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

Paper Reference:	**TABASC_50_0602_14**
Action:	**For Information**

DP098 'Incorporation of multiple Issue Resolution Proposals into the SEC – Batch 3'

1. Purpose

This paper has been produced to inform the Technical Architecture and Business Architecture Sub-Committee (TABASC) of the 21 non DCC System impacting Issue Resolution Proposals (IRPs) that have been included in DP098. The table below sets out the IRPs and states which technical specification they affect. More information can be found in the embedded Word documents.

2. Non DCC System impacting IRPs

Non DCC system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP547**	Default Response in GCS21k message 'profile cluster' flag v0_1	GBCS	IRP547 Default Response in GCS21k
IRP567	Tariff prices for Twin-Element ESME query	SMETS	IRP567 twin element active tariff price displ
IRP587	Marking CCS05-CCS04 deprecated Use Case v0_1	GBCS	IRP587 Marking CCS05-CCS04 deprec
IRP588	Issue Title Mirror Reporting attribute not available in ZCLv4	GBCS	IRP588 Mirror Reporting attribute nc
IRP589*	CS02b authentication sequence v0_1	GBCS	IRP589 CS02b authentication sequer

Non DCC system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP590	References in T16.2 for 81BE 81BF + 8F84 v0_1	GBCS	 IRP590 References in T16.2 for 81BE 81BF _
IRP591*	Clarification of HCALCS Time Cluster	GBCS and SMETS	 IRP591 Clarification of HCALCS Time Clust
IRP592	Clarification required for channel change operation	GBCS	 IRP592 Clarification required for channel c
IRP596*	TransCoS Execution Counters – CS02b query	GBCS	 IRP596 transCoS Execution Counters - (
IRP599	Correcting references to Section 23 in GBCS	GBCS	 IRP599 Correcting references to Section
IRP601**	ZigBee spec reference for removal	GBCS	 IRP601 ZigBee spec reference for removal
IRP594	Mirroring Tariff Block Counters	GBCS	 IRP594 mirroring tariff block counters v
IRP604	Query on IRP550 - Frame Control	GBCS	 IRP604 Query on IRP550 - Frame Contr
IRP605*	Clarify DLMS COSEM Device Requirements in GBCS V2.1	GBCS	 IRP605 Clarify DLMS COSEM Device Requi
IRP606*	GBCS Glossary change for Encryption Remote Party	GBCS	 IRP606 GBCS Glossary change for E

Non DCC system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP608	Modify SMETS glossary term for Time-of-use Band	SMETS	IRP608 Modify SMETS glossary term
IRP600	Typo Errors in ZB Commands in T7.4	GBCS	IRP600 Typo Errors in ZB Commands in T
IRP607*	Max Demand: Script table LN reference ambiguous	GBCS	IRP607 Max Demand Configurable time v0_
IRP609	CCS07 Use Case Template Conflict with COSEM	GBCS	IRP609 CCS07 Use Case Template Conflic
IRP611*	Discrepancy in CS02a & CS02b for Commands Integrity Verification	GBCS	IRP611 Discrepancy in CS02a & CS02b for
IRP614	Device suspension requirements for Devices on 2.4GHz band	GBCS	IRP614 Device suspension requireme

*A number of these IRPs are included in the BEIS Auxiliary Proportionate Control (APC) consultation, which closed on 25 November 2019. However, the IRPs will remain included in this Draft Proposal and will be reviewed once the consultation responses have been published.

**These IRPs have previously been identified as DCC System impacting, however after discussions with the DCC this has proved to be inaccurate. IRP547 was previously confirmed as DCC System impacting, however a further code review has indicated that the DCC System already comply with this IRP. In relation to IRP601, BEIS have confirmed that there should be no impacts to CH Vendors stacks, as the IRP will not forbid the stack to issue the command in the specific condition described in the IRP. This has been clearly communicated and accepted by both CSPs and all CH vendors.

Please note that we are currently querying the status of IRP599, as the changes required in the IRP document appear to already have been implemented. We will provide an update to TABASC at the meeting.

3. Recommendations

The TABASC is requested to:

- **NOTE** the contents of this paper;
- **CONSIDER** the 21 IRPs included in the draft proposal; and
- **AGREE** that the 21 IRPs should be implemented under the revised IRP process.

Bradley Baker

SECAS Team

30 January 2020

Attachments:

Appendix A: DP098 Modification Report

Appendix B: DP098 Draft Legal Text

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

DP098

'Incorporation of multiple Issue Resolution Proposals into the SEC – Batch 3'

Modification Report

Version 0.1

About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

Contact

If you have any questions on this modification, please contact:

Bradley Baker

020 7770 6597

bradley.baker@gemserv.com

1. Summary

This Draft Proposal was raised by Paul Saker from EDF Energy.

The Department for Business, Energy and Industrial Strategy (BEIS) has previously implemented Issue Resolution Proposals (IRPs) via BEIS-led designations; however this process was handed over to the Smart Energy Code Administrator and Secretariat (SECAS) for changes to be implemented through the Modifications Process. To improve efficiency, it was agreed these changes should be progressed under a single proposal at regular intervals. This Proposal has been raised to introduce 21 non Data Communication Company (DCC) System impacting IRPs.

2. Issue

What are the current arrangements?

Issue Resolution Proposals

IRPs identify issues within the Smart Energy Code (SEC) Technical Specification documents and put forward a solution to the identified problem. BEIS took the lead in developing the Technical Specifications that sit under the SEC during the early stages of the Smart Metering Implementation Program. BEIS has taken responsibility for receiving and responding to issues raised internally, by the DCC and by other interested Industry Parties. Since inception, several hundred issues have been raised in relation to technical specifications under the SEC through the Technical Specification Issue Resolution Sub-group (TSIRS). In some cases, these queries have been resolved by providing an explanation of the specifications, whilst other have resulted in proposed amendments to the specifications in the form of IRPs.

What is the issue?

This Proposal has been raised to implement 21 non system impacting IRPs, which can be found in the table below.

IRPs identify issues in the SEC Technical Specification documents. The IRPs included in this proposal require changes to the GB Companion Specification (GBCS) and the Smart Metering Equipment Technical Specifications (SMETS), with initial key impacts identified by SECAS below.

Non system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP547	Default Response in GCS21k message 'profile cluster' flag v0_1	GBCS	IRP547 Default Response in GCS21k i
IRP567	Tariff prices for Twin-Element ESME query	SMETS	IRP567 twin element active tariff price displ
IRP587	Marking CCS05-CCS04 deprecated Use Case v0_1	GBCS	IRP587 Marking CCS05-CCS04 deprec
IRP588	Issue Title Mirror Reporting attribute not available in ZCLv4	GBCS	IRP588 Mirror Reporting attribute nc

Non system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP589*	CS02b authentication sequence v0_1	GBCS	IRP589 CS02b authentication sequer
IRP590	References in T16.2 for 81BE 81BF + 8F84 v0_1	GBCS	IRP590 References in T16.2 for 81BE 81BF _
IRP591*	Clarification of HCALCS Time Cluster	GBCS and SMETS	IRP591 Clarification of HCALCS Time Clust
IRP592	Clarification required for channel change operation	GBCS	IRP592 Clarification required for channel c
IRP596*	TransCoS Execution Counters – CS02b query	GBCS	IRP596 transCoS Execution Counters - (
IRP599	Correcting references to Section 23 in GBCS	GBCS	IRP599 Correcting references to Section
IRP601	ZigBee spec reference for removal	GBCS	IRP601 ZigBee spec reference for removal
IRP594	Mirroring Tariff Block Counters	GBCS	IRP594 mirroring tariff block counters v
IRP604	Query on IRP550 - Frame Control	GBCS	IRP604 Query on IRP550 - Frame Contr
IRP605*	Clarify DLMS COSEM Device Requirments in GBCS V2.1	GBCS	IRP605 Clarify DLMS COSEM Device Requi

Non system impacting IRPs			
IRP number	**IRP title**	**Impacted Technical Specification**	**IRP document**
IRP606*	GBCS Glossary change for Encryption Remote Perty	GBCS	IRP606 GBCS Glossary change for E
IRP608	Modify SMETS glossary term for Time-of-use Band	SMETS	IRP608 Modify SMETS glossary term
IRP600	Typo Errors in ZB Commands in T7.4	GBCS	IRP600 Typo Errors in ZB Commands in T
IRP607*	Max Demand: Script table LN reference ambiguous	GBCS	IRP607 Max Demand Configurable time v0_
IRP609	CCS07 Use Case Template Conflict with COSEM	GBCS	IRP609 CCS07 Use Case Template Conflic
IRP611*	Discrepancy in CS02a & CS02b for Commands Integrity Verification	GBCS	IRP611 Discrepancy in CS02a & CS02b for
IRP614	Device suspension requirements for Devices on 2.4GHz band	GBCS	IRP614 Device suspension requireme

*A number of these IRPs are included in the BEIS Auxiliary Proportionate Control (APC) consultation, which closed on 25 November 2019. However, the IRPs will remain included in this Draft Proposal and will be reviewed once the consultation responses have been published.

What is the impact this is having?

IRPs add clarity and corrections to the Technical Specifications documents. Device manufacturers are required to follow these documents for the specifications of their Devices. As a result, any errors or miscommunication of these specifications will mean the Device will not work as intended. The TSIRS agreed that these are issues and has agreed the solutions. Not implementing these solutions would mean that these problems would remain.

Appendix 1: Progression timetable

The recommended progression for this proposal is that it progresses to the Report Phase. In order to do this, the draft legal text must be approved by Panel. SECAS is preparing the draft legal text, which will be published on the SEC website ahead of the Panel meeting for comment.

If approved to progress to the Report Phase, the proposal will be sent out for Modification Report Consultation for final industry comment before going for decision at the Change Board. DP098 is recommended to be implemented in the November 2020 SEC Release.

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
BEIS	Department for Business, Energy and Industry Strategy
DCC	Data Communications Company
GBCS	Great Britain Companion Specification
IRP	Issue Resolution Proposal
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specifications
TSIRS	Technical Specification Issue Resolution Sub-Group

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

DP098 'Incorporation of multiple Issue Resolution Proposals into the SEC – Batch 3'

Legal text – version 0.1

About this document

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

These changes have been drafted against SEC Version 6.22.

This document contains the changes required to deliver the Proposed Solution.

Amend Section 6.4.4.1 as follows:

6.4.4 Information pertaining to the Supply of electricity to the Premises

The IHD shall be capable, upon establishment of a Communications Link with ESME (as set out in *Section* ***Error! Reference source not found.***), of providing the following information[1] on its User Interface and

The IHD shall be capable of displaying Currency Units in GB Pounds and European Central Bank Euro.

6.4.4.1 Active Tariff Price(s) [NUM]

~~The active Tariff Price~~ Whichever is supported by ESME, for Consumption in Currency Units per kWh~~.~~, of:

i. the *Active Tariff Price [INFO](5.7.5.5)*; or
ii. the *Primary Active Tariff Price [INFO](5.13.2.6)* and the *Secondary Active Tariff Price [INFO](5.13.2.9)*.

6.4.4.2 Cumulative Consumption [NUM]

i. Current Day cumulative Consumption;
ii. Current Day cost to the Consumer of cumulative Consumption in Currency Units;
iii. Current Week cumulative Consumption;
iv. Current Week cost to the Consumer of cumulative Consumption in Currency Units;
v. Current month cumulative Consumption; and
vi. Current month cost to the Consumer of cumulative Consumption in Currency Units.

Amend Section 7.4.6 as follows:

7.4.6 Information Pertaining to the Supply of Electricity to the Premises

A PPMID shall be capable, upon establishment of a Communications Link with ESME (as set out in *Section* ***Error! Reference source not found.***), of displaying the following information on its User Interface, and displaying updates of any changes to the information every 10 seconds thereafter:

i. whichever is supported by ESME:
   a) the ***Error! Reference source not found.*** *[INFO](**Error! Reference source not found.**)*; or
   ~~a)~~b) the *Primary Active Tariff Price [INFO](5.13.2.6)* and the *Secondary Active Tariff Price [INFO](5.13.2.9)*.

~~vii.~~ii. the **Error! Reference source not found.** *[INFO](**Error! Reference source not found.**)* where Emergency Credit is activated (including a clear indication that Emergency Credit has been activated);

~~viii.~~iii. whether Emergency Credit is available for activation on ESME;
~~ix.~~iv. any low credit condition;
~~x.~~v. the **Error! Reference source not found.** [INFO](**Error! Reference source not found.**);
~~xi.~~vi. the Debt to Clear when ESME is operating in Prepayment Mode;
~~xii.~~vii. whether ESME has suspended the Disablement of Supply during a period defined in the **Error! Reference source not found.** *[INFO](**Error! Reference source not found.**)* (as set out in *Section **Error! Reference source not found.***);
~~xiii.~~viii. either Aggregate Debt or time-based and payment-based debts when ESME is operating in Prepayment Mode;
~~xiv.~~ix. either Aggregate Debt Recovery Rate or each Time-based Debt Recovery rate when ESME is operating in Prepayment Mode;
~~xv.~~x. any **Error! Reference source not found.** [INFO](**Error! Reference source not found.**);
~~xvi.~~xi. **Error! Reference source not found.** [INFO](**Error! Reference source not found.**); and
~~xvii.~~xii. the **Error! Reference source not found.** [INFO](**Error! Reference source not found.**).

