:ResponseDateTime>
```

<sr:ResponseCode>I0</sr:ResponseCode>
T4: <sr:ResponseDateTime>2021-03-17T13:56:33.35Z</sr:ResponseDateTime>

T4 = SR8.9 IO response time

T4a = SR8.9 I99 response time

Send SR 6.13 (Read Event Or Security Log) to obtain T3 covering the time SR 8.9 was sent, record the timestamp as per the example below.

There are limitations on the operational configuration of the SRV6.13 which are included in this document to make sure that the response contains the timestamped T3 entry.

<LogEntry>

T3: <Timestamp>2021-03-17T13:56:33.35Z</Timestamp>

<LogCode>8154</LogCode>

<LogMeaning>Immediate HAN Interface Command Received and Successfully Actioned</LogMeaning>

<OtherInformation>010F000000000000<OtherInformation>

</LogEntry>

T3 = Device Time which is the timestamp against the Event / Alert Code “0x8154” in the event log. The other information should be 0x010F when CH processed the SR8.9 command

Work out the WAN Latency following the below calculation:

WAN Latency= (T4 – T4a – CH Processing Time – DSP processing time) /2

but given the order of magnitude of processing times, it can be approximated by

WAN Latency= (T4 – T4a)/2

In order to calculate the time drift, carry out the below calculation:

T3 – T4 + WAN Latency + DSP Drift

DSP Drift will be unknown at the point of assessment. Given an unknown DSP drift, the supplier should only raise an incident when *(t3 – t4 + WAN latency)* is greater than 20 seconds or less than -20 seconds.

2.2 Guidance Point 2: Improved usage of Synchronise Clock (SRV6.11 and SRV8.1.1) commands

Guidance Point Number 2	GBCS 1.0	GBCS 2.0	
	X	X	
Guidance Type	Option to handle unexpected behaviour		
Functional Area	Time Drift		
Keywords	TS1316, SRV6.11, SRV8.1.1, 0x8F0C		

TOC data reviews have uncovered regular failures by Service Users to set the time in meters (ESME and GSME). This applies to both SRV6.11 SynchroniseClock (GBCS commands ECS70 or GCS28) and SRV8.1.1 CommissionDevice (GBCS commands ECS70 or GCS28).

The aim of this guidance is to propose a methodology to maximise success when setting meter times (ESME and GSME) via SRV6.11 and SRV8.1.1. It handles the case where the Communications Hub time falls slightly behind the DSP time, and is considered 'Unreliable', thereby triggering Alert 0x8F0C.

Both commands, SRV6.11 and SRV8.1.1, rely on two configuration parameters to succeed setting the time in the recipient meter to match the Communications Hub time,

• **CurrentDateTime:** Defined in DUIS as "The Supplier's current date-time, that define the "validity interval start", where a valid set is a valid date-time".

• **TolerancePeriod:** Defined in DUIS as "The maximum number of seconds that, added to the CurrentDateTime, define the "validity interval end", where valid set is >= 0 and <= 86400 (Note that for the GSME this may need to be at least 1800)".

These two parameters are used in combination to establish a validity time window, which the recipient meter would use as reference to decide if it can accept the Communications Hub time or not.

• **Validity_interval_start** (start time of the validity window) = CurrentDateTime

• **Validity_interval_end** (end time of the validity window) = CurrentDateTime + TolerancePeriod where the maximum TolerancePeriod is 86,400s or 24h.

As defined in GBCS sections 9.1.4 ECS70 Set Clock on ESME and 9.1.7 GCS28 Set Clock on GSME, the SRV6.11 or SRV8.1.1 success or failure criteria when processed by a meter is the following,

• Success (TimeStatus of 'Reliable'):

$$validity\_interval\_start <= Communications\ Hub\ Time <= validity\_interval\_end$$

• Failure (TimeStatus of 'Unreliable'):

$Communications\ Hub\ Time < validity\_interval\_start\ Communications\ Hub\ Time > validity\_interval\_end$

When configuring SRV6.11 or SRV8.1.1, Service Users default to the following values,

• CurrentDateTime = NOW datetime (timestamp of command creation in their DCC adapter)

• TolerancePeriod = 120s, 1,860s, 1,900s, 5,000s, 5,400s or other values (different values for different Service Users)

However, none of these configurations address the case where the Communications Hub time falls slightly behind the DSP time, CH time1, and hence outside the validity time window as illustrated in the diagram below.

Service User approach with reference (1) in diagram:

o CurrentDateTime = NOW datetime

o TolerancePeriod = 5,400s (or any other value smaller than the maximum value of 86,400s)

o CH time1 falls outside this validity time window causing SRV6.11 or SRV8.1.1 to fail.

Service User approach with reference (2) in diagram:

o CurrentDateTime = NOW datetime

o TolerancePeriod = 86,400s (24h)

o CH time1 falls outside this validity time window causing SRV6.11 or SRV8.1.1 to fail.

Improved Time Sync approach with reference (3) in diagram:

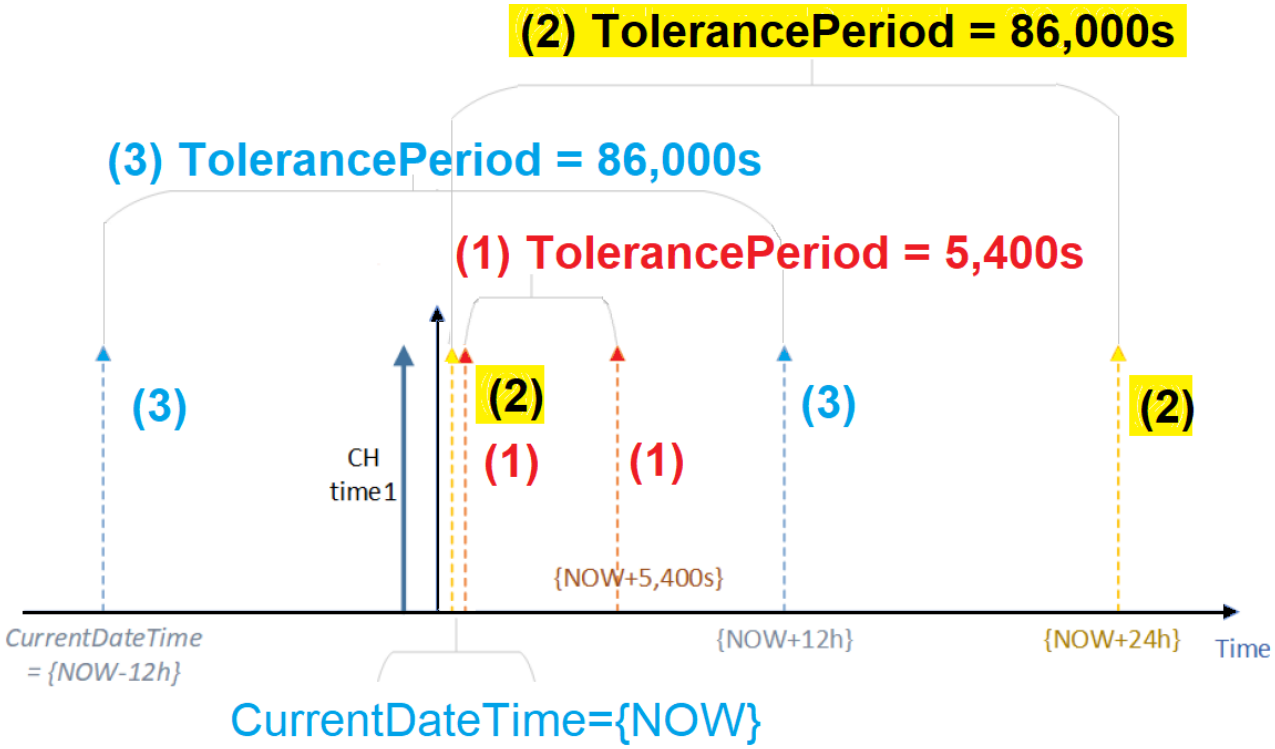
o CurrentDateTime = NOW datetime – 12h

o TolerancePeriod = 86,400s (24h)

o CH time1 falls inside this validity time window causing SRV6.11 or SRV8.1.1 to succeed.

When the Communications Hub time falls outside the validity time window, like for **CH time1** reference below, even by 1 second, an SRV6.11 or SRV8.1.1 would fail for approaches (1) and (2) and such failures could trigger an alert with alert code 0x8F0C “Clock not adjusted (adjustment greater than 10 seconds)” as per TS1316 – 8F0C Alert Triggers Query.

However, the improved Time Sync approach with reference (3) below would always cover the **CH time1** scenario and succeed.



DCC guidance to be followed by Users

Service User are recommended to adopt the proposed configuration to maximise success for SRV6.11 and SRV8.1.1:

- Set CurrentDateTime to NOW datetime (timestamp of command creation in their DCC adapter) minus 12h
- Set TolerancePeriod to 86,400s (24h).

Note to Service User about the DCC adapter limitations to this approach

DCC adapters have displayed some limitations when it comes to the configuration of the CurrentDateTime and the TolerancePeriod parameters in both SRV6.11 and SRV8.1.1. Generally, they are quite rigid and can even hardcode the configuration of both parameters not allowing any configurability level.

As a result, for some DCC adapters this improved Time Sync approach cannot be delivered, unless those DCC adapters are modified to allow for the required configuration ranges specified here.

2.3 Guidance Point 3: Billing Calendar Periodicity & Start Time

Guidance Point Number 3	GBCS 1.0	GBCS 2.0+	
		x	
Guidance Type	Clarification on system behaviour – this covers GBCS2.0+ working in comparison to GBCS1.0		
Functional Area	Billing Calendar, Configuration Data		
Keywords	GCS21d, GCS21k, GCS25, GCS25a, SRV6.2.3, SRV6.8, 0x8F0A Alert, TS0961, TS0742		

Clarification is provided on the Billing Calendar, covering Periodicity of Billing Calendar Data and Authority to Change. This is in response to DCC customers reporting that they do not know when the first billing alert will be generated.

A single Gas Billing Schedule is in place at any point in time, provided by the DCC Supplier, and snapshots are taken according to this schedule and added to the Billing Data Log. Once a new billing schedule is activated, the previous billing schedule is completely superseded.

2.3.1 Start Date Recommendations in SR 6.8

The reason for Billing Snapshots is given in Zigbee SEP v1.4 section D.3.4.5: "Where a permanent back-haul connection is not guaranteed, there are occasions when the values of data items need to be frozen for purposes such as consumer billing. The Snapshot mechanism is provided to satisfy this requirement."

DCC Users should recognise that the setting of a specific date-time and periodicity is equivalent to setting up a regime to action a reading on a particular day/interval. There is only ever one schedule in place (SMETS 4.6.4.2) and the readings are taken according to this schedule, so a new Billing Calendar Sequence will always result in snapshots being taken according to the new time.

In order for our customers to use the billing calendar effectively, the table below covers the factors that should be understood to resolve issues and make effective use of their back end system:

Start Date	Comments
Past	If a new Billing Calendar is set up with Start Date in the Past, the periodicity of time intervals is calculated to take the snapshot in the current time frame. In the Billing Calendar Mapping Table, the “startDateTimeAndPeriodicity” component within Billing Calendar object is defined as: “The date-time of the first billing calendar snapshot and the periodicity of following ones after that”. (GBCS Table 20)
Current	The GSME and GPF will be aligned to the new “startDateTimeAndPeriodicity” as soon as the GCS25 response is received. There are no readings for Nested and Overlapping Billing Periods between an old Billing schedule and its replacement.
Future	In setting a Billing Calendar to a future date, the old calendar details are lost as soon as the new date time becomes active. There are no readings during any Gaps created between an old Billing schedule and its replacement.

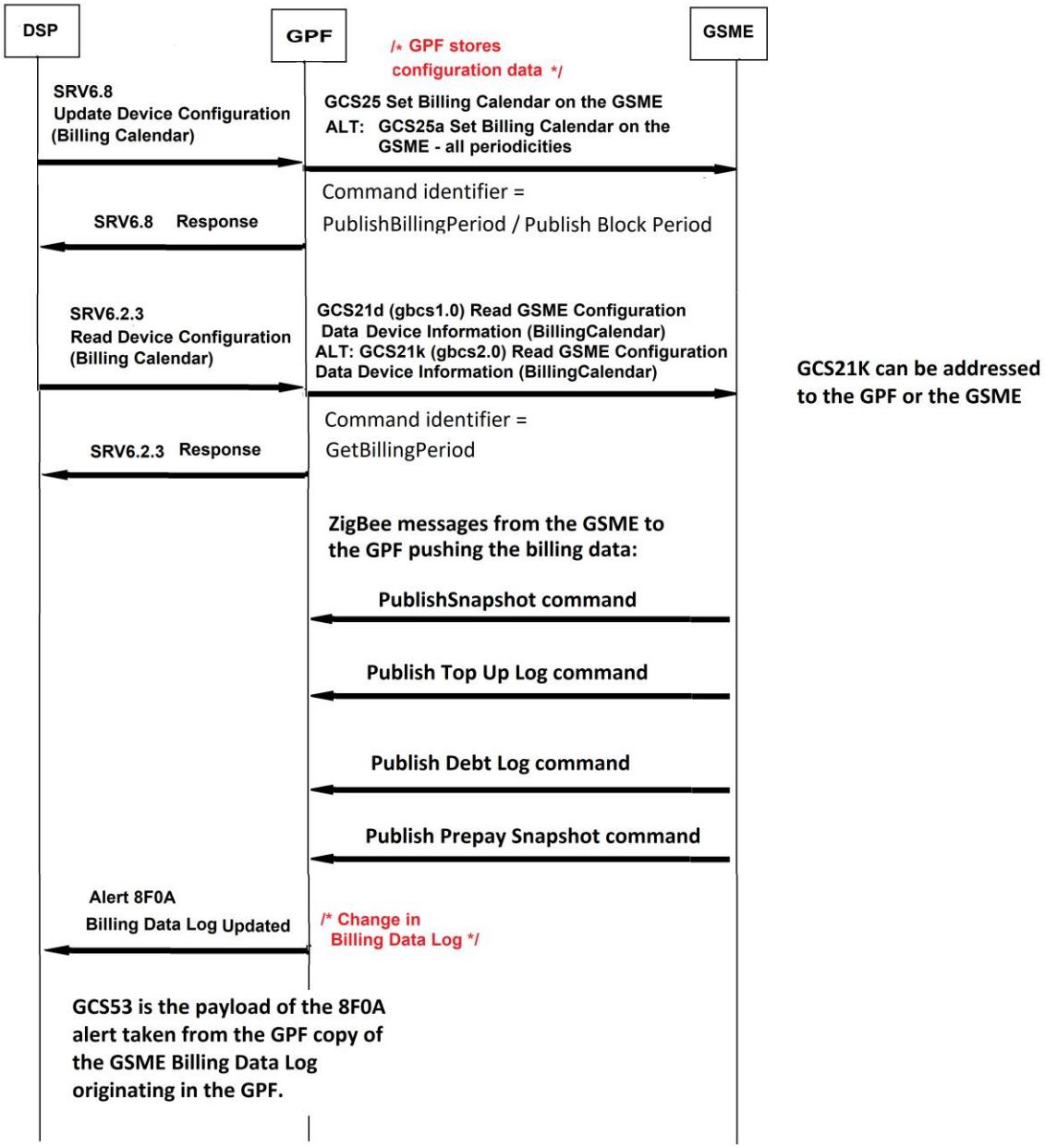
Start Date	Comments
	There is no mechanism in GBCS to cancel a billing calendar; this can only be done by replacement. However, if a supplier wishes there to be no snapshots taken, they can set a billing calendar start date-time a long way in the future.

It is recognised that the Configuration Data for the Billing Calendar can only be set by a Command and cannot be modified by the GSME or by the GPF, or other HAN devices.

2.3.2 The Expected Billing Calendar Sequence

The following scenario diagram (MSC) shows normal operation. It is designed to enable consistent behaviour of billing calendars and ensure that no consumption data is lost or duplicated when these data items are changed.

SR 6.2.3 could be used to read the billing Calendar on the GSME/GPF/ESME as set in SR6.8 (shown below), SR 4.4.3 could be used to retrieve the GSME/GPF/ESME billing log.



Setting Billing Calendar configuration data startDateTimeAndPeriodicity

Upon receipt of a SRV6.8 for GSME, the CH sends the TOM command CGS25 (SR 6.8) down to the GSME to provide SMETS configuration data to the meter, keeping a copy of this TOM command in the GPF. Configuration Data for the Billing start date-time and periodicity is provided in the GCS25 / GCS25a, which causes the GSME to set its Billing Calendar snapshot collection routine. This can only be set by a Command and cannot be modified by the GSME or by the GPF, which taps off a copy.

SMETS 4.6.4.2 requires that the GSME only support a single Billing Calendar. When a replacement start date-time and periodicity is received, this overrides the previously set instance.

Note that a GSME is not required to produce Billing Alerts - for Gas, these are produced by the GPF. See also GBCS section 10.4.2 for a list of triggers and contents for the Billing Data Log.

The 8F0A Alert has a Target Response Time (TRT) of 24 hours, not 60 secs as are common for most alerts. This is to handle any traffic peaks associated with a common reporting time and allows for it to be stored prior to or during transport.

2.4 Guidance Point 4: CoT Data Availability & Restrictions

Guidance Point Number 4	GBCS 1.0	GBCS 2.0 Onwards	
	x	x	
Guidance Type	Clarification on Comms Hub behaviour associated with Change of Tenancy (CoT).		
Functional Area	CoT		
Keywords	SRV3.2		

2.4.1 CoT date processing of Future Dated CoT Commands

The CHTS section 4.5.4.10 ‘Restrict GPF Data’ (SR 3.2 "Restrict Access For Change Of Tenancy") define a command that restricts 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 start).

SR3.2 could be DSP future-dated, but it 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. This field should match the ‘RestrictionDateTime’ value.
'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.

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

1. If the Supplier wants an immediate execution when the new tenancy 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 starting at a future date, it is recommended for the Supplier to build SR3.2 with a specified 'ExecutionDateTime' not earlier than the 'RestrictionDateTime'.

2.4.2 CoT and Data Restrictions

2.4.2.1 Data Group Items affected by CoT

In the event of a CoT, GBCS requires the following items to be restricted:

Data Group	Ref.	Comments
1. GPF Profile Data Log	CHTS 4.6.3.10	Provided via GPF
2. GPF Daily Gas Consumption Log	CHTS 4.6.3.7	
3. GPF Cumulative & Historical Value Store	CHTS 4.6.3.6	
4. Daily Read Log	GBCS 10.4.2.1	CH does not provide this data to PPMID/IHD. See GBCS section 7.4 on support by GPF / CHF.
5. Prepayment Daily Read Log	GBCS 10.4.2.2	
6. Billing Data Log	GBCS 10.4.2.3	

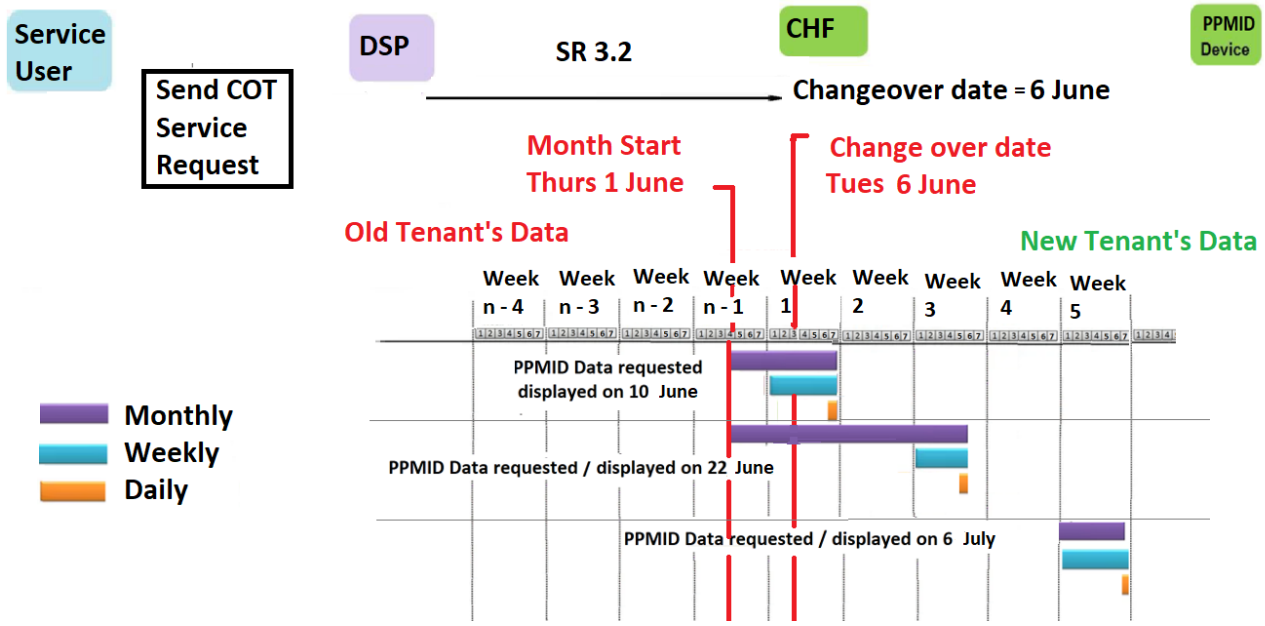
2.4.2.2 Interactions with HAN Devices

When IHD/PPMID requests tenant data for display from the GPF, the request will contain a start and end time (or equivalent).

For example, if the COT is set to 15-Mar-2019 8:15am, then for Half hour Profile data:

- The first available Readings will be the entry with timestamp as 15-Mar-2019 8:30am

The diagram below shows an example of the data from the CH that may be expected to be displayed on an IHD/PPMID:



DCC Users should note that this guidance point documents the current approach which is shared by all CH vendors on Cumulative Consumption (Current Day, Current Week and Current month).

2.5 Guidance Point 5: Device Interoperability Guidance

Guidance Point Number 5	GBCS 1.0	GBCS 2.0	
	x	x	
Guidance Type	Clarification on System Behaviour		
Functional Area	Interoperability		
Keywords	Device Compatibility, Device Interworking		

2.5.1 Issue Definition

DCC R2.0 has introduced 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.

Most of GBCS 2.0 Devices (SMETS2v3.1 or SMETS2v4.2) with a higher ZigBee version stack has been noted to work against R1 (GBCS 1.x) CH on a lower ZigBee version stack to get through installation & commission successfully.

2.5.2 GSME Potential Interoperability issue

As more billing periodicity is introduced in SR 6.8 from GBCS 2.x onwards, an interoperability issue has been identified between any SMETS2+ GSME built to GSMETS v3.1 or later connected to CHTS v1.0 CH. As detailed in Technical-Specification-Incompatibility-Matrix-v1.0 published by SECAS.

- A CHTS v1.0 GPF may not accurately mirror the GSME Billing Calendar.
- The frequency options available to the Billing Calendar for GBCS1.0 GSME are Daily, Weekly & Monthly. Later versions can also use Quarterly (three monthly), six monthly and yearly as well and so will not be recorded in CHTS v1.0 GPF.

The DCC user should be aware that

- CH/GPF compliant to GBCS 1.0 has stopped entering supply chain; DCC will upgrade Firmware from GBCS1.0 to GBCS 2.1 in accordance with the BAU process.
- It is recommended that the DCC User resends SR6.8 once the CH is upgraded to GBCS2.0, in order to avoid interoperability issues.

The table below is derived from Technical-Specification-Incompatibility-Matrix-v1.0 published by SECAS.

GSME version	CH/GPF version	Interoperability Status
1.0	1.0	No interoperability problem identified
1.0	2.0	No interoperability problem identified
2.0	1.0	• GPF will not support TOM Commands for Use Case GCS25a (SR 6.8) correctly. • Interoperability issues may arise as the Gas meter supports more billing periods than the GPF. CH/GPF compliant to GBCS 1.0 has stopped entering supply chain; DCC will upgrade Firmware from GBCS1.0 to GBCS 2.1 in accordance with the BAU process. It is recommended for DCC User to resend SR6.8 once CH is upgraded to GBCS2.0 in order to avoid interoperability issues.
