**MP158 ‘Incorporation of multiple Issue Resolution Proposals into the SEC – Batch 5’**

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.

**Annex A**

**Legal text – version 1.0**

About this document

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

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

Schedule 8 ‘GB Companion Specifications’ version 4.x

These changes have been drafted against GBCS v4.0.

These changes will be applied to the next Sub-Version of the GBCS v4.x series at the time the modification is implemented. These will also be applied to the next Sub-Version of any subsequent GBCS series introduced on or before the modification is implemented.

## Amend Section 7.2.11.4 as follows:

***7.2.11.4 GBT Message processing***

The GBT Initiator shall, once the Remote Party Message is fully constructed and all cryptographic protections are applied, slice the octet string produced so that:

1. GBT Block Data with GBT Initiator Block Number of 1 is the 1149 most significant octets of the Remote Party Message, or all of the octets if the size of the Remote Party Message is less than 1149 octets;
2. GBT Block Data with GBT Initiator Block Number of 2 is the next 1149 most significant octets of the Remote Party Message, or all of the octets if the size of the remaining octets in Remote Party Message is less than 1149 octets; and
3. remaining GBT Block Data are created by repeating Step 2, each time incrementing GBT Initiator Block Number by 1, until there are no remaining octets in the Remote Party Message.

The GBT Recipient shall not undertake any processing, in the sense of Section 6, of the Remote Party Message carried in a GBT Message Series until it has received:

* a GBT Message in this GBT Message Series where the ‘last-block’ field contains 0b1 (meaning last block); and
* all GBT Messages in this GBT Message Series with ‘block-number’ fields less than the ‘block-number’ field in the last block. Where the GBT Recipient has not received all such GBT Messages, it shall send a GBT Message (Request Block Resend) for each missing block-number. Where the GBT Recipient is a Device, it may discard all blocks in a GBT Message Series if it has received no response to a GBT Message (Request Block Resend) after 60 minutes.

For clarity, the GBT Recipient may, where it is a Device, immediately discard, without any further processing, any GBT Message where:

* the Message Code in the Message Routing Header is for a Command, which requires Protection Against Replay; and
* the Device’s Execution Counter, for the Business Originator ID and Message Code specified in the Message Routing Header, is equal to or greater than the Originator Counter in the Message Routing Header.

When a GBT Message Series carries a Response and that GBT Message Series consists of more than 63 GBT Messages, the GBT Recipient shall, if it wishes to receive all parts of the GBT Message Series, send a GBT Message (Acknowledgement) when it has received each complete set of 63 sequential GBT Messages. Note, when the Device sending the Response receives such a GBT Message (Acknowledgement), it is able to begin sending the next sequence of GBT Messages in the GBT Message Series.

GBT Recipient Block Number shall be set to 0x0001 in the first GBT Message sent by the GBT Recipient. It shall be incremented by 1 in each subsequent GBT Message it sends.

GBT Initiator Block Number Ack shall be the highest of:

* 0x0000; and
* the highest block-number in any GBT Message the GBT Initiator has received in this GBT Message Series.

GBT Recipient Block Number Ack shall:

* in a GBT Message (Acknowledgement), be the highest block-number in any GBT Message the GBT Recipient has received in this GBT Message Series; and
* in a GBT Message (Request Block Resend), the value of block-number up to which the GBT Recipient has received all the prior numbered GBT Messages in this GBT Message Series.

Where the GBT Initiator is a Device, the Device shall be able to resend any GBT Message within a GBT Message Series, for a minimum period from when it sends the first GBT Message in that series, to whichever is the sooner of:

* it receiving an authenticated GBT Message (Acknowledgement) where the GBT Recipient Block Number Ack contains a value equal to the highest value of GBT Initiator Block Number in this GBT Message Series; or
* 24 hours later.

For clarity, Devices shall discard malformed GBT messages without further processing in the sense of Section 6. For example, the following GBT Messages would be malformed:

* one with ‘block-number’ equal to zero (this does not comply with the GBCS); and
* one delivered to a recipient where ‘block-number-ack’ is greater than the greatest ‘block-number’ in any GBT Message the recipient has sent in that GBT Message Series.

Where the GBT Recipient is an ESME or an SAPC, the Device shall not send a GBT Message (Request Block Resend), in relation to a GBT Message Series, until and unless 30 seconds have elapsed since receipt of the most recent GBT Message in that GBT Message Series. If 30 minutes elapse without the Device receiving corresponding GBT Message(s) in response, the Device may discard the GBT Messages it has received in this GBT Message Series.

## Amend Section 7.3.6.1 as follows:

***7.3.6.1 Auxiliary Controller related scripts***

All italicised terms in this Section 7.3.6.1 shall have their DLMS COSEM meanings.

As required by DLMS COSEM, the *execute* method (*method 1)* of a *script table* object (*class\_id = 9*) takes a *long-unsigned* value, so two octet value, as its parameter. To have an effect, the *value* of that *long-unsigned* parameter has to match one of the *script\_identfiers* in that object’s *scripts* attribute (*so attribute 2*). Similar requirements apply to the *script\_selector* values in *schedule* objects (*class\_id = 10*).

This Section 7.3.6.1 specifies the *script\_identifier* values that SAPC and ESME shall support (and so the values such Devices shall accept in associated Use Cases) for *script table* objects with OBIS codes 0-0:10.0.103.255 and 0-0:10.0.107.255, and the functionality that such Devices shall implement when each such *script\_identifier* in these two objects is executed.