Amend Section 8.5.1 as follows:

8.5 Interface Requirements

This Section sets out the minimum required interactions which an HCALCS shall be capable of undertaking with ESME via its HAN Interface.

8.5.1 HAN Interface Commands

~~An HCALCS shall be capable of executing immediately the Commands set out in this Section following their receipt via its HAN Interface.~~ HCALCS shall be capable of executing the Commands set out in this Section.

HCALCS shall be capable of executing Commands immediately on receipt ('immediate Commands') and where specified in the Great Britain Companion Specification at a future date ('future dated Commands'). A future dated Command shall include the UTC date and time at which the Command shall be executed.

HCALCS shall be capable of cancelling a future dated Command. A future dated Command shall be capable of being cancelled by an Authorised party. HCALCS shall be capable of generating and sending a Response acknowledging that a future dated Command has been successfully cancelled.

8.5.1.1 Add Device Security Credentials

A Command to add Security Credentials for ESME to the ***Error! Reference source not found.(Error! Reference source not found.)***.

In executing the Command, the HCALCS shall be capable of verifying the Security Credentials.

Amend Section 9 – Glossary as follows:

Time-based Debt Recovery

A means of recovering debt based on an amount in Currency Units per unit time.

Time-of-use Band

A contiguous or non-contiguous number of Days for GSME or half-hour periods for ESME over which Tariff Prices do not change due to the passage of time ~~are constant~~.

Time-of-use Pricing

A pricing scheme with one or more Time-of-use Bands.

Amend Section 4 Security as follows:

4 Security

4.1 Introduction – informative

This Section 0 is informative and summarises Section 0.

Section **Error! Reference source not found.** lays out security provisions that are common across Messages, specifically stating that:

- at the application layer, all Messages must have integrity and authenticity protections, Critical Messages must have non-repudiation protections and some parts of Messages must have Confidentiality protections applied to specific data content; and
- ZSE protections will be relied upon when Devices within the same Smart Metering Home Area Network (SMHAN) communicate with each other.

Section **Error! Reference source not found.** lays out security provisions that are common across Remote Party Messages, specifically:

- *Identifiers, Counters and Protection Against Replay*: lays out requirements in relation to identifiers, counters and their use in Protection Against Replay;
- *Security Credentials*: lays out requirements for all Devices, except for Type 2 Devices, to:
    - have Public-Private Key Pairs, and to make their Public Keys available; and
    - have Trust Anchor Cells, including those which are storage areas within a Device, capable of holding Public Key Security Credentials for a number of Remote Parties, with the set of Remote Parties being derived from the functionality the Device supports; and
- *Cryptographic Primitives and their Usage*: lays out requirements for Cryptographic Algorithms and their usage, in relation to Remote Party Messages.

Note that the cryptographic protections are intentionally independent of whether a Message Payload is structured according to the ZSE, ASN.1 or DLMS COSEM standards. This means that Suppliers, Network Operators, the Access Control Broker and Other Users who may communicate with Devices need only implement cryptographic requirements in one way, regardless of the type of Device they are communicating with.

The same requirements for security apply regardless of whether a Message is delivered by the Wide Area Network (WAN), SMHAN, Hand Held Terminal (HHT) or local interface. Note that, for Prepayment Top Up, there are a number of different Messages. The content of each particular Message will always be processed in the same way regardless of delivery mechanism.

The following additional points are to be noted:

- the governance and structures to ensure uniqueness of identifiers are set out in the Smart Energy Code (SEC) and are outside the scope of the GBCS.

- a single Originator Counter can be used for the whole of a Remote Party Organisation (e.g. by that Party counting small enough time intervals). A separate counter per Device is not required;
- the Supplementary Originator Counter as specified in Section **Error! Reference source not found.** is required where the corresponding Response has to be cryptographically protected (by way of both Encryption and a MAC), to the Supplementary Remote Party. In all other cases, the Response containing Supplementary Remote Party details is protected back to the Access Control Broker; and
- Smart Metering entities make extensive use of a range of Counters as part of the unique identification of Smart Metering Messages. Counters are also a key component used to support Protection Against Replay functionality.

Amend Section 6 Message Categories as follows:

6.2.4 Command Authenticity and Integrity Verification

Requirements in this Section **Error! Reference source not found.** shall apply to Message Category SME.C and all subordinate categories.

6.2.4.1 Checks to be undertaken

The Device shall undertake the checks in Section **Error! Reference source not found.** before any other checks in this Section **Error! Reference source not found.**, except where relevant, as specified in Sections 13.5.4 and 13.7.4.2.2, ~~and shall undertake the other checks in the sequence set out in this Section 6.2.4.1~~ before undertaking any other processing of the Command.

Amend Section 7.3.8 DLMS Device Requirements Tables as follows:

7.3.8 DLMS Device Requirements Tables

Table 0a: Objects tab in embedded file

Table 0b: Scripts tab in embedded file

Table 0c: Application Associations tab in embedded file

Table 0d: Association LN Object Content tab in embedded file

Table 0e: Security Setup Object Content tab in embedded file

Table 0f: SAP Assignment Object content tab in embedded file

Table 0g: Conformance Content tab in embedded file

Table 0h: End to End Communications tab in embedded file

GBCS V3.3 Table 7.3.8.xlsx

GBCS V3.2 Table 7.3.8.xlsx

Amend Section 7.4 Device requirements - ZSE as follows:

7.4 Device requirements – ZSE

This Section 0 details the ZigBee clusters, attributes and commands that shall be supported by Devices in their interactions with other Devices on the same HAN, including whether the support is as a ZSE client or a server. Note, this Section does not detail the ZCL / ZSE commands that Devices will need to process as part of processing Remote Party Commands, or Commands sent by a PPMID to a GSME. Such requirements are detailed in Sections **Error! Reference source not found.** and **Error! Reference source not found.**.

Only Devices capable of operating at Sub-GHz shall be required to support the requirements in rows of Table 0 where the cell in the column labelled 'Sub GHz capable Devices only?' contains 'Yes'.

For clarity and as required by ZSE, all Devices shall support the Key Establishment Cluster as both Client and Server.

A GSME shall implement a ZSE *Metering Device* and shall implement all *the clusters, commands, attribute sets and attributes* in Table 0 where column A is 'GSME: Metering Device'.

A GPF shall implement a *ZSE Metering Device* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'GPF: Metering Device (Gas Mirror Endpoint)'.

A GPF shall implement a *ZSE Energy Services Interface* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'GPF: Energy Services Interface (Gas ESI Endpoint)'

A CHF shall implement a *ZSE Remote Communications Device* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'CHF: Remote Communications Device (Remote Communications Endpoint)'.

An ESME which is not a Twin Element ESME shall implement a *ZSE Energy Services Interface* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'ESME: Energy Services Interface (Electricity ESI Endpoint)'.

An ESME which is a Twin Element ESME shall implement three *ZSE Energy Services Interfaces*:

1. the first which shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'ESME: Energy Services Interface (Twin ESME aggregate ESI Endpoint)';
2. the second which, in relation to the primary measuring element, shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'ESME: Energy Services Interface (Twin ESME primary/secondary ESI Endpoint)'; and
3. the third which, in relation to the secondary measuring element, shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'ESME: Energy Services Interface (Twin ESME primary/secondary ESI Endpoint)'.

A PPMID shall implement a *ZSE In-Home Display*, shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'PPMID: In-Home Display', and shall support the other clusters, attributes and commands necessary to meet the SMETS requirements.

An HCALCS shall implement a *ZSE Load Control Device* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'HCALCS: Load Control Device'.

An HHT shall implement a *ZSE Remote Communications Device* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 0 where column A is 'HHT: Remote Communications Device'.

An IHD shall implement all the clusters, commands, attribute sets and attributes in Table 0 where column A is 'IHD: In-Home Display' and shall support the other clusters, attributes and commands necessary to meet the SMETS requirements.

Where a row in Table 0 is required for a Device, that Device shall support the cluster, attribute or command specified in that row as client or server, as specified in column C (labelled 'Client / Server').

Support for *clusters, commands, attribute sets and attributes* shall be as defined in columns B ('Cluster'), D ('Command'), E ('Attribute Set') and F ('Attribute').

Note that the other columns in Table 0 are informative and for requirements traceability only.

Except where explicitly required by this Section 0 or by Section **Error! Reference source not found.**, a Device shall not execute any ZSE command, be that in a GBZ Command Payload or provided as a native ZSE command, that could, if executed, constitute a Critical action. For clarity, a Device shall not execute a ZSE *Publish Change of Supplier* command if bits 11-12 of the *Provider Change Control* parameter (*Meter Contactor State*) of that command has any value other than 0b11 (*Supply UNCHANGED*).

GBCS V3.3 Table 7.4.xlsx

GBCS V3.2 Table 7.4.xlsx

Table 0: Device Requirements

Amend Section 10.6 Sub GHz Requirements as follows:

10.6 Sub GHz Requirements

In this Section **Error! Reference source not found.**, 'Duty Cycle' shall mean the percentage of time a Device is transmitting on Sub GHz frequencies. For clarity, any actions taken in relation to managing 'Duty Cycle', including the processing of *ZSE Suspend ZCL Messages* commands, shall only relate to communications with *End Devices* operating on Sub GHz frequencies.

10.6.1 Introduction – informative

This Section **Error! Reference source not found.** specifies requirements for Devices which are capable of operating on Sub GHz for their SMHAN operations. Data items defined in this Section **Error! Reference source not found.** shall have their defined meaning throughout this Section **Error! Reference source not found.**.

Amend Section 10.2.2.2 Tunneling Requirements as follows:

10.2.2.2 GSME

When a GSME has successfully established a shared secret key using *CBKE* with a Communications Hub, the GSME shall:

- send a request to the *ZigBee Gas ESI Endpoint* requesting the creation of mirrored *Basic, Metering* and *Prepayment Clusters* using the *RequestMirror* command;
- configure, using the *ConfigureMirror* command, the *ZigBee Gas Mirror Endpoint* to use the two way mirroring notification scheme '*Predefined Notification Scheme B'* ; and
- send a *RequestTunnel* command to the CHF to request a tunnel association with the CHF.

In line with ZSE, when a GPF sends a *RequestMirrorResponse* command in response to a *RequestMirror* command, the *RequestMirrorResponse* command shall contain the *EndPointID* to be used by the GSME regardless of whether the *RequestMirror* created the mirror.

A GPF shall only send a *RequestMirrorResponse* containing the *EndPointID* to the Device which caused the GPF to create the mirror.

Where a GPF receives a *ConfigureMirror* command to use the two way mirroring notification scheme '*Predefined Notification Scheme B*' which has the *Disable Default Response Sub-field* in its *Frame Control Field* set to zero, the GPF shall respond with a *Default Response* indicating *SUCCESS* if it has a mirror configured to use '*Predefined Notification Scheme B*', regardless of whether that was configured by the *ConfigureMirror* command.

Where the Communications Hub has successfully actioned a *ConfigureMirror* command, the GPF shall set the *Push All Static Data - Basic Cluster*, *Push All Static Data - Metering Cluster* and *Push All Static Data - Prepayment Cluster flags*.

Where a GSME reports a value for the *ManufacturerName* attribute or the *ModelIdentifier* attribute, the GPF shall accept that value. For clarity, there are no requirements for the GPF to subsequently process or make available any such value.

For clarity, the GSME:

- shall not action ZSE / ZCL commands received from the GPF in relation to any of the flags within *NotificationFlags2*, *NotificationFlags3* and *NotificationFlags5*;
- for *NotificationFlags4*, shall only action ZSE / ZCL commands received from the GPF in relation to the flags specified in Table **Error! Reference source not found.**a.