2.0 onwards	2.0 onwards	No interoperability problem identified

2.5.3 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.

For Service Users introducing a new Meter FW compliant to SMETS2v3.1 or SMETS2v4.2 or SMETS2v5.0 with a R1.0 (GBCS v1.x) CH, the following actions are recommended:

- Test the I&C process in UIT/RTL to ensure that there are no I&C issues identified which may block the I&C process. This should include a 7-day soak test in addition to the on-site I&C process.
- Resend SR6.8 to configure the GSME after the CH upgrade has completed, otherwise the GSME Billing and associated functionality may not work as expected.

It is expected that the DCC User will incorporate these recommendations as part of their standard procedure when introducing new Meter FW into production.

2.6 Guidance Point 6: GPF default values

Guidance Point Number 6	GBCS 1.0	GBCS 2.0	
	x	x	
Guidance Type	Clarification on aspects of GPF defaults		
Functional Area	Gas Proxy Function default values		
Keywords	TS0956 IRP584 CRP620 SECMP0055		

2.6.1 Setting CommodityType on GPF

As per TS0956 and IRP584, the CommodityType value in the Gas ESI Endpoint shall be set to 0x01.

2.6.2 CF and CV default values for GSME & GPF

As per CRP620, the following table contains the default values to be used for calorific value (CV), conversion factor (CF), and associated variables. These CF and CV default values align to UK legislation.

Default Data Values for GSME and GPF Devices				
ZSE attribute	**ZSE Reference**	**SMETS Reference**	**Value**	**Notes**
CalorificValue	ZSE D.4.2.2.4.5	SMETS 4.6.4.3	0x190 (400)	Corresponding to 40.0 MJ/m^3
CalorificValue TrailingDigit	ZSE D.4.2.2.4.7	SMETS 4.6.4.3	0x10	
CalorificValueUnit	ZSE D.4.2.2.4.6	SMETS 4.6.4.3	0x01	MJ/m^3
Conversion Factor	ZSE D.4.2.2.4.3	SMETS 4.6.4.5	0x18F78 (102264)	Corresponding to 1.02264
ConversionFactor TrailingDigit	ZSE D.4.2.2.4.4	SMETS 4.6.4.5	0x50	

CRP620: Data items and values to be configured prior to installation of GSMEs and GPF

Note that the ZigBee Alliance is understood, at the time of writing, to be considering a change to the ZSE Conversion Factor default value, so that it is close to (but not the same as) that required by UK legislation (specifically, it would have a have a default value of 1, as opposed to the value of 1.02264 required by 'The Gas (Calculation of Thermal Energy) Regulations 1996').

2.6.3 Additional Note on CV & CF

There is a known issue in brand new CHs where the GAS consumption conversion in KwH will be wrong until SR6.6 corrects it. All CHs are impacted by this: the table below captures the values used in the currently supplied production CHs.

Prior to implementation of CRP620, the defaults used in the CH are based on the Zigbee values but contain errors which lead to inaccurate displayed data.

ZSE attribute	CRP620 Value	Zigbee Value	TOSHIBA	EDMI	WNC
CalorificValue	0x190 (400)	0x2625A00 (40000000)	0x2625A00 (40000000)	0x2625A00 (40000000)	0x2625A00 (40000000)
CalorificValue TrailingDigit	0x10	0x60	0x60	0x60	0x10
Actual CalorificValue	**40**	**40**	**40**	**40**	**4000000**
CalorificValueUnit	0x01	0x1	0x1	0x1	0x1
Conversion Factor	0x18F78 (102264)	0x10000000 (268435456)	0x10000000 (268435456)	0x10000000 (268435456)	0x10000000 (268435456)
ConversionFactor TrailingDigit	0x50	0x70	0x60	0x60	0x50
Actual Conversion Factor (CF) - volume correction factor	**1.02264**	**26.8435456**	**268.435456**	**268.435456**	**2684.35456**
Meter Energy Calculation					
Sample meter reading (1 unit)	1	1	1	1	1
Multiply by the volume correction factor (CF).	1.02264	26.8435456	268.435456	268.435456	2684.35456
Multiply by calorific value (CV).	40.9056	1073.741824	10737.41824	10737.41824	10737418240
Divide by kWh conversion factor [MJ into kWh] (3.6)	11.36266667	298.2616178	2982.616178	2982.616178	2982616178
Difference Factor	1	26.2492623	262.492623	262.492623	**262492623**

The following formula is used for the **Meter Energy Calculation** to convert gas volume to energy

$$\text{Energy (kWh)} = \frac{\text{Calorific Value (MJ/m}^3\text{)} * \text{Conversion Factor (CF)} * \text{Gas Consumption (m}^3\text{)}}{\text{Energy Conversion (MJ/kWh)}}$$

The value '3.6' is the Energy Conversion factor from MegaJoules [MJ] into kWh

2.7 Guidance Point 7: GPF behaviours associated with GSME half hour push

Guidance Point Number 7	GBCS 1.0	GBCS 2.0	
	x	x	
Guidance Type	Data Alignment between GPF & GSME		
Functional Area	GPF Half Hour Profile Data log, Daily Gas Consumption log, Historical Attributes		
Keywords	SR4.8.1, SR4.17, TS1323 TS1349		

2.7.1 Issue Definition

As explained in TS1323/TS1349, the GPF Active Import Profile Data, Daily Consumption Log, and Historical Attributes may not always be aligned with what is held in the GSME. Additionally, it has been noted that there are variations in CHTS/GBCS implementation between CHs from different regions resulting from differing interpretation of the Technical Specifications in this area. This has led to a level of Service User confusion as to expected behaviour and incidents raised.

This Guidance Point aims to:

- Provide Service Users with clarification on CH behaviour in different scenarios to tailor operations accordingly.

- Provide a core level of information to enhance understanding in this area and act as a basis for discussion points. These may assist with future specification change or SEC MOD if Service Users find a mismatch between the current CH behaviour detailed here and their expectations.

The main focus in this section is on the timings of the communication of data between GSME and GPF. Because the data is heavily time-dependant, accurate timing information allows the GPF to build up a clear picture of what is held on the GSME. Where the timing is less accurate or more open to interpretation, greater understanding of the underlying mechanisms and interpretations are needed to manage this.

Scenario	Summary of CH behaviour
1: GSME meter push at half hour but not exactly at GPF half hour boundary	The GPF is designed to use a 'sliding window' technique to assign the push data from the GSME into the appropriate half hour entry.

Scenario	Summary of CH behaviour
2: Multiple entries reported by the GSME for the same slot	CSP-S&C region: Before recording the value, the GPF checks if a value has already been reported for this time window, and if so the new value is ignored. CSP-N region: The GPF stores the value received, and waits until the next mirror to trigger the sample selection and profile log update. The sample nearest to the nominal time will be used for the record.
3: Time discrepancies between GPF and GSME of more than 20 secs	Generally, where the GSME time is consistently more than 20 secs slower than the GPF time, there will be no impact to the GPF half hour entry, but where the GSME time is consistently more than 20 secs faster than the GPF time, this will lead to a GPF entry offset with what is stored in the GSME time. In summary: Missing entries trigger a catch-up at a later stage, mistimed entries or duplicate entries may be ignored by the GPF.
4: Catch-up for missing values	For Toshiba and EDMI CHs: Checking for missing values takes place every 30 minutes For WNC CH: Catch-up is triggered at midday, on a 48-hour cycle.
5: CHF Clock time lost	For Toshiba and EDMI CHs: stops recording any updates in the Profile Data Log. Missing entries are marked as 0xFFs. Once the clock is set, the GPF will begin to record data items. The resulting gap in the Profile Data Log will later be filled using the catch-up process. For WNC CH: continues to record data in the Profile Data Log. This may lead to an offset in the values recorded in the Profile Data Log. Offsets and duplications in the GPF copy of the Profile Data Log are corrected by catch-up processing.
6: GSME recording and performing a push outside the half hour boundary	When a GSME does not record at the half hour boundary, the 'sliding window' technique applies to both data push and to the catch-up process. Unaligned timestamps will be rounded when matching the data to entries in the Profile Data Log, which may cause discrepancies between GPF and GSME.

2.7.2 CH behaviour associated with Half Hour Profile Data log

2.7.2.1 Scenario 1: GSME meter push at half hour but not exactly at GPF half hour boundary

In order for the GPF to build the GPF Profile Data Log for SR4.8.1, the CH expects that the GSME will push the gas consumption information to the GPF every half hour. Since the data pushed by the GSME does not contains a GSME timestamp, the GPF time when receiving the GSME push data will be used by GPF to calculate the half hour profile data.

From the GPF time point of view, if the CHF time is accurate, in the worst case, the time of receiving the GSME push data for the half hour could be any time between 20s before the half hour boundary to 20s before the next half hour, for following reasons: (see TS1349)

- the GSME may chose not to push the gas consumption data immediately if there are other priority tasks on GSME wake up,

- even when the GSME choses to push the gas consumption data immediately on wake up, there will still be a slight delay due to processing time

- radio conditions may lead to delayed message delivery and/or ZigBee retries

- since the Specifications (SMETS/CHTS/GBCS) allow for a maximum of 10 secs clock drift on both GSME and GPF, this means there could be up to 20 secs discrepancy between the respective GSME and GPF clocks.

To allow for the above conditions, the GPF was designed to use a 'sliding window' technique to assign the push data from the GSME into the appropriate half hour entry. There are differences between regions as to the timings of the sliding window. In the South and Central region, the window is 20 secs offset from the half hour boundary, and in the North region, the window is 15 minutes offset from the half hour boundary. This means it is possible the GSME push data for the half hour maybe allocated into different half hour in the GPF which cause mismatch as explained below with the example.

For CSP-S&C region, for half hour boundary x, GPF will accept GSME push data received between times x – 20 seconds inclusive, through to x + 29 minutes, 40 seconds exclusive, according to its own clock.

As an example, this rule means that updates received according to the GPF clock

- for GSME push data for 23:30:00,

o if received between 23:29:40.000 and 23:59:39.999 is considered to provide data for the 23:30:00 GPF Profile Data Log entry,

o if received, for example, at 23:29:38 will be considered to provide data for the 23:00:00 GPF Profile Data Log entry,

- for GSME push data for 00:00:00,

o if received between 23:59:40.000 and 00:29:39.999 is considered to provide data for the 00:00:00 GPF Profile Data Log entry,

o if received, for example, at 23:59:38 will be considered to provide data for the 23:30:00 GPF Profile Data Log entry,

- for GSME push data for 00:30:00,

o if received between 00:29:40.000 and 00:59:39.999 is considered to provide data for the 00:30:00 GPF Profile Data Log entry,

o if received, for example, at 00:29:38 will be considered to provide data for the 00:00:00 GPF Profile Data Log entry,

For CSP-N region, for half hour boundary x, GPF will accept GSME push data received between times x – 15 minutes inclusive, through to x + 15 minutes exclusive, according to its own clock.

As an example, this rule means that updates received according to the GPF clock

- for GSME push data for 23:30:00,

- o if received between 23:15:00.000 and 23:44:59.999 is considered to provide data for the 23:30:00 GPF Profile Data Log entry,

- o if received, for example, at 23:45:03 will be considered to provide data for the 00:00:00 GPF Profile Data Log entry,

- for GSME push data for 00:00:00,

- if received between 23:45:00.000 and 00:14:59.999 is considered to provide data for the 00:00:00 GPF Profile Data Log entry,

- if received, for example, at 00:15:03 will be considered to provide data for the 00:30:00 GPF Profile Data Log entry,

- for GSME push data for 00:30:00,

- if received between 00:15:00.000 and 00:44:59.999 is considered to provide data for the 00:30:00 GPF Profile Data Log entry,

- if received, for example, at 00:45:03 will be considered to provide data for the 01:00:00 GPF Profile Data Log entry,

Please note for the CSP-N region, processing and selection of the sample may not happen until the next mirror reporting, for example the 14:00 sample will not be available until the 14:30 mirror reporting, and if there is any communication outage, the 14:00 sample will not be available until the first mirror reporting received by GPF after communication outage.

As explained in the examples above, it is possible there will be half hour offset between the GPF Profile Data Log entry and the GSME Profile Data Log entry.

It is possible that either there is no data push (see Scenario 3) or multiple data pushes (see Scenario 2) being received for the same 30 minutes boundary. This could happen, for example, in the event of a Clock drift or of a Clock reset during any particular half hour period.

2.7.2.2 Scenario 2: Multiple entries reported by the GSME for the same slot

Multiple data pushes within the 30 minutes boundary would typically happen, for example, if the GSME submitted a report at the very beginning of the current rounding slot (e.g. 17:29:40 for a C&S hub), and the current value is reported at the very end of the current rounding slot (e.g. 17:59:39).

The situation of multiple entries reported by the GSME for the same slot may also happen if a GSME reports at shorter intervals, for instance if the GSME is reporting at time intervals shorter than the typical wake up cycle, such as at every 15-minute intervals.

For CSP-S&C region, before recording the value, the GPF will check if a value has already been reported for this time window, and if such a value has already been recorded, the new value will be ignored.

For CSP-N region, GPF stored the value received, and wait until the next mirror to trigger the sample selection and profile log update. The sample nearest the nominal time will be used for the record.

This will then cause mismatch between GPF and GSME half hour data log. The detail of the mismatch between GPF and GSME associated with this situation will be explained in Scenario 3 and 4 with examples.

2.7.2.3 Scenario 3: Time discrepancies between GPF and GSME of more than 20 secs

In production, it has been observed that, for some HAN sets, the time discrepancies between GPF and GSME are more than 20 secs. This is particularly pertinent for the CSP-S&C region.

In the situation where the GSME time is consistently more than 20 secs slower than the GPF time, there will be no impact to the GPF half hour entry, as found in the example below

GSME push time	GSME gas consumption	GSME half hour profile data	GPF receiving time	GPF half hour profile entry timestamp	GPF log
00:00:00	1		00:00:25		
00:30:00	3	2	00:30:24	00:30:00	2
01:00:00	6	3	01:00:26	01:00:00	3
01:30:00	10	4	01:30:27	01:30:00	4
02:00:00	15	5	02:00:25	02:00:00	5
02:30:00	21	6	02:30:24	02:30:00	6
03:00:00	28	7	03:00:23	03:00:00	7

Conversely, in the situation where the GSME time is consistently more than 20 secs faster than the GPF time, this will lead to a GPF entry offset with what is stored in the GSME time, as shown in the example below

GSME push time	GSME gas consumption	GSME half hour profile data	GPF receiving time	GPF half hour profile entry timestamp	GPF log
00:00:00	1		23:59:37		
00:30:00	3	2	00:29:35	00:00:00	2
01:00:00	6	3	00:59:36	00:30:00	3
01:30:00	10	4	01:29:37	01:00:00	4
02:00:00	15	5	01:59:36	01:30:00	5
02:30:00	21	6	02:29:38	02:00:00	6
03:00:00	28	7	02:59:34	02:30:00	7

In a more complex situation, where the time discrepancies between GPF and GSME are occasionally more than 20s, there will be missing and offset entries as well as duplicate pushes when this happens, as seen in the example below (showing potential errors/anomalies)

GSME push time	GSME gas consumption	GSME half hour profile data	GPF receiving time	Time Difference (in secs)	GPF half hour profile entry timestamp	GPF log
00:00:00	1		23:59:38	+22		
00:30:00	3	2	00:29:39	+21	00:00:00	2
01:00:00	6	3	00:59:39	+21	00:30:00	3
					01:00:00	Missing (this will trigger a catch-up at a later stage)
01:30:00	10	4	01:29:40	+20	01:30:00	4
02:00:00	15	5	01:59:40	+20	02:00:00	5
02:30:00	21	6	02:29:41	+19	02:30:00	6
03:00:00	28	7	02:59:41	+19	03:00:00	7
03:30:00	36	8	03:29:42	+18	03:30:00	8
04:00:00	45	9	03:59:41	+19	04:00:00	9

GSME push time	GSME gas consumption	GSME half hour profile data	GPF receiving time	Time Difference (in secs)	GPF half hour profile entry timestamp	GPF log
04:30:00	55	10	04:29:41	+19	04:30:00	10
05:00:00	66	11	04:59:40	+20	05:00:00	11
05:30:00	78	12	05:29:40	+20	05:30:00	12
06:00:00	91	13	05:59:39	+21	05:30:00	12 (the GSME push received at 5:59:39 is ignored by the GPF)
06:30:00	105	14	06:29:39	+21	06:00:00	27 (duplicate counting and the previous one is ignored)
07:00:00	120	15	06:59:38	+22	06:30:00	15
07:30:00	136	16	07:29:38	+22	07:00:00	16
08:00:00	153	17	07:59:39	+21	07:30:00	17
					08:00:00	Missing (this will trigger a catch-up at a later stage)
08:30:00	171	18	08:29:40	+20	08:30:00	18
09:00:00	190	19	08:59:41	+19	09:00:00	19
09:30:00	210	20	09:29:41	+19	09:30:00	20
Total		209				209

Please note all examples above are for CSP-S&C region. For CSP-N region, the same principle applies however with a window of 15 minutes rather than 20secs.

2.7.2.4 Scenario 4: Catch-up for missing values

It is possible that there are missing values in the GPF Profile Data Log, for example due to any of the following:

- Power outage
- Temporary loss of HAN communication
- OTA
- Conditions explained in Scenario 2 above, when GPF ignores later reports if multiple entries are reported by the GSME for the same slot
- Specific rare situations where catch-up is not possible

GPF will check for missing values periodically and then trigger the catch-up process by requesting the GSME Profile Data Log to retrieve missing values.

For Toshiba and EDMI GPF catch-up

- Checking for missing values taking place every 30 minutes,

- When retrieving missing samples, the GPF requests data for the range which covers the expected samples. For instance, if the GPF only has reports for 14:00 and 15:30, it will attempt to retrieve values for 14:30 and 15:00. The GPF will do this by requesting two Profile Data Log entries with timestamps greater or equal to 14:00:01. It may do this by requesting two Profile Data Log entries with timestamps greater or equal to 14:30:00.

For WNC GPF catch-up

- Catch-up is triggered at midday, on a 48-hour cycle.

- If a missing Profile Data Log entry is detected in the period since the last catch-up attempt, the start time is set to that of the previous valid entry plus one second, and the count is set to include all entries from this point until the current time. Data in the catch-up response will overwrite any data already held in the Profile Data Log

- For example, if the present time is 10/5 12:00, we will check from 10/3 12:00 to 10/5 12:00 if there is any missing data. If data is missing, we use last entry time +1 second as start time and the number of entries from missing data to 10/5 12:00 to catch-up. Missing the 10/4 12:00 entry would therefore request 24 entries, starting at time 10/3 11:30:01.

If the timestamps reported by the meter are not aligned to the “00” and “30” minute marks (which is a non-compliant GSME defective behaviour, as per TS1349), they will be rounded as previously described. Values will be ignored if the rounded timestamp already has a value assigned (for example if the GSME reports a value with timestamp 15:29:55; or values at both 14:30:00 and 14:45:00). As ZigBee Smart Energy uses a start time and count, if the meter reports at shorter sampling interval than 30 minutes (which is a non-compliant GSME defective behaviour), gaps may remain at the end of the catch-up log period.

In the majority of cases, the missing value is caused by GPF not receiving the GSME push for some specific reason (e.g. power outage, GSME OTA), the catch-up process will provide the missing entry and the GPF will be aligned with GSME for the missing entry.

However, in some situations, the catch-up process may lead to double counting if the missing value is the result of time discrepancies between GPF and GSME. This is more likely to happen with Toshiba GPF due to the short window of 20s and the catch-up happens every 30 minutes.

Using the CSP-S&C example above, it can be demonstrated that there is a potential discrepancy between GPF and GSME before and after catching up. This is shown below

GSME push time	GSME gas consum-ption	GSME half hour profile data	GPF receiving time	Time Diff. (in secs)	GPF half hour profile entry timestamp	GPF log before catch-up	GPF log after catch-up
00:00:00	1		23:59:38	+22			
00:30:00	3	2	00:29:39	+21	00:00:00	2	2
01:00:00	6	3	00:59:39	+21	00:30:00	3	3
					01:00:00	Missing (this will trigger a catch-up at a later stage)	4
01:30:00	10	4	01:29:40	+20	01:30:00	4	4
02:00:00	15	5	01:59:40	+20	02:00:00	5	5
02:30:00	21	6	02:29:41	+19	02:30:00	6	6

GSME push time	GSME gas consum-ption	GSME half hour profile data	GPF receiving time	Time Diff. (in secs)	GPF half hour profile entry timestamp	GPF log before catch-up	GPF log after catch-up
03:00:00	28	7	02:59:41	+19	03:00:00	7	7
03:30:00	36	8	03:29:42	+18	03:30:00	8	8
04:00:00	45	9	03:59:41	+19	04:00:00	9	9
04:30:00	55	10	04:29:41	+19	04:30:00	10	10
05:00:00	66	11	04:59:40	+20	05:00:00	11	11
05:30:00	78	12	05:29:40	+20	05:30:00	12	12
06:00:00	91	13	05:59:39	+21	05:30:00	12 (the GSME push received at 5:59:39 is ignored by the GPF)	12 (the GSME push received at 5:59:39 is ignored by the GPF)
06:30:00	105	14	06:29:39	+21	06:00:00	27 (duplicate counting and the previous one is ignored)	27 (duplicate counting and the previous one is ignored)
07:00:00	120	15	06:59:38	+22	06:30:00	15	15
07:30:00	136	16	07:29:38	+22	07:00:00	16	16
08:00:00	153	17	07:59:39	+21	07:30:00	17	17
					08:00:00	Missing (this will trigger a catch-up at a later stage)	17
08:30:00	171	18	08:29:40	+20	08:30:00	18	18
09:00:00	190	19	08:59:41	+19	09:00:00	19	19
09:30:00	210	20	09:29:41	+19	09:30:00	20	20
Total		209				209	230

As shown above, the catch-up process results in a total consumption figure calculated based on an over-estimation. Because the half hour profile figures are more than real consumption of the day - and the ‘missing’ value is not really ‘missing’ - some incorrect double counting is found in the catch-up figure results.

2.7.2.5 Scenario 5: CHF Clock time lost

CHF supports 3 different Time Status values, namely:

- 'Invalid' time : typically occurring due to a reboot, for example caused by a power outage or by a firmware upgrade and no Time Sync command received from WAN yet

- ‘Reliable’ time: occurs when received a Time Sync command from WAN

- ‘Unreliable’ time: occurs when no periodic Time Sync is received at the time the CH expects it.

If the Comms Hub has an 'Invalid' time (i.e. no time at all), it will not record any updates in the Profile Data Log. Once the clock is set, the GPF will begin to record data items. The resulting gap in the Profile Data Log will later be filled using the catch-up process. (Note that catch-up cannot proceed until a ‘Reliable’ clock is re-established as this is required to provide an end time for the

catch-up process). The Comms Hub is expected to restore its clock after the reboot, but the GSME may attempt to report during this interval.

'Unreliable' time is treated differently by the 3 Comms Hubs, as described below.

For Toshiba and EDMI CH catch-up:

Toshiba and EDMI GPFs will NOT continue to record data in the Profile Data Log while the CH time is 'Unreliable'. While CH time is 'Unreliable', CH GPF will mark the entry as 0xFF as missing values and ignore the GSME push data.

As soon as the CH time becomes 'Reliable' (for example, the WAN communication re-establish or Time Sync), Toshiba CH will:

- Retrieve the missing entries which are marked as 0xFFs by request data from GSME
- Start accepting the half hour push from GSME

For WNC CH catch-up:

It will continue to record data in the Profile Data Log. This may lead to an offset in the values recorded in the Profile Data Log, where they are rounded to an incorrect time slot (note that GSMEs will not synchronise with an 'Unreliable' clock, and as such the meter and GPF clocks would be expected to begin to diverge).

The GSME and GPF clocks may drift in different directions at different times, so the two clocks may drift in and out of phase until a 'Reliable' clock is re-established. This may lead to offsets and duplications in the GPF copy of the Profile Data Log, particularly when combined with catch-up processing.