SAPC and ESME shall support all *script\_identifiers* in objects 0-0:10.0.103.255 and 0-0:10.0.107.255 where:

* the most significant nibble of the most significant octet has a value of either 0x1, indicating output to the controlled load, or 0x2, indicating input;
* the least significant nibble of the most significant octet has a value of either 0x1, 0x2, 0x3, 0x4 or 0x5, indicating ‘n’ in relation to Auxiliary Controller [n];
* for 0-0:10.0.103.255, the most significant bit of the least significant octet has a value of 0b0 or 0b1;
* for 0-0:10.0.107.255, the most significant bit of the least significant octet has a value of 0b0; and
* the seven least significant bits of the least significant octet have a value between 0b0000000 and 0b1100100 inclusive, so between 0 and 100.

SAPC and ESME shall undertake the following processing based on the value of *script\_identifier*, when a *script* in these *script tables* is invoked:

* where the most significant octet has a value of 0x1n, the Device shall only undertake any further script invocation processing where there is currently an Auxiliary Controller associated with Auxiliary Controller [n] and shall only undertake processing in relation to that Auxiliary Controller;
* where the most significant octet has a value of 0x2n, the Device shall only undertake any further script invocation processing where there is currently an Auxiliary Proportional Controller associated with Auxiliary Controller [n] and shall only undertake processing in relation to that Auxiliary Proportional Controller;
* where the script invocation is being requested as part of an ‘ECS47e Limit APC [n] Level’ Command’s execution, the Device shall only undertake any further script invocation processing where the currently associated Auxiliary Controller is an Auxiliary Proportional Controller;
* for 0-0:10.0.103.255, where the most significant bit of the least significant octet has a value of 0b1, the Device shall only take script invocation action where the *script* execution is being requested by the Auxiliary Controller Calendar (with its SMETS meaning) and so the *schedule* object with OBIS code 0-0:12.0.2.255;
* where the most significant bit of the least significant octet has a value of 0b0, the Device shall only take script invocation action where the *script* execution is being requested as part of an ‘ECS47a Set Auxiliary Controller [n] State’ or ‘ECS47e Limit APC [n] Level’ Command’s execution (so where the value of the *data* parameter in the *execute* method / the controllerNumberAndCommandedState field meets this requirement);
* where the preceding conditions are all met, the Device shall undertake processing for the commanded state of the Auxiliary Controller [n] according to the SMETS requirements, using the following interpretation of the seven least significant bits of the least significant octet and, where relevant, the most significant nibble of the most significant octet:
  + - * + for an Auxiliary Proportional Controller (with its SMETS meaning), the value of the seven least significant bits of the least significant octet shall be interpreted as a percentage between 0% (so 0b0000000) and 100% (so 0b1100100), which shall relate:
    - to the output state, if the most significant nibble of the most significant octet is 0x1; or
    - to the input state, if the most significant nibble of the most significant octet is 0x2;
      * + for an ALCS, the value of 0b1100100 in the seven least significant bits of the least significant octet shall be interpreted as meaning closure of the switch (so allowing energy to flow) and any other value shall be interpreted as meaning opening of the switch (so not allowing energy to flow); and
        + for HCALCS, the value of 0b1100100 in the seven least significant bits of the least significant octet shall be interpreted as meaning closure of the switch (so allowing energy to flow) and so requiring the ‘Duty Cycle’ parameter in any resulting Load Control Event command to be 0x64; any other value shall be interpreted as meaning opening of the switch (so not allowing energy to flow) and so requiring the ‘Duty Cycle’ parameter in any resulting Load Control Event command to be 0x00.

Where that processing leads to a change in the commanded state of Auxiliary Controller [n], the Device shall update the Auxiliary Controller [n] State’s commanded state (so the value of either ‘*p*’ or *‘q’* in Section 7.2.9.2 and, where the Alerts are required by SMETS, the value of ‘resultingLevel’ in each of Use Cases ‘ECS101 Limit APC [n] Level Command processed’ and ‘ECS102 Limit APC [n] Level ended or cancelled’) to reflect the current commanded state:

* where Auxiliary Controller [n] is an ALCS or HCALCS and its current commanded state is closure of the switch, ‘*p*’ and *‘q’* shall have the value 100. If its current commanded state is opening of the switch, ‘*p*’ and *‘q’* shall have the value 0; and
* where Auxiliary Controller [n] is an Auxiliary Proportional Controller, ‘*p*’ shall have a value between 0 and 100 inclusive, reflecting the percentage to which its commanded output state is currently set, ‘*q*’ shall have a value between 0 and 100 inclusive, reflecting the percentage to which its commanded input state is currently set.

Correspondingly, as part of the step 4 checks in Section 6.2.4.1.1, Devices shall, for:

* *script\_selector* values in Use Case ‘ECS46d Set Auxiliary Controller Calendar’ Commands; and,
* *data* values in the *execute method* of Use Case ‘ECS47a Set Auxiliary Controller [n] State’ / ‘ECS47e Limit APC [n] Level’ Commands,

apply the following validation to each of those values:

* the most significant nibble of the most significant octet has a value of 0x1 or 0x2;
* the least significant nibble of the most significant octet has a value of either 0x1, 0x2, 0x3, 0x4 or 0x5;
* the seven least significant bits of the least significant octet has a value between 0b0000000 and 0b1100100 inclusive, so between 0 and 100; and
* for Use Case ‘ECS46d Set Auxiliary Controller Calendar’, the most significant bit of the least significant octet is 0b1; and
* for Use Cases ‘ECS47a Set Auxiliary Controller [n] State’ and ‘ECS47e Limit APC [n] Level’, the most significant bit of the least significant octet is 0b0.

When creating an entry in the Auxiliary Controller Event Log (with its SMETS meaning) which relates to the execution of a script in objects 0-0:10.0.103.255 and 0-0:10.0.107.255, the Device shall record the *script\_identifier* value in the entry\_auxiliaryControllerLogEntry.switchNumberAndAction field of that log entry.