Bit Number	Waiting Command
6	*Get Prepay Snapshot*
7	*Get Top Up Log*
9	*Get Debt Repayment Log*

Table **Error! Reference source not found.**a: flags in *NotificationFlags4* to be actioned by the GSME

- for *FunctionalNotificationFlags*, shall only action ZSE / ZCL commands received from the GPF in relation to the flags specified in Table **Error! Reference source not found.**b:

Bit Number	Waiting Command
0	*New OTA Firmware*
1	*CBKE Update Request*
4	*Stay Awake Request HAN*
5	*Stay Awake Request WAN*
6-8	*Push Historical Metering Data Attribute Set*
9-11	*Push Historical Prepayment Data Attribute Set*
12	*Push All Static Data - Basic Cluster*
13	*Push All Static Data - Metering Cluster*
14	*Push All Static Data - Prepayment Cluster*
15	*NetworkKeyActive*
21	*Tunnel Message Pending*
22	*GetSnapshot*
23	*GetSampledData*
25	*Energy Scan Pending*
26	*Channel Change Pending*

Table **Error! Reference source not found.**b: flags in *FunctionalNotificationFlags* to be actioned by the GSME

- shall have access to the *Notification Flags* on the Communications Hub whenever it can communicate with the Communications Hub; and
- shall not provide any metering data to the *ZigBee Gas Mirror Endpoint* until and unless the GPF's Entity Identifier is recorded in the GSME Device Log.

The GSME shall send a *RequestTunnel* command to the CHF to request a tunnel association with the CHF whenever it does not have a currently valid tunnel association with the CHF, and one of the following is true:

- the GSME has created an Alert or Response that is to be sent; or
- the GSME has ascertained, via the *Tunnel Message Pending* flag, that there is a Command for it buffered on the Communications Hub.

Where the GSME receives a *RequestTunnelResponse* command from the CHF with a *TunnelStatus* of 0x01 (*Busy*), the GSME shall send another *RequestTunnel* command the next time it turns its HAN Interface on.

Where the GSME receives a *RequestTunnelResponse* command from the CHF with a *TunnelStatus* of 0x02 (*No More Tunnel IDs*), the GSME shall send a *CloseTunnel* command for any *TunnelID* that may relate to an active tunnel association between it and the CHF and, after receiving responses to all such commands, send another *RequestTunnel* command. Immediately following the successful establishment of the tunnel between the CHF and ESME / GSME, the ESME / GSME shall send an Alert with Alert Code 0x8F69.

10.2.2.2.1 MirrorReportAttributeResponse command support

GPF shall:

- support *ConfigureMirror* commands where the *'Mirror Notification Reporting'* field is set to 0x01, and treat such a value as a request from the GSME for the GPF to push

FunctionalNotificationFlags values using the *MirrorReportAttributeResponse* command;

- treat ZSE references to *'when the MirrorReporting attribute is set'* as references to '*when the Mirror Notification Reporting field in the most recently accepted ConfigureMirror command was set to 0x01'*; and
- send a *MirrorReportAttributeResponse* command to the GSME, containing the *FunctionalNotificationFlags* and *NotificationFlags#N* values required for '*Predefined Notification Scheme B'*, whenever it receives a *ReportAttributes* command from the GSME for any '*Attribute Reporting Status*' attribute with a value of '*Attribute Reporting Complete*'. Note that the GSME may support one such '*Attribute Reporting Status*' attribute in each ZSE cluster.

Therefore, and for clarity, where a GSME wishes to receive *MirrorReportAttributeResponse* commands from the GPF, the GSME should:

- notify the GPF of that wish by setting the *'Mirror Notification Reporting'* field to 0x01 in *ConfigureMirror* commands it sends;
- support the '*Attribute Reporting Status*' attribute on each of the mirrored clusters, so *Basic*, *Metering* and *Prepayment*; and
- send a *ReportAttributes* command from the GSME for an *Attribute Reporting Status* attribute with a value of '*Attribute Reporting Complete'*, each time it wishes to trigger the GPF to send a *MirrorReportAttributeResponse* command.

Amend Section 10.6.2.4 CHF Sub GHz Alerts and Corresponding events as follows:

10.6.2.4 CHF Sub GHz Alerts and corresponding events

Dual Band CH shall be capable of generating all Sub GHz Alerts and corresponding Log Entries, and shall generate the triggering events, and corresponding Alerts and Log Entries in line with the requirements of Table **Error! Reference source not found.** and Table 0.

For clarity, in relation to any Sub GHz Alert:

- the Business Target ID shall always be the Entity Identifier in the CHF's {`accessControlBroker, keyAgreement, management`} Trust Anchor Cell;
- the Business Originator ID shall be the CHF's Entity Identifier; and
- the Alert Payload shall always, as a DLMS COSEM based payload, be constructed as per Table **Error! Reference source not found.**c.

Event / Alert Code Meaning	Requirements
Limited Duty Cycle Action Taken	This event shall occur when the CH measurement of Duty Cycle rises above the Normal-Limited Duty Cycle Threshold. When this occurs, the CH shall: 1) identify the Device which has the largest value from the MacRxUcastDeltaSum Matrix and set 'Device ID' accordingly; 2) create an entry in the Event Log with Event Code set to 0x8F20 and otherInfo set to 'Device ID'; 3) send a 'DBCH06 Limited Duty Cycle Action Taken Sub GHz Alert' with: a) the Message Code set to 0x0110; b) the Alert Code set to 0x8F20; and

Event / Alert Code Meaning	Requirements
	c) the Use Case Specific Additional Content set to the concatenation 0x0908 || 'Device ID'; 4) if 'Device ID' is not that of a GSME, the CH shall send to that Device a *Suspend ZCL Messages* command with the *Suspension Period* parameter set to Suspension Period; and 5) if 'Device ID' is that of a GSME, in the *Suspend ZCL Messages* command response to the next *Get Suspend ZCL Messages Status* command received by the CH from that GSME, the CH shall set the *Suspension Period* parameter to Suspension Period. For clarity, SMHAN communications with the specified Device will not be possible for Suspension Period
Duty Cycle fallen below Normal-Limited Duty Cycle Threshold	This event shall occur when the CH measurement of Duty Cycle falls back below the Normal-Limited Duty Cycle Threshold
Critical Duty Cycle Action Taken	This event shall occur when the CH takes the action in ZSE 5.14.6 point 6 For clarity, SMHAN communications with any Sub GHz End Device except GSME will not be possible for Suspension Period starting at the date-time in the Alert / CHF Event Log Entry. Further, OTA firmware downloads to GSME will pause for this period. No Remote Party Commands will be sent to Sub GHz End Devices during this period (although Alerts and Responses may be received from GSME)
Duty Cycle fallen below Limited-Critical Duty Cycle Threshold	This event shall occur when the CH measurement of Duty Cycle falls back below the Limited-Critical Duty Cycle Threshold
Regulated Duty Cycle Action Taken	This event shall occur when the CH takes the action in ZSE 5.14.6 point 7
Duty Cycle fallen below Critical-Regulated Duty Cycle Threshold	This event shall occur when the CH measurement of Duty Cycle falls back below the Critical-Regulated Duty Cycle Threshold
Sub GHz Channel Changed	This event shall occur when a CH begins operating on a new Sub GHz Channel. For clarity, this includes the Sub GHz Channel selected by the CH on SMHAN network formation The resulting Alert and Log entry shall be created as per the requirements of Section **Error! Reference source not found.** and Section 0. Note these events are recorded in the dedicated Sub GHz Channel Log and not in the CHF Event Log
Sub GHz Channel Scan initiated	This event shall occur whenever the CH undertakes the processing of Section **Error! Reference source not found.**.
Sub GHz Channel Scan Request	This event shall occur when a Sub GHz Channel Scan trigger has been assessed by the CH, as per the requirements of Section **Error! Reference source not found.**. The resulting Alert and Event shall record both the nature of the triggering event and the

Event / Alert Code Meaning	Requirements
Assessment Outcome	outcome of the assessment checks, so including whether a resulting Sub GHz Channel Scan was triggered
Sub GHz Channel not changed due to Frequency Agility Parameters	This event occurs when a Sub GHz Channel scan has been undertaken but the CH determines not to change the Sub GHz Channel
Three Lost GSME Searches Failed	When 'Unrequited Lost GSME Searches' reaches three and 24 hours has elapsed since the most recent Sub GHz Channel Change, this event shall occur
Sub GHz Configuration Changed	This event shall occur when the CHF updates attribute 2 of object with OBIS Code 0-0:94.44.10.0
Message Discarded Due to Duty Cycle Management	The event shall occur as specified in Section **Error! Reference source not found.**
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 or HCALCS; • there are already four Devices in the CHF Device Log, which are not HCALCS 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'

Table **Error! Reference source not found.**: CHF Sub GHz Alerts and related Events

Amend Section 10.6.4 Sub GHz GSME – functional requirements as follows:

10.6.4 Sub GHz GSME - functional requirements

Sub GHz GSME shall wait at least 2 hours from detecting SMHAN interference before indicating that the interference is continuing by way of sending a *Mgmt_NWK_Unsolicited_Enhanced_Update_notify* command to the CH.

When operating on Sub GHz, GSME shall, on each wake up, check the *Functional Notification Flags* for bits 25 (*Energy Scan Pending*) and 26 (*Channel Change Pending*).

If either bit is set (so has a value 0b1) then the GSME shall attempt to retrieve any Commands buffered for it on the CH before turning off its SMHAN radio. For clarity and in line with Section 10.6.2.8, the GSME should attempt such retrieval before reading the CHF *Channel Change* attribute, if it is to maximise the likelihood of Command retrieval before it turns off its SMHAN radio.

If bit 25 is set, the GSME shall disable the SMETS User Interface Commands '4.5.2.4 Check for HAN Interface Commands' and '4.5.2.8 Find Smart Metering Home Area Network and Re-establish Communications Links' until it next turns on its SMHAN radio.

Note that CH may change Sub GHz Channel once every 24 hours to attempt to communicate with a lost GSME. On each such change, the CH will undertake a Sub GHz Channel Scan, meaning that it cannot communicate with a GSME for a period of time. GSME should factor both the 24 hour period and the associated Sub GHz Channel Scan in to their attempts to re-establish lost communications with the CH.

Amend Section 10.7.3 Network Key related requirements as follows:

10.7.3 Network Key related requirements

In this Section, all terms in italics shall have their ZSE or ZigBee Specification meaning and ZS shall mean the ZigBee Specification.

When a Device, which is not a CH, receives a new *Network Key*, the Device shall only store that *Network Key* where either:

1. the Device does not currently hold any *Network Key* (so meaning it is being installed); or
2. the Device receives the new *Network Key* encrypted with a hash of its *Trust Center Link Key* (so meaning that a *Trust Center Swapout* is in progress); or
3. the Device receives the new *Network Key* encrypted with its *Trust Center Link Key* (and potentially with an existing *Network Key*) and either:
   a) the value of *KeySeqNumber* for the new *Network Key* is greater than the value of the Device's *nwkActiveKeySeqNumber*; or
   b) the Device's *nwkActiveKeySeqNumber* is greater than 127 and the value of *KeySeqNumber* for the new *Network Key* is not greater than (*nwkActiveKeySeqNumber* + 128) modulo 256.

Where a Device, which is not a CH, stores a new *Network Key*, it shall switch to using that new *Network Key* for outgoing messages where either:

- it does not hold any other *Network Key*;
- it received the new *Network Key* encrypted only with a hash of its *Trust Center Link Key*; or
- it receives a message validly encrypted with the new *Network Key*.

Where a Device stores a new *Network Key* and that storage leads to the Device needing to remove details related to an old *Network Key*, the Device shall remove the *Network Key* that it received furthest back in time, and remove the *nwkSecurityMaterialSet* details associated with that key. Note that, in cases (2.) and (3.b) above, that key would likely not be the one with the lowest *KeySeqNumber*.

Where a Device, which is not a CH, receives a *switch-key* command requesting that it switches to using a new *Network Key*, the Device shall only take action in response to that command where either:

1. the value of the '*sequence number*' parameter in the *switch-key* command is greater than the value of the Device's *nwkActiveKeySeqNumber*; or
2. the Device's *nwkActiveKeySeqNumber* is greater than 127 and the value of the '*sequence number*' parameter in the *switch-key* command is not greater than (*nwkActiveKeySeqNumber* + 128) modulo 256.

Where a Device, which is not a CH, switches to using a new *Network Key*, the Device shall:

- in line with ZS 4.3.4 (and contrary to ZS 4.6.3.4.2), only set the associated *OutgoingFrameCounter* to zero if *OutgoingFrameCounter* is currently greater than 0x80000000; and
- ensure that, in the *IncomingFrameCounterSet* within the *nwkSecurityMaterialSet* for this new *Network Key*:
  - For a Device which is not an *End Device*, any *SenderAddress* is an identifier for a Device that is in the Device's *nwkNeighborTable*;
  - For a Device which is an *End Device*, the only *SenderAddress* is the identifier for Device's current *parent* Device; and
  - In line with ZS 4.6.3.4.2, all *IncomingFrameCounters* are set to zero.