2.7.2.6 Scenario 6: GSME recording and performing a push outside the half hour boundary

In GBCS section 10.4.2.8 it is stated that "The GSME shall, on each half hour, record the following information and push to the GPF"

DCC was notified by an Industry forum that some GSMEs do not record and push the data to the GPF at half hour boundary.

In the event of a GSME recording at half hour boundary but doing the push outside the associated half hour boundary, the 'sliding window' technique may result in the GSME data being associated by the GPF to a different time entry. This will depend on the time of the entry and the behaviour associated with the specific region where the GSME is located. Thus, if the push is more than 15 minutes after the "00" and "30" minute marks (e.g. at 17 and 47 minutes past the hour), the CSP-N GPF will assign the value to the following entry (e.g. data received at 14:17:23 will be recorded as the 14:30 Profile Data Log entry). The CSP-C&S region CHs will record this data as being in the earlier entry (i.e. 14:00 in the previous example).

A GSME may not record at the half hour boundary (defective non-complaint behaviour TS1349). For example, when the half hour intervals have been aligned to take place from the moment when it was powered on or commissioned, instead of aligning to the half-hour points. In this instance, the same principle of the 'sliding window' technique applies to both data push and to the catch-up process.

When performing a catch-up, the GSME may publish the unaligned timestamps, rather than at “00” and “30” minute points (although this is regarded as defective non-complaint behaviour). Such timestamps will be rounded as described before when matching the data to entries in the Profile Data Log, leading to further discrepancies between GPF and GSME.

2.7.3 CH behaviour associated with Daily Consumption Log (SR4.17)

The detailed scenarios described in this Guidance Point also apply across the longer daily period associated with the Daily Consumption log. The same principles for addressing them and timing considerations apply for this data as well.

Please note

1. The GPF profile log entry with timestamp of 23:30:00 will be used for the end of day calculation instead of 00:00:00. Consequentially, the consumption of the final half hour of the day will be used for the next day.

2. For Toshiba CH GPF daily consumption, the CH always adds the half hour consumption to work out the total consumption for the day, and this is from 00:00:00 (inclusive) to 23:30:00 (inclusive).

3. Different CH behaviour in relation to ‘Unreliable’ time also applies to the Daily Consumption log.

2.7.4 CH behaviour associated with Historical Attributes

While the detailed scenarios described in 2.39.2 also has applicability to Historical Attributes along with principles and timing considerations, suppliers should note that this data is limited in its availability to HAN only, impacting HAN device displays on PPMID/ IHDs.

Please note the different CH behaviour in relation to ‘Unreliable’ time also applies to Historical Attributes.

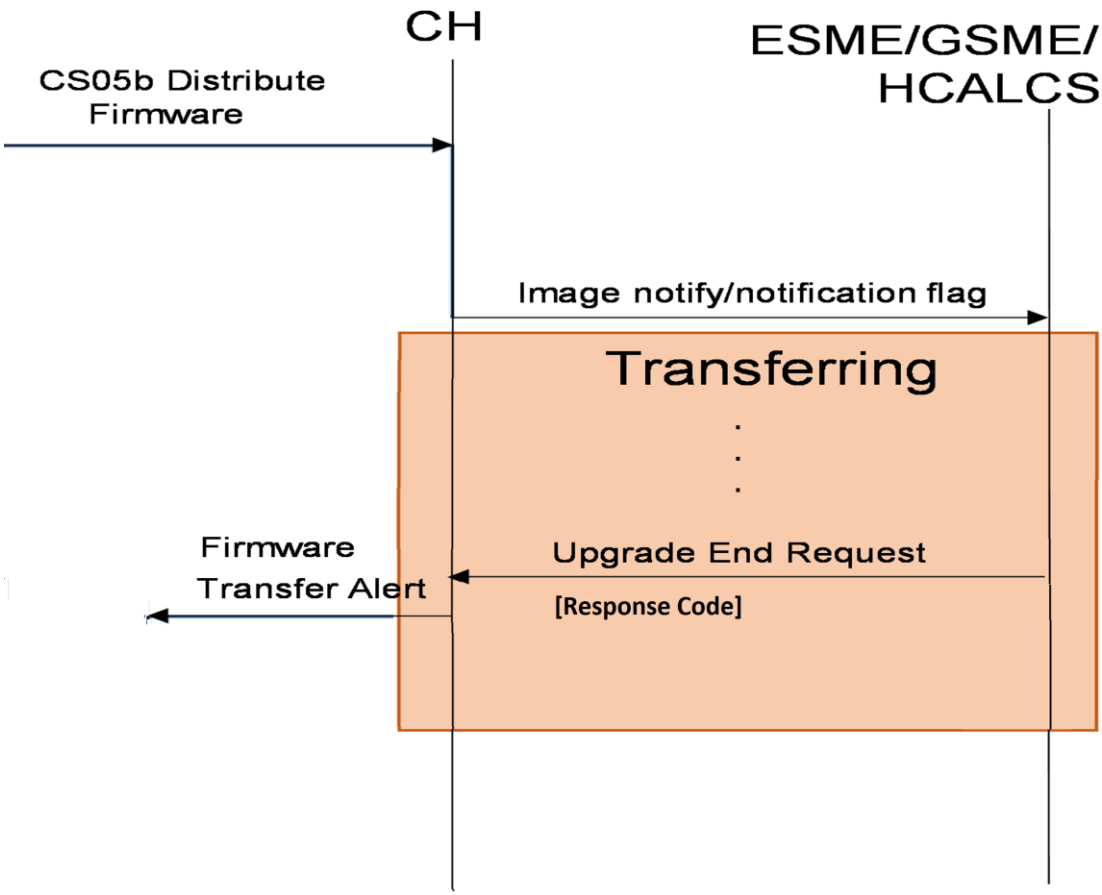
2.8 Guidance Point 8: Upgrade End Request status values

Guidance Point Number 8	GBCS 1.0	GBCS 2.0	
	x	x	
Guidance Type	Clarification on Upgrade End Request after OTA transfer to Device		
Functional Area	OTA		
Keywords	SRV11.1 SRV11.4 TS1519 SECMOD007		

2.8.1 OTA Transfer Handling

TS1519 was raised to clarify responses by the CH to an Upgrade End Request, which occurs at the end of the transfer of FW Image from CH to Device.

As well as successful transfer, the Device can indicate it has received an incorrect image or that the transfer process was prematurely aborted, e.g. due to HAN stability problems.



ImageNotify and the FunctionalNotificationFlags are used by ESME/HCALCS and by GSME respectively.

CH alerts the Supplier to indicate fileTransferSuccess or fileTransferFailure.

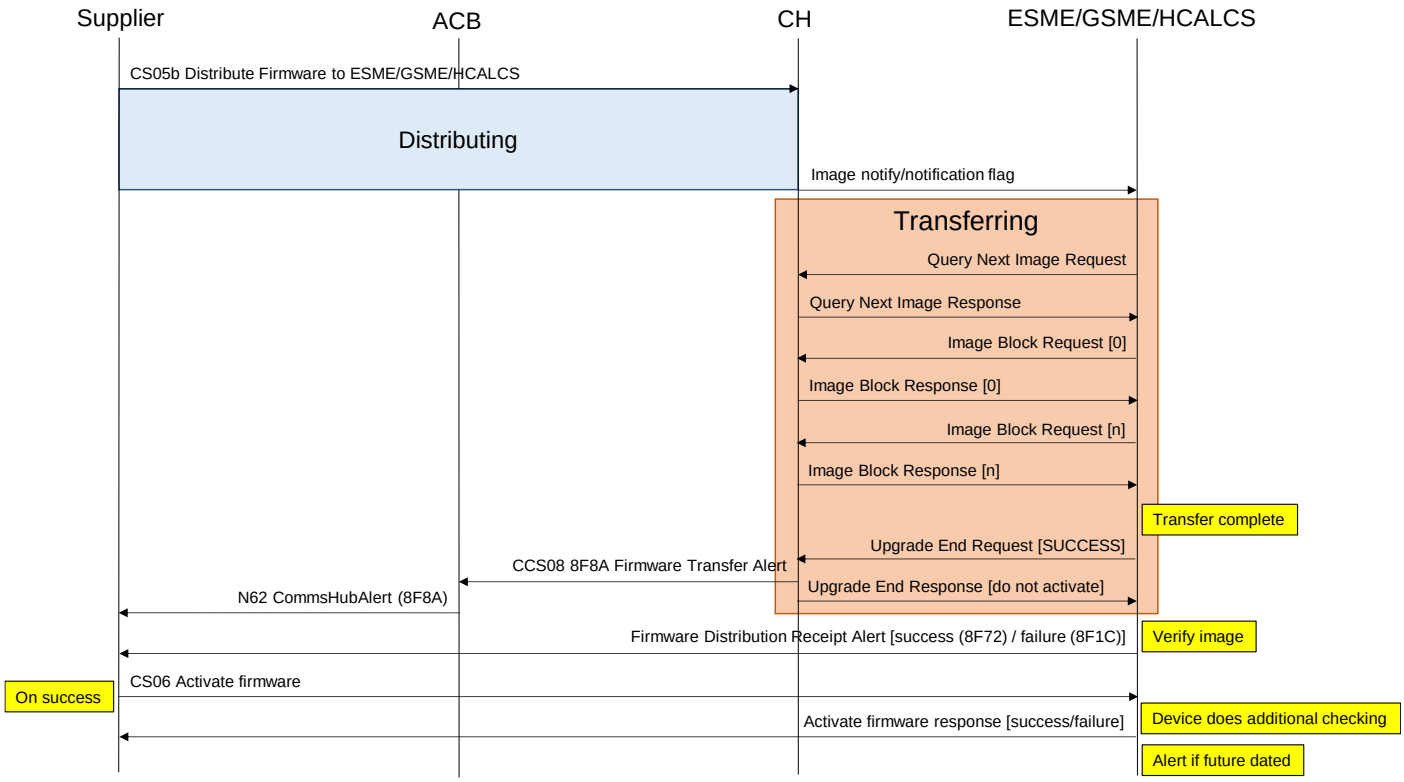
Upgrade End Request Response Code	FW Transfer Alert	Transfer response code	New OTA FW Flag / FunctionalNotificationFlags (GSME)
SUCCESS	0x8F8A	fileTransferSuccess	reset
INVALID_IMAGE	0x8F8A	fileTransferSuccess	reset
ABORT	0x8F89	fileTransferFailure	Not reset
REQUIRE_MORE_IMAGE	0x8F8A	fileTransferSuccess	reset

FW Transfer Alert is the same for all Devices, however there are differences between PPMID and other Device types (shown in MSCs here)

CH Implementations, whilst complying to the SEC Specifications, exhibit different behaviours which are covered below.

2.8.2 OTA Transfer to ESME/GSME/HCALCS successfully

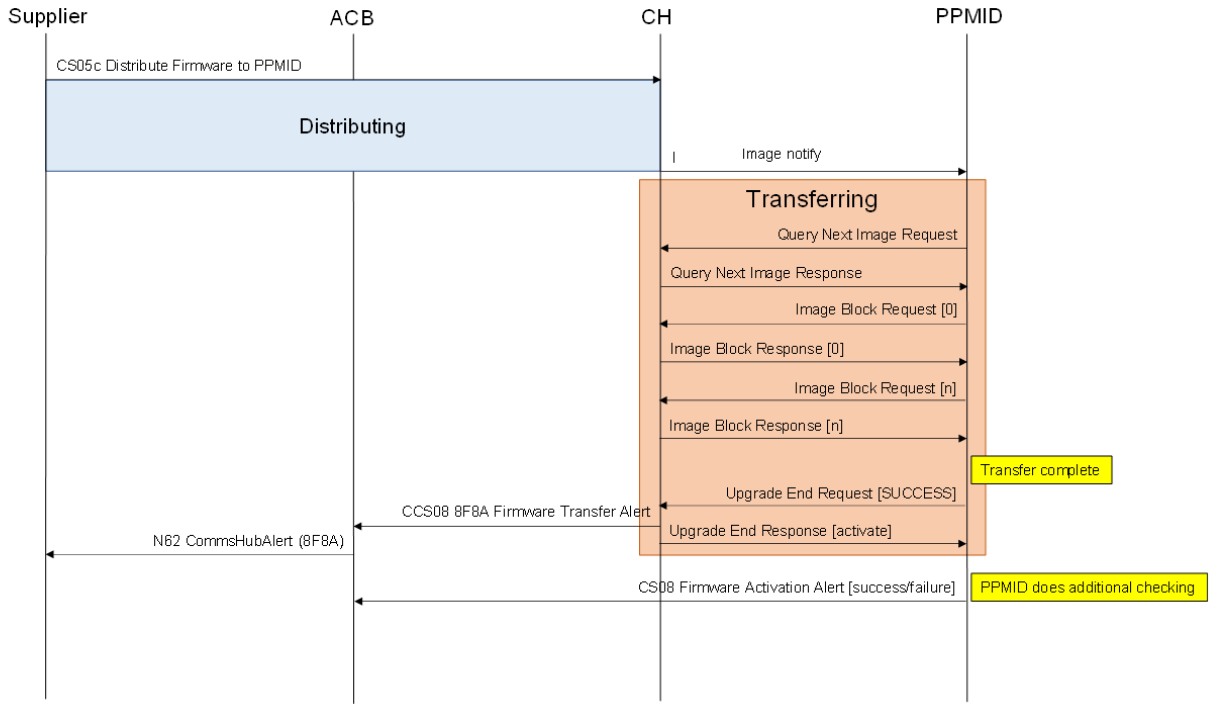
After the FW Image is transferred, the End Device performs additional verification checks and a further Alert.



“Verify image” in the scenario diagram above covers the Authorising Remote Party Signature check as per GBCS section 11.2.5.

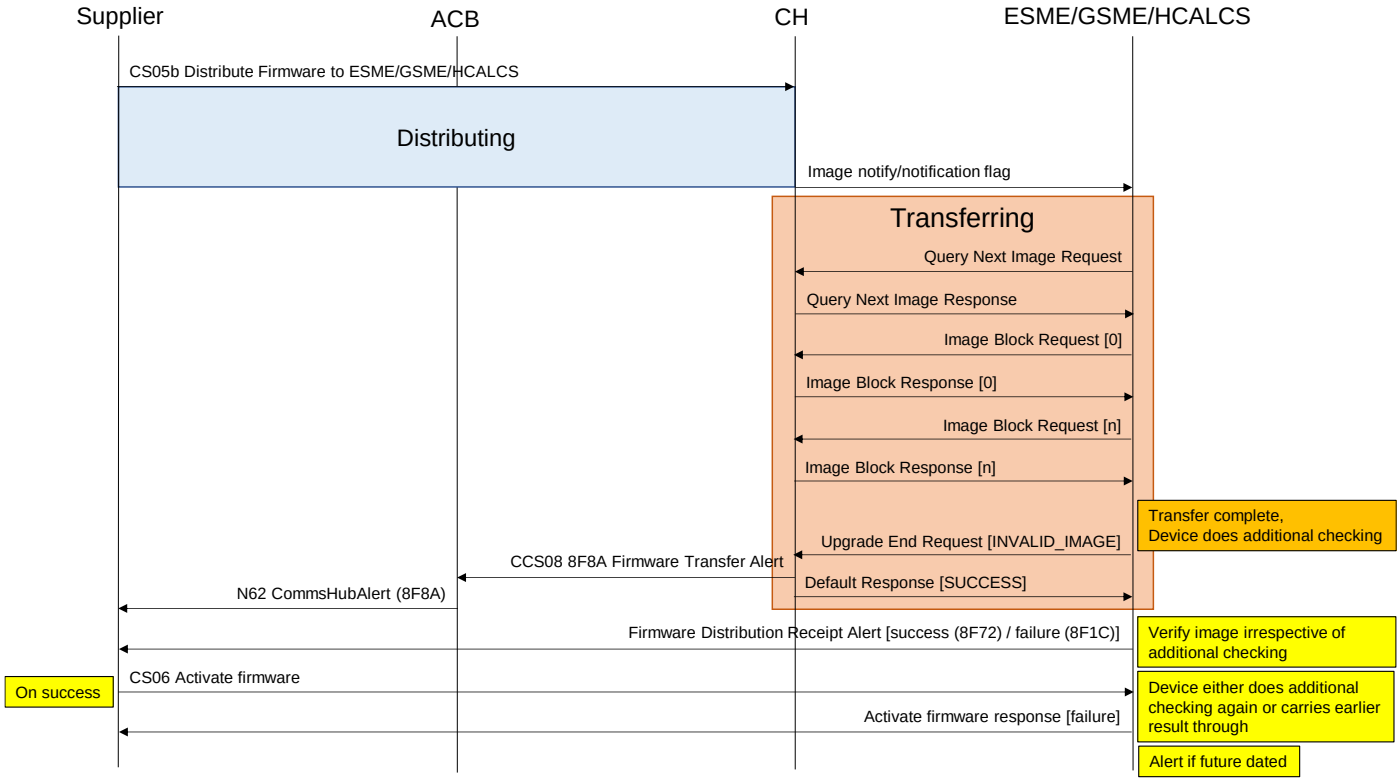
2.8.3 OTA Transfer to PPMID successfully

After the FW Image is transferred, the PPMID sends an activation Alert.



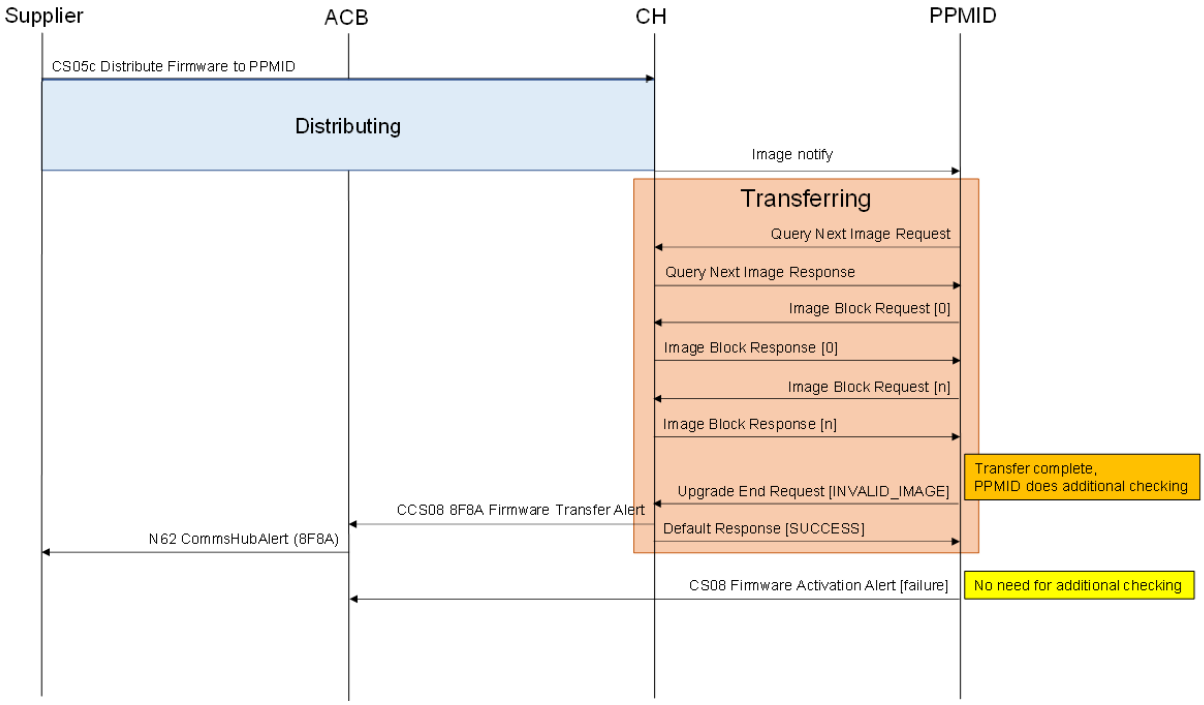
2.8.4 Incorrect FW Image Transferred to ESME/GSME/HCALCS

After the FW Image is INVALID, the End Device performs additional verification checks and a further FAILURE Alert.



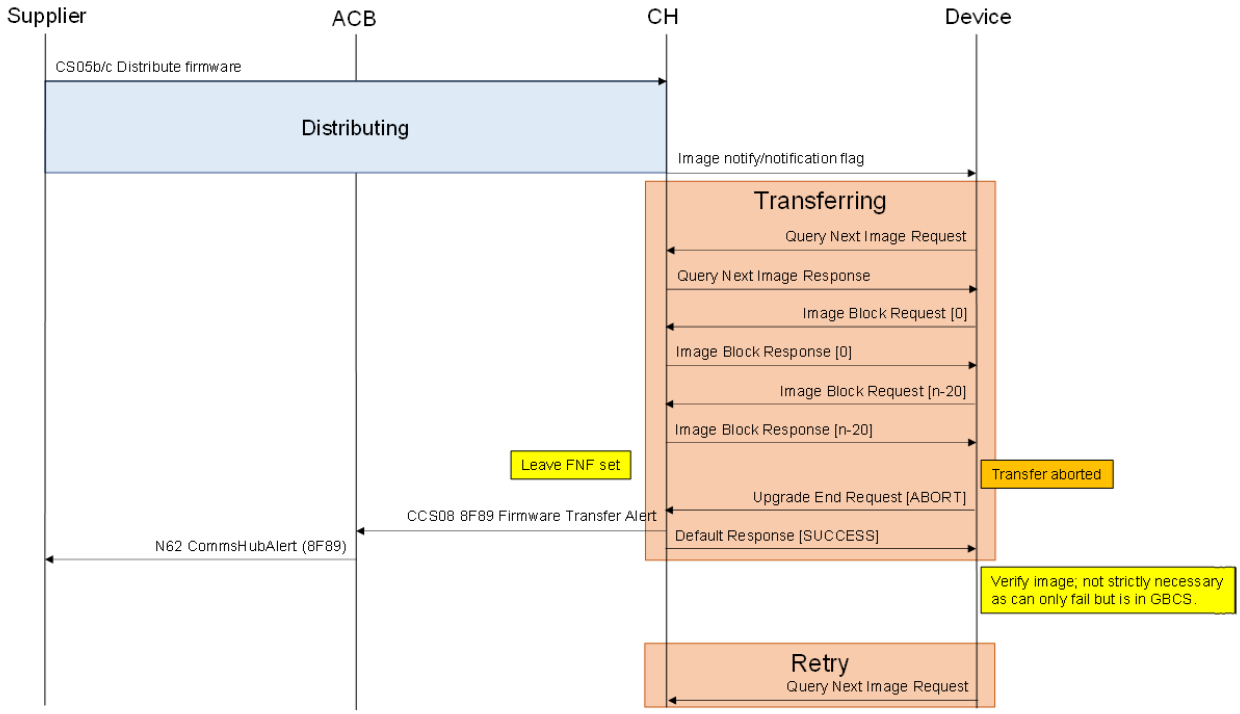
2.8.5 Incorrect FW Image Transferred to PPMID

After the FW Image is INVALID, the PPMID sends an Activation FAILURE Alert.



2.8.6 OTA Transfer to Device Aborted

After the FW Image is ABORTED, the End Device sends a further FAILURE Alert.



2.8.7 Different Behaviour between CHs: Handling a FW Image after Transfer

The table below shows different handling of FW Image when the end device sends an Upgrade end request with cause “Invalid Image” or “Abort”. The table below shows different handling of FW Image after download has been performed. Note that this applies to all Status Responses in the Upgrade End Request.

	End Device Upgrade end request with cause value		
CH	**“Invalid Image”**	**“Abort”**	**“Success”**
Toshiba	Multiple N62 with 8F8A (FileTransferSuccess) are sent until image is replaced. The CH solution allows the same image to be downloaded again and again by the end device.	Multiple N62 with 8F89 (FileTransferFailure) are sent until the FW image is replaced.	After the completion of a FW Download to Device, the Image is retained. This allows for multiple downloads, and multiple N62s for the same FW Image.
WNC	Only one N62 with 8F8A (FileTransferSuccess) will be received. The same image is not available anymore for an end device to repeat a download.	Multiple N62 with 8F89 (FileTransferFailure) until the FW image is replaced. Additionally, the GSME image is retained for up to 14 days.	After the completion of a FW Download to Device, the Image is retained. This allows for multiple downloads, and multiple N62s for the same FW Image.