## Amend Section 7.3.8 DLMS Device Requirements Tables as follows:

**7.3.8 DLMS Device Requirements Tables**

Table 7.3.8a: Objects tab in embedded file

Table 7.3.8b: Scripts tab in embedded file

Table 7.3.8c: Application Associations tab in embedded file

Table 7.3.8d: Association LN Object Content tab in embedded file

Table 7.3.8e: Security Setup Object Content tab in embedded file

Table 7.3.8f: SAP Assignment Object content tab in embedded file

Table 7.3.8g: Conformance Content tab in embedded file

Table 7.3.8h: End to End Communications tab in embedded file



## Amend Section 7.4 Device requirements - ZSE as follows:

**7.4 Device requirements – ZSE**

This Section 7.4 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 18 and 19.

Only Devices capable of operating at Sub-GHz shall be required to support the requirements in rows of Table 7.4 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 7.4 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 7.4 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 7.4 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 7.4 where column A is ‘CHF: Remote Communications Device (Remote Communications Endpoint)’.

An SAPC shall implement a *ZSE Energy Services Interface* and shall implement all the *clusters, commands, attribute sets and attributes* in Table 7.4 where column A is ‘SAPC: Energy Services Interface (Electricity ESI Endpoint)’.

Where it supports the corresponding SMETS functionality, an SAPC shall implement the *clusters, commands, attribute sets and attributes* in Table 7.4 where column A is ‘SAPC optional: Energy Services Interface (Electricity ESI Endpoint)’.

Additionally, an SAPC may support other *clusters, commands, attribute sets and attributes* in Table 7.4 where column A is ‘ESME: Energy Services Interface (Electricity ESI 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 7.4 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 7.4 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 7.4 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 7.4 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 7.4 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 7.4 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 7.4 where column A is ‘HHT: Remote Communications Device’.

An IHD shall implement all the clusters, commands, attribute sets and attributes in Table 7.4 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 7.4 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 7.4 are informative and for requirements traceability only.

Except where explicitly required by this Section 7.4 or by Section 19.3, 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*).

In relation to the *calendar cluster’s* use for exchanging information about the Auxiliary Controller Calendar (with its SMETS meaning) between Devices:

* the *Calendar Type* value of 0x04 (named *Auxillary Load Switch Calendar*) shall be used, to differentiate from the values of 0x00 (named *Delivered Calendar*) and 0x03 (named *Friendly Credit Calendar*) for the Tariff Switching Table and Non-Disablement Calendar, respectively (with their SMETS meanings); and
* the *Auxiliary Load Switch State* parameters in *PublishDayProfile* commands shall be set so that:
* *bit0* to *bit4* have values corresponding to Auxiliary Controller [1] to Auxiliary Controller [5] respectively, with each such bit being 0b1 where the commanded output state is 100 for the switching instruction in question (so the value of ‘p’ with its Section 7.3.6.1 meaning), or 0b0 otherwise; and
* *bit5* to *bit7* have the value 0b0.

For clarity, this means that settings related to commanded input states are not shared, and commanded output settings of 99 or less on an Auxiliary Proportional Controller (with its SMETS meaning) are all represented as 0b0 to other HAN Devices.



Table 7.4: Device Requirements

## Amend Section 10.4.2.5 and 10.4.2.6 as follows:

***10.4.2.5 Billing Data Log – value of prepayment credits***

Upon completion of processing of a valid Prepayment Top Up, the GSME shall push the Prepayment Top Up’s details to the GPF using the *PublishTop Up Log* command.

The GPF shall store the data contained in the *Publish Top Up Log* command in the GPF copy of the GSME Billing data Log.

If there has been a communications outage, the GPF shall use the *Get Top Up Log* command to retrieve all Prepayment Top Ups that may have been processed during the communications outage. The GSME shall set the *Date / Time* field of the *Get Top Up Log* command to the current UTC time.

***10.4.2.6 Billing Data Log – payment-based debt payments***

Upon completion of processing of a valid Prepayment Top Up where the GSME has made a debt payment using part of that Prepayment Top Up, the GSME shall push details of that debt payment only to the GPF using the *Publish Debt Log* command.

The GPF shall record the details provided in the GPF copy of the GSME Billing Data Log.

In cases of communications outages, the GPF shall request any outstanding payment-based debt payments by use of the *GetDebtRepaymentLog* command (and *GetDebtRepaymentLog* notification flag) with the Debt Type field set to 0x02 (Debt 3).