A Device shall:

- only increment the value of the *IncomingFrameCounter* for the sending Device as a result of processing incoming messages from the sending Device which are secured with the *Network Key* the receiving Device is currently using for outgoing messages; and
- whenever it removes a Device from its *nwkNeighborTable*, also remove that Device's details from the *IncomingFrameCounterSet* within the *nwkSecurityMaterialSet* for the *Network Key* it is currently using to secure outgoing messages.

For the purposes of aging out entries from the *nwkNeighborTable*, a Device shall, where it is a *Router*:

- only use the ZS table 3-58 specified default values for *nwkRouterAgeLimit* and *nwkLinkStatusPeriod*, so 3 and 15 seconds respectively;
- set bit 0 of *nwkParentInformation* to 0b0, and so bit 1 to 0b1, meaning that *End Devices* need to send *End Device Timeout Request* commands as a unicast to refresh the *keepalive timer*;
- Only refresh the *keepalive timer* when the *Network Key* used to secure such *End Device Timeout Request* commands is that currently in use by the Device for its outgoing messages; and
- have the *nwkEndDeviceTimeoutDefault* set to the default 8 (so meaning 256 minutes) in line with ZS table 3-58 and not change the value of a Device's *keepalive* timeout where it receives an *End Device Timeout Request* command with a *Requested Timeout Enumeration Value* greater than 10 (so meaning greater than 1,024 minutes).

When a Device has chosen a network to join, it shall remove *Neighbor table entries* corresponding to Devices that are not members of the chosen network.

Where a Device is an *End Device*, the Device shall not send an *End Device Timeout Request* command with a *Requested Timeout Enumeration Value* greater than 10 (so meaning greater than 1,024 minutes).

CH shall not send any new *Network Key* encrypted only with an existing *Network Key*.

Where a CH creates a switch-key command, it shall treat the reference in ZS 4.4.6.1.3 to ZS 4.4.9.6 (which does not exist) as a reference to ZS 4.4.10.5.

A CH shall not attempt to remove Devices from the network using the APSME-REMOVE-DEVICE primitives, and so shall not send Remove Device commands to remove Devices from the network. A CH may send Remove Device commands only as required by ZSE 5.4.2.2. For clarity, this means that the values in the ParentAddress and TargetAddress parameters of such an APSME-REMOVE-DEVICE.request shall never be the same.

Amend Section 13.2.3.1 Summary - Informative as follows:

Common Requirements

Summary – informative

Remote Party Security Credentials are provided to Devices as Certificates which are X.509 based, DER encoded ASN.1 structures. Hence, the Command's structure is specified using ASN.1 with DER encoding to be applied to Command instances. Note that the details provided in the Response include the related ~~Protection Against Replay~~ Execution C~~c~~ounter details held on the Device.

Amend Section 13.2.3.3 The @ProvideSecurityCredentialDetails.Command and @ProvideSecurityCredentialDetails.Response structure definition as follows:

The @ProvideSecurityCredentialDetails.Command and @ProvideSecurityCredentialDetails.Response structure definition

Each instance of `@ProvideSecurityCredentialDetails.Command` and of `@ProvideSecurityCredentialDetails.Response` shall be an octet string containing the DER[2] encoding of the populated structure defined in this Section 0 which specifies the structure in ASN.1 notation[3].

```
ProvideSecurityCredentialDetails DEFINITIONS ::= BEGIN

Command ::=                                 SEQUENCE
{
-- Identify which of the Public Keys on the Device is to be used in verifying the Signature or MAC
-- (so defining the nature of the verification by way of the KeyUsage parameter held on the
-- Device for the Public Key so identified).

authorisingRemotePartyTACellIdentifier      TrustAnchorCellIdentifier,

-- List the Remote Party Role(s) for which credential details are required

remotePartyRolesCredentialsRequired         SEQUENCE OF RemotePartyRole
}

Response ::=                                SEQUENCE OF RemotePartyDetails

RemotePartyDetails ::=                      SEQUENCE
{

-- Which Remote Party do these details relate to?
remotePartyRole                             RemotePartyRole,

-- statusCode shall be success unless the role is not valid on this type of Device or there is a processing failure
```

[2] https://www.itu.int/rec/T-REC-X.690/en
[3] https://www.itu.int/rec/T-REC-X.680/en

```
statusCode                                  StatusCode,

-- What is the current Update Security Credentials ~~Protection Against Replay number~~Execution Counter~~-~~on the Device for this role,
where there is such a number for this role (see Table 13.2.4.4)?

currentSeqNumber                            SeqNumber OPTIONAL,

-- What are the details held on the Device for each of the Cells related to this role? The list shall have between one and
-- three entries (e.g. there will be one if role is transitional change of supplier; there may be three if role is supplier)

trustAnchorCellsDetails                     SEQUENCE OF TrustAnchorCellContents OPTIONAL
}

SeqNumber ::=                               INTEGER (0.. 18446744073709551615)

TrustAnchorCellContents ::=                 SEQUENCE
{
-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles
-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have
-- a single cryptographic use.

trustAnchorCellKeyUsage                     KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote
-- Party Role. This will be absent except where used to refer to the Supplier Key Agreement Key.
-- This Key is used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions.

trustAnchorCellUsage                        CellUsage DEFAULT management,

-- The existingSubjectUniqueID shall be the 64 bit Entity Identifier of the Security Credentials in this Trust Anchor Cell.

existingSubjectUniqueID                     OCTET STRING,

-- The APKI requirements mean that KeyIdentifier attributes will all be 8 byte SHA-1 Hashes.
-- existingSubjectKeyIdentifier shall be set accordingly based on the contents of the Trust Anchor Cell

existingSubjectKeyIdentifier                OCTET STRING
}
```

```
TrustAnchorCellIdentifier ::=                SEQUENCE
{
-- Which Remote Party Role does this Cell relate to?

trustAnchorCellRemotePartyRole               RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles
-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have
-- a single cryptographic use.

trustAnchorCellKeyUsage                      KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote
-- Party Role. This may be absent except where use to refer to the Supplier Key
-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions

trustAnchorCellUsage                         CellUsage DEFAULT management
}

CellUsage ::=                                INTEGER {management(0), prePaymentTopUp(1)}

RemotePartyRole ::=                          INTEGER
{
-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake
-- processing. Note that most Devices will only support processing in relation to a subset of these.

root                                         (0),
recovery                                     (1),
supplier                                     (2),
networkOperator                              (3),
accessControlBroker                          (4),
transitionalCoS                              (5),
wanProvider                                  (6),
issuingAuthority                             (7),    -- Devices will receive such Certificates but they do not
                                                     -- need to store them over an extended period
```

```
-- The 'other' RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from
-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid
-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is bought in to operation
other                                   (127)

}

-- KeyUsage is only repeated here for ease of reference. It is defined in RFC 5912

KeyUsage ::=                            BIT STRING
{
-- Define valid uses of Public Keys.

digitalSignature                        (0),
contentCommitment                       (1),    -- not valid for GBCS compliant transactions
keyEncipherment                         (2),    -- not valid for GBCS compliant transactions
dataEncipherment                        (3),
keyAgreement                            (4),
keyCertSign                             (5),
cRLSign                                 (6),
encipherOnly                            (7),
decipherOnly                            (8)     -- not valid for GBCS compliant transactions
}

-- The GBCS only allows for a constrained set of Trust Anchor Cell operations and so the list of possible outcomes
-- is more limited than in IETF RFC 5934. The list below is that more constrained subset

StatusCode ::=                          ENUMERATED {

success                                 (0),

-- trustAnchorNotFound indicates that details of a trust anchor were requested, but the referenced trust anchor
-- is not represented on the Device

trustAnchorNotFound                     (25),

other                                   (127)}
```

```
END
```

Amend Section 13.2.4.4 Response Construction as follows:

13.2.4.4 Response Construction

The Device shall populate Grouping Header according to the requirements of Section **Error! Reference source not found.**.

The `@ProvideSecurityCredentialDetails.Response` shall have the structure defined in Section 0, and the Device shall populate with values according to Table 0.

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
`@ProvideSecurityCredentialDetails.Response ::=`	`SEQUENCE OF`			
`SEQUENCE`				

`remotePartyRole`	`INTEGER`	`root (0) ,`
		`recovery (1) ,`
		`supplier (2) ,`
		`networkOperator (3) ,`
		`accessControlBroker (4) ,`
		`transitionalCoS (5) ,`
		`wanProvider (6) ,`
			Mandatory if `SEQUENCE` is present	The role to which the credentials in this `SEQUENCE` relate

`statusCode`	`ENUMERATED`	`success (0) ,`
		`trustAnchorNotFound (25) ,`
		`other (127)`
			Mandatory if `SEQUENCE` is present	Whether the Device can supply the details

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
currentSeqNumber	INTEGER	The corresponding Counter value	Present if statusCode=0	The ~~Protection Against Replay number~~ Execution Counter held by the Device for this role's use of the Update Security Credentials Command. Where this role is root, the value of the anyByContingency Execution Counter shall be returned: where this role is transitionalCoS, the value of the transCoSByTransCos Execution Counter shall be returned.
trustAnchorCellsDetails	SEQUENCE OF		At least one in the SEQUENCE OF must be present if statusCode=0	
SEQUENCE				
trustAnchorCellKeyUsage	BIT STRING	digitalSignature (0) , keyAgreement (4) , keyCertSign (5)	Mandatory if SEQUENCE is present	To what use can the public key in this Cell be put
trustAnchorCellUsage	INTEGER	prePaymentTopUp(1)	DEFAULT management (0)	Only needs to be present for the {supplier, keyAgreement, prePaymentTopUp} Cell

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
existingSubjectUniqueID	OCTET STRING	Entity Identifier in this Cell	Mandatory if SEQUENCE is present	See Section **Error! Reference source not found.**
existingSubjectKeyIdentifier	OCTET STRING	Key Identifier of the key in this Cell	Mandatory if SEQUENCE is present	

Table 0: Attribute values for Provide Security Credentials Response

Amend Section 13.3.4.1 Common Payload construction as follows:

13.3.4 Updating Security Credentials on a Device – Processing Steps

This Section lays out the requirements for the construction, protection and Authentication of the Update Security Credentials Command Payload, the processing required on the Device of the Command, the construction of the corresponding Response Payload and, where required, the Alert Payload.

13.3.4.1 Command Payload construction

The `@UpdateSecurityCredentials.CommandPayload` shall have the structure defined in Section 0, and the Remote Party constructing the Command shall populate with values according to Table 0.

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
`@ UpdateSecurityCredentials.Command ::=`	`SEQUENCE`			
`authorisingRemotePartyControl`	`SEQUENCE`			This structure provides details to allow the Device to identify the Remote Party Role authorising this Command, check whether the rest of the payload is allowable and allow counters / counter caches on the Device to be reset, if the command changes the Remote Party in control

`credentialsReplacementMode`	`INTEGER`	`supplierBySupplier (2) ,`
		`networkOperatorByNetworkOperator (3),`
		`accessControlBrokerByACB (4) ,`
		`wanProviderByWanProvider (5) ,`
		`transCoSByTransCoS (6) ,`
		`supplierByTransCoS (7) ,`
		`anyExceptAbnormalRootByRecovery (8) ,`
		`anyByContingency (9)`
			Mandatory	Specify the replacement mode so that the Device can check that the Remote Party Role authorising the command is allowed to authorise this type of replacement(s) and that all replacements in the payload are allowed within this replacement mode. The structure of the label is *kindOfCertificate(s)BeingReplacedBypartydoingthereplacement* . For example, `supplierBySupplier` is where a new supplier Certificate is being provided to the Device by its Supplier

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
plaintextSymmetricKey	[0] IMPLICIT OCTET STRING	The symmetric key that will decrypt the encrypted Contingency Key held on the Device	OPTIONAL	Only to be present if the Contingency Key arrangements are being used (so if credentialsReplacementMode = anyByContingency). The contents provide the symmetric key to decrypt the Contingency Public Key in the (root, digitalSignature, management) Trust Anchor Cell
applyTimeBasedCPVChecks	[1] IMPLICIT INTEGER	disapply(1)	DEFAULT apply	Only to be present if the Remote Party sending the Command is instructing the Device not to apply time based checks as part of Certification Path Validation. This should only be in exceptional circumstances (e.g. supplier credentials on the Device have expired without replacement for unforeseen reasons)
authorisingRemotePartyTACellIdentifier	[2] IMPLICIT SEQUENCE		OPTIONAL	This structure identifies which Public Key on the Device is to be used in verifying KRP Signature. The key is identified by way of Trust Anchor Cell and so the nature of the check, by way of the KeyUsage parameter, is also identified. 'authorisingRemotePartyTACellIdentifier' can only be