	End Device Upgrade end request with cause value		
CH	**"Invalid Image"**	**"Abort"**	**"Success"**
EDMI	Only one N62 with 8F8A (FileTransferSuccess) will be received. The same image is not available anymore for an end device to repeat a download.	Multiple N62 with 8F89 (FileTransferFailure) will be received until the FW image is replaced or 14 days has passed for all images.	After the completion of a FW Download to Device, the Image is deleted. Only one N62 Alert in received for a single FW Image.

2.9 Guidance Point 9: Triggers for 8F84 Alert Generation

Guidance Point Number 9	GBCS 1.0	GBCS 2.0 and above	
	N/A	x	
Guidance Type	Comms Hub behaviors and alert triggers		
Functional Area	Comms Hub alerts		
Keywords	8F84 alert, ZigBee Keep Alive Cluster, CCS06 (SRV8.9 ReadDeviceLog), last_communication_date-time, TS1376 Alert Code 0x8F84 Query, DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1		

2.9.1 Issue Definition

The generation of 8F84 alerts (Failure to Deliver Remote Party Message to ESME) presents some differences across the three Comms Hubs and this guidance has the purpose of explaining the various scenarios under which such alerts are triggered.

Having access to such information would inform DCC Users and ESME manufacturers under which conditions they are able to receive N53 DCC alerts for any undelivered service request to an ESME they target.

2.9.2 Comms Hubs scenarios and triggers

To establish the expectations from the technical specifications perspective for 8F84 alert generation, DCC raised *TS1376 Alert Code 0x8F84 Query* to receive confirmation from BEIS for three different scenarios,

- Scenario1: the Comms Hub has a valid entry in its neighbour table (see section 2.9.2.1 for more details) and an active tunnel for the target ESME.
- Scenario2: the Comms Hub does not have a valid entry in its neighbour table and a previously requested tunnel is still active and yet to expire for the target ESME.
- Scenario3: the Comms Hub does not have either a valid entry in its neighbour table nor does it have an active tunnel for the target ESME (tunnel has expired).

As a summary, BEIS established that *"Where the CH cannot maintain the Communications Link, including via any required remediations, the Alert is not required but can be sent"*, which would apply for scenarios 2) and 3) or any other scenario besides scenario 1) above.

Next the handling of all three scenarios are presented for each CSP separately.

TS1376 Scenario	ARQ CH Behaviour (Confirmation of Comms Hub 8F84 alerts for each TS1376 scenario)	VMO2 CH Behaviour (Confirmation of Comms Hub 8F84 alerts for each TS1376 scenario)
1. The Comms Hub has a valid entry in its neighbour table and also an active tunnel for this ESME?	Yes	Yes
2. The Comms Hub does not have a valid entry for the ESME in its neighbour table and a previously requested tunnel is still active and yet to expire?	Yes	Yes
3. The Comms Hub does not have either a valid entry for the ESME in its neighbour table, nor does it have an active tunnel for this ESME (tunnel has expired)?	No. However if the ESME has become unreachable and the tunnel has expired which usually takes up to 18.2 hrs, DCC time out responses to commands targeted at the ESME will be received by the service user (N13).	Yes

Comms Hub 8F84 alert triggers table.

2.9.2.1 Indicators of communications link status

There are two ZigBee connectivity elements that indicate a communications link between the Comms Hub and the ESME exists, hence Service Requests should potentially be delivered successfully to the ESME, and those are,

1. **Comms Hub neighbour table**

a) Comms Hub contains an entry in its neighbour table for the target ESME, which must be in its CHF Device Log, as long as there are regular ZigBee ReadAttributes commands for Keep Alive cluster from ESME to Comms Hub.

b) The operating model for this feature is as follows,

i) Comms Hub and ESME support ZigBee Keep Alive cluster (0x0025).

ii) Comms Hub configures two ZigBee Keep Alive cluster attributes, *Keep-Alive Base* and the *TC Keep-Alive Jitter*, to received periodic reads from ESME.

iii) The ESME sends periodic ZigBee read requests to the Comms Hub for the previous ZigBee attributes, where the frequency of requests is based on their values.

1) For instance, according to *ZSE* the ZigBee default value for *TC Keep-Alive Base* is 0x0A (10min) and for *TC Keep-Alive Jitter* is 0x012C (5min).

The ESME random request period would be defined as,

[*TC Keep-Alive Base*, *TC Keep-Alive Base* + *TC Keep-Alive Jitter*]

2) Having a random request period in the range of,

[*10 min*, *10 min + 5 min*], that is, [10 min, 15 min]

Meaning an ESME would request those attributes periodically at random time between 10 min and 15 min.

3) For more details on the ZigBee Keep Alive cluster mechanism, please refer to Guidance Point 10 in the *DCC Guidance Note Communications Hub Usage*.

iv) Comms Hub would delete ESME from its neighbour table after 256 min of not receiving any ReadAttributes commands for Keep Alive cluster (ZS default value for *Device Timeout* is 256min, although ESME could negotiate a different value through a ZigBee *NWK Command End Device Timeout Request*).

c) There is NO mechanism whereby a Service User can read a Comms Hub neighbour table and check whether an ESME entry is active, however there is a verification that can offer some support there by means of the *last_communication_date-time* in CCS06 (SRV8.9 ReadDeviceLog). If such timestamp is less than twenty minutes old (*TC Keep-Alive Base* + *TC Keep-Alive Jitter* + *CCS06 roundtrip delay*), then most likely the ESME is in the Comms Hub neighbour table.

2. Comms Hub ZigBee tunnel

a) A Comms Hub relies on an active ZigBee tunnel established with the ESME, where the Comms Hub is the tunneling client and the ESME is the tunneling server, to exchange Service Requests, Service Responses and Device Alerts.

b) As the client, the Comms Hub requests for a ZigBee tunnel from an ESME through a ZigBee *RequestTunnel* message from the *Smart Energy Tunneling* cluster (0x0704).

c) Such tunnel would expire after 18.2h of inactivity.

d) There is NO mechanism whereby a Service User can verify the status of the tunnel and whether it is active or inactive.

2.9.2.2 Comms Hub 8F84 alert triggers message sequence charts

In this section the three scenarios defined in the Section 1.2 above are presented in message sequence charts. The DCC guidance “DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1” in the SECAS website has been referenced to extract the DSP retry periods for Service Requests that fail to receive a response. The examples include SRV1.1.1 (UpdateImportTariff(Primary Element)).

Scenario 1 (Both CSPs) – Valid neighbour table and active ZigBee tunnel

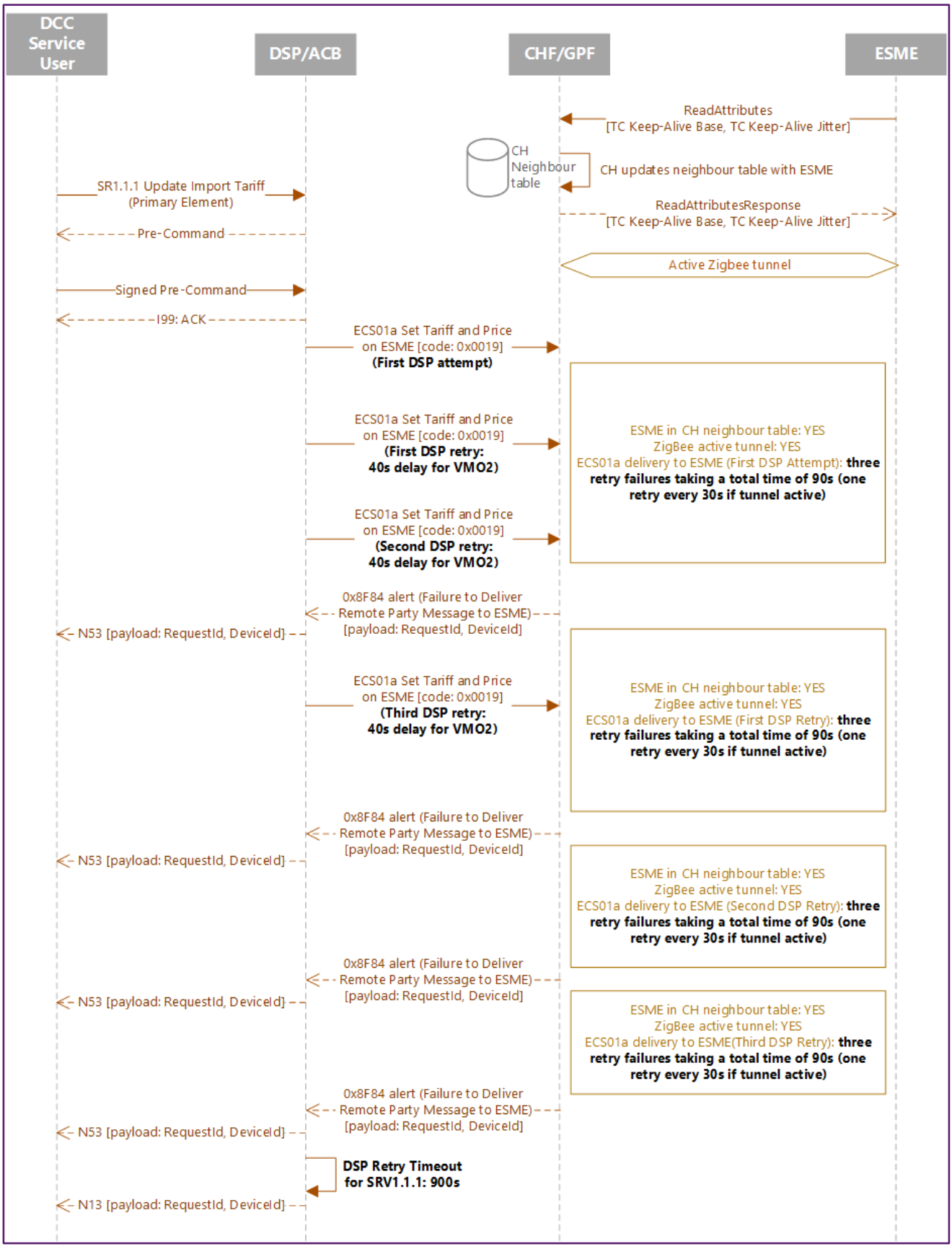
Scenario applicable to CSP C&S and CSP N characterised by the following,

- DCC User sends a SR1.1.1 which fails to be delivered to the ESME.

- If the communications issues do not resolve, a Comms Hub may generate up to four 8F84 alerts where each one is mapped by the DSP to a single N53 DCC alert. The first 8F84 alert is linked to the original SRV and the other three 8F84 alerts are linked to DSP retries.

- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of the example below is 900s for SRV1.1.1.

- NOTE: The SRV1.1.1 DSP retry times are different for VMO2 (40s) and for Arqiva (180s). The diagram below applies to VMO2 SRV1.1.1 with consecutive N53 alerts spread out 90s, however for Arqiva consecutive N53 alerts would be spread out 180s.

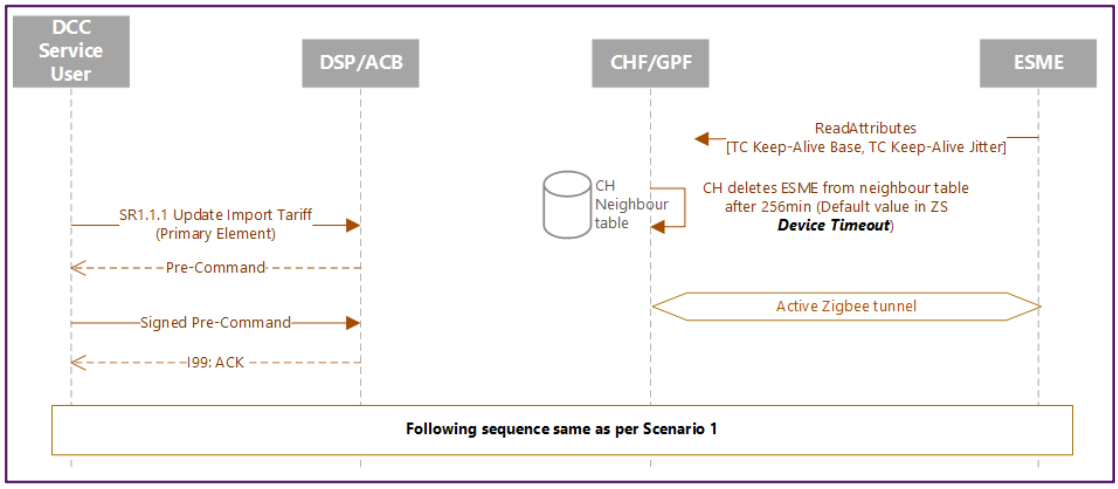


Scenario 1 (CSP C&S only chart) – Valid neighbour table and active ZigBee tunnel.

Scenario 2 (Both CSPs) – Invalid neighbour table and active ZigBee tunnel

Scenario applicable to CSP C&S and CSP N characterised by the following,

- CH deletes ESME from neighbour table after 256min of not receiving any ReadAttributes for *Keep Alive cluster* from that ESME.
- DCC User sends a SR1.1.1 which fails to be delivered to the ESME.
- If the communications issues do not resolve, a Comms Hub may generate up to four 8F84 alerts where each one is mapped by the DSP to a single N53 DCC alert. The first 8F84 alert is linked to the original SRV and the other three 8F84 alerts are linked to DSP retries.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of the example below is 900s for SRV1.1.1.
- NOTE: The SRV1.1.1 DSP retry times are different for VMO2 (40s) and for Arqiva (180s). The diagram below applies to VMO2 SRV1.1.1 with consecutive N53 alerts spread out 90s, however for Arqiva consecutive N53 alerts would be spread out 180s.



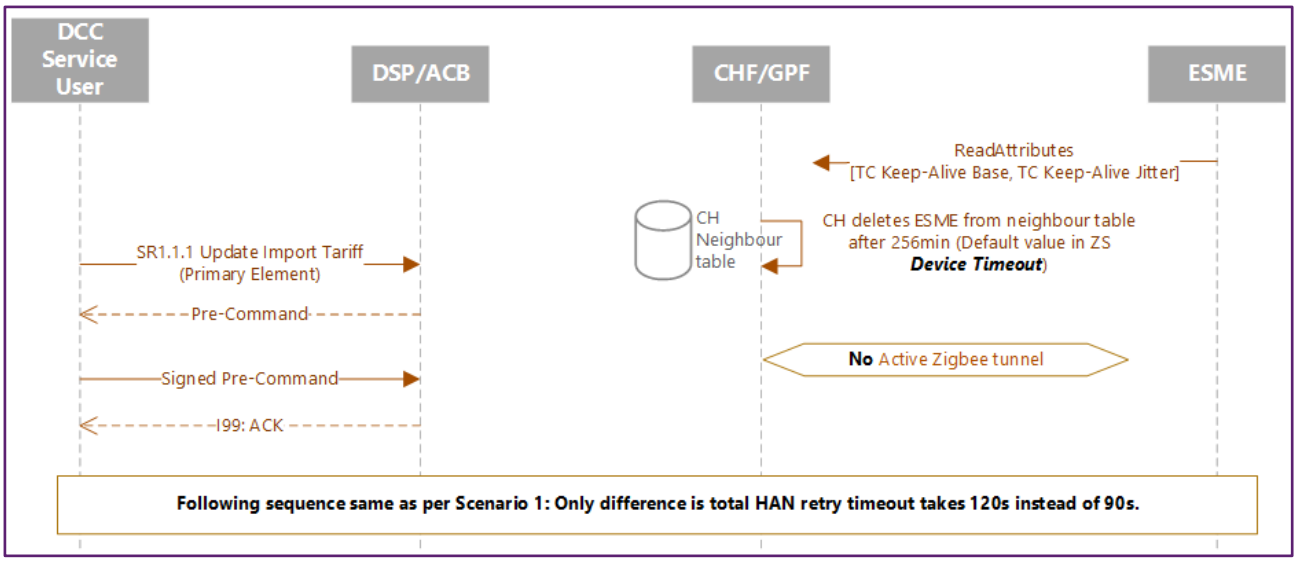
Scenario 2 (Both CSPs) – Invalid neighbour table and active ZigBee tunnel.

Scenario 3 CSP C&S – Invalid neighbour table and inactive ZigBee tunnel

Scenario applicable to CSP C&S characterised by the following,

- CH deletes ESME from neighbour table after 256min of not receiving any ReadAttributes for Keep Alive cluster from that ESME. ZigBee tunnel is inactive (expired after 18.2 hours of no tunnel messages, that is, no SRV request./response or Device Alerts).
- Service User sends a SR1.1.1 which fails to be delivered to the ESME.
- If the communications issues do not resolve, a Comms Hub may generate up to four 8F84 alerts where each one is mapped by the DSP to a single N53 DCC alert. The first 8F84 alert is linked to the original SRV and the other three 8F84 alerts are linked to DSP retries.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of the example below is 900s for SRV1.1.1.

- NOTE: A SRV1.1.1 could result in consecutive N53 alerts spread out 120s when there is no active tunnel as per the Flow Control Replay in GBCS 10.2.2.3 CHF requirements for ESME Transfer Data commands.

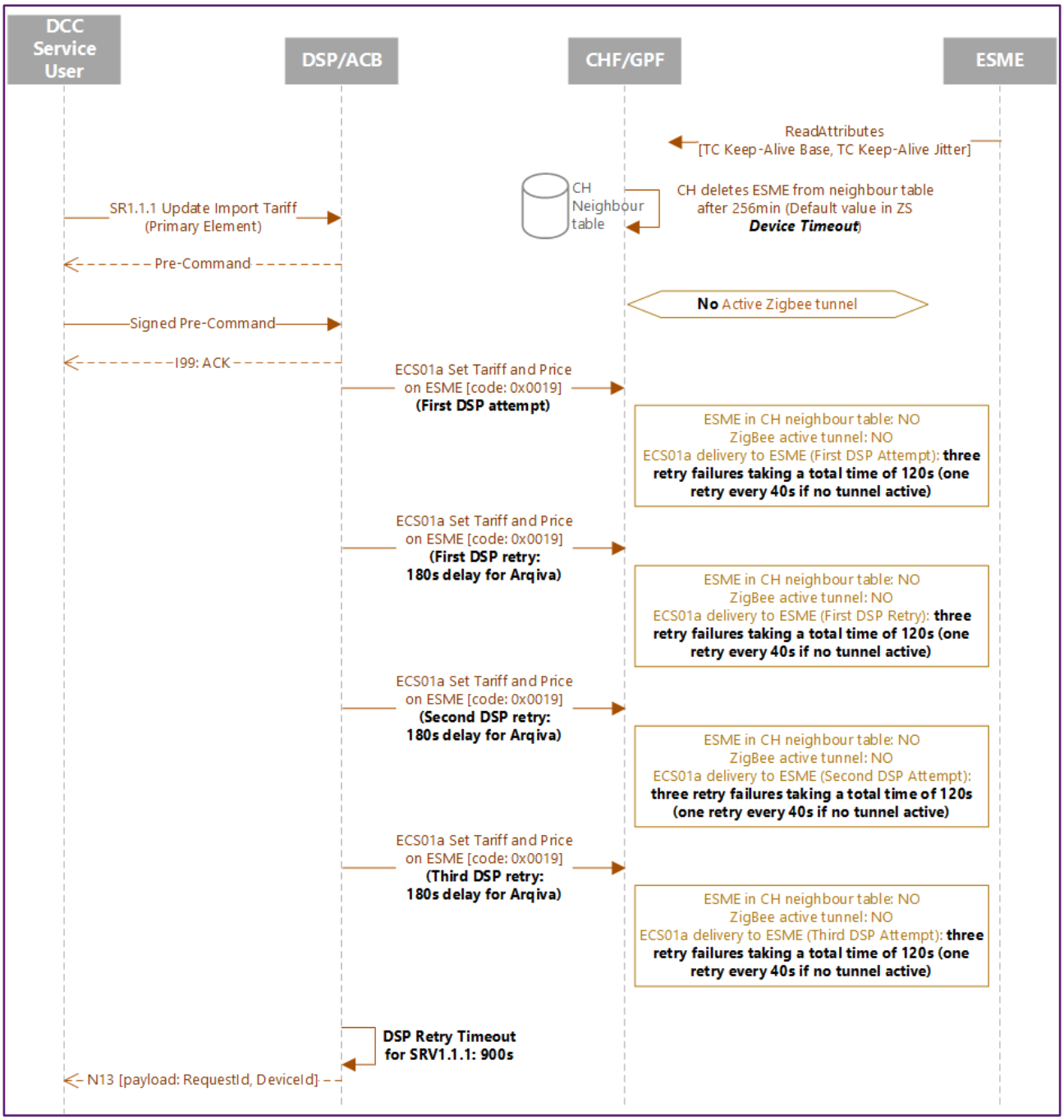


Scenario 3 CSP C&S Invalid neighbour table and inactive ZigBee tunnel.

Scenario 3 CSP N – Invalid neighbour table and inactive ZigBee tunnel

Scenario applicable to CSP N characterised by the following,

- CH deletes ESME from neighbour table after 256min of not receiving any ReadAttributes for Keep Alive cluster. ZigBee tunnel is inactive.
- Service User sends a SR1.1.1 which fails to be delivered to the ESME.
- Comms Hub DOES NOT generate any 8F84 alerts and DSP DOES NOT generate any N53 alerts either.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of the example below is 900s for SRV1.1.1.



Scenario 3 CSP N Invalid neighbour table and inactive ZigBee tunnel.

2.9.3 Conclusion

The behaviour for both CSPs differ for Scenario 3 as per the table in Section 2.9.2, where CSP Central & South generates 8F84 alerts, however CSP North DO NOT generate any 8F84 alerts in that scenario. However, according to TS1376 both behaviours are compliant with the GBCS technical specifications. Hence to align the behaviour of Comms Hubs for Scenario 3 would require taking the SECMOD route.

DCC Users cannot rely on N53 DCC alerts for Scenario 3 in the CSP North region, however they still can rely on the receipt of N13 DCC alerts in that scenario as per the message sequence charts for Scenario 3 CSP N in Section 2.9.2.2.

2.10 Guidance Point 10: Comms Hub Last Communication with HAN devices (SRV8.9 & SSI Comms Hub Diagnostic)

Guidance Point Number 10	GBCS 1.0	GBCS 2.0 and above	
	N/A	x	
Guidance Type	Comms Hub Behaviour & HAN Communication		
Functional Area	HAN Communication, off HAN detection		
Keywords	8F84 Alert, ZigBee Keep Alive Cluster, CCS06 (SRV8.9 ReadDeviceLog), last_communication_date-time, SSI, Comms Hub Diagnostic Information		

2.10.1 Issue Definition

DCC Users have queried the inconsistencies across the information extracted from Comms Hubs through SRV8.9 ReadDeviceLog (CCS06) particularly for the *last_communication_date-time* and the Comms Hub diagnostic interface exposed by SSI.

Evidence was shared by DCC Users where it appeared the information across the two data sources did not match, that is, the SRV8.9 response showed devices (GSME, ESME, PPMIDs) active in the HAN while the SSI diagnostic interface displayed devices as not contactable.

To allow DCC Users to understand how the information across the two data interfaces is mapped, DCC gathered the following inputs to document clearly both interface data sources,

1. SSI Comms Hub Diagnostic full description containing each HAN device last communication requested in real-time through the SSI interface and retrieved directly from Comms Hubs.
2. How info in 1) is presented through the SSI interface to DCC Users.
3. Full description of how Comms Hubs populate the *last_communication_date-time* for each HAN device in the SRV8.9 ReadDeviceLog (CCS06) service responses.
4. How info in 1) and 3) relate to each other.

Such information aims to offer DCC Users a clear path to evaluate the status of HAN devices and whether potential communication issues exist.