## Amend Section 4.3.2.6 and as follows:

***4.3.2.6 What is the Public Key in each Trust Anchor Cell to be used for – informative***

| **TrustAnchorCellIdentifier** | | | **Usage of the Public Key in the Trust Anchor Cell** |
| --- | --- | --- | --- |
| **remotePartyRole** | **keyUsage** | **cellUsage** |
| root | keyCertSign | management | Used only in Certification Path Validation to check that Certification Authority Certificates and Certificates related to change of root credentials were validly issued |
| recovery | digitalSignature | management | Used only to verify recovery’s signature on Update Security Credentials Commands addressed to the Device |
| supplier | digitalSignature | management | Used to verify the supplier’s signature on Critical Commands the supplier has addressed to the Device |
| supplier | keyAgreement | management | Used in applying MACs to Alerts and Responses addressed to the supplier, where they are not Critical.  Used in encrypting data in Alerts and Responses addressed to the supplier |
| supplier | keyAgreement | prePaymentTopUp | Used to check the supplier MAC on Prepayment Top Up Commands. The supplier can decide whether this is the same key as the Key Agreement key used for other purposes |
| networkOperator | digitalSignature | management | Used to check the signature of the networkOperator on Critical Commands the networkOperator has sent to the Device. This only equates to Update Security Credentials Commands |
| networkOperator | keyAgreement | management | Used in applying MACs to Alerts and Responses addressed to the networkOperator, where they are not Critical.  Used in encrypting data in Responses addressed to the networkOperator |
| accessControlBroker | digitalSignature | management | Used to verify the accessControlBroker’s signature on Commands addressed to the Device |
| accessControlBroker | keyAgreement | management | Used in checking the accessControlBroker MAC on Commands received and to calculate the MAC for Responses addressed to the accessControlBroker |
| transitionalCoS | digitalSignature | management | Used only to check transitionalCoS’s signature on Update Security Credentials Commands received by the Device |
| wanProvider | digitalSignature | management | Used by the Communications Hub (CHF) to verify the wanProvider’s signature on Critical Commands addressed to the Communications Hub (CHF) |
| loadController | digitalSignature | management | Used to check the signature of the loadController on Critical Commands the loadController has sent to the Device |
| loadController | keyAgreement | management | Used in encrypting data in Alerts and Responses addressed to the loadController |

Table 4.3.2.6: Use of Public Keys in each Trust Anchor Cell

## Amend Section 27 as follows:

1. **Annex 6 –** **Deducing the UTRN Counter from the Truncated UTRN Counter – informative**

This annex provides a worked example of the calculation described in Section 14.6.4.1.5. The calculation uses the 10-bit Truncated UTRN Counter received with the Prepayment Top Up command is received via Consumer Entry to the Device, either directly or via a PPMID. The calculation uses the highest UTRN Counter value held in the Device’s UTRN Counter cache, and a window of 512 either side of this value in making the deduction.

In this case, the UTRN Counter being entered into the Device is 5 greater than the highest thus far received by the Device.

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Value (Binary)** | **Decimal Representation** |
| *Vended by supplier* |  |  |
| Originator Counter (64 bits) | 1001001010001111110001110010110000000000000000000000000000000000 | 10,560,878,642,999,590,912 |
| UTRN Counter (32 bits) | 10010010100011111100011100101100 | 2,458,896,172 |
| PTUT Truncated UTRN Counter (10 bits) | 1100101100 | 812 |
| *Recorded on Device* |  |  |
| Highest entry in UTRN Counter Cache (32 bits) = *V* | 10010010100011111100011100100111 | 2,458,896,167 |

| **Step** | **Description** | **Example** | |
| --- | --- | --- | --- |
| **Binary Representation** | **Decimal Representation** |
| 1 | The method requires 4 signed 32 bit integers, *p, q, r* and *s* |  |  |
| 2 | Set *p* = the numeric value of the least significant 10 bits of the highest UTRN Counter value in the UTRN Counter cache (V) | 1100100111 | 807 |
| 3 | Set *q* = V *– p*  q = 2,458,896,167 – 807 | 10010010100011111100010000000000 | 2,458,895,360 |
| 4 | Set *r =* PTUT Truncated Originator Counter | 1100101100 | 812 |
| 5 | Calculate p – 29 (Call this variable, *x*) (See footnote [[1]](#footnote-1))  x = 807 – 512 | 100100111 | 295 |
| 6 | Calculate p + 29 (Call this variable, *y*)  y = 807 + 512 | 10100100111 | 1319 |
| 7 | Test r against x and y and set s accordingly   * If r < x then s = r + 210 * If r > y then s = r – 210 * Else s = r   295 < 812 < 1319, therefore s = r | 1100101100 | 812 |
| 8 | Set deduced Originator Counter = (q + s) \*232 | 1001001010001111110001110010110000000000000000000000000000000000 | 10,560,878,642,999,590,912 |
| 9 | Set deduced UTRN Counter as most significant 32 bits of Deduced Originator Counter | 10010010100011111100011100101100 | 2,458,896,172 |

Table 27: Derivation of the UTRN Counter from the PTUT Truncated UTRN Counter – a worked example

## Amend Section 13.3.4.1 as follows:

***13.3.4.1 Command Payload construction***

The @UpdateSecurityCredentials.CommandPayload shall have the structure defined in Section 13.3.5.11, and the Remote Party constructing the Command shall populate with values according to Table 13.3.4.1.

| **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 |
| 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 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 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 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, Execution Counters need also to be reset for that other Remote Party Role |
| SEQUENCE |  |  |  |  |
| otherRemotePartyRole | INTEGER | supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) , | Mandatory if otherRemotePartySeqNumberChanges present | The Remote Party Role of the party whose credentials are being placed on the Device but which did not authorise the command 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 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 |
| 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. |
| 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 13.3.4.1: Attribute values for Update Security Credentials Command

## Amend Section 13.3.4.6 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) ,  networkOperatorByNetworkOperator (3) ,  accessControlBrokerByACB (4) ,  wanProviderByWanProvider (5) ,  transCoSByTransCoS (6) ,  supplierByTransCoS (7) ,  anyExceptAbnormalRootByRecovery (8) ,  anyByContingency (9)} , | Mandatory | Provide details of the corresponding Command that are not in the standard GBCS message 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 Execution Counter held on the Device |
| SEQUENCE |  |  |  |  |
| otherRemotePartyRole | INTEGER | root (0) ,  recovery (1) ,  supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) , | Mandatory if SEQUENCE is present | The role which has had its Execution Counter values changed on the Device |
| 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 |
| 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) ,  prePaymentTopUp(1)} | DEFAULT management | 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. |
| 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 |
| 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 13.3.4.6: Attribute values for executionOutcome

## Amend Section 13.3.5.12 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 Execution Counters for that other role or roles |

Table 13.3.5.12: Requirements for AuthorisingRemotePartyControl elements

## Amend Section 14.3.8 as follows:

**14.3.8 Validating the Maximum Credit Values**

***14.3.8.1 Maximum Credit Threshold***

The Device shall ensure that the Prepayment Top Up’s value specified by PTUT Value Class and PTUT Value does not exceed the Device’s Maximum Credit Threshold parameter.