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
				omitted when the Access Control Broker is changing its own Key Agreement credentials
trustAnchorCellRemotePartyRole	INTEGER	root (0), recovery (1) , supplier (2) , networkOperator (3) , accessControlBroker (4) , transitionalCoS (5) , wanProvider (6)	Mandatory if authorisingRemotePartyTACellIdentifier present	The role of the Party applying KRP Signature. Note that where root is used, this refers only to the encrypted Contingency key in the root TA Cell, so is only valid if credentialsReplacementMode = anyByContingency and plaintextSymmetricKey is populated with the symmetric key required to decrypt that public key
trustAnchorCellKeyUsage	BIT STRING	digitalSignature (0) if credentialsReplacementMode <> anyByContingency, keyCertSign (5) if credentialsReplacementMode = anyByContingency	Mandatory if authorisingRemotePartyTACellIdentifier present	KRP Signature is a digital signature
trustAnchorCellUsage	INTEGER	management(0)	DEFAULT management	Must be absent since the prePaymentTopUp key pair

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
				cannot be used in relation to this Command
authorisingRemotePartySeqNumber	[3] IMPLICIT INTEGER	Originator Counter of Remote Party authorising the Command	Mandatory	Specify the Originator Counter for the Remote Party applying KRP Signature, or (for the Access Control Broker changing its credentials) the Access Control Broker's Originator Counter
newRemotePartyFloorSeqNumber	[4] IMPLICIT INTEGER	Originator Counter of Remote Party who will have control of this Remote Party Role if the update is successful	OPTIONAL	If the Command is to effect a change of control, then newRemotePartyFloorSeqNumber should be included and will be the value used to prevent replay of Update Security Credentials Commands, and other Commands, for the new controlling Remote Party
newRemotePartySpecialistFloorSeqNumber	[5] IMPLICIT SEQUENCE OF		OPTIONAL	Some Commands on the Device may use a different Originator Counter sequence for Protection Against Replay. The only example is the Prepayment Top Up Command on ESME and GSME. The SpecialistSeqNumber structure allows such Counters to also be reset on change of control. Should only be present if this Command changes supplier credentials and the

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
				new `supplier` uses different counters for its Prepayment Top Ups than it does for other Commands
`SEQUENCE`				
`seqNumberUsage`	`INTEGER`	`prepaymentTopUp (0)`	Mandatory if `newRemotePartySpecialistFloorSeqNumber` present	Specify the usage of the `SeqNumber`
`seqNumber`	`INTEGER`	Relevant Originator Counter	OPTIONAL	Specify the associated `SeqNumber`
`otherRemotePartySeqNumberChanges`	`[6] IMPLICIT SEQUENCE OF`		OPTIONAL	In some cases, one party acting in one Remote Party Role may be replacing certificates for a different Remote Party Role (e.g. `transitionalCoS` changing Supplier Credentials). In such cases, ~~sequence c~~Execution Counters need also to be reset for that other Remote Party Role
`SEQUENCE`				
`otherRemotePartyRole`	`INTEGER`	`supplier (2) , networkOperator (3) ,`	Mandatory if `otherRemotePartySeqNumbe`	The Remote Party Role of the party whose credentials are being placed on the Device but which didn't authorise the command

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
		accessControlBroker (4) , transitionalCoS (5) , wanProvider (6) ,	rChanges present	directly. Note that this is not valid for root or recovery
otherRemotePartyFloorSeqNumber	INTEGER	Relevant Originator Counter	Mandatory if otherRemotePartySeqNumberChanges present	Specify the associated SeqNumber
newRemotePartySpecialistFloorSeqNumber	SEQUENCE OF		OPTIONAL	Should only be present if otherRemotePartyRole = supplier, and that new supplier uses different counters to prevent replay on Prepayment Top Up
SEQUENCE				
seqNumberUsage	INTEGER	prepaymentTopUp (0)	Mandatory if newRemotePartySpecialistFloorSeqNumber present	Specify the usage of the SeqNumber
seqNumber	INTEGER	Relevant Originator Counter	OPTIONAL	Specify the associated SeqNumber
replacements	SEQUENCE OF			Provide a list of the replacements. Each

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
				replacement contains a new 'end entity' Certificate and the identity of the Trust Anchor Cell which is to have its contents replaced using that Certificate.
SEQUENCE			At least one SEQUENCE must be present	One structure is required for each Trust Anchor Cell that is to be updated
replacementCertificate	Certificate	End entity Certificate	Mandatory if SEQUENCE is present	Provide the new end entity certificate
targetTrustAnchorCell	SEQUENCE			Specify where it is to go (specifically which Trust Anchor Cell is to have its details replaced using the new end entity certificate)
trustAnchorCellRemotePartyRole	INTEGER	root (0) , recovery (1) , supplier (2) , networkOperator (3) , accessControlBroker (4) , transitionalCoS (5) , wanProvider (6)	Mandatory if SEQUENCE is present	To which Remote Party Role does the Trust Anchor Cell relate

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
trustAnchorCellKeyUsage	BIT STRING	{digitalSignature (0) , keyAgreement (4) , keyCertSign (5)} ,	Mandatory if SEQUENCE is present	To what use can the public key in this Cell be put
trustAnchorCellUsage	INTEGER	prePaymentTopUp(1)}	DEFAULT management	Should be absent unless: • the deviceType is eSME or gSME; and • the supplier operating the Device wishes to use prepayment top up functionality on the Device, and this is a replacement of the corresponding certificate. Note the certificate specified for use in the {supplier, keyAgreement, prePaymentTopUp} Trust Anchor Cell may be the same key as that specified for the {supplier, keyAgreement, management} Trust Anchor Cell or may be different.

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
certificationPathCertificates	SEQUENCE OF Certificate	The list of certificates needed for Certification Path Validation	At least one Certificate must be present	Provide the certificates needed to undertake Certification Path Validation against the root public key held on the Device. The number of these may be less than the number of replacement certificates (e.g. a supplier may replace all of its certificates but may only need to supply one Certification Authority Certificate to link them all back to root
executionDateTime	GeneralizedTime	The date-time at which the replacements are to be used in updating the Device's Security Credentials	OPTIONAL	This field may only be present if credentialsReplacementMode is either supplierBySupplier or supplierByTransCoS

Table 0: Attribute values for Update Security Credentials Command

Amend Section 13.3.4.3 Command Processing as follows:

13.3.4.3 Command Processing

Before undertaking any further processing, the Device shall update ~~Highest Prior Sequence Number~~ Execution Counter to the value of authorisingRemotePartySeqNumber.

If executionDateTime is present then the Device shall:

record against the remotePartyRole (as specified in authorisingRemotePartyControl), authorisingRemotePartyControl, replacements; and executionDateTime;

construct a Response where executionOutcome is not present according to the requirements of Section **Error! Reference source not found.**; and

at the date-time specified in executionDateTime, undertake the processing of Section **Error! Reference source not found.** then construct an Alert according to the requirements of Section **Error! Reference source not found.**.

If executionDateTime is not present then the Device shall:

undertake the processing of Section **Error! Reference source not found.**; and

construct a Response where executionOutcome is present according to the requirements of Section **Error! Reference source not found.**.

Amend Section 13.3.4.6 executionOutcome construction as follows:

13.3.4.6 executionOutcome construction

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
executionOutcome	SEQUENCE			
authorisingRemotePartySeqNumber	INTEGER	Originator Counter of Remote Party authorising the Command, as specified in the corresponding Command	Mandatory	This is to allow the Alert to be linked to the Command that caused execution
credentialsReplacementMode	INTEGER	supplierBySupplier (2) ,	Mandatory	Provide details of the corresponding Command that are not in the standard GBCS message

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
		networkOperatorByNetworkOperator (3) , accessControlBrokerByACB (4) , wanProviderByWanProvider (5) , transCoSByTransCoS (6) , supplierByTransCoS (7) , anyExceptAbnormalRootByRecovery (8) , anyByContingency (9)} ,		header. Specifically the mode in which the Command was invoked
remotePartySeqNumberChanges	SEQUENCE OF		Mandatory containing zero, one or many occurrences of the following structure	The resulting changes to ~~any replay c~~Execution Counters held on the Device
SEQUENCE				
otherRemotePartyRole	INTEGER	root (0) , recovery (1) ,	Mandatory if SEQUENCE is present	The role which has had its Execution C~~e~~ounter values changed on the Device

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
		supplier (2) , networkOperator (3) , accessControlBroker (4) , transitionalCoS (5) , wanProvider (6) ,		
otherRemotePartyFloorSeqNumber	INTEGER	The corresponding Execution Counter value	Mandatory if SEQUENCE is present	
newRemotePartySpecialistFloorSeqNumber	SEQUENCE OF		OPTIONAL	Only present where Remote Party Role is supplier
SEQUENCE				
seqNumberUsage	INTEGER	{prepaymentTopUp (0)} ,	Mandatory if newRemotePartySpecialistFloorSeqNumber present	Specify the usage of the SeqNumber
seqNumber	INTEGER		Mandatory if newRemotePartySpecialistFloorSeqNumber present	Specify the associated SeqNumber

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
replacementOutcomes	SEQUENCE OF		One per replacement in the corresponding Command so at least one	For each replacement in the Command, detail the outcome and impacted parties
SEQUENCE				
affectedTrustAnchorCell	SEQUENCE		Mandatory if SEQUENCE is present	Specify which Trust Anchor Cell was the target of this replacement
trustAnchorCellRemotePartyRole	INTEGER	root (0) , recovery (1) , supplier (2) , networkOperator (3) , accessControlBroker (4) , transitionalCoS (5) , wanProvider (6)	Mandatory if SEQUENCE is present	Specify the Remote Party Role to which the Trust Anchor Cell relates
trustAnchorCellKeyUsage	BIT STRING	digitalSignature (0) , keyAgreement (4) , keyCertSign (5)	Mandatory if SEQUENCE is present	To what use can the public key in this Cell be put
trustAnchorCellUsage	INTEGER	{management(0) ,	DEFAULT management	Absent unless:

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
		prePaymentTopUp(1) }		• the deviceType is eSME or gSME; and • the supplier operating the Device wishes to use prepayment top up functionality on the Device, and this is a replacement of the corresponding certificate. Note the certificate specified for use in the {supplier, keyAgreement, prePaymentTopUp} Trust Anchor Cell may be the same key as that specified for the {supplier, keyAgreement, management} Trust Anchor Cell or may be different.
statusCode	ENUMERATED	success (0) , badCertificate (5) , noTrustAnchor (10) , insufficientMemory (17) , resourcesBusy (30) , other (127)	Mandatory if SEQUENCE is present	Whether the replacement to this Cell was successful or, if it failed, why it failed
existingSubjectUniqueID	OCTET STRING		Mandatory if SEQUENCE is present	The 64 bit Entity Identifier of the Remote Party whose credentials were in this Cell prior to receipt of the corresponding Command

Attribute name	Data Type	Value (blank cells mean the command specific value is derived by the encoding process)	Mandatory, OPTIONAL or DEFAULT value	Notes
existingSubjectKeyIdentifier	OCTET STRING		Mandatory if SEQUENCE is present	For the public key in this Cell prior to receipt of the corresponding Command
replacingSubjectUniqueID	OCTET STRING		Mandatory if SEQUENCE is present	The 64 bit Entity Identifier of the Remote Party whose credentials were to be placed in this Cell
replacingSubjectKeyIdentifier	OCTET STRING		Mandatory if SEQUENCE is present	For the public key which was to be placed in this Cell

Table 0: Attribute values for executionOutcome

Amend Section 13.3.5.1 Update Security Credentials Command Verification as follows:

13.3.5 Common Requirements

13.3.5.1 Update Security Credentials Command Verification

The Device shall undertake the checks set out in this Section 0 before undertaking any other processing of the Command. The checks ~~should~~ may be carried out in ~~the~~ any order ~~specified~~. Checking shall cease at the point that any one check fails. The checks required are shown in Table 0.