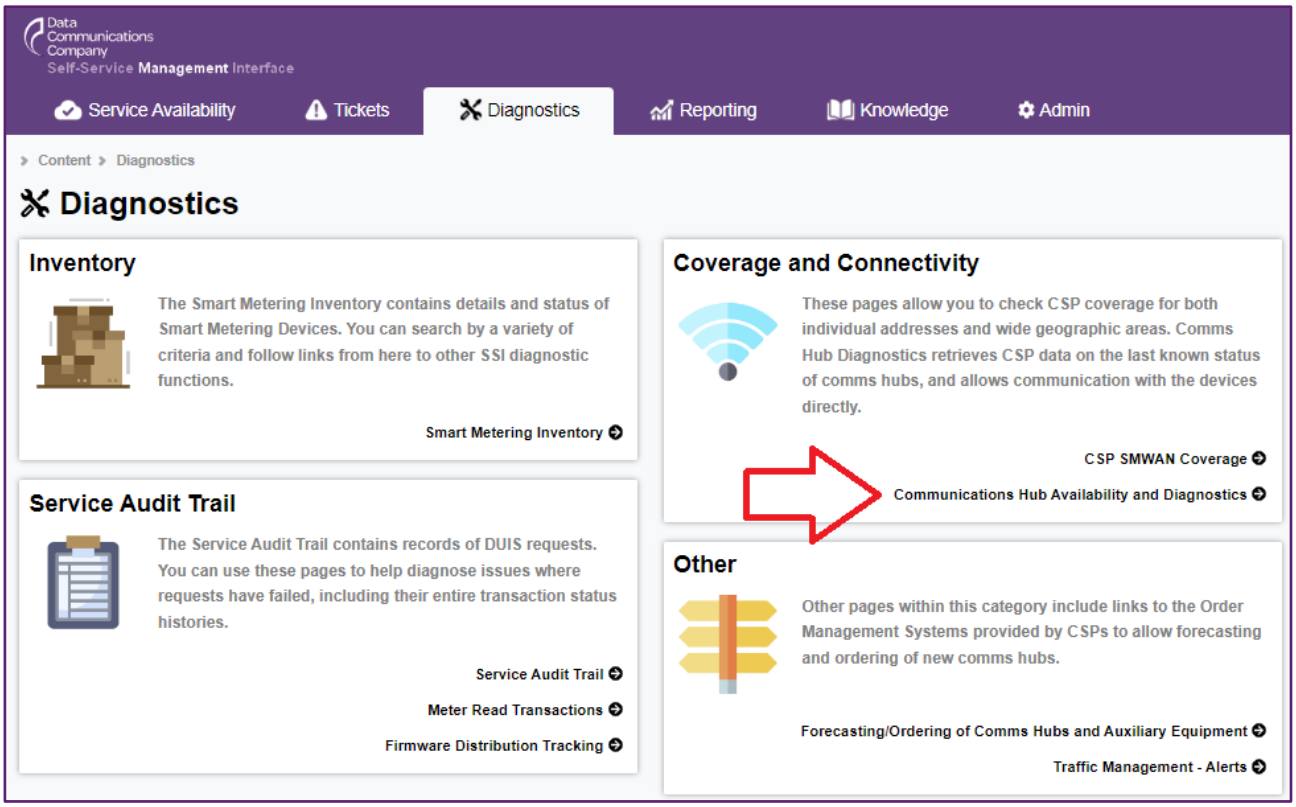
2.10.2 SSI Comms Hub Diagnostic & Display Interface

2.10.2.1 SSI Comms Hub Diagnostic Menu Access & Description

This section covers the steps associated with requesting Comms Hub diagnostic data via SSI Diagnostic menu.

STEP 1 – SSI User Interface Diagnostic Main Screen

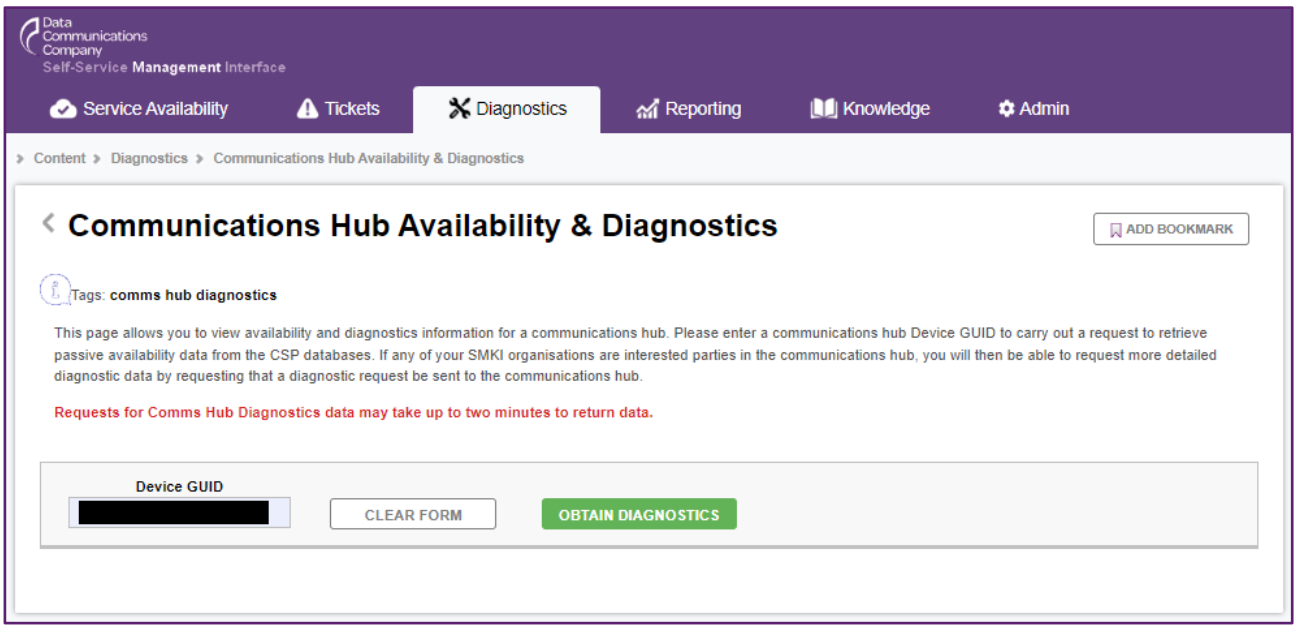
By clicking on the option “Communications Hub availability and Diagnostics” (red arrow in picture below) a new menu will open up to enter the Comms Hub GUID to be inspected.



STEP 1 - SSI user interface diagnostic main screen.

STEP 2 - Communications Hub Availability and Diagnostic CH GUID selection

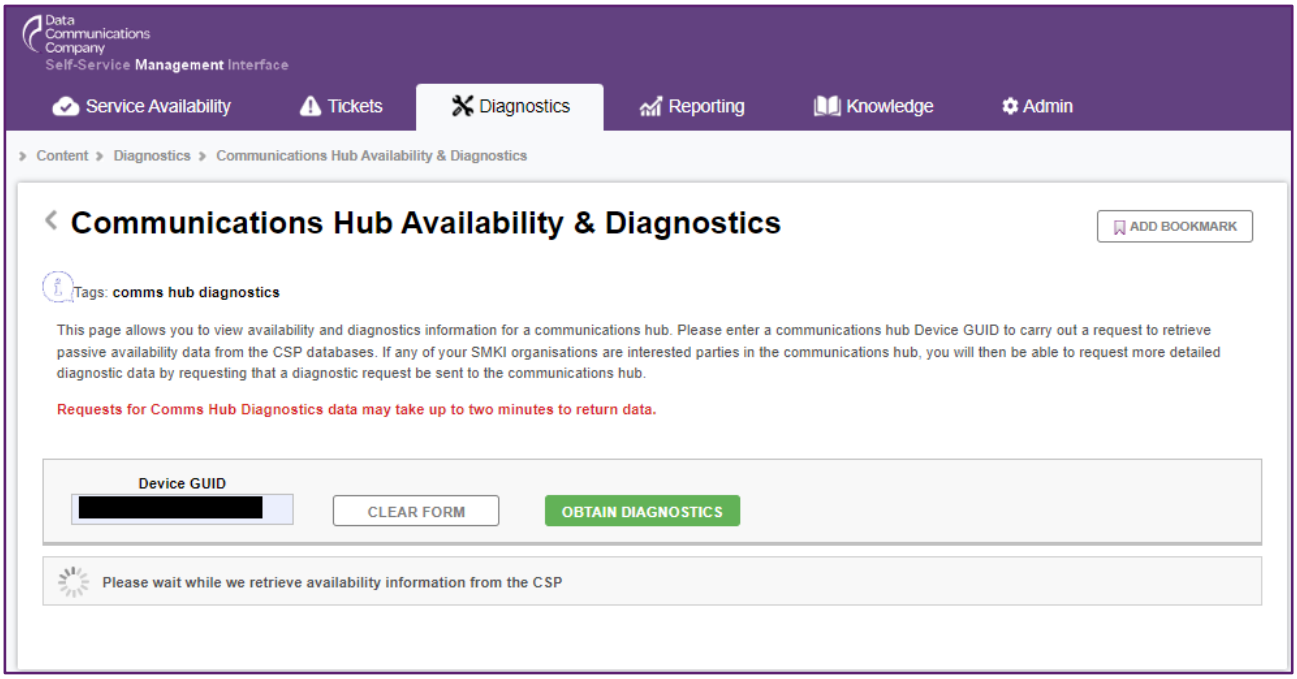
At this point a Comms Hub GUID (formatted with or without dashes, XX-XX-XX-XX-XX-XX-XX-XX or XXXXXXXXXXXXXXXX) to be inspected is to be entered into the text box called “Device GUID”. Click on the “OBTAIN DIAGNOSTICS” green button.



STEP 2 – Comms Hub GUID selection.

STEP 3 – Wait for Comms Hub Status Diagnostic Information Retrieval from CSP

At this point the DSP will send a request to the CSP for the Comms Hub status diagnostic information and the interface will show the message *"Please wait while we retrieve availability information from CSP"*.

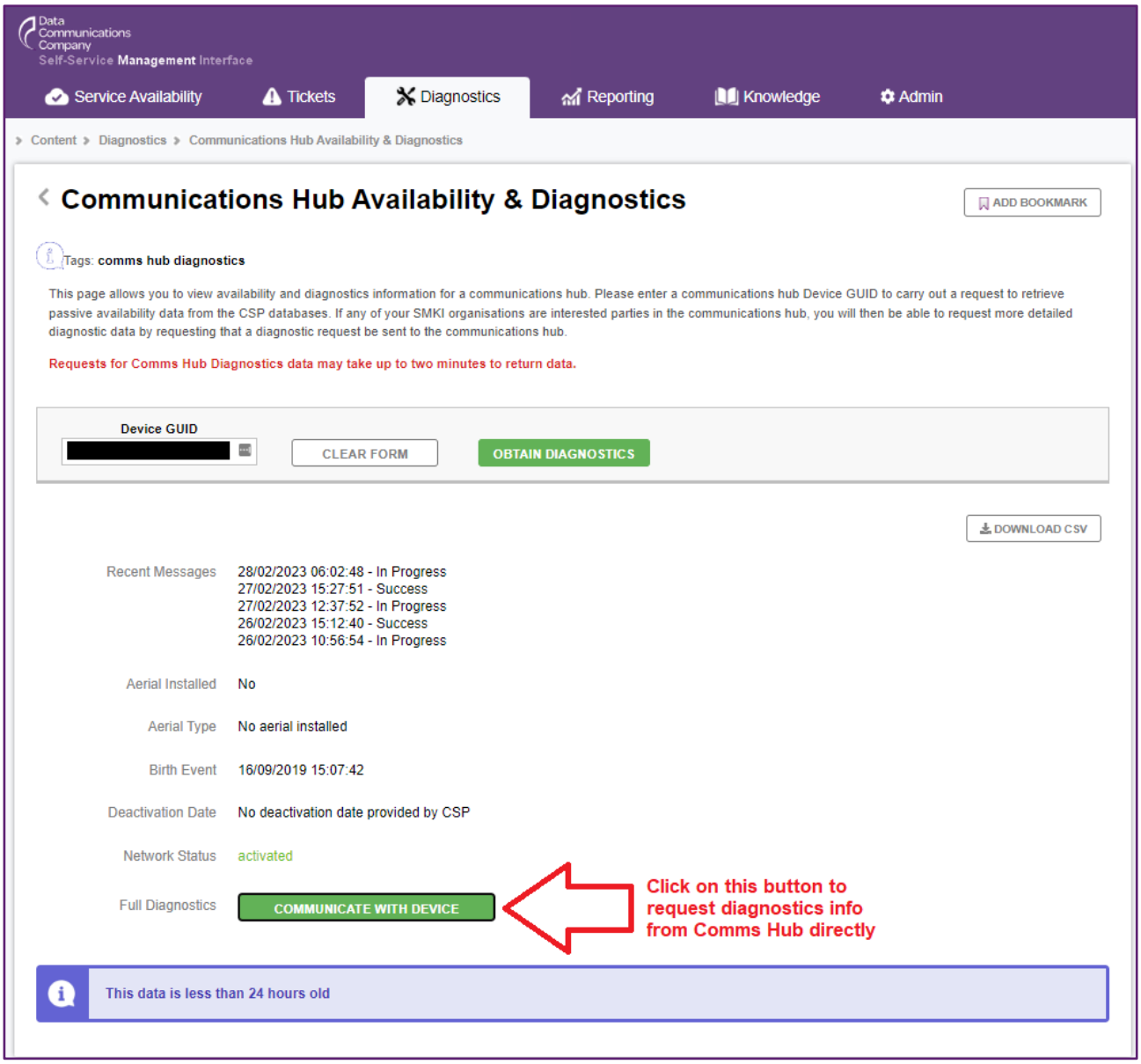


STEP 3 – Wait for Comms Hub status diagnostic information retrieval from CSP.

STEP 4 – Comms Hub Diagnostic Information Retrieval from CSP

Eventually, if successful, the CSP provides the following information to DSP for display:

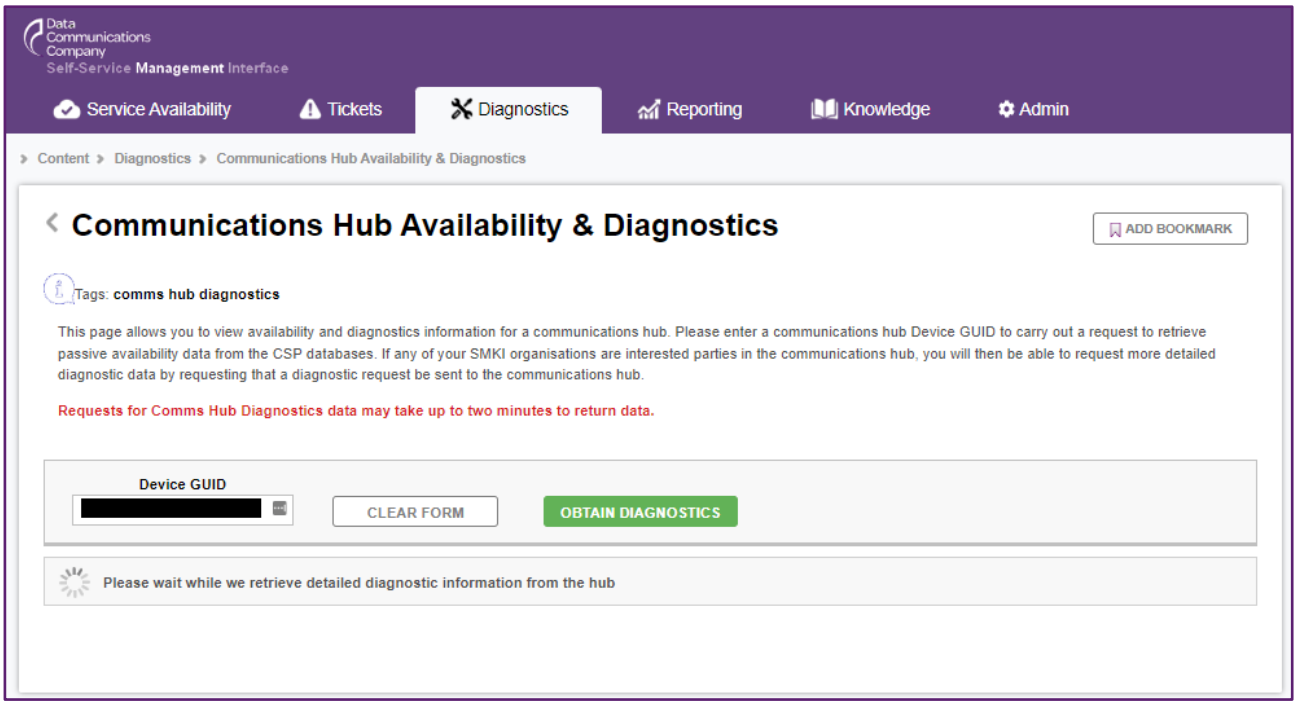
- Recent Messages: The last five messages recorded in the DSP Service Audit Trail for that Comms Hub.
- Aerial Installed:
  - CSP C&S: Indication whether an aerial is installed. Options are "YES" or "NO".
  - CSP N: Not supported.
- Aerial Type:
  - CSP C&S: Text describing the aerial type if installed, otherwise "No aerial installed" is displayed.
  - CSP N: Not supported.
- Birth Event: The date and time of the birth event (format "DD/MM/YYYY HH:MM:SS" or empty if not available).
- Deactivation Date: Data/time the Hub was removed from the network if networkStatus is "DEACTIVATED".
- Network Status: "ACTIVATED" or "DEACTIVATED".
  - CSP C&S: Whether the Communications Hub should be contactable (i.e. has had a birth event and has not been decommissioned or barred).
  - CSP N: "ACTIVATED" is equivalent to "installed" status.



STEP 4 – Comms Hub diagnostic information retrieval from CSP.

STEP 5 – Wait for Comms Hub Diagnostic Information Retrieval from Comms Hub

After clicking on the “COMMUNICATE WITH DEVICE” green button in Step 4, the DSP will send a request via the CSP to the Comms Hub to retrieve a series of diagnostic fields. While waiting for the Comms Hub response the SSI user interface will display *“Please wait while we retrieve detailed diagnostic information from the hub”*.

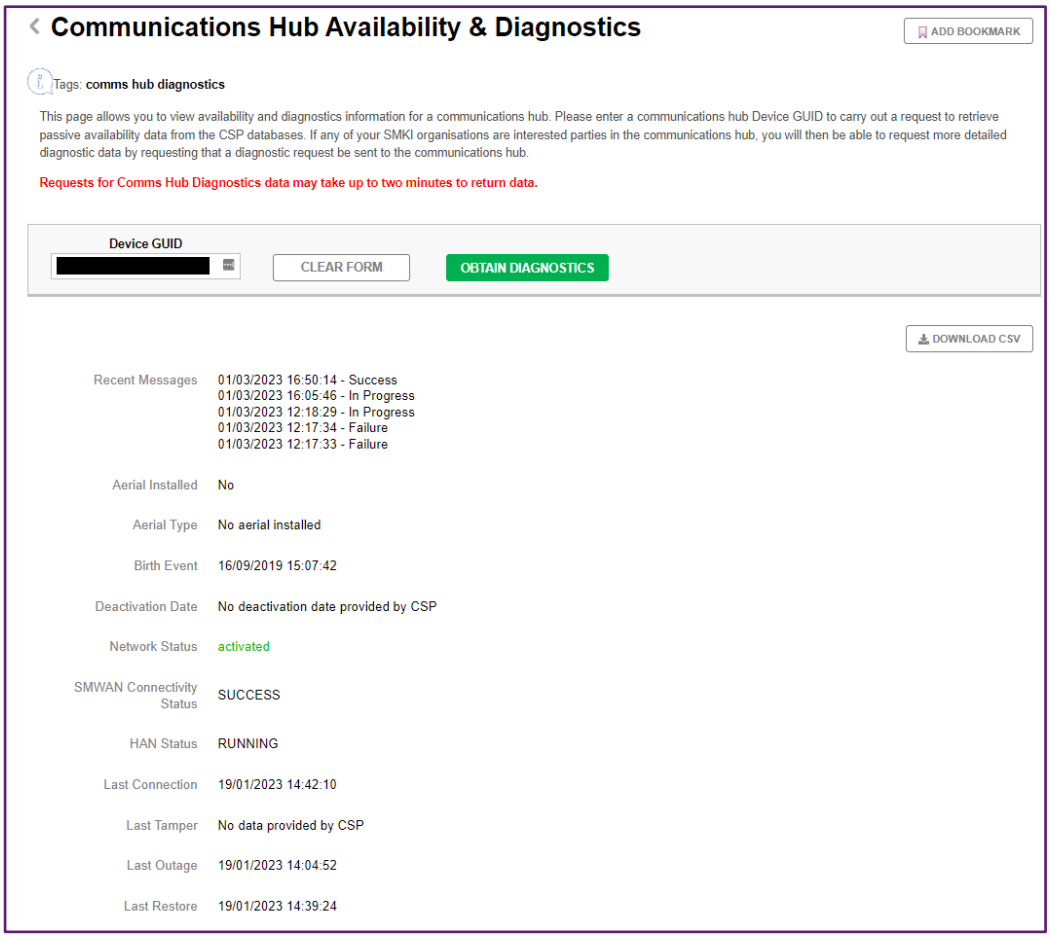


STEP 5 – Wait for Comms Hub Diagnostic Information Retrieval from Comms Hub.

STEP 6 - Comms Hub Diagnostic Information Retrieval from Comms Hub

Eventually, if successful, the Comms Hub responds to the request and provides the following information to DSP for display as per the picture below,

- SMWAN Connectivity Status: Status of the SM WAN connectivity to the Communications Hub (“SUCCESS” or “FAILURE”).
- HAN Status:
    - CSP C&S: Status of the HAN with values “RUNNING” or “STOPPED”. In DBCH, only if both bands are running, Comms Hub will return “RUNNING”, otherwise “STOPPED”.
    - CSP N: Status of the HAN with values “RUNNING” or “ERROR”.
- Last Connection: Date and time of last connection to the SM WAN (format “DD/MM/YYYY HH:MM:SS” or empty if not available).
    - CSP C&S: Date and time of last successful data connection between a Comms Hub and the CSP C&S or empty if data connection never succeeded.
    - CSP N: Date and time of last GBCS message received by the Comms Hub.
- Last Tamper: Date and time of the last tamper alert (format “DD/MM/YYYY HH:MM:SS” or empty if not available).
- Last Outage: Date and time of the last power outage alert (format “DD/MM/YYYY HH:MM:SS” or empty if not available).
- Last Restore: Date and time of the last power restore alert (format “DD/MM/YYYY HH:MM:SS” or empty if not available).



STEP 6 – Comms Hub Diagnostic Information Retrieval from Comms Hub part 1.

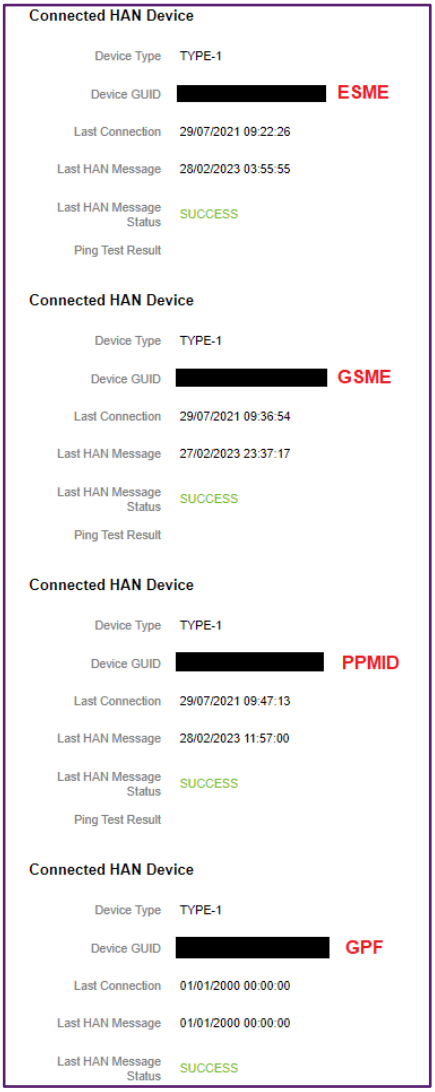
HAN devices diagnostic information follows (picture below contains SSI production data),

- Type: “TYPE-1” or “TYPE-2”.
    - CSP C&S: In case of TCSO and device type identification has not been completed, it returns the default error response, found in section 2.10.2.3 .
- Device GUID: MAC address of the device on the HAN.
- Last Connection:
    - CSP C&S:
        - Toshiba: Date-time of HAN device last connection establishment with CH which gets updated for ZigBee device join and rejoin.
        - WNC: Same as *last_communication_date-time* in SRV8.9 ReadDeviceLog (CCS06)
    - CSP N: Date-time when the last ZigBee KEC (Key Establishment Cluster) ran successfully for a device, meaning that a new ZigBee link key was negotiated between the Comms Hub and the device and an 0x8F12 alert (CHF Device Log Changed) was generated with the new key.