***14.3.8.2 Maximum Meter Balance Threshold***

The Device shall ensure that the Prepayment Top Up’s value specified by PTUT Value Class and PTUT Value when added to the Device’s Credit Balance does not exceed the Device’s Maximum Meter Balance Threshold parameter.

## Amend the glossary as follows:

Unique Transaction Reference Number (UTRN)

A 20 decimal digit number that is used to convey a Prepayment Top Up Remote Party Command to an ESME / GSME / SAPC (where it supports such functionality).

## Amend Section 13.3.4.1 as follows:

***13.3.4.1 Command Payload construction***

The @UpdateSecurityCredentials.CommandPayload shall have the structure defined in Section 13.3.5.11, and the Remote Party constructing the Command shall populate with values according to Table 13.3.4.1.

Table 13.3.4.1: Attribute values for Update Security Credentials 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** |
| --- | --- | --- | --- | --- |
| @ 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 |
| 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, keyCertSign, 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 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 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 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, Execution Counters need also to be reset for that other Remote Party Role |
| SEQUENCE |  |  |  |  |
| otherRemotePartyRole | INTEGER | supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) , | Mandatory if otherRemotePartySeqNumberChanges present | The Remote Party Role of the party whose credentials are being placed on the Device but which did not authorise the command 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 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 |
| 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. |
| 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 |

## Amend Section 13.3.5.8.1 as follows:

*13.3.5.8.1 Decrypting the contingency public key and verifying Authorising Remote Party’s digital signature against that decrypted key*

The Device shall decrypt the Contingency Key that it holds in Trust Anchor Cell {root, keyCertSign, management} by undertaking Decryption using the following parameters:

* setting Ciphertext to be encrypted value of the Contingency Key;
* setting Additional Authenticated Data to be 0x31;
* setting the Initialization Vector to be 0xFFFFFFFF0000000000000000; and
* setting the shared symmetric key to be the value in plaintextSymmetricKey.

Where Decryption is successful, the Device shall use the Plaintext produced as the Public Key to verify KRP Signature according to the requirements at Section 6.3.4.

The Contingency Key shall have been Encrypted accordingly.

## Amend Section 13.3.5.9 as follows:

***13.3.5.9 Verifying the authenticity of replacement certificates***

The Device shall first apply the requirements of Section 12.6 (Device processing of Certificates). If any of those checks fail, the Section 13.3.5.9 check fails.

Where Certification Path Validation is required by this Section 13.3.5.9, the application of time based checks shall be determined as follows:

* if, in the Command, applyTimeBasedCPVChecks = disapply then time based checks shall NOT be applied by the Device; and
* otherwise time based checks shall be applied or not applied in line with the requirements of Section 4.3.2.8.

If (credentialsReplacementMode <> anyByContingency) and (replacements does NOT include a targetTrustAnchorCell of {root, keyCertSign, management}) then the Device shall, for each replacementCertificate in replacements, undertake Certification Path Validation according to the requirements of Section 4.3.2.8.

If (credentialsReplacementMode = anyExceptAbnormalRootByRecovery) and (replacements does include a targetTrustAnchorCell of {root, keyCertSign, management}) then the Device shall:

* first undertake the checks at Section 13.3.5.9.1 in relation to the root Certificates; and
* then shall, for each of the other replacementCertificate in replacements, undertake Certification Path Validation according to the requirements of Section 4.3.2.8. In so doing the Device shall use the details from the replacementCertificate in replacements specified for updating {root, keyCertSign, management} as the root for Certification Path Validation.

If (credentialsReplacementMode = anyByContingency) and (replacements does include a targetTrustAnchorCell of {root, keyCertSign, management}) then the Device shall, for each of the other replacementCertificate in replacements, undertake Certification Path Validation according to the requirements of Section 4.3.2.8. In so doing the Device shall use the details from the replacementCertificate in replacements specified for updating {root, keyCertSign, managment} as the root for Certification Path Validation.

If any of the above checks fail, the Section 13.3.5.9 check fails.

## Amend Section 13.3.5.11 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 13.3.4, 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, keyCertSign, 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, 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 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 13.7.4.2.2 as follows:

*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 13.7.4.2.2. Should a step after step 1 be unsuccessful, the Device shall create a Response according to the requirements of Section13.7.4.5.2, 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 13.7.4.2.2.

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 I 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 13.7.4.5.3;
3. add the otherDeviceEntityIdentifier and otherDeviceType to its Device Log as specified in Section 13.7.4.5.4;
4. if deviceType is eSME then undertake Key Establishment with the other Device as specified in Section 13.7.4.5.5;
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; and
6. set joinResponseCode to success, create a Response according to the requirements of Section 13.4.7, apply the Response Cryptographic Protection required for a Response of the relevant Message Category, and send the Response.