Check Number	Criteria that must be tested by the Device	How the Device shall test the Criteria
1.1	The Message is for the Device	The value of the Business Target ID in the Grouping Header in Command instance must be equal to the Device's Entity Identifier
1.2	The Message Code is for Update Security Credentials	The value in the Message Code field of the Grouping Header must be equal to the value specified in Table **Error! Reference source not found.** for the `CredentialsReplacementMode` specified in `CommandPayload`
1.3	If `executionDateTime` is present the Command is to replace Supplier Security Credentials.	If `executionDateTime` is present then `credentialsReplacementMode` must either `supplierBySupplier` or `supplierByTransCoS`
1.4	The Device has not already actioned this Command.	As specified in Section 0
2.1	The `targetTrustAnchorCells` all exist on a Device of this type	As specified in Section **Error! Reference source not found.**
2.1	The `trustAnchorCellUsage` in the `authorisingRemotePartyTACellIdentifier` must be `ABSENT`	As specified in Section 13.3.4.1
2.2	The `credentialsReplacementMode` is one that can be Authorised by the Remote Party / Parties authorising the Command	As specified in Section **Error! Reference source not found.**
2.2	The `replacements` specified are all allowed in this `credentialsReplacementMode`.	As specified in Section **Error! Reference source not found.**
2.2	The `trustAnchorCellUsage` in the `targetTrustAnchorCell` in each entry in `replacements` must be `ABSENT` unless it has the value `prePaymentTopUp`, as specified in the Notes column of Table 13.3.4.1	As specified in Section 13.3.4.1

Check Number	Criteria that must be tested by the Device	How the Device shall test the Criteria
2.3	The keyUsage in each of the replacement certificates provided is consistent with the target Trust Anchor Cells identified in replacements	As specified in Section **Error! Reference source not found.**
3.1	The Cryptographic Protections are valid	As specified in Section 0

Table 0: Update Security Credentials Command authenticity and integrity verification

Amend Section 13.3.5.3 Preventing Replay of Commands as follows:

13.3.5.3 Preventing Replay of Commands

The Protection Against Replay mechanisms for the Update Security Credentials Command shall be that specified in this Section 0 (which is different than that for other GBCS Commands).

For each of RemotePartyRole from which the Device can receive a valid Updated Security Credentials Command, the Device shall allocate storage for an ~~Highest Prior Sequence Number~~ Execution Counter which shall be capable of storing a 64 bit unsigned integer and which shall initially be set to the value zero at manufacture. For transitionalCoS, the Device may allocate storage for an additional Execution Counter, credentialsReplacementModes.

Before executing any Update Security Credentials Command, a Device shall confirm that, if CredentialsReplacementMode <> accessControlBrokerByACB, then

(authorisingRemotePartyTACellIdentifier is populated in the Command) and (the authorisingRemotePartySeqNumber is strictly numerically greater than the ~~Highest Prior Sequence Number~~ Execution Counter the Device has recorded for the RemotePartyRole identified in authorisingRemotePartyTACellIdentifier and, where relevant for transitionalCoS, the credentialsReplacementMode);

else

(the authorisingRemotePartySeqNumber is strictly numerically greater than the ~~Highest Prior Sequence Number~~ Execution Counter the Device has recorded for the accessControlBroker).

Amend Section 13.3.5.8 Verifying the CryptographicProtections as follows:

Verifying the CryptographicProtections

In verifying Cryptographic Protections pursuant to this Section **Error! Reference source not found.**:

- KRP Signature shall, where required by Section 13.3.3.1 for the specified Message Code and `credentialsReplacementMode`[JC1], be verified according to the requirements in this Section 13.3.5.8~~4.3.2.7.2~~; and
- ACB-SMD MAC, where required by Section 13.3.3.1 for the specified Message Code and `credentialsReplacementMode`, shall be verified according to the requirements in Section **Error! Reference source not found.**.

If `credentialsReplacementMode` = `anyByContingency` or Message Code =<> 0x0109 then KRP Signature shall be verified using the public key established according to the requirements of Section **Error! Reference source not found.**.

If `credentialsReplacementMode` = <> `anyByContingency` or Message Code =<> 0x0109 then KRP Signature shall be verified using the public key identified as per Section **Error! Reference source not found.**.

If `credentialsReplacementMode` = `accessControlBrokerByACB` or Message Code = 0x0104 `and deviceType is not communicationsHubCommunicationsHubFunction` then ACB-SMD MAC shall be verified as per Section **Error! Reference source not found.**.

Amend Section 13.3.5.11 The@UpdateSecurityCredentials.CommandPayload,@UpdateSecurityCredentials.ResponsePayload and @UpdateSecurityCredentials.AlertPayload structure definition as follows:

13.3.5.11 The `@UpdateSecurityCredentials.CommandPayload`,`@UpdateSecurityCredentials.ResponsePayload` and `@UpdateSecurityCredentials.AlertPayload` structure definition

Each instance of `@UpdateSecurityCredentials.CommandPayload`, `@UpdateSecurityCredentials.ResponsePayload` and of `@UpdateSecurityCredentials.AlertPayload` shall be an octet string containing the DER encoding of the populated structure defined in this Section 0, which specifies the structure in ASN.1.

The structure of `Certificate` shall be as defined in ASN.1 in IETF RFC 5912. Note that the `Certificate` structures within IETF RFC 5912 begin after the phrase 'Certificate- and CRL-specific structures begin here'.

```
UpdateSecurityCredentials DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE
{
-- Provide details to allow the Device to identify the Remote Party Role authorising
-- this Command, check whether the rest of the payload is allowable, prevent replay attacks
-- and allow counters / counter caches on the Device to be reset, if the Command changes the Remote Party
-- in control.
-- The Remote Party authorising the Command is that party which generated the KRP Signature (or the Access Control Broker
-- if there is no KRP Signature)

authorisingRemotePartyControl                AuthorisingRemotePartyControl,

-- One TrustAnchorReplacement structure is required for each Trust Anchor Cell that is to be updated

replacements                                 SEQUENCE OF TrustAnchorReplacement,

-- Provide the certificates needed to undertake Certification Path Validation of the new
-- end entity certificate against the root public key held on the Device. The number of these may be less
-- than the number of replacement certificates (e.g. a supplier may replace all of its certificates but
-- may only need to supply one Certification Authority Certificate to link them all back to the root public
-- key as currently stored on the Device.

certificationPathCertificates                SEQUENCE OF Certificate,

-- If the Command is to be future dated, specify the date-time at which the certificate replacement is to happen

executionDateTime                            GeneralizedTime OPTIONAL

}

ResponsePayload ::=                          SEQUENCE
{
   -- if the Command is future dated, the Response will not have any details of execution (those will be in the subsequent alert)

   commandAccepted                           NULL,
```

```
   -- if the Command is for immediate execution, the Response will detail the outcomes

   executionOutcome                          ExecutionOutcome OPTIONAL

}

AlertPayload ::=                             SEQUENCE
{
   -- specify the Alert Code
   alertCode                                 INTEGER(0..4294967295),

   -- specify the date-time of execution
   executionDateTime                         GeneralizedTime,


   -- detail what happened when the future dated Command was executed

   executionOutcome                          ExecutionOutcome

}

ExecutionOutcome ::=                         SEQUENCE
{
-- Provide details of the corresponding Command that may not be in the standard GBCS message header. Specifically the
-- mode in which the Command was invoked, the Originator Counter in the original Command and the resulting changes to any
-- replay counters held on the Device

authorisingRemotePartySeqNumber              SeqNumber,
credentialsReplacementMode                   CredentialsReplacementMode,
remotePartySeqNumberChanges                  SEQUENCE OF RemotePartySeqNumberChange,

-- For each replacement in the Command, detail the outcome and impacted parties

replacementOutcomes                          SEQUENCE OF ReplacementOutcome

}

AuthorisingRemotePartyControl ::=            SEQUENCE
```

```
{
-- Specify the replacement mode so that the Device can check that the Remote Party Role is allowed to
-- authorise this type of replacement and that all replacements in the payload are allowed within this
-- replacement mode

credentialsReplacementMode                    CredentialsReplacementMode,

-- Only if credentialsReplacementMode = anyByContingency, provide the symmetric key to decrypt
-- the Contingency Public Key in the (root, digitalSignature, management) Trust Anchor Cell

plaintextSymmetricKey                         [0] IMPLICIT OCTET STRING OPTIONAL,

-- Specify whether the time based checks as part of any Certificate Path Validation should be applied

applyTimeBasedCPVChecks                       [1] IMPLICIT INTEGER {apply(0), disapply(1)} DEFAULT apply,

-- Identify which of the Public Keys on the Device is to be used in checking KRP Signature
-- 'authorisingRemotePartyTACellIdentifier' may only be omitted when
-- the access control broker is updating its own credentials and the target device is not a CHF.
-- In all other cases it is mandatory.

authorisingRemotePartyTACellIdentifier        [2] IMPLICIT TrustAnchorCellIdentifier OPTIONAL,

-- Specify the Originator Counter for the Remote Party Applying KRP Signature, or (for the
-- Access Control Broker changing its credentials) the Access Control Broker's Originator Counter.

authorisingRemotePartySeqNumber               [3] IMPLICIT SeqNumber,

-- If the Command is to effect a change of control, then newRemotePartyFloorSeqNumber must be included
-- and will be the value used to prevent replay of Update Security Credentials Commands for the
-- new controlling Remote Party.

newRemotePartyFloorSeqNumber                  [4] IMPLICIT SeqNumber OPTIONAL,

-- Some Commands on the Device may use a different Originator Counter sequence for Protection Against Replay. At this
-- version of the GBCS, the only example is the Prepayment Top Up Command on ESME and GSME. The
-- SpecialistSeqNumber structure allows such Counters to also be reset on change of control.

newRemotePartySpecialistFloorSeqNumber        [5] IMPLICIT SEQUENCE OF SpecialistSeqNumber OPTIONAL,
```

```
-- In some cases, one party acting in one Remote Party Role may be replacing certificates for a different Remote Party Role.
-- In some cases, ~~sequence c~~Execution Counters need also to be reset for those other Remote Party Role(s)

otherRemotePartySeqNumberChanges              [6] IMPLICIT SEQUENCE OF RemotePartySeqNumberChange OPTIONAL
}

RemotePartySeqNumberChange ::=                 SEQUENCE
{
otherRemotePartyRole                          RemotePartyRole,
otherRemotePartyFloorSeqNumber                SeqNumber,
newRemotePartySpecialistFloorSeqNumber        SEQUENCE OF SpecialistSeqNumber OPTIONAL
}

SpecialistSeqNumber ::=                       SEQUENCE
{
-- Specify the usage of the SeqNumber
seqNumberUsage                                SeqNumberUsage,

-- Specify the associated SeqNumber
seqNumber                                     SeqNumber
}

SeqNumberUsage ::=                            INTEGER
{
-- Define the full set of discrete usages on a Device. The only specialist
-- counter is for Prepayment Top Up (which is set independently of other counters). This may only be
-- included when changing Supplier Security Credentials on an ESME or GSME.

prepaymentTopUp                               (0)
}

SeqNumber ::=                                 INTEGER (0.. 18446744073709551615)


TrustAnchorReplacement ::=                    SEQUENCE
{
-- Provide the new end entity certificate
```

```
replacementCertificate                          Certificate,

-- Specify where it is to go (specifically which Trust Anchor Cell is to have its details replaced using
-- the new end entity certificate)

targetTrustAnchorCell                           TrustAnchorCellIdentifier
}


ReplacementOutcome ::=                          SEQUENCE
{
affectedTrustAnchorCell                         TrustAnchorCellIdentifier,
statusCode                                      StatusCode,

-- The GBCS Certificate requirements mean that the Subject Unique ID attribute in the subject field of a certificate will always
-- contain the 64 bit unique number that equates to Entity Identifier. existingSubjectUniqueID should be set
-- accordingly based on the contents of the Trust Anchor Cell prior to Command processing.

existingSubjectUniqueID                         OCTET STRING,

-- The GBCS Certificate requirements mean that subjectKeyIdentifier attributes will all be 8 byte SHA-1 Hashes.
-- existingSubjectKeyIdentifier should be set accordingly based on the contents of the Trust Anchor Cell prior to
-- Command processing.

existingSubjectKeyIdentifier                    OCTET STRING,

-- The Subject Unique ID in the subject field of the certificate in this TrustAnchorReplacement

replacingSubjectUniqueID                        OCTET STRING,

-- The subjectKeyIdentifier in the certificate in this TrustAnchorReplacement

replacingSubjectKeyIdentifier                   OCTET STRING
}

TrustAnchorCellIdentifier ::=                   SEQUENCE
{
-- Which Remote Party Role does this Cell relate to?
```

```
trustAnchorCellRemotePartyRole                RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles
-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have
-- a single cryptographic use.

trustAnchorCellKeyUsage                       KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote
-- Party Role. It will be absent except where used to refer to the Supplier Key
-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up
-- transactions

trustAnchorCellUsage                          CellUsage DEFAULT management
}

CellUsage ::=                                 INTEGER {management(0), prePaymentTopUp(1)}

RemotePartyRole ::=                           INTEGER
{
-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake
-- processing. Note that most Devices will only support a subset of these.

root                                          (0),
recovery                                      (1),
supplier                                      (2),
networkOperator                               (3),
accessControlBroker                           (4),
transitionalCoS                               (5),
wanProvider                                   (6),
issuingAuthority                              (7),    -- Devices will receive such Certificates but they do not need to store
                                                      -- them over an extended period

-- The 'other' RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from
-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid
-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is brought in to operation

other                                         (127)
```

```
}

-- KeyUsage is only repeated here for clarity. It is defined in RFC 5912

KeyUsage ::=                                BIT STRING
{
-- Define valid uses of Public Keys held by Devices in their Trust Anchor Cells.

digitalSignature                            (0),
contentCommitment                           (1),    -- not valid for GBCS compliant transactions
keyEncipherment                             (2),    -- not valid for GBCS compliant transactions
dataEncipherment                            (3),    -- not valid for GBCS compliant transactions
keyAgreement                                (4),
keyCertSign                                 (5),
cRLSign                                     (6),
encipherOnly                                (7),    -- not valid for GBCS compliant transactions
decipherOnly                                (8)     -- not valid for GBCS compliant transactions
}

CredentialsReplacementMode ::=              INTEGER
{
-- Define the valid combinations as to which Remote Party Roles can replace which kinds of Trust Anchors.

-- Normal operational replacement modes
supplierBySupplier                          (2),
networkOperatorByNetworkOperator            (3),
accessControlBrokerByACB                    (4),
wanProviderByWanProvider                    (5),
transCoSByTransCoS                          (6),
supplierByTransCoS                          (7),

-- Recovery modes
anyExceptAbnormalRootByRecovery             (8),
anyByContingency                            (9)
}

-- The GBCS only allows for a constrained set of Trust Anchor Cell operations and so the list of possible outcomes
-- is more limited than in RFC 5934. The list below is that more constrained subset
```

```
StatusCode ::=                                  ENUMERATED {

success                                         (0),

-- badCertificate is used to indicate that the syntax for one or more certificates is invalid.

badCertificate                                  (5),

-- noTrustAnchor is used to indicate that the authorityKeyIdentifier does not identify the public key of a
-- trust anchor or a certification path that terminates with an installed trust anchor

noTrustAnchor                                   (10),

-- insufficientMemory indicates that the update could not be processed because the Device did not
-- have sufficient memory

insufficientMemory                              (17),

-- resourcesBusy indicates that the resources necessary to process the replacement are not available at the
-- present time, but the resources might be available at some point in the future.

resourcesBusy                                   (30),

-- other indicates that the update could not be processed, but the reason is not covered by any of the assigned
-- status codes.  Use of this status code SHOULD be avoided.

other                                           (127) }

END
```