- Last HAN Message:
    - CSP C&S: Same as *last_communication_date-time* in SRV8.9 ReadDeviceLog (CCS06). Applies to both Toshiba and WNC hubs.

- CSP N: The date-time at which the CH last received a (GBCS) default response from the HAN device. That would indicate that a device successfully acknowledged the receipt of a Service Request.

- Last HAN Message Status: Delivery status of last HAN interface message to a type 1 device (“SUCCESS” or “FAILURE”).
  - Toshiba: It returns failure if Comms Hub fails to deliver ZigBee packet to HAN device or APS ACK is not received from HAN device.
  - WNC: Always returns SUCCESS.
- Ping Test Result:
  - CSP C&S: Not supported.
  - CSP N: Same as *last_communication_date-time* in SRV8.9 ReadDeviceLog (CCS06).

NOTE: The screen capture below for a production HAN setup shows four HAN devices. The first one was identified as an ESME as per its Device GUID information, the second one as a GSME, the third one as a PPMID and the fourth one as a GPF.



STEP 6 – Comms Hub Diagnostic Information Retrieval from Comms Hub part 2.

2.10.2.2 SSI Common Errors

This section shares the errors that a DCC User can experience while requesting for Comms diagnostic information through the SSI.

Error code SSI-CSP-01

The CSP Management Gateway reports that it was unable to interpret the response received from the CSP.

Error code SSI-CSP-05

The CSP Management Gateway reports that the Communications Hub ID is unknown by the CSP.

Error code SSI-CSP-20

The CSP Management Gateway reports that it is temporarily unable to process your request due to unusually high system load.

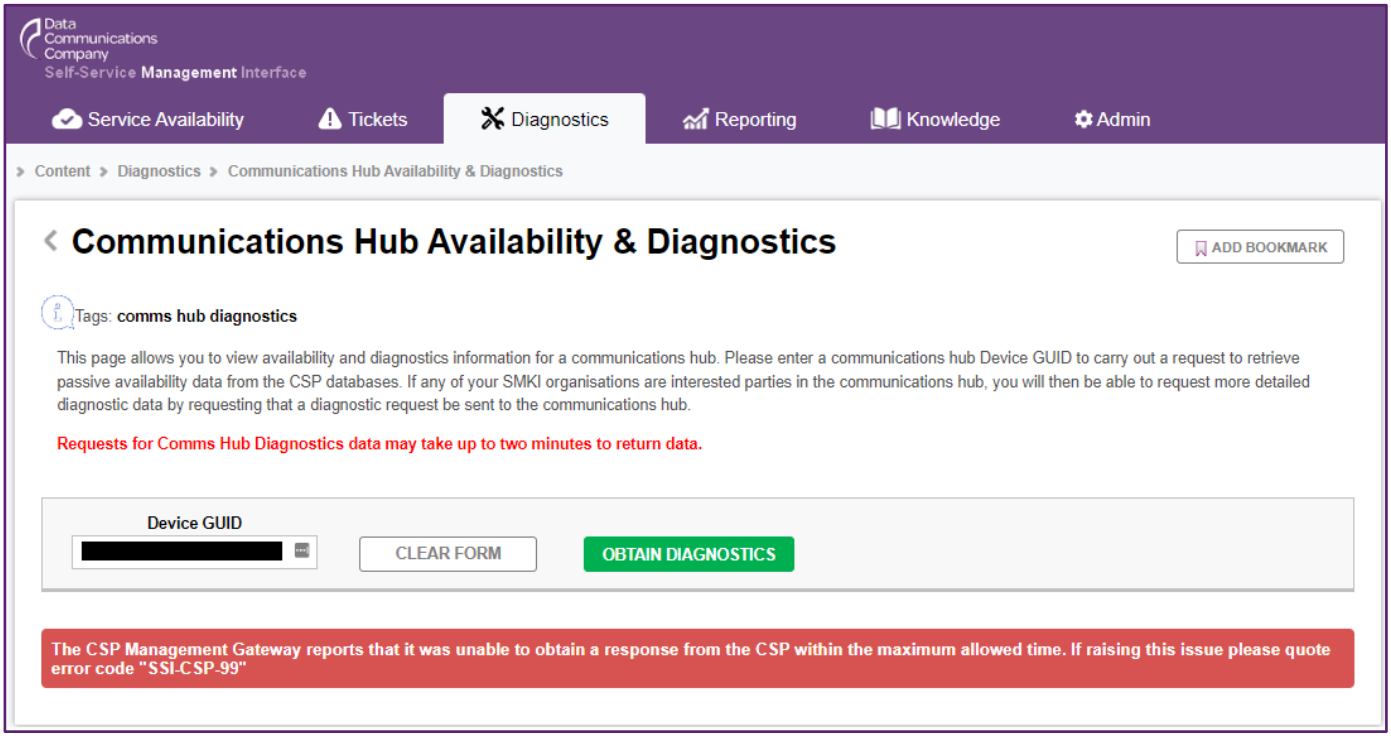
Error code SSI-CSP-21

The CSP Management Gateway reports that an unexpected internal error has occurred.

Error code SSI-CSP-99

The CSP Management Gateway reports that it was unable to obtain a response from the CSP within the maximum allowed time.

An example of how the SSI user interface displays one of the errors listed previously is presented below for a production Comms Hub.



Error SSI-CSP-99 SSI in Communications Hub Availability & Diagnostics.

2.10.2.3 CSP Central & South Default Error Response

CSP-C&S sends a default response if it fails to validate the response received by a Toshiba or WNC Comms Hub due to parsing errors, or if it has not received any response from the Comms Hub.

- SMWAN Connectivity Status: “FAILURE”
- HAN Status: “STOPPED”
- Last Connection: Empty string
- Last Tamper: Empty string
- Last Outage: Empty string
- Last Restore: Empty string
- HAN Devices
    - Type: "TYPE-1"
    - Device GUID: Empty string
    - Last Connection: Empty string
    - Last HAN Message: Empty string
    - Last HAN Message Status: “FAILURE”

2.10.2.4 CSP North Default Error Response

CSP-N do not currently provide a default response. This may be subject to change in future.

2.10.3 Comms Hubs Handling of *last_communication_date-time* in SRV8.9 ReadDeviceLog (CCS06) Service Responses

This section covers all details on Comms Hub operations related to the *last_communication_date-time* attribute part of SRV8.9 ReadDeviceLog (CCS06) including memory storage, trigger conditions, ZigBee message routing and device approaches.

According to GBCS Section 19.3 *Embedded Use Cases*, the *last_communication_date-time (lastCommsTimestamp) is* defined as,

- *The UTC date and time at which the Communications Hub last communicated with the Device with the corresponding entry in DeviceLog(CHF).logEntries[0..16].*

This general definition does not make clear whether any communications at ZigBee level would update the attribute in question or not.

The value of such attribute can be significant to DCC Users in the process of verifying whether HAN devices have been contactable by the Comms Hub recently or not to explain Service Request delivery failures.

The following sections document the inputs provided by Comms Hub vendors on how their hubs manage the *last_communication_date-time* attribute.

2.10.3.1 Storage of *last_communication_date-time* in Comms Hub Memory

All Comms Hubs use volatile (RAM) and non-volatile (flash) storage for the *last_communication_date-time* for each device in its CHF Device Log (ESME, GSME, PPMID, etc).

RAM Copy Update

All three Comms Hubs update a RAM copy every time a HAN device in the CHF Device Log communicates with them at the ZigBee level as per the provided triggers in section 2.10.3.2.

Flash Copy Update

- Toshiba hub approach
    - The flash copy gets updated in the next scheduled periodic flash write cycle (within 24hrs) or earlier if any of the below events occur:
        - During Comms Hub shutdown (for whatever reason, excluding unplanned Comms Hub reboots).
        - Immediately after HAN device join or re-join.
        - Whenever a device is added or removed from CHF device log.
- WNC/EDMI hub approach
    - The flash copy gets updated every 30 minutes, which might or might not coincide with the hour and half hour points.

2.10.3.2 Triggers for Updating last_communication_date-time

Common Triggers Across All Three Comms Hubs

- Key establishment messages to create security keys
- Attribute requests/commands
- Receipt of Default Response

Toshiba/WNC Hub Specific Triggers

- Rejoin requests

EDMI Hub Specific Triggers

- Receipt of APS Acknowledgement

2.10.3.3 Retrieval of *last_communication_date-time* to Populate SRV8.9 Response

All three Comms Hubs populate the *last_communication_date-time* from the RAM copy, hence always offering the most up-to-date value in each SRV8.9 response.

2.10.3.4 ZigBee Message Routing

All three Comms Hubs have the same behaviour whereby the *last_communication_date-time* RAM or flash copies for a given device are NOT modified in the scenario where the Comms Hub acts as a router and not as the destination of the ZigBee message from that device.

2.10.3.5 HAN Device Strategies

This section addresses the different permitted approaches taken by HAN devices in regard to *last_communication_date-time* information.

GSME

The expectation is for a GSME to communicate with a Comms Hub every wakeup cycle, that is, every thirty minutes. Note that this wakeup cycle period is manufacturer specific.

The previous statement means that the *last_communication_date-time* attribute in CCS06 (SRV8.9 ReadDeviceLog) for a target GSME would change values more frequently than once per day. Hence a DCC User verifying the last communication between a Comms Hub and a GSME would expect to see a timestamp in the *last_communication_date-time* attribute within the last thirty minutes (GSME wakeup cycle) under normal operating conditions.

ESME

The expectation is for an ESME to communicate with Comms Hub multiple times in a day through a series of events,

- Request for the *ZigBee Time attributes* from the Time cluster (0x000A) from a Comms Hub once every 24h by means of *ZigBee ReadAttributes commands*.
- Handle *ZigBee RequestTunnel* from the Tunneling cluster (0x0704) from Comms Hub every 18.2h approximately.
- Send multiple daily *ZigBee ReadAttributes commands* to the Keep-Alive cluster (0x0025) in the Comms Hub to read the TC Keep-Alive Base (Default value: 10min) and the TC Keep-Alive Jitter attributes (Default value: 300s) as per Comms Hub configuration (see Section 2.10.3.6).
- Periodic *ZigBee OTA Query Next Image Request command* to check for a new ESME OTA upgrade image.
- Deliver WAN device alerts to Comms Hub if any take place.
- Handle Service Requests and produce Service responses if any take place.

The previous event list establishes that the *last_communication_date-time* attribute in CCS06 (SRV8.9 ReadDeviceLog) for a target ESME would change values more frequently than once per day and most likely within the last fifteen or twenty minutes determined by the *Keep Alive attributes configuration* by the Comms Hub. Hence a DCC User verifying the last communication between a Comms Hub and ESME would expect to see a timestamp in the *last_communication_date-time* attribute within the last fifteen to twenty minutes under normal operating conditions.

PPMID and Type 2 Devices

The expectation is for a PPMID/Type 2 Devices to communicate with Comms Hub at least once per day, as long as such device is powered up. The series of events that would update the *last_communication_date-time* are the following,

Events applicable to all PPMID/Type 2 Devices

- Request for the *ZigBee Time attributes* from the Time cluster (0x000A) from its Comms Hub once every 24h by means of *ZigBee ReadAttributes commands*.
- **Only applicable to non-sleepy devices and device manufacturer specific:** Send multiple daily *ZigBee ReadAttributes commands* to the Keep-Alive cluster (0x0025) in the Comms Hub to read the TC Keep-Alive Base (Default value: 10min) and the TC Keep-Alive Jitter attributes (Default value: 300s) as per Comms Hub configuration (see Section 2.10.3.6).
- **Dual fuel or gas only installs:** *ZigBee ReadAttributes command* to read GPF device information on a very frequent basis (generally more frequent than once per minute).

PPMIDs ONLY

- Periodic *ZigBee OTA Query Next Image Request command* to check for a new PPMID OTA upgrade image.
- Deliver WAN device alerts to Comms Hub if any take place.
- Handle Service Requests and produce Service responses if any take place.

Dual fuel or gas only installs

A PPMID/Type 2 Devices would request for GPF data on a frequent basis, meaning that a DCC User verifying the last communication between a Comms Hub and PPMID/Type 2 Devices would expect to see a timestamp in the *last_communication_date-time* attribute within the last few minutes under normal operating conditions.

Electricity only installs

There would be two possible scenarios for the timestamp in the *last_communication_date-time* attribute provided by the Comms Hub.

- PPMID/Type 2 Devices supports Keep Alive cluster: A DCC User verifying the last communication between a Comms Hub and a PPMID/Type 2 Devices would expect to see a timestamp in the *last_communication_date-time* attribute within the last fifteen to twenty minutes under normal operating conditions.
- PPMID/Type 2 Devices does NOT support Keep Alive cluster: A DCC User verifying the last communication between a Comms Hub and PPMID/Type 2 Devices would expect to see a timestamp in the *last_communication_date-time* attribute within the last 24h under normal operating conditions.

2.10.3.6 Comms Hub Configuration for ZigBee Keep Alive cluster attributes

The ZigBee Keep Alive Cluster (0x0025) is used to define a mechanism covered in ZSEr21 Section 5.4.2.2.3.4 Keep Alive Method by which routers (ESME) and End Devices (PPMID/Type 2 Devices, etc) can detect whether a Trust Center (Comms Hub) is no longer available and initiate a search for it.

The frequency of requests by the routers and end devices are determined by the value of two Keep Alive attributes in the Comms Hub, and those are,

- *TC Keep-Alive Base Attribute*: It represents the base time (in minutes) used for calculating each interval used by the keep-alive mechanism.
- *TC Keep-Alive Jitter Attribute*: It indicates the range (in seconds) for the random element added to value of the TC Keep-Alive Base attribute when calculating each interval for the keep-alive mechanism.

Calculation of random request period by routers and end devices

A client device would calculate the random request period to send to a Comms Hub a new *ZigBee ReadAttributes* for the *TC Keep-Alive Base* and *TC Keep-Alive Jitter Attributes* as follows,

- Minimum random period: *TC Keep-Alive Base - TC Keep-Alive Jitter*
- Maximum random period: *TC Keep-Alive Base + TC Keep-Alive Jitter*
- Random request period: [Minimum random period, Maximum random period] or [*TC Keep-Alive Base - TC Keep-Alive Jitter*, *TC Keep-Alive Base + TC Keep-Alive Jitter]*.

A device would then send a periodic request with a period within the random request period above.

The configuration of those attributes by each Comms Hub is as follows,

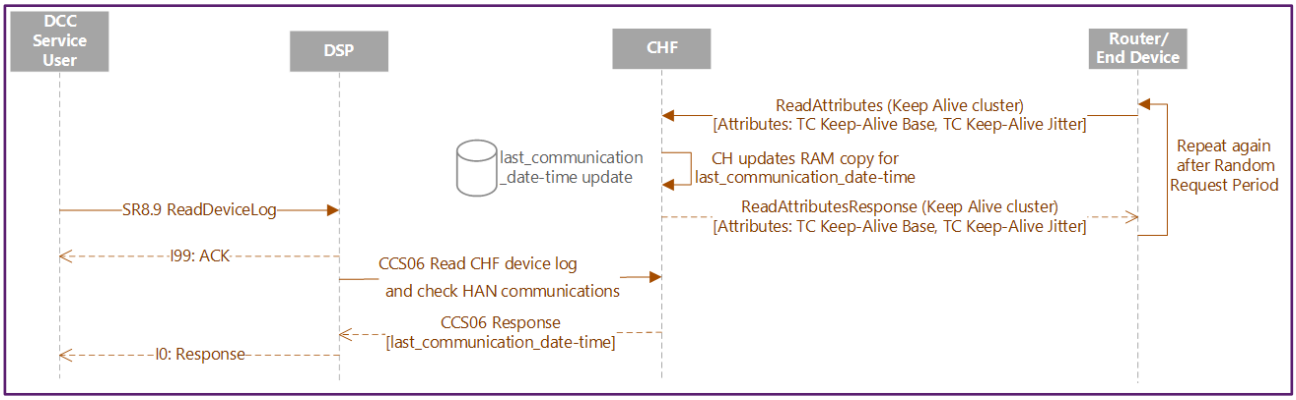
Field	WNC Current Configuration	WNC New Configuration *	TOSHIBA	EDMI
TC Keep-Alive Base	0x01 (1 min)	0x0A (10 mins)	0x0A (10 mins)	0x0A (10 mins)
TC Keep-Alive Jitter	0x003C (60 secs or 1 min)	0x012C (300 secs or 5 mins)	0x012C (300 secs or 5 mins)	0x012C (300 secs or 5 mins)
Minimum Random Period	1 minute	10 mins	10 mins	10 mins
Maximum Random Period	1 min + 1 min = 2 mins	10 min + 5 min = 15 mins	10 min + 5 min = 15 mins	10 min + 5 min = 15 mins
Random Request Period [Minimum Period, Maximum Period]	[0 mins, 2 mins]	[10 mins, 15 mins]	[10 mins, 15 mins]	[10 mins, 15 mins]

Comms Hub configuration of Keep Alive attributes and random request periods.

* NOTE: WNC New Configuration will occur after Deployment of SB 5.1 and DB 3.1. Indicative dates are 1Q 2024.

As can be seen in the table above, the WNC New Configuration aligns with the values used by the other CH vendors.

ZigBee Keep Alive mechanism message flow



ZigBee message flow for Keep Alive mechanism.

2.10.3.7 Overview tables

QUERY	WNC	TOSHIBA	EDMI
Storage of ***last_communication_date-time***	Uses RAM and flash memory storage. 1) The RAM copy is updated every time a HAN device in the CHF Device Log communicates with the Comm Hub at the ZigBee application layer as per the provided triggers. 2) The flash copy gets updated every 30 minutes.	Uses RAM and flash memory storage. 1) The RAM copy is updated every time a HAN device in the CHF Device Log communicates with the Comm Hub at the ZigBee application layer as per the provided triggers. 2) The flash copy gets updated in the next scheduled periodic flash write cycle (within 24hrs) or earlier if any of the below events occur: * During CH shutdown (for whatever reason) * Immediately after HAN device join or rejoin. * Whenever a device is added or removed from CHF device log	Uses RAM and flash memory storage. 1) The RAM copy is updated every time a HAN device in the CHF Device Log communicates with the Comm Hub at the ZigBee application layer as per the provided triggers. 2) The flash copy gets updated every 30 minutes.

Table showing different CH handling for last communication data-time storage and updating

QUERY	ALL CHs (same behaviour)
Trigger for update of ***last_communication_date-time***	1) Rejoin requests 2) Key establishment messages to create security keys 3) Attribute requests/commands 4) Receipt of Default Response
CCS06 (SRV8.9 ReadDevicelog) to read the CHF Device Log	The ***last_communication_date-time*** is retrieved from the RAM copy.
ZigBee messages routed through Comms Hub with other device as destination	The ***last_communication_date-time*** RAM or flash copies for the source device are not modified by the Comms Hub acting as a router.

Table showing same CH handling for selected last communication date-time actions

QUERY	ALL CHs (same behaviour)
Approach per device	Same implementation applies to all devices in the CHF Device Log
PPMID and Type 2 Devices The expectation is for a PPMID/IHD/CAD to communicate with Comms Hub at least once per day, as long as the HAN device is powered up. In dual fuel or gas only installs, a PPMID/IHD/CAD would request for GPF data on a frequent basis, meaning that a Service User verifying the best communication between a Comms Hub and PPMID/IHD/CAD would expect to see a timestamp in	Agreed with expected behaviour.

QUERY	ALL CHs (same behaviour)
the ***last_communication_date-time*** attribute within the last few minutes under normal operating conditions. In electricity only installs, there would be two possible scenarios for the timestamp in the ***last_communication_date-time*** attribute. * Device supports Keep Alive cluster: A Service User verifying the last communication between a Comms Hub and PPMID/IHD/CAD would expect to see a timestamp in the ***last_communication_date-time*** attribute within the last been to twenty minutes under normal operating conditions. * Device does NOT support Keep Alive cluster & Service User verifying the last communication between a Comms Hub and PPMID/IHD/CAD would expect to see a timestamp in the ***last_communication_date-time*** attribute within the last 24h under normal operating conditions inked to daily time synchronisation with the Comms Hub.	
GSME (expected behaviour): The expectation is for a GSME to communicate with Comms Hub every wakeup cycle, that is, every thirty minutes. Important to be in mind that such a period is manufacturer specific. The ***last_communication_date-time*** attribute in CCS06 (SRV8.9 ReadDeviceLog) for a target GSME would change values more frequently than once per day. Hence a Service User verifying the last communication between a Comms Hub and GSME would expect to see a timestamp in the ***last_communication_date-time*** attribute within the last thirty minutes (GSME wakeup cycle) under normal operating conditions.	Agreed with expected behaviour.
ESME: The expectation is for an ESME to communicate with Comms Hub multiple times in a day through a series of events, * Request for the ZigBee Time attributes from the Time cluster (0x000A) from its Comms Hub once every 24h by means of ZigBee ReadAttributes commands. * Handle Zigbee RequestTunnel from the Tunneling cluster (0x0704) from Comms Hub every 18.2h approximately. * Send multiple daily ZigBee ReadAttributes commands to the Keep-Alive cluster (0x0025) in the Comms Hub to read the TC Keep-Alive Base (Default value: 10min) and the TC Keep-Alive cluster attributes (Default value: 300s) as Comms Hub configuration see Section 2.10.3.6). * Periodic ZigBee OTA Query Next Image Request command to check for a new ESME OTA upgrade image. * Deliver WAN device alerts to Comms Hub if any take place. * Handle Service Requests and produce Service Responses if any take place. The previous event list establishes that the ***last_communication_date-time*** attribute in CCS06 (SRV8.9 ReadDevicelog) for a target ESME would change values more frequently than once per day and most likely within the last fifteen or twenty minutes determined by the *Keep Alive attributes configuration* in the Comms Hub. Hence a Service User verifying the last communication between a Comms Hub and ESME would expect to see a timestamp in the ***last_communication_date-time*** attribute within the last fifteen or twenty minutes under normal operating conditions.	Agreed with expected behaviour.

Table showing same CH approach per HAN device type.

2.10.4 Mapping between SSI Comms Hub Diagnostic and SRV8.9 ReadDeviceLog (CCS06) Service Responses

A summary of how the *last_communication_date-time* from CCS06 is mapped into the SSI Comms Hub Diagnostics is presented in the table below. For more details please refer to section 2.10.2.1.

Mapping of last Communication date-time to SSI Comms Hub Diagnostic user interface	Toshiba Hub Mapping	WNC Hub Mapping	EDMI Hub Mapping
ReadDeviceLog (CCS06) *last_communication date-time*	SSI HAN Device - Last HAN Message	SSI HAN Device - Last Connection SSI HAN Device - Last HAN Message	SSI Ping Test Result

Mapping of CCS06 last_communication_date-time to SSI Comms Hub Diagnostic.

2.11 Guidance Point 11: GBCS 4.1 CH FW handling of GSME/PPMID/HCALCS OTA

Guidance Point Number 11	GBCS 1.0/2.0/3.2	GBCS 4.1	GBCS 4.2+	
Applicability	Issue Not Seen	Yes	Issue Not Seen	
Guidance Type	Clarification on Shared memory Slot for OTA transfer to GSME/PPMID/HCALCS. Addresses specific issue associated with WNC CH upgrade to Release 4.1			
Functional Area	Device OTA			
Keywords	SRV11.1, SRV11.4, TS1520, SECMOD0007, GBCS 4.1			

2.11.1 Problem Statement

This issue applies only for WNC CH after the initial GBCS 4.1 CH FW upgrade.