## Amend Section 13.7.4.5.4 as follows:

*13.7.4.5.4 Adding the otherDeviceEntityIdentifier and otherDeviceType to the Device Log*

The Device shall undertake the following steps in the sequence specified:

1. if the otherDeviceEntityIdentifier matches an Entity Identifier currently recorded in its Device Log, then the Device shall compare deviceType in that log entry with otherDeviceType. If the Device types match then the addition is successful and processing within this Section 13.7.4.5.4 shall cease; otherwise the Device shall set joinResponseCode to incompatibleWithExistingEntry and processing within this Section 13.7.4.5.4 shall cease;
2. the Device shall check if there is capacity for an additional entry in its Device Log, including confirmation that, where otherDeviceType is type1HANConnectedAuxiliaryLoadControlSwitch the Device does not currently have an Auxiliary Controller associated with all five of Auxiliary Controller [n]. If there is not, the Device shall set joinResponseCode to deviceLogFull and processing within this Section 13.7.4.5.4 shall cease; and
3. the Device shall attempt to create a new Device Log entry using otherDeviceEntityIdentifier and otherDeviceType. If that entry is not successfully created, the Device shall set joinResponseCode to writeFailure. If that entry is successfully created and otherDeviceType is type1HANConnectedAuxiliaryLoadControlSwitch, the Device shall associate one of its Auxiliary Controller [n] with this new HCALCS, including setting the corresponding Auxiliary Controller [n] Type, with its SMETS meaning, to indicate that this is an HCALCS whose Entity Identifier is otherDeviceEntityIdentifier.

## Amend Section 14.3.7 as follows:

**14.3.7 Updating the UTRN Counter Cache**

Where the Prepayment Top Up is successfully applied and prior to sending any Response, the Device shall add a new entry to the UTRN Counter Cache whose UTRN Counter value shall be set to the 32 most significant bits of Originator Counter.

## Amend Section 14.7.4.1.3 as follows:

*14.7.4.1.3HAN Only Command Validation by the ESME / GSME*

If the ESME / GSME has no PPMID in its Device Log, the ESME / GSME shall apply the requirements of Section 6.2.4.2 to reflect the failed check, and undertake no additional processing.

If the ESME / GSME has a PPMID in its Device Log:

* if the receiving Device is an ESME, the ESME shall use ZSE cryptographic processes to establish whether the Command was authentically issued by a PPMID that is in its Device Log; or
* if the receiving Device is a GSME, the GSME shall undertake Command Authenticity and Integrity Verification, as required for a Command of Message Category SME.C.PPMID-GSME to establish whether the Command was authentically issued by the PPMID that is in its Device Log. For clarity, the ‘PPMID entity ID’ and the ‘Meter entity ID’ from PCS01 and PCS02 Commands are the Business Originator ID and Business Target ID respectively used in the Section 6.2.4.1.1 checks.

If the Command was not authentically issued by a PPMID within the Device Log, the ESME / GSME shall apply the requirements of Section 6.2.4.2 to reflect the failed check.

If the Command was authentically issued by a PPMID within the Device Log, the ESME / GSME shall comply with the requirements of Section 14.6.4 (but excluding requirements in Sections 14.6.4.1.1, save that the ESME / GSME shall disregard the 20th digit before undertaking any further steps), and so process the contents of the Command accordingly.

## Due to changes in Section 20 Mapping Table amend Section 18.2 as follows:

**18.2 DLMS COSEM Message Templates**

Table 18.2 contains Message Templates for all Use Case with DLMS COSEM payloads. These Message Templates are derived from the Mapping Table, and shall be complied with in the construction and population of all such Messages.



Table 18.2: DLMS COSEM Message Templates

## Due to changes in Section 20 Mapping Table amend Section 19.3 as follows:

**19.3 Embedded Use Cases**

Table 19.3 contains the Use Cases that fulfil the interface requirements to cover Commands (and their Responses) and Alerts (where applicable). In addition, it includes ZSE Message Templates.

Note: DLMS COSEM methods that have values which have an impact on the execution of the method (that is, methods with input values that are not integer(0)), the DLMS part of the Mapping Table and the Use Case include two or more rows. One row contains the method, and the subsequent row(s) contain the value(s) to be sent with the method.

A number of Use Cases are also covered in GBCS main body. These are identifiable from the Table of Contents.



Table 19.3: Use Cases

## Amend Section 20 as follows:

**20 Mapping Table**

Table 20 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.

## 

## Amend Section 21 as follows:

**21 Glossary**

||

X || Y shall mean the concatenation of the two octet strings X and Y.

Abstract Syntax Notation One (ASN.1)

ASN.1 is a standard notation for the definition of data types and values. A data type (or type for short) is a category of information (for example, numeric, textual, still image or video information). A data value (or value for short) is an instance of such a type. ASN.1 defines several basic types and their corresponding values, and rules for combining them into more complex types and values. In some protocol architectures, each message is specified as the binary value of a sequence of octets. However, standards-writers need to define quite complex data types to carry their messages, without concern for their binary representation. In order to specify these data types, they require a notation that does not necessarily determine the representation of each value. ASN.1 is such a notation.

Access Control Broker (ACB)

In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the {accessControlBroker, digitalSignature, management} Trust Anchor Cell where present, and stored in the {accessControlBroker, keyAgreement, management} Trust Anchor Cell otherwise.

The ACB applies Cryptographic Protections to all Commands addressed to the Device in question, except potentially for certain recovery scenarios catered for by the Security Credentials Commands.

Access Control Broker to Device MAC (ACB-SMD MAC)

A MAC generated by the Access Control Broker in relation to a Command which can only be verified by the Device which is the target of the Command.

Activate Emergency Credit

A Command described in SMETS.

Active Energy

The integral with respect to time of the Active Power in units of watt-hours (Wh) or standard multiples thereof (for example, kWh).

Additional Authenticated Data (AAD)

One of the inputs to the calculation of a MAC. The AAD is protected by the MAC but is not encrypted. AAD has the same meaning as in *NIST Special Publication 800-38D:* <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>.