Amend Section 13.3.5.12 Requirements for AuthorisingRemotePartyControl elements – informative as follows:

13.3.5.12 Requirements for `AuthorisingRemotePartyControl` elements – informative

All bar two parts of the `AuthorisingRemotePartyControl` structure are optional. This Section summarises when each of the optional elements needs to be present.

AuthorisingRemotePartyControl element	Notes
credentialsReplacementMode	Always required
plaintextSymmetricKey	Only required if credentialsReplacementMode = anyByContingency (when it is always required)
applyTimeBasedCPVChecks	Only required if the Device is to ignore time when undertaking Certification Path Validation, in which case it needs to have the value 'disapply'
authorisingRemotePartyTACellIdentifier	For a Communications Hub, always present. For all other Devices, always present unless the Access Control Broker is replacing its own Key Agreement credentials (in which case it should be omitted)
authorisingRemotePartySeqNumber	Always required
newRemotePartyFloorSeqNumber	If the Command is to effect a change of control, then newRemotePartyFloorSeqNumber should be included. It can be present in all other situations
newRemotePartySpecialistFloorSeqNumber	Only required on Change of Supplier where the new Supplier has decided to use a different sequence of Originator Counters for prepayment top ups.
otherRemotePartySeqNumberChanges	Should be present if one role (e.g. recovery, transitionalCoS) is changing credentials for another role or roles (e.g. supplier). In such cases, this should be present to set ~~Protection Against Replay c~~Execution Counters for that other role or roles

Table 0: Requirements for AuthorisingRemotePartyControl element

Amend Section 13.5.4 Device processing of Commands and Response handing as follows:

13.5.4 Device processing of Commands and Response handling

The Device receiving an Update Device Certificate on Device Command shall undertake processing steps in the sequence defined in this Section 0.

In processing an Update Device Certificate on Device Command, the Device shall:

4. undertake Command Authenticity and Integrity Verification as required for a Command of Message Category SME.C.C, except that check 4 in Section 6.2.4.1.1 may be undertaken after the checks in Section 6.2.4.1.2. The Security Credentials used to verify Cryptographic Protection I shall be:
    - those held in the {`wANProvider, digitalSignature, management`} Trust Anchor Cell, if the target Device's `deviceType` equals `communicationsHubCommunicationsHubFunction`; or
    - those held in the {`supplier, digitalSignature, management`} Trust Anchor Cell, if the target Device's `deviceType` does not equal `communicationsHubCommunicationsHubFunction`.
5. establish the values of `keyUsage`, `subjectPublicKey` and `hwSerialNum` in certificate in the `CommandPayload`. If any of the values cannot be established then the Device shall set `updateDeviceCertResponseCode` to `invalidCertificate`, and process from step 13;
6. validate that `hwSerialNum` established at step 5 is the Device's Entity Identifier. If this validation fails then the Device shall set `updateDeviceCertResponseCode` to `wrongDeviceIdentity`, and process from step 13;
7. validate that `keyUsage` established at step 5 is either `digitalSignature` only or `keyAgreement` only. If this validation fails then the Device shall set `updateDeviceCertResponseCode` to `invalidKeyUsage`, and process from step 13;
8. validate that the Device holds a Pending Private Key for the `keyUsage` as established at step 5. If this validation fails then the Device shall set `updateDeviceCertResponseCode` to `noCorrespondingKeyPairGenerated`, and process from step 13;
9. validate that `subjectPublicKey` established at step 5 is the bit string representation of the Public Key corresponding to the Pending Private Key identified at step 8. If this validation fails then the Device shall set `updateDeviceCertResponseCode` to `wrongPublicKey`, and process from step 13;
10. store certificate. If this step fails then the Device shall set `updateDeviceCertResponseCode` to `certificateStorageFailed`, and process from step 13;

11. set the Current Private Key to have the value of the Pending Private Key for the `keyUsage` established at step 5. If this step fails then the Device shall set `updateDeviceCertResponseCode` to `privateKeyChangeFailed`, and process from step 13;
12. set `updateDeviceCertResponseCode` to success; and
13. create a Response according to the requirements of Section **Error! Reference source not found.**, apply the Response Cryptographic Protection required for a Response of Message Category SME.C.C, and send the Response.

If all steps were successful and this was a change of `digitalSignature certificate`, the Response shall be signed using the private key corresponding to the new `certificate`. If there was a failure, the Response shall be signed using the private key corresponding to the pre-existing key pair.

Once the Pending Private Key becomes the Current Private Key, the Device will be using the new Private Key and this will affect all Remote Parties interacting with the Device; specifically they will need to use the new Certificate corresponding to the Private Key now in use.

Amend Section 13.7.4.2.2 Device processing of Commands and Response handling as follows:

13.7.4.2 Join Device Command and Response Processing

13.7.4.2.1 Construction of Commands

'Join Device' Command Payloads shall be constructed as specified in Section **Error! Reference source not found.** and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of the relevant Message Category.

For a Command (1) which complies with either Use Case 'CS03A2 Method A Join (non Meter)' or Use Case 'CS03C Method C Join' and (2) where the Device to which it is addressed has a `deviceType` equal to `type1PrepaymentInterfaceDevice`, the Access Control Broker's Digital Signing Private Key shall be used in generating the KRP Signature.

13.7.4.2.2 Device processing of Commands and Response handling

The Device receiving a 'Join Device' Command shall undertake processing steps in the sequence defined in this Section 0. Should a step after step 1 be unsuccessful, the Device shall create a Response according to the requirements of Section **Error! Reference source not found.**, apply the Response Cryptographic Protection required for a Response of the relevant Message Category, and send the Response and shall not undertake any further steps defined in this Section 0.

In processing a 'Join Device' Command, the Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of this Message Category, except that check 4 in Section 6.2.4.1.1 may be undertaken after the checks in Section 6.2.4.1.2. The Security Credentials used to verify Cryptographic Protection 1 shall be:

- those held in the {accessControlBroker, digitalSignature, management} Trust Anchor Cell, if deviceType equals type1PrepaymentInterfaceDevice; or
- those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if deviceType does not equal type1PrepaymentInterfaceDevice;

2. verify the joinMethodAndRole as specified in Section **Error! Reference source not found.**;
3. add the otherDeviceEntityIdentifier and otherDeviceType to its Device Log as specified in Section **Error! Reference source not found.**;
4. if deviceType is eSME then undertake Key Establishment with the other Device as specified in Section **Error! Reference source not found.**;
5. if joinMethodAndRole is methodC, and so the join is between a gSME and a type1PrepaymentInterfaceDevice, check that otherDeviceCertificate is present and validly structured. If the check succeeds the Device shall store, linked to this Device Log entry, details relating to otherDeviceCertificate, such that the Device is able to use subsequently the Shared Secret derived from otherDeviceCertificate and its own Private Key Agreement Key. If this check fails the Device shall set joinResponseCode to invalidOrMissingCertificate and processing shall be unsuccessful;
6. set joinResponseCode to success, create a Response according to the requirements of Section **Error! Reference source not found.**, apply the Response Cryptographic Protection required for a Response of the relevant Message Category, and send the Response.

Amend Section 16.2 Event and Alert Codes as follows:

16.2 Event and Alert Codes

Table 16.2 lists the valid Event and Alert Codes, and sets out their requirements.

GBCS V3.3 Table 16.2.xlsx GBCS V3.2 Table 16.2.xlsx

Table 0: Event and Alert Codes

Amend Section 18.1.1.4 ZSE Report Event Status command as follows:

18.1.1.4 ZSE Report Event Status command

Element	Meaning	Value	Octets
ZCL header			

Element	Meaning	Value	Octets
Frame control	Cluster-specific; not manufacturer specific; client-server; allow default response;	0b00000001	1
Transaction sequence number		0x00	1
Command identifier	Report Event Status	0x00	1
ZCL payload			
Issuer Event ID (UINT32)	Set to the event ID from the corresponding ZSE command received from the ESME	See 'Meaning' column	4
Event Status (UINT8)	Refer to ZigBee standard	As per the requirements of this Section **Error! Reference source not found.**	1
Event Status Time (UTCTime)	~~An HCALCS is not required to have a clock and therefore the HCALC is not required to know UTC time~~Fixed value	0x00000001	4
Criticality Level Applied (UINT8)	0x01 = Voluntary	0x01	1
Cooling Temperature Set Point Applied (UINT16)	Not used	0x8000	2
Heating Temperature Set Point Applied (UINT16)	Not used	0x8000	2
Average Load Adjustment Percentage Applied (INT8)	Not used	0x80	1
Duty Cycle Applied (UINT8)	0x00 (0) = switched OFF; 0x64 (100) = switched ON	See 'Meaning' column	1
Event Control (BITMAP8)	Do not randomise	0x00	1
Signature Type (UINT8)	No signature	0x00	1

Table 0: ZSE Report Event Status command

Amend Section 18.3 Illustrative command and response installation and DER encoding as follows:

18.3 Illustrative command and response instantiation and DER encoding

18.3.1 Illustrative `@UpdateSecurityCredentials.CommandPayload` instantiation and its DER encoding – informative

`supplierUpdatingAllSupplierCertificates` in Table 0a is an ASN.1 structured value assignment. This specific example is where a Device's Supplier is instructing the Device to replace both the Supplier Digital Signing and Key Agreement credentials on the Device, and resetting ~~Protection Against Replay c~~Execution Counters. In business terms, an example of this would be at Change of Supplier.

The black text specifies the parts of the ASN.1 structure, the blue text specifies the value it is set to and the comments explain each of the values.

ASN.1	Notes
supplierUpdatingAllSupplierCertificates CommandPayload ::=	
{authorisingRemotePartyControl	
{credentialsReplacementMode *supplierBySupplier*,	This message is for the supplier replacing supplier credentials
authorisingRemotePartyTACellIdentifier	
{trustAnchorCellRemotePartyRole *supplier*,	The public key to be used to check the signature on this message is the supplier digital signing key currently held by the Device.
trustAnchorCellKeyUsage { *digitalSignature*}},	
authorisingRemotePartySeqNumber *123456789*,	This is the existing supplier's counter, so greater than any this supplier has used

ASN.1	Notes
newRemotePartyFloorSeqNumber 987654321} replacements {{replacementCertificate '0A7C8E9F123456789ABCDEF01234'H, targetTrustAnchorCell {trustAnchorCellRemotePartyRole supplier, trustAnchorCellKeyUsage { digitalSignature}}} {replacementCertificate '0B34269F123456789ABCDEF01234'H, targetTrustAnchorCell {trustAnchorCellRemotePartyRole supplier, trustAnchorCellKeyUsage {keyAgreement}}}} certificationPathCertificates {'FFAABB9F123456789ABCDEF01234'H }}	This is the new supplier's counter, which the Device should use if the Command is successful The new supplier's digital signing certificate … … which is to be placed in the Device's supplier, digital signature Trust Anchor Cell The new supplier's key agreement certificate… which is to be placed in the Device's supplier, key agreement Trust Anchor Cell The Certificate for the CA which issued the new supplier's certificates. The Device will use this to check that the new supplier certificates were properly issued.