When Energy suppliers perform a FW OTA for GSME/ PPMID/ HCALCS, they will receive N60 & N62 alerts in response under the specific conditions which follow. This happens after a WNC CH is initially upgraded to GBCS 4.1 CH FW. Energy suppliers will also receive an N64 alert when WNC CH FW is upgraded to GBCS 4.1 CH FW (SBCH- 5.0.0.7 & DBCH- 3.0.0.7). The following 3 Steps need to happen in order for this issue to be seen:

1. A successful GSME FW OTA is completed.
2. WNC Comms Hub upgrades its FW to GBCS 4.1.
3. HCALCS/PPMID/GSME OTA FW attempt made within 14 days of Step 2.

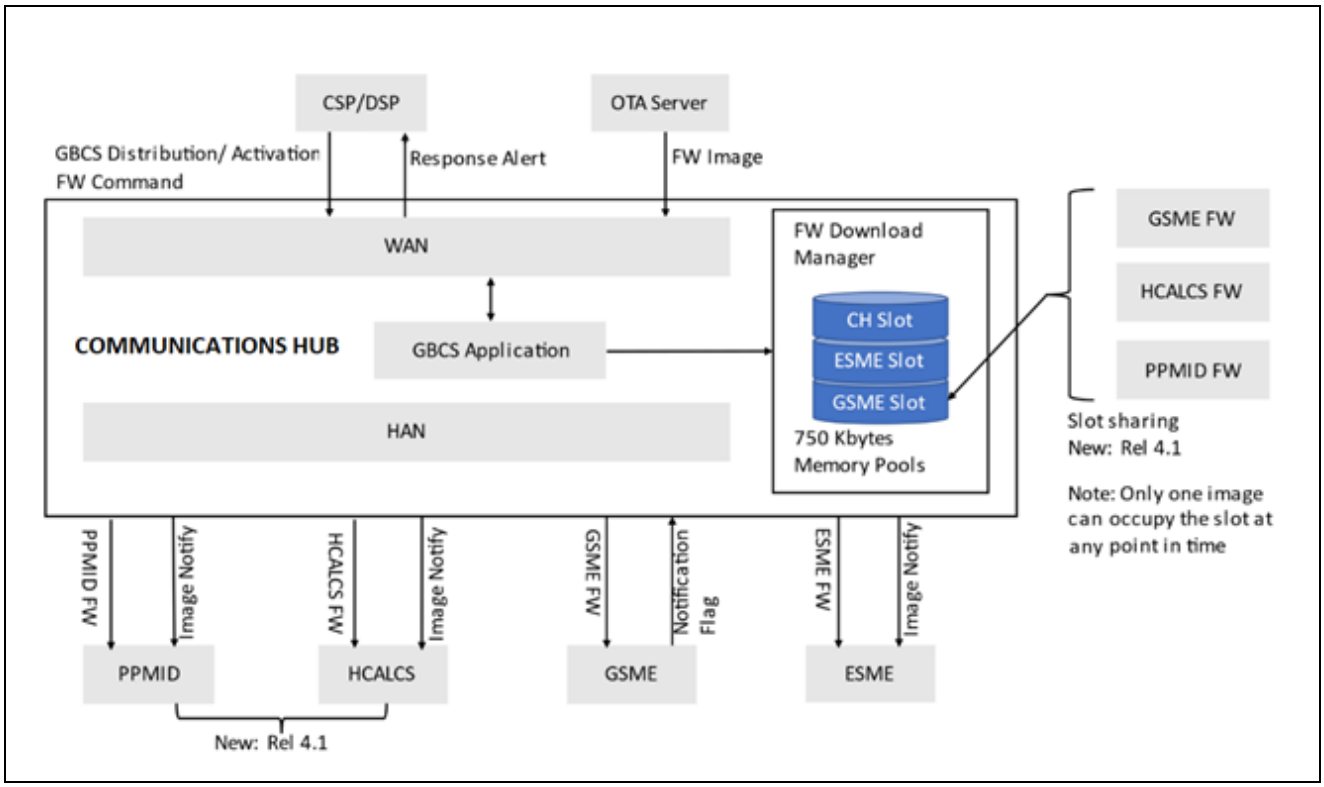
Because this issue only occurs for around 14 days after WNC CH is upgraded to GBCS 4.1 it will not be seen on every CH upgrade.

This guidance point provides scenario diagrams and a description of CH standard working practice for FW OTA along with a description of the problem and a suggested workaround.

2.11.2 Background

The following diagram gives an architectural overview of the CH FW Download Management on the HAN. The CH acts as a 'store and forward' location for passing FW onto other devices on the HAN.

As shown, with the support of GBCS 4.1 functionality in CH FW, the GSME Slot is shared between 3 device types (GSME, PPMID & HCALCS). The ESME Slot / CH Slot are used only to store ESME & CH firmware images respectively & that storage is not shared.



In order to overwrite FW data associated with a previous FW DL, the following general rules apply:

- An image can be stored for 14 days, after which it can be deleted or overwritten. At this point the slot becomes freed up for a new image, whether or not the image is retained in the slot. (The freeing up of the slot is a matter of internal CH housekeeping.)
- Once a successful transfer of the FW to the target device has been performed, the slot is freed up for a new image. This can occur within the 14 days.
- An image that has been retained after the successful transfer to a device can be used for further transfers to similar compatible devices.
- A Force Replace flag is used for GSME/ /ESME (SR 11.1) to ensure that the previous FW is overwritten. This is not available for the PPMID (SR 11.4)

For an ESME, GSME, HCALCS or Communications Hub the Upgrade Image shall be the concatenation:

Manufacturer Image || Force Replace || 0x40 || Authorising Remote Party Signature

2.11.3 Upgrades taking place within 14 days of CH Firmware Download

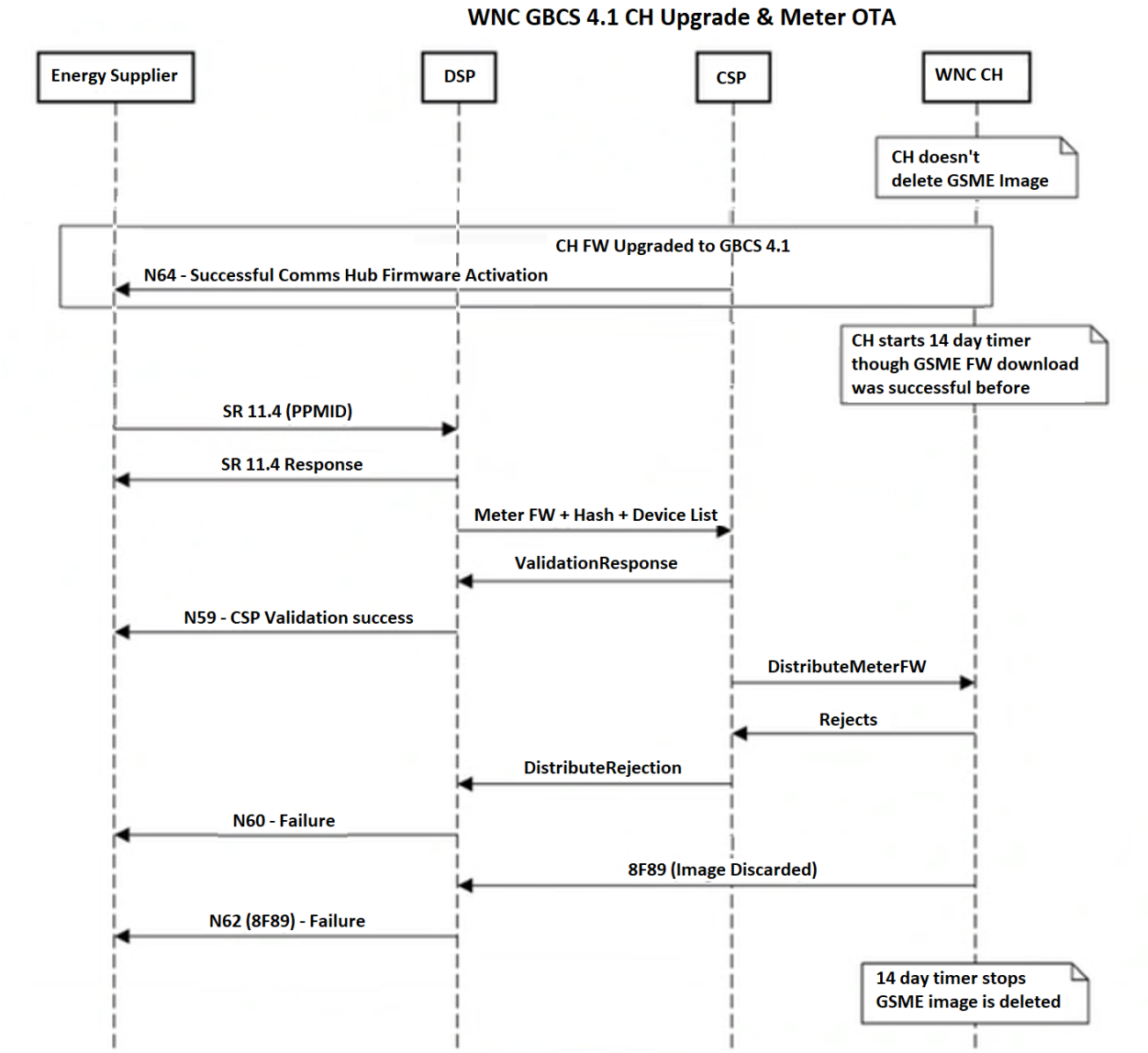
After upgrading WNC CH to GBCS 4.1 CH FW, if there was successful GSME OTA in the past with older WNC CH FW, SR 11.1 to Meter OTA GSME/HCALCS & SR 11.4 to PPMID will result in N60 & N62 (8F89 – Failure as image discarded) for 14 days after the GBCS 4.1 CH FW upgrade.

The Trigger condition for this issue to happen is as follows:

❑ WNC Comms Hub in Pre-GBCS 4.1 CH FW had successful GSME/HCALCS/PPMID OTA

❑ WNC Comms Hub is upgraded by OTA to GBCS 4.1 CH FW from Pre-GBCS 4.1 CH FW.

❑ New HCALCS/PPMID OTA FW sent within 14 days of CH FW or GSME with Force Replace set to 0x00.



The impact of this issue is summarized in the table below.

Issue	Suggested Workaround	Production Impact
SR 11.1 to OTA GSME without force replace flag set (0x00) will be rejected by WNC CH for 14 days since GBCS 4.1 upgrade. Energy supplier will get N60 & N62 alerts.	SR 11.1 to OTA GSME to be retried after 14 days OR Set force replace flag (0x01) to true when GSME image is loaded through adapter before issuing SR 11.1	Energy suppliers could try to perform GSME OTA just after WNC CH FW upgraded to GBCS 4.1. Six Energy Suppliers have indicated they always trigger GSME OTA with force replace flag set to true.
SR 11.4 to OTA PPMID or SR 11.1 to OTA HCALCS will be rejected by WNC	SR 11.4 to OTA PPMID to be retried after 14 days.	In production, DCC isn't aware of any capable PPMID / HCALCS

Issue	Suggested Workaround	Production Impact
CH for 14 days since GBCS 4.1 upgrade. Energy supplier will get N60 & N62 alerts.	SR 11.1 to OTA HCALCS to be retried after 14 days	product that could be candidates for OTA immediately.

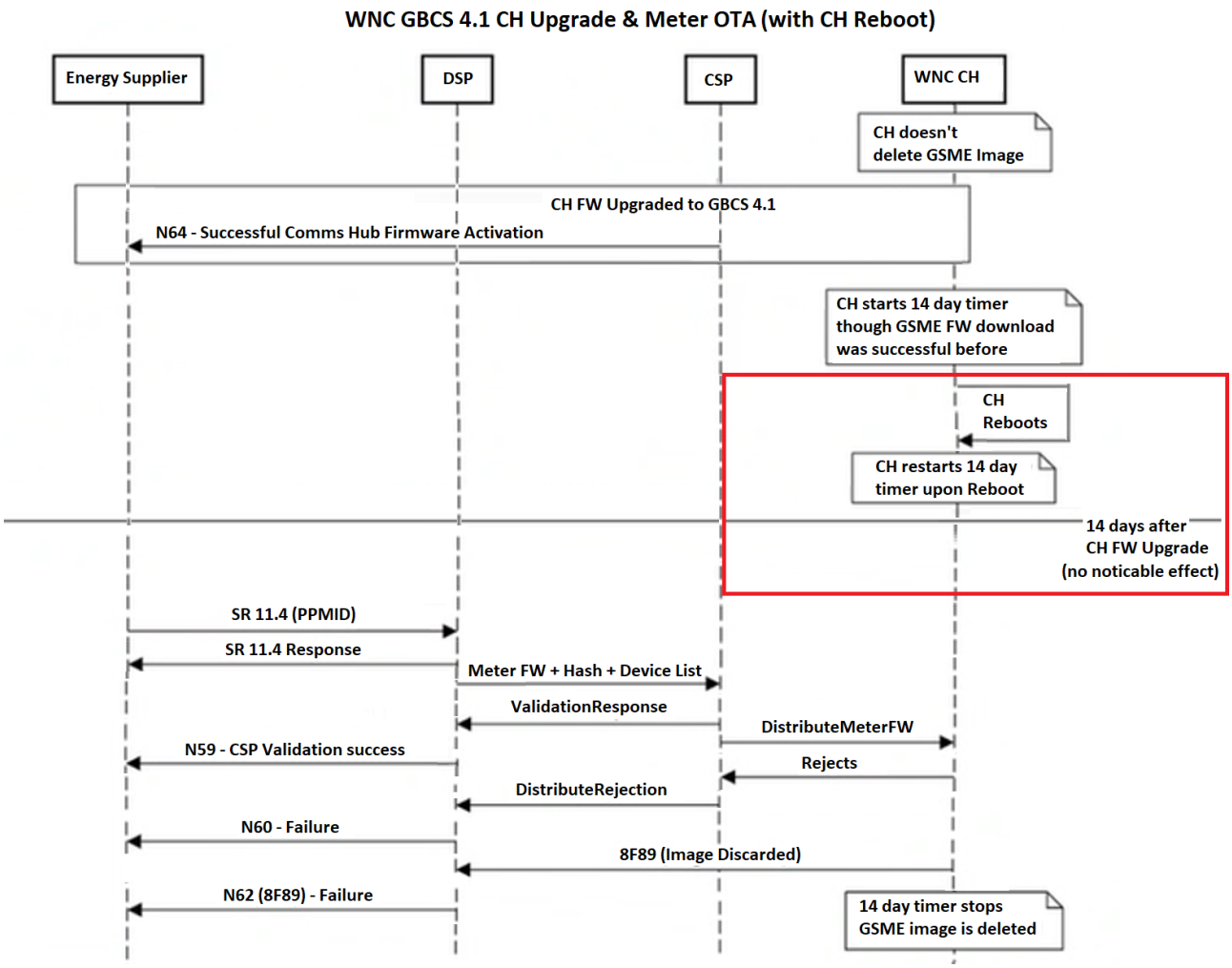
Note that after a period of 14 days has elapsed from the CH FW upgrade, the PPMID or HCALCS OTA can be successfully performed on the WNC CH.

This issue has not been observed on EDMI or Toshiba 2G/3G/4G CHs when upgrading GSME/HCALCS/PPMIDs. The table below summarises the impact.

Scenario	GBCS 4.1 CH FW			
	WNC Hub Handling	EDMI Hub Handling	Toshiba 2G/3G Hub Handling	Toshiba 4G Hub Handling
Sending SR 11.1 to perform GSME / HCALCS OTA without force replace flag set to True.	Any attempt to download a PPMID/HCALCS/GSME image during the 14 day period will be rejected. After future CH FW upgrades, the Device FW will always be accepted and this rejection won't happen.	Device FW OTA Accepted / Succeeds	Device FW OTA Accepted / Succeeds	Device FW OTA Accepted / Succeeds. Trigger condition of CH FW upgrade to GBCS 4.1 after successful GSME OTA will not be met in 4G CH.
Sending SR 11.4 to perform PPMID OTA.				
Sending SR 11.1 to perform GSME / HCALCS OTA with force replace flag set to True.	If it is a GSME image and it is urgent, the force replace flag can be used. • GSME OTA will be accepted. • HCALCS OTA will be rejected for 14 days. After future CH FW upgrades, this rejection won't happen & the Device FW OTA will be accepted.			

2.11.4 Retention of 14-Day Timer during Reboot

Related to the scenario in the previous section, it should be noted that the period of 14 days may be extended if the CH reboots for any reason, which causes the 14-day timer to be reset. Resetting the timer results in the period from the original CH upgrade being lengthened.



The reboot causes the CH to restart the 14-day timer. This occurs fundamentally because there is no requirement for a CH to maintain knowledge of the state of a GSME image apart from whether it is replaceable or not.

Any attempt to download a PPMID/HCALCS/GSME image during the 14-day period after the reboot / reset will be rejected.

As a workaround, if the FW OTA is for a GSME image and it is urgent, the force replace flag can be used.

This CH approach is ratified by TS1520 “Query on the 14-day Image Storage Timer & Image Discarded Alert Generation”, which states the following,

- That the image is required to be retained on the CH for a minimum of 14 days.
- That it is acceptable for the CH to restart a 14-day timer on reboot.

2.12 Guidance Point 12: Usage of Alerts 819D and 819E targeting ACB

Guidance Point Number	GBCS 1.0	GBCS 2.0	
12	NA	x	
Guidance Type	Comms Hub behaviors and alert triggers		
Functional Area	Comms hub alerts		
Keywords	819D alert, 819E alert, N13, *DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1*		

2.12.1 Problem statement

The purpose of this guidance is to help DCC Service Users understanding how each Comms Hub handles the generation of 819D (GSME Command Not Retrieved) and 819E (Tap Off Message Response or Alert Failure) by describing the underlying mechanisms that govern the communication link status between Comms Hub and GSME to handle TOM and non-TOM commands.

It is important to highlight that from DUIS2.0 onwards DCC Service Users have received one N53 (Command not delivered to ESME) DCC alert for each 8F84 (Failure to Deliver Remote Party Message to ESME) device alert generated, however there is no equivalent DCC mapping alert for 819D and 819E alerts. DCC Service Users would still receive N13 alerts for any SRV targeted to a GSME that times out.

2.12.2 Comms Hubs scenarios and triggers

GBCS defines the generation of both 819D and 819E alerts to Access Control Broker (DSP), as follows.

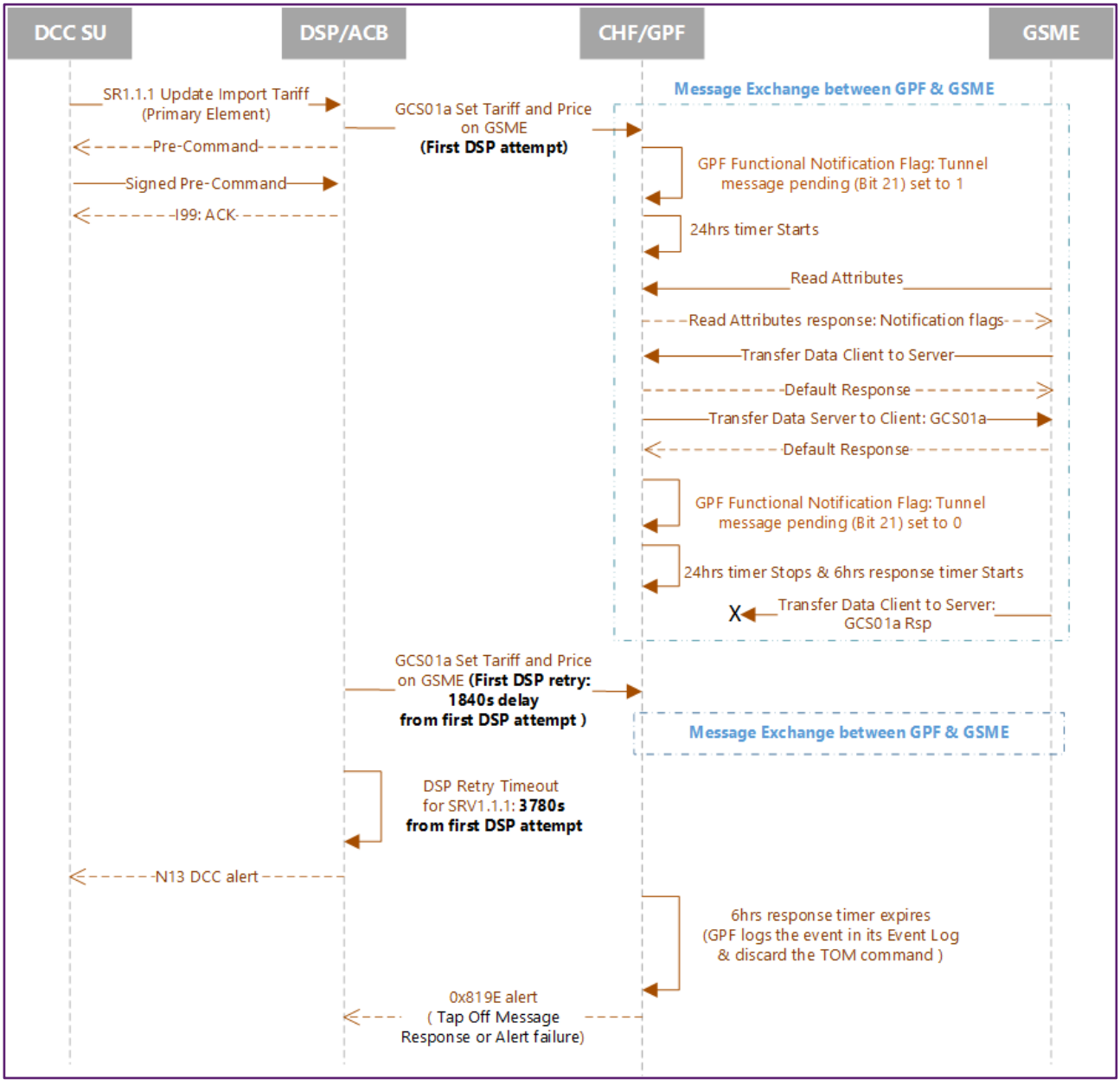
- If 24 hours elapse after setting the GPF *Tunnel Message Pending* flag without the Command being retrieved by the GSME, the CHF may discard the Command. If the CHF discards a Command in this way, it shall notify the GPF and the GPF shall log the event in its Event Log and send an Alert with a GBZ Payload containing an Alert Code 0x819D. and send such alert.
- If a Response to a TOM Command has not been received by the Communications Hub when the corresponding response timer reaches 6 hours … the GPF shall log the event in its Event Log and send an Alert with a GBZ Payload containing an Alert Code 0x819E.

Three scenarios are defined here to cover both TOM and non-TOM commands with a view into timeouts.

Scenario 1 (Toshiba/WNC/EDMI hubs) - GSME TOM command SRV1.1.1 (command retrieved by GSME)

- A DCC Service User sends a SR1.1.1, which is delivered to the GSME successfully, but either the GSME fails to respond, or the response fails to reach the hub for some reason.