Alert

A Message generated by a Device including in response to a problem or the risk of a potential problem.

Alert Code

A 16 bit unsigned integer taking the values specified in Section 16. The Alert Code and Event Code are the same for a given Event.

Application Association

Shall have the meaning specified in the DLMS COSEM standards.

Application Layer Protocol Data Unit (APDU)

Information delivered as a unit among peer entities of networks.

Association LN Object

A DLMS Component specified in the Blue Book which provides role based access control.

Authenticated Decryption

Has the same meaning as specified in *NIST Special Publication 800-38D*: <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>

Authenticated Encryption (AE)

Has the same meaning as specified in *NIST Special Publication 800-38D*: <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>

Authentication

The method used to confirm the identity of entities or Devices wishing to communicate and ‘Authenticated’ and ‘Authenticity’ shall be construed accordingly.

Authentication Key

Shall be as defined in the Green Book.

Authorisation

The process of granting access to a resource and ‘Authorised’ shall be construed accordingly.

Authorised Public Key Infrastructure (APKI)

A key infrastructure that is compliant with the Certificate related requirements of this GBCS.

Auxiliary Controller

Shall have the meaning defined in SMETS.

Auxiliary Controller Calendar

Shall have the meaning defined in SMETS.

Auxiliary Load Control Switch

Shall have the meaning defined in SMETS.

Blue Book

The DLMS Blue Book Version *DLMS UA 1000-1 Ed. 12.0*. This document can be obtained from the DLMS User Association: <http://www.dlms.com>.

Boost Function

ESME and SAPC functionality described in SMETS.

Break On Error

Shall have the Green Book meaning of Break On Error used in relation to ‘Processing\_Option’.

Business Originator

The Smart Metering Entity sending the first Message in a Use Case.

Business Target

The Smart Metering Entity receiving the first Message in a Use Case.

Certificate

An electronic document that binds an identity, and possibly other information, to a Public Key.

Certification Request

A message requesting the issue of a Certificate by a Certification Authority.

Certification Authority (CA)

A trusted entity which issues Certificates.

Certification Authority Certificate

A Certificate issued to a Certification Authority that allows Certification Path Validation in relation to Remote Party’s Certificates.

Certification Path Validation

Shall have the meaning defined in Section 4.3.2.8.

Certification Revocation List (CRL) Validation

Shall have the meaning defined in Section 4.3.2.8.

Ciphered Information

Shall have the meaning defined in Section 8.4.

Ciphertext

An output of the Authenticated Encryption function or an input of the Authenticated Decryption function defined in *NIST Special Publication 800-38D*. The unencrypted form of the Ciphertext is the Plaintext.

Clock

A timing mechanism that has a minimum resolution of 1 second.

Command

An instruction to perform a function received or sent via any interface.

Command Response Alert (CRA) Flag

An element within a Message Header that enumerates whether the Message is a Command or a Response or an Alert.

Commercial Product Assurance Security Characteristic

The security characteristics for the relevant Device as indicated in Section 1.0.

Common Name

The Subject X520 Common Name within an Organisation Certificate, where those terms have their SEC Appendix B Organisation Certificate Policy meaning.

Communications Hub

A device complying with the CHTS.

Communications Hub Function (CHF)

A Communications Hub Function as defined in the Communications Hub Technical Specifications.

Communications Hub Technical Specifications (CHTS)

Communications Hub Technical Specifications set out in Schedule 10 of the Smart Energy Code.

Confidentiality

The state of information, in transit or at rest, where there is assurance that it is not accessible by Unauthorised parties through either unintentional means or otherwise.

Consumer

A person who lawfully resides at the Premises that is being Supplied.

Consumer Access Device (CAD)

A Device which, in terms of this GBCS, is permitted to use the same Messages as an IHD.

Consumption

In the context of GSME, Gas Consumption or in the context of ESME, Electricity Consumption information.

Contingency Key

A feature of Trust Anchor Management Protocol (RFC 5934), and only ever used in a recovery scenario when the root Certificate (Apex Trust Anchor) needs to be replaced.

Critical Message

A Remote Party Message which may relate to supply being affected, financial fraud or the compromise of Device security. Critical, Critical Commands, Critical Alerts and Critical Responses shall be construed accordingly.

Cryptographic Algorithm

An algorithm for performing one or more cryptographic functions which may include Encryption; Decryption; Digitally Signing or Hashing of information, data, or messages; or exchange of Security Credentials.

Cryptographic Protection

A part of a Message constructed to provide assurance to the Message recipient in terms of one or more of integrity, authenticity, non-repudiation and Confidentiality.

Currency Units

The units of monetary value in major and minor units.

Current Private Key

A Device’s Private Key for which the Device has most recently successfully received and processed a Certificate for the corresponding Public Key as defined in Section 13.5.

Data and Communications Company (DCC)

The holder of the licence for the provision of a smart meter communication service granted pursuant to section 6(1)(f) or 6(1A) of the Electricity Act 1989 or section 7AB of the Gas Act 1986.

Data Store

An area of a Device capable of storing information for future retrieval.

Decryption

The process of converting Encrypted information by an Authorised party to recover the original information. Like terms shall be construed accordingly.

Device

A Device that is one of ESME, GSME, Gas Proxy Function, Communications Hub Function, HCALCS, PPMID, SAPC or a Type 2 Device.

Device Based Access Control (DBAC)

Shall have the meaning defined in Section 13.7.3.

Device Certificate

Shall have the meaning set out in Section 12.

Device Log

A data item having the meaning set out in SMETS or CHTS (as relevant).