Table 0a: Illustrative @UpdateSecurityCredentials.CommandPayload instantiation – ASN.1 structure

The message sent to the Device would contain the DER encoding of the above ASN.1 value assignment. This DER encoding is laid out and explained in Table 0b. For these purposes, the Certificate is simply shown as an OCTET STRING.

Component	Value	Notes
CommandPayload SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x64	100 octet length follows
contents =:		
authorisingRemotePartyControl AuthorisingRemotePartyControl SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x18	Length of authorisingRemotePartyControl
contents =:		
credentialsReplacementMode CredentialsReplacementMode INTEGER:		
tag = [UNIVERSAL 2] primitive;	0x02	
length =	0x01	
contents =:	0x02	Representing supplierBySupplier
authorisingRemotePartyTACellIdentifier TrustAnchorCellIdentifier SEQUENCE:		
tag = [2] constructed;	0xA2	Tag for authorisingRemotePartyTACellIdentifier
length =	0x07	Length of authorisingRemotePartyTACellIdentifier
contents =:		
trustAnchorCellRemotePartyRole RemotePartyRole INTEGER:		
tag = [UNIVERSAL 2] primitive;	0x02	Tag for INTEGER
length =	0x01	1 octet length INTEGER
contents =:	0x02	Representing supplier RemotePartyRole
trustAnchorCellKeyUsage KeyUsage BIT STRING:		
tag = [UNIVERSAL 3] primitive;	0x03	Tag for BIT STRING
length =	0x02	2 octet length BIT STRING
contents =:	0x0780	Representing digitalSignature

Component	Value	Notes
authorisingRemotePartySeqNumber SeqNumber INTEGER:		
tag = [3] primitive;	0x83	Tag for INTEGER
length =	0x04	4 octet length INTEGER
contents =:	0x075bcd15	The old supplier's ~~Protection Against Replay c~~Execution Counter in hex
newRemotePartyFloorSeqNumber SeqNumber INTEGER:		
tag = [4] primitive;	0x84	Tag for INTEGER
length =	0x04	4 octet length INTEGER
contents =:	0x3ade68b1	The new supplier's ~~Protection Against Replay c~~Execution Counter in hex
replacements SEQUENCE OF:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x36	Length of replacements
contents =:		
TrustAnchorReplacement SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x19	Length of first TrustAnchorReplacement
contents =:		
replacementCertificate Certificate OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0x04	Tag for OCTET STRING
length =	0x0e	Length of certificate
contents =:	0x0a7c8e9f123456789abcdef01234	New supplier's digitalSignature certificate
targetTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x07	Length of targetTrustAnchorCell
contents =:		

Component	Value	Notes
trustAnchorCellRemotePartyRole RemotePartyRole INTEGER:		
tag = [UNIVERSAL 2] primitive;	0x02	Tag for INTEGER
length =	0x01	1 octet length INTEGER
contents =:	0x02	Representing supplier RemotePartyRole
trustAnchorCellKeyUsage KeyUsage BIT STRING:		
tag = [UNIVERSAL 3] primitive;	0x03	Tag for BIT STRING
length =	0x02	2 octet length BIT STRING
contents =:	0x0780	Representing digitalSignature
TrustAnchorReplacement SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x19	Length of second TrustAnchorReplacement
contents =:		
replacementCertificate Certificate OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0x04	Tag for OCTET STRING
length =	0x0e	Length of certificate
contents =:	0x0b34269f123456789abcdef01234	New supplier's keyAgreement certificate
targetTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x07	Length of targetTrustAnchorCell
contents =:		
trustAnchorCellRemotePartyRole RemotePartyRole INTEGER:		
tag = [UNIVERSAL 2] primitive;	0x02	Tag for INTEGER
length =	0x01	1 octet length INTEGER
contents =:	0x02	Representing supplier RemotePartyRole
trustAnchorCellKeyUsage KeyUsage BIT STRING:		
tag = [UNIVERSAL 3] primitive;	0x03	Tag for BIT STRING

Component	Value	Notes
length =	0x02	2 octet length BIT STRING
contents =:	0x0308	Representing keyAgreement
certificationPathCertificates SEQUENCE OF:		
tag = [UNIVERSAL 16] constructed;	0x30	Tag for SEQUENCE
length =	0x10	Length of certificationPathCertificates
contents =:		
Certificate OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0x04	Tag for OCTET STRING
length =	0x0e	Length of certificate
contents =:	0xffaabb9f123456789abcdef01234	CA certificate for new supplier

Table 0b: Illustrative @UpdateSecurityCredentials.Command instantiation – DER encoding

18.3.2 Illustrative `@UpdateSecurityCredentials.ResponsePayload` instantiation and its DER encoding – informative

`supplierUpdatingAllSupplierCertificatesResponse` in Table 0a is an ASN.1 structured value assignment. This specific example is where a Device is responding successfully to a Command.

The black text specifies the parts of the ASN.1 structure, the *blue text* specifies the value it is set to by the Device and the comments explain each of the values.

ASN.1	Notes
supplierUpdatingAllSupplierCertificatesResponse ResponsePayload ::=	
{ commandAccepted NULL,	The corresponding Command was for the Supplier replacing supplier credentials
executionOutcome	
{authorisingRemotePartySeqNumber 123456789,	This is the new supplier's counter, which the Device will now use for Protection Against Replay in relation to the supplier role
credentialsReplacementMode *supplierBySupplier*,	

ASN.1	Notes
remotePartySeqNumberChanges {{otherRemotePartyRole supplier, otherRemotePartyFloorSeqNumber 987654321} }, replacementOutcomes {{ {affectedTrustAnchorCell { trustAnchorCellRemotePartyRole supplier, trustAnchorCellKeyUsage { digitalSignature}}, statusCode success, existingSubjectUniqueID '123456789ABCDEF0'H, existingSubjectKeyIdentifier '1234567890123456'H, replacingSubjectUniqueID 'FEDCBA9876543210'H, replacingSubjectKeyIdentifier 'ABCDEABCDEABCDEA'H}, {affectedTrustAnchorCell {trustAnchorCellRemotePartyRole supplier, trustAnchorCellKeyUsage { keyAgreement}}, statusCode success, existingSubjectUniqueID '123456789ABCDEF0'H, existingSubjectKeyIdentifier '0987654321098765'H, replacingSubjectUniqueID 'FEDCBA9876543210'H, replacingSubjectKeyIdentifier 'FEDCBFEDCBFEDCBF'H}}}}	This outcome is for the supplier digital signing store The old supplier's Entity Identifier The KeyIdentifier for the old supplier's digital signing key The new supplier's Entity Identifier The KeyIdentifier for the old supplier's digital signing key This outcome is for the supplier key agreement store

Table 0a: Illustrative @UpdateSecurityCredentials.Response instantiation – ASN.1 structure

The message sent by the Device would contain the DER encoding of the above ASN.1 value assignment. This DER encoding is laid out and explained in Table 0b.

Component	Value	Notes
ResponsePayload SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X8189	Length 137
content =		
commandAccepted NULL		
tag = [UNIVERSAL 5] primitive		0X05
length =	0X00	
executionOutcome ExecutionOutcome SEQUENCE		
tag = [UNIVERSAL 16] constructed	0X30	Tag for SEQUENCE
length =	0X8184	Length 132
content =		
authorisingRemotePartySeqNumber SeqNumber INTEGER:		
tag = [UNIVERSAL 2] primitive	0x02	Tag for INTEGER
length =	0x04	4 octet length INTEGER
contents =	0X075BCD15	The old supplier's ~~Protection Against Replay c~~Execution Counter in hex
credentialsReplacementMode CredentialsReplacementMode INTEGER:		
tag = [UNIVERSAL 2] primitive;	0X02	Tag for INTEGER
length =	0X01	
content =	0X02	Value for supplierBySupplier
remotePartySeqNumberChanges SEQUENCE OF:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X0B	

Component	Value	Notes
content =		
RemotePartySeqNumberChange SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X09	
content =		
otherRemotePartyRole RemotePartyRole INTEGER:		
tag = [UNIVERSAL 2] primitive;	0X02	Tag for INTEGER
length =	0X01	
content =	0X02	Value for supplier
otherRemotePartyFloorSeqNumber SeqNumber INTEGER:		
tag = [UNIVERSAL 2] primitive;	0X02	Tag for INTEGER
length =	0X04	
content =	0X3ADE68B1	The new supplier's ~~Protection Against Replay c~~Execution Counter in hexadecimal
replacementOutcomes SEQUENCE OF:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X6C	Length of 108
content =		
ReplacementOutcome SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X34	Length of 52
content =		
affectedTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X07	
content =		
trustAnchorCellRemotePartyRole RemotePartyRole INTEGER:		

Component	Value	Notes
tag = [UNIVERSAL 2] primitive;	0X02	Tag for INTEGER
length =	0X01	
content =	0X02	Value for supplier
trustAnchorCellKeyUsage KeyUsage BIT STRING:		
tag = [UNIVERSAL 3] primitive;	0x03	Tag for BIT STRING
length =	0X02	
content =	0X0780	Tag for digitalSignature
statusCode StatusCode ENUMERATED:		
tag = [UNIVERSAL 10] primitive;	0X0A	Tag for ENUMERATED
length =	0X01	
content =	0X00	Value for success
existingSubjectUniqueID OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	8 octet length of Entity Identifier
content =	0X123456789ABCDEF0	
existingSubjectKeyIdentifier OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	length of KeyIdentifier
content =	0X1234567890123456	KeyIdentifier
replacingSubjectUniqueID OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	8 octet length of Entity Identifier
content =	0XFEDCBA9876543210	
replacingSubjectKeyIdentifier OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	length of KeyIdentifier
content =	0XABCDEABCDEABCDEA	KeyIdentifier

Component	Value	Notes
ReplacementOutcome SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X34	
content =		
affectedTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE:		
tag = [UNIVERSAL 16] constructed;	0X30	Tag for SEQUENCE
length =	0X07	
content =		
trustAnchorCellRemotePartyRole RemotePartyRole INTEGER:		
tag = [UNIVERSAL 2] primitive;	0X02	Tag for INTEGER
length =	0X01	
content =	0X02	Value for supplier
trustAnchorCellKeyUsage KeyUsage BIT STRING:		
tag = [UNIVERSAL 3] primitive;	0x03	Tag for BIT STRING
length =	0X02	
content =	0X0308	
statusCode StatusCode ENUMERATED:		
tag = [UNIVERSAL 10] primitive;	0X0A	Tag for ENUMERATED
length =	0X01	
content =	0X00	Value for success
existingSubjectUniqueID OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	8 octet length of Entity Identifier
content =	0X123456789ABCDEF0	
existingSubjectKeyIdentifier OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	length of KeyIdentifier

Component	Value	Notes
content =	0X0987654321098765	KeyIdentifier
replacingSubjectUniqueID OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	8 octet length of Entity Identifier
content =	0XFEDCBA9876543210	
replacingSubjectKeyIdentifier OCTET STRING:		
tag = [UNIVERSAL 4] primitive;	0X04	Tag for OCTET STRING
length =	0X08	length of KeyIdentifier
content =	0XFEDCBFEDCBFEDCBF	KeyIdentifier

Table 0b: Illustrative @UpdateSecurityCredentials.ResponsePayload instantiation – DER encoding

Amend Section 20 Mapping Table as follows:

20 Mapping Table

Table 0 contains the Mapping Table from which the Use Cases and Message Templates were generated. These tables map between SMETS attributes and methods, SEC Service Requests, Use Cases, DLMS COSEM attributes and methods and ZSE clusters, attributes and commands.

In addition to the Use Cases, certain columns in the Mapping Table are directly referenced from this document.

Please note that in the SMETS required objects tab only rows marked 'E' (External to HAN) in column F are fully specified, since those rows relate to Remote Party Messages. Other rows are only specified to the extent that these elements of Remote Party Messages rely on them.

GBCS V3.3 Table 20.xlsx GBCS V3.2 Table 20.xlsx

Table 0: Mapping Table

Amend Section 21 Glossary as follows:

Encryption Remote Party

The Remote Party that can decrypt ~~encrypted~~ Encrypted data items.

Execution Counter

Shall have the meaning defined in Section **Error! Reference source not found.** and in Section 13.3.5.3.

~~Highest Prior Sequence Number~~

~~Shall have the meaning defined in Section 13.3.5.3.~~

Supplementary Originator Counter

Shall have the meaning defined in Section **Error! Reference source not found.**.