- If the communications issues do not resolve, the Comms Hub generates one 819E alert targeted to the DSP and one N13 DCC alert from DSP to the DCC Service User.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of SRV1.1.1 is 3780s, as described in *DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1.*

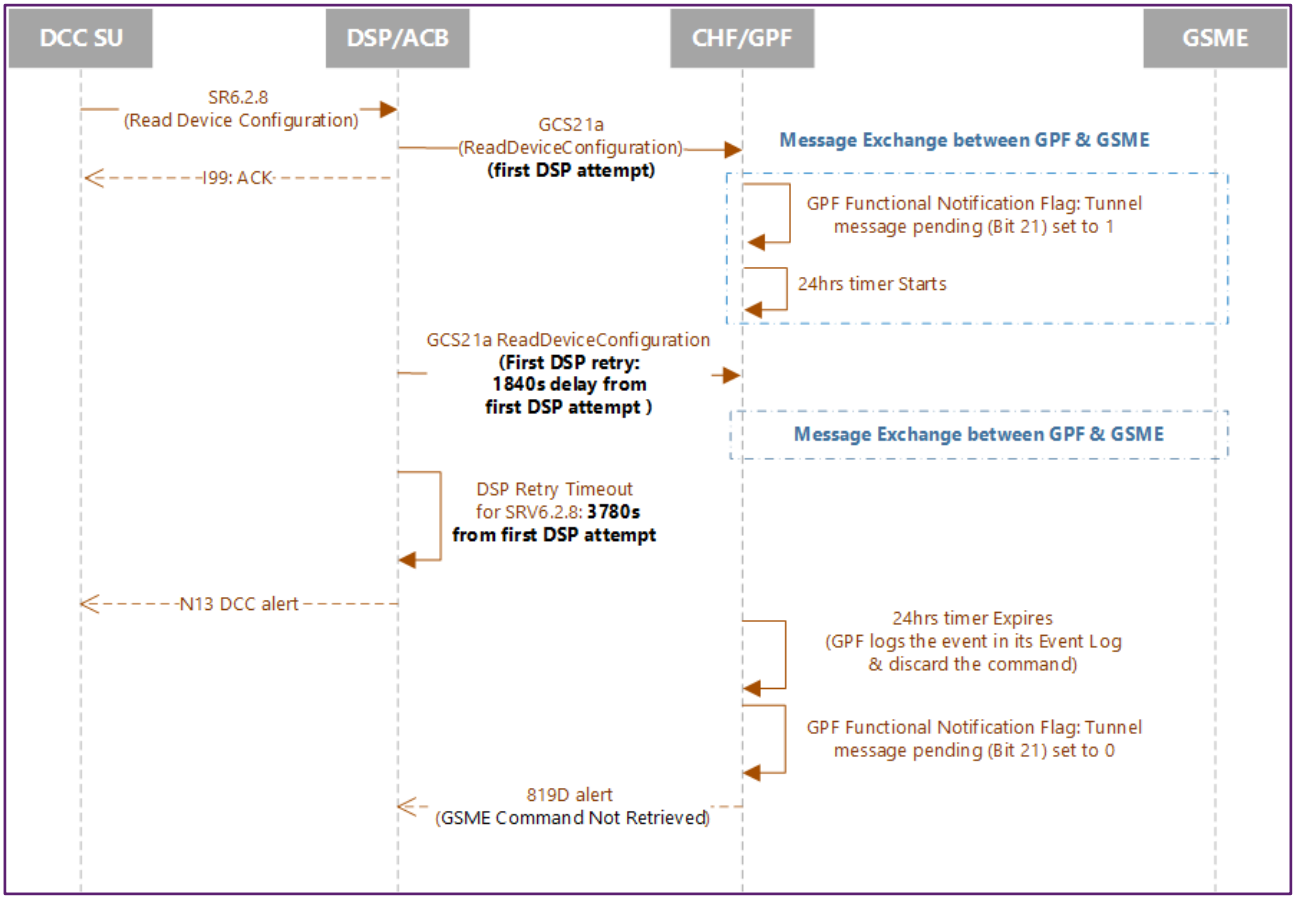


Scenario 1 - GSME TOM command SRV1.1.1 (command retrieved by GSME).

Scenario 2 (Toshiba/WNC/EDMI hubs) – GSME non TOM command SRV6.2.8 (command not retrieved by GSME)

- A DCC Service User sends a SR6.2.8, which fails to be delivered to the GSME.

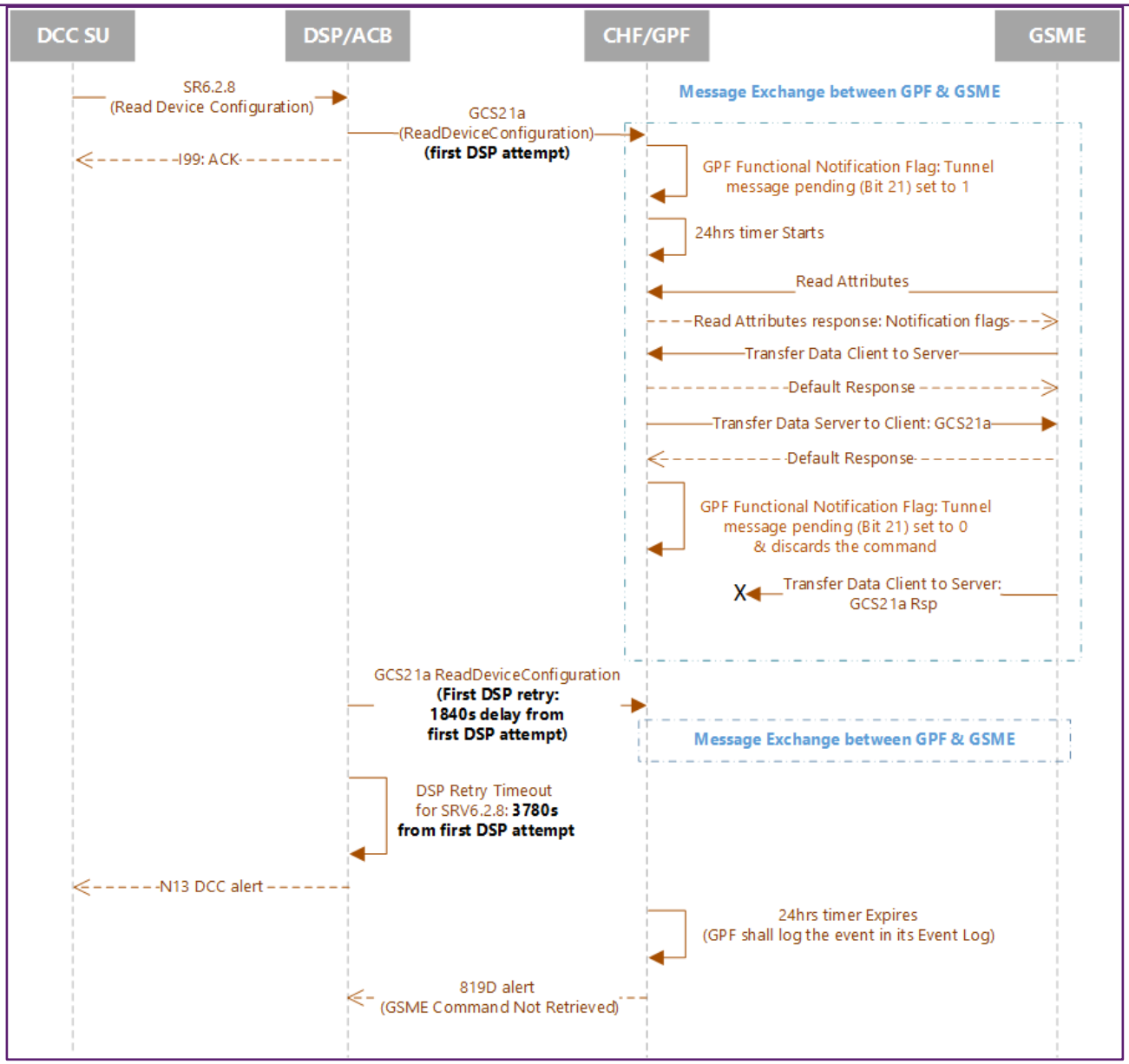
- If the communications issues do not resolve, the Comms Hub generates one 819D alert targeted to DSP and one N13 DCC alert from DSP to DCC Service User.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of SRV6.2.8 is 3780s, as described in *DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1*.



Scenario 2 - GSME non TOM command SRV6.2.8 (command not retrieved by GSME).

Scenario 3 (Toshiba/WNC/EDMI hubs) - GSME non TOM command SRV6.2.8 (command retrieved by GSME)

- DCC User sends a SR6.2.8, which is delivered to the GSME, but either the GSME fails to respond, or the response fails to reach the hub for some reason.
- If the communications issues do not resolve, the Comms Hub generates one 819D alert targeted to DSP and one N13 DCC alert from DSP to DCC Service User.
- DSP generates one N13 alert after the SRV retry timeout expires, which in the case of SRV6.2.8 is 3780s, as described in *DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1.*



Scenario 3 - GSME non TOM command SRV6.2.8 (command not retrieved by GSME).

2.12.3 Conclusions

The behaviour for all three Comms Hubs (Toshiba, WNC and EDMI) are the same, where one N13 alert is generated by the DSP to the DCC Service User after a given SRV times out as defined in *DCC-Retry-and-Timeout-Configuration-for-SMETS2-v1.14-1 (published in the SECAS website)*.

Similarly, either one 819D or 819E alert would be generated by a given Comms Hub with the DSP as target when the defined 24h or 6h timer expires as covered in the previous flow charts.

2.13 Guidance Point 13: Comms Hub behaviour for joining Devices in Sub GHz band during TCSO

Guidance Point Number	GBCS 1.0	GBCS 2.0 or later	
13	x	x	
Guidance Type	Comms Hub behavior on HAN		
Functional Area	HAN Device joins, order of rejoining, DBCH only.		
Keywords	TS1209, TS1235, TS1632, IRP617, CHTS 4.4.2.1, GBCS 10.6.2.4, SRV8.11, SRV 8.12.1, 8F2D alert		

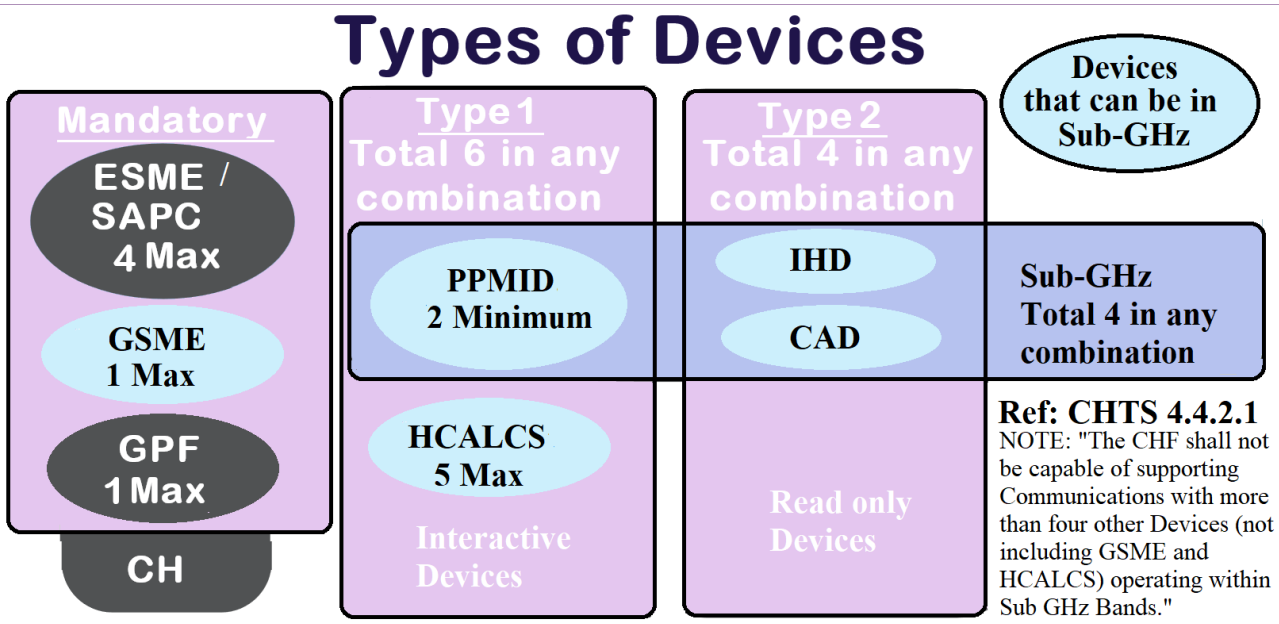
2.13.1 Background

This Guidance Point relates to the CH behaviour and the capacity limits for the number of devices allowed on the Sub GHz channel during TCSO (Trust Centre Swap Out, also known as Comms Hub replacement).

The limits on the number of devices that can join a Comms Hub are defined in CHTS 4.4.2.1 *Communications Links with the CHF* (see snapshot below). In summary, the Communications Hub can support up to 16 devices on both bands, with up to 10 devices supported on the Sub GHz band (1 GSME, 5 HCALCSs, 4 other devices either PPMID or Type 2 devices).

> **4.4.2 Communications**
>
> ***4.4.2.1 Communications Links with the CHF***
>
> The CHF shall be capable of establishing and maintaining Communications Links via the HAN interface with a minimum of:
>
> - any combination of four ESME and SAPC;
> - one GSME;
> - one GPF;
> - six Type 1 Devices (including a minimum of two PPMIDs); and
> - four Type 2 Devices.
>
> Of those Communications Links, the CHF shall not be capable of supporting more than one GSME or more than five HCALCS. The CHF shall not be capable of supporting Communications with more than four other Devices (not including GSME and HCALCS) operating within Sub GHz Bands.

The limits by device type are shown below:



GBCS section 10.6.2.4 CHF *Sub GHz Alerts and corresponding events* (table below) describes

- how Comms Hubs are to manage adding new devices to the CHF Device Log
- when 8F2D alerts *No More Sub GHz Device Capacity* are to be sent by Comms Hub to the DSP (ACB/Access Control Broker), and then mapped in the DSP into an N54 DCC alert *Dual Band CH Sub GHz Alert* with error code E59 targeted to Energy Suppliers.

Event / Alert Code Meaning	Requirements
No More Sub GHz Device Capacity	The event shall occur when: • a Device is added to the CHF Device Log which is not a GSME, SAPC or HCALCS; • there are already four Devices in the CHF Device Log, which are not HCALCS, SAPC or GSME, that joined the SMHAN on a Sub GHz frequency; and • the Device added then attempts to join the SMHAN on a Sub GHz Frequency. On occurrence of this event, the CH shall: 1) not allow the Device to join the SMHAN on a Sub GHz Frequency; 2) create an entry in the Event Log with Event Code set to 0x8F2D and otherInfo set to 'Device ID' of the Device concerned; and 3) send a 'DBCH11 No More Sub GHz Device Capacity Sub GHz Alert' with: a) the Message Code set to 0x0115; b) the Alert Code set to 0x8F2D; and c) the Use Case Specific Additional Content set to the concatenation 0x0908 || 'Device ID'

According to TS1209 *How should a DBCH apply Sub-GHz capacity restrictions when running TCSO?*, TS1235 *TCSO Edge Case for DBCH for No More Sub GHz Device Capacity* and the withdrawn IRP617 *TCSO Edge Case for DBCH for No More Sub GHz Device Capacity*, the 8F2D alert *No More Sub GHz Device Capacity* is only generated whenever a new PPMID or Type 2 Device (IHD or CAD) is added to the CHF Device Log via a SRV8.11 *Update HAN Device Log* (CCS01) and there are already four of those device types in the Sub GHz band.

Hence, it is not applicable to the Comms Hub replacement scenario and SRV8.12.1 *Restore HAN Device Log*, where no 8F2D alerts would be expected from a Comms Hub. This is due to a limitation in the SRV8.12.1, that does not include the device types. For that reason, the Comms Hub does not know a device type until it has completed CBKE and got ZigBee security keys. This is very different from SRV8.11 *Update HAN Device Log*, where the device type is part of the command payload, so the Comms Hub can decide whether to reject such device when joining.

According to production data, no 8F2D alerts were registered in one month observation window in December 2023, indicating that this scenario is extremely unlikely.

2.13.2 Comms Hub behaviours for Sub GHz device capacity detection

During Comms Hub replacement, all 3 Dual Band Comms Hubs will allow the device to join in Sub-GHz as device type could only be established afterwards. This could result in the maximum capacity being exceeded but should result in an 8F2D CHF Sub GHz Alert (No More Sub GHz Device Capacity) once this is detected.

CH Vendor	Comms hub replacement scenario: Unknown device type potentially exceeding maximum capacity	Install and commission: Known device type
Toshiba EDMI	As the device type is unknown during TCSO, CH will allow the first 4 Sub-GHz devices to join the CH. If all four were not GSME/HCALCS and a 5th unknown device (incl. GSME/HCALCS) tries to join in Sub-GHz: • Device is allowed to join (ZigBee join, service discovery) • CH sends 0x8F2D alert with IEEE Address of the device that has joined if it is identified as not being a GSME/HCALCS. • In the event that the 5th device is not a GSME/HCALCS, CH ages out this new device (no communication with device). CH shall not process any messages received from the aged-out end-device child and shall not send any response. CH will send NWK-LEAVE with REJOIN bit set on handling Data-Request/poll message from the Child Device. • Note that if the 5th device is not GSME/HCALCS, this behaviour could present misleading information to the consumers; as it will show as 'Joined to the Network', but there would be no Meter specific info/communication.	• Device Type checked and verified. CH will allow maximum of 4 Sub-GHz devices other than GSME/ HCALCS. • 5th device not GSME/HCALCS is not allowed to join. • CH sends 0x8F2D alert with IEEE Address of the device trying to Join.
WNC	As the device type is unknown during TCSO, CH will allow the first 4 Sub-GHz devices to join the CH. If all four were not GSME/HCALCS and a 5th unknown device (including GSME/HCALCS) tries to join in Sub-GHz: • Device is allowed to join (ZigBee join, CBKE, service discovery) • CH sends 0x8F2D alert with IEEE Address of the device that has joined if it is identified as not being a GSME/HCALCS.	

CH Vendor	Comms hub replacement scenario: Unknown device type potentially exceeding maximum capacity	Install and commission: Known device type
	• CH does not age out the new device and allows ZigBee communications.	

2.13.3 Alert 8F2D Generation

As per TS1632 *Generation of 8F2D alert*, the GBCS in section 10.6.2.4 CHF *Sub GHz Alerts and corresponding events* does not disallow Comms Hubs from sending 8F2D alerts *No More Sub GHz Device Capacity* in the Comms Hub replacement scenario.

All three Comms Hubs generate 8F2D alerts under certain conditions, as described in section 2.1.2 of this document.

2.13.4 Scenario for Sub GHz band capacity limit after TCSO.

Devices will re-join the Communications hub as part of the Comms Hub replacement process and all Dual Band comms hub variants can join with a mix of up to 9 type1/type 2 devices and 1 Gas Meter on the Sub GHz frequencies. This would be considered an extreme edge case.

According to GBCS 10.6.3 *Sub GHz End Devices – functional requirements* (see snapshot below), end devices can only change band during a Trust Centre re-join (Comms Hub replacement). In the extreme case a Comms Hub replacement can take place where there is 1 GSME, 5 HCALCS, 1 PPMID and 4 IHDs or CADs, operating across both bands after install and commission. If all such devices were to join the Sub GHz band, then the limit of 10 Sub GHz devices, defined in CHTS, would be exceeded. This would result in the last device being denied joining the Sub GHz band. The highest impact would occur if a GSME was to join last, as it would be blocked from joining.

10.6.3 Sub GHz End Devices - functional requirements

A Sub GHz End Device shall:

- not act as a ZigBee router when operating on a Sub GHz Channel;
- where the Device can also support 2.4 GHz operation:
  - on first connecting to a ZigBee network, attempt to establish network communication in the 2.4GHz band. Only where communications are not of sufficient quality, shall the Device attempt to establish network communications in the Sub GHz band; and
  - having connected to a ZigBee network at either 2.4 GHz or at Sub GHz, not attempt to change to the other of 2.4 GHz or Sub GHz except when undertaking a *Trust Centre re-join*, with its ZSE meaning; and
- not use the *Mgmt_NWK_Unsolicited_Enhanced_Update_notify* command to notify the CH of problems with its communications link more frequently than once in any 30-minute period.

2.13.5 DCC recommendation for industry.

As suggested by the withdrawn IRP617 *TCSO Edge Case for DBCH for No More Sub GHz Device Capacity*, to avoid blocking a dual band GSME from joining a dual band Comms Hub after a Comms Hub replacement in the edge scenario described in section 2.1.4, the best recommended sequence is:

- any Sub GHz GSME is powered on and connected first;
- any Sub GHz HCALCS are powered on and connected; and then
- any remaining Sub GHz capable Devices are powered on.

3 Recourse

Any concerns that SEC Parties have with information documented within this guidance should be raised with DCC in accordance with the SEC defined Testing Issue Resolution Process.

4 Appendix – Deprecated Guidance

There is no Deprecated Guidance in the current version.

5 Appendix - Document Control

Revision History

Revision Date	Summary of Changes	Version Number
16/05/21	Initial Version Created – GP1&2	0.01
20/07/21	Revisions prior to publication on SECAS Website	1.0
09/09/21	Added further guidance entries - Up to GP05	1.01
13/10/21	Revisions prior to publication on SECAS Website	1.1
08/02/22	Added further guidance entries - Up to GP7 for publication on SECAS Website	1.2
11/04/22	Added further guidance entries - Up to GP8 and additions to GP1	1.2.1
08/06/22	Revisions prior to publication on SECAS Website	1.3
08/03/23	Added further guidance entry - GP9	1.4
28/03/23	Added further guidance entry – GP10	1.5
03/11/23	Added further guidance entries - Up to GP12 and corrections to GP10	1.6
14/02/24	Added further guidance entry - GP13	1.7
15/02/24	Revisions prior to publication on SECAS Website	1.7.1
21/02/24	Further Revisions prior to publication on SECAS Website	1.7.2

Reviewers

Each individual guidance is reviewed internally followed by Industry review via TSIRS before being added to this guidance document. All versions, before release to Industry, are reviewed internally by DCC Design Authority including DCC, CSP and DSP.

6 Appendix - Technical Specifications References

TS #	GP Ref	Title	Comment
TS0742	3	Changing billing calendar	Asks question: When setting a Billing Calendar, what happens to the old calendar details?
TS0885	6	Gas Tariff Changes - Clarification on when to push the updated price structures to the IHD / PPMID	
TS0932	6	GPF requirements to push information - query TS0885	Asks question: Should there be a publish price on every price change?
TS0953	6	GPF setting notification flags and GSME behaviour	Asks question: When a GPF sets notification flags, should the GSME act on these before the GPF is added to the GSME Device Log?
TS0956	7	Clarification on what value to set CommodityType to on GPF	
TS0961	3	Clarification on startDateTime And Periodicity	Asks question: Can the Meter change the configuration data defined by SMETS by itself (ie self-triggered based on time/events) or is this configuration data changed only by remote party?
TS1029	6	Device Binding Requirement Clarification	Asks questions: Does CH need to maintain a large binding table all the time and of what size? Is there a requirement to support minimum 5 clusters per device, taking into account certain exceptions and assumptions?
TS1209	13	How should a DBCH apply Sub-GHz capacity restrictions when running TCSO?	
TS1235	13	TCSO Edge Case for DBCH for No More Sub GHz Device Capacity	Addresses issue of adding entry to Device Log in the instance where the Device Type is not known prior to the joining attempt.
TS1316	2	8F0C Alert Triggers Query	Addresses issues of timing relativity between HAN devices, ‘Reliable’ & ‘Unreliable’ Time and sending SR6.11
TS1323	7	GPF handling of multiple GSME reports within a single 30 minute period	
TS1349	7	Queries following TS1323 Clarification	Asks questions: When is a GSME meant to capture and push to the GPF the ZigBee

TS #	GP Ref	Title	Comment
			attributes “CurrentSummationDelivered, CurrentDayAlternativeConsumptionDelivered and CurrentDayCostConsumptionDelivered”? Are the data capture and push events expected to occur on each hour and half hour timepoints as indicated in the GBCS section 10.4.2.8? Are GBCS section 10.4.2.8 and SMETS2 section 4.5.1 mandating different approaches?
TS1376	9	Alert Code 0x8F84 Query	Asks question: What is the expectation from the technical specifications in terms of the generation of the Alert with Alert code 0x8F84 when an ESME cannot receive any Remote Party Commands because it is powered down or its ZigBee connectivity between the ESME and Comms Hub is limited temporarily? Several Scenarios are addressed.
TS1405	1	How can the Supplier diagnose the source of time drift?	
TS1423	1	Max CH time drift without ‘Reliable’ WAN communication	Asks questions: What will the CH use as an internal time source on power restoration + no WAN? What will the CH use as an internal time source on reboot? On reboot + no WAN, what would its power up behaviour be?
TS1519	8	How should CH behave if end device sends Upgrade End Request status value other than SUCCESS?	Asks questions: What should happen if the end device sends Upgrade End Request status value other than SUCCESS i.e., INVALID_IMAGE, REQUIRE_MORE_IMAGE & ABORT? Is the expected behaviour different for different image type, ESME / GSME / HCALCS / PPMID?
TS1520	11	Query on the 14-day Image Storage Timer & Image Discarded Alert Generation	Clarifies that the image is required to be retained on the CH (bar a force replace) for a minimum of 14 days. Therefore, it is acceptable for the CH to restart a 14-day timer on reboot.
TS1632	13	Generation of 8F2D alert	Asks questions: Under which conditions should the CH generate 8F2D alert “No More Sub GHz Device Capacity” during TCSO? Is this affected by the order in which devices join? Should 8F2D alerts be sent when the device limit is exceeded for GSME, SAPC or HCALCS? If any of the device categories are

TS #	GP Ref	Title	Comment
			exceeded, would the devices still be able to communicate and remain in the CHF Device Log?