Digital Signature

The information appended to a Message which is created using the sender’s Private Key, that can be verified using the corresponding Public Key contained in the sender’s Certificate, and provides the receiver with assurance that the sender is who they claim to be, the message has not been altered in transit and that the holder of the the sender’s Private Key created the Message.

Digital Signing

The creation of a Digital Signature.

Digital Signing Certificate

A Certificate which states that the Public Key contained within, and its associated Private Key, may be used for Digital Signing purposes.

Distinguished Encoding Rules

Shall have the meaning defined in <https://www.itu.int/rec/T-REC-X.690/en>

DLMS COSEM

Device Language Message Specification / Companion Specification for Energy Metering - an Application Layer protocol.

Dual Band Communications Hub (Dual Band CH)

A Communications Hub that is capable of operating at 2.4 GHz and Sub GHz frequencies simultaneously.

Electricity Consumption

The Active Energy Imported into the Premises and ‘Consumed’ shall be construed accordingly.

Elliptic Curve DSA (ECDSA)

The Elliptic Curve Digital Signature Algorithm (see <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>) as specified in Section 4.3.3.

Encoding(X)

The encoding of a variable length integer X, as specified in Section 3.3.

Encryption

The process of converting information in order to make it unintelligible other than to Authorised parties. Like terms shall be construed accordingly.

Encryption Originator Counter

Shall have the meaning defined in Table 23.

Encryption Remote Party

The Remote Party that can decrypt Encrypted data items.

Entity Identifier

A 64 bit unsigned integer uniquely identifying a Smart Metering Entity.

ESME

Electricity Smart Metering Equipment, as described in SMETS.

ESMETS

The Electricty Smart Metering Equipment (ESME) Technical Specifications in SMETS.

Event

A change in state generated by a Device in response to an internal or external trigger.

Event Code

A 16 bit unsigned integer taking the values specified in Section 16, which equates to the ZigBee *Event ID* parameter. The Alert Code and Event Code are the same for a given Event.

Event Log

Data item described in the Technical Specifications.

Execution Counter

Shall have the meaning defined in Section 4.3.1.5 and in Section 13.3.5.3.

Firmware

The embedded software programmes and / or data structures that control Devices.

Firmware Distribution Receipt Alert

Shall have the meaning set out in Section 11.2.6.

Force Replace

The means to instruct a Communications Hub to replace an ESME, SAPC or GSME Firmware image that it holds, e.g. when the image has only been partially downloaded to the ESME, SAPC or GSME. This enables recovery from failures.

Gas Consumption

The volume of gas in cubic metres (m3) Supplied to the Premises and ‘Consumed’ shall be construed accordingly.

Gas Proxy Function (GPF)

A Gas Proxy Function as defined in the Communications Hub Technical Specifications.

Galois Counter Mode (GCM)

The mode of operation specified in *NIST Special Publication 800-38D*.

GBZ

A set of structures in the GBCS which carry ZCL / ZSE commands.

General Block Transfer (GBT) / GBT Message

General Block Transfer is a DLMS COSEM mechanism for decomposing APDUs above maximum sizes that can be transported in to a number of smaller APDUs, which are no larger than the maximum sizes. A GBT Message is one of these smaller APDUs.

GMAC

Variant of GCM that is used to generate Message Authentication Code from non-Confidential data, as specified in *NIST Special Publication 800-38D.*

Green Book

The DLMS Green Book Version *DLMS UA 1000-2 Ed.8*. This document can be obtained from the DLMS User Association: <http://www.dlms.com>.

GSME

Gas Smart Metering Equipment, as described in SMETS.

GSMETS

The Gas Smart Metering Equipment (GSME) Technical Specifications in SMETS.

HAN Only Message

A Message where both the sender and recipient are Devices on the same Smart Metering Home Area Network.

HAN Connected Auxiliary Load Control Switch (HCALCS)

HAN Connected Auxiliary Load Control Switch, as described in SMETS..

Hashing

A repeatable process to create a fixed size condensed representation of a Message or any arbitrary data, as further set out in Section 4.3.3. Hash and like terms shall be construed accordingly.

HCALCSTS

The HAN Connected Auxiliary Load Control Switches (HCALCS) Technical Specifications in SMETS.

Home Area Network Interface (HAN Interface)

A component of GSME, ESME, IHD or other Device that is capable of sending and receiving information to and from other Devices.

IHDTS

The In Home Display Technical Specifications in SMETS.

IHD

In Home Display with its SMETS meaning.

Initialization Vector (IV)

An input to the Authenticated Encryption and Authenticated Decryption functions defined in *NIST Special Publication 800-38D*. Where the GBCS applies, it shall have the values as specified at Section 4.3.3.4.

Inter-PAN

Shall have the meaning defined in CHTS.

Join

The process of authorising two Devices to communicate at the application layer.

Key

Data used to determine the output of a cryptographic operation.

Key Agreement

A means to calculate a shared Key between two parties.

Key Agreement Certificate

A Certificate which states that the Public Key contained within, and its associated Private Key, may be used for Key Agreement purposes.

Key Derivation Function (KDF)

A function to generate derived keying material from a Shared Secret and other information.

Known Remote Party (KRP)

In the context of a specific Device, a Remote Party whose Security Credentials are stored on that Device in at least one Trust Anchor Cell.

KRP Signature

A Digital Signature generated by a Known Remote Party.

Len(X)

The number of octets in the variable length octet string X.

Load Controller

In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the { loadController, digitalSignature, management} Trust Anchor Cell.

MAC Header

As defined in Section 6, a part of a message which is only present when the Message contains a MAC but which is additional to the MAC.

Manufacturer Image Hash

Shall have the meaning defined in Section 11.2.4.

Mapping Table

The spreadsheet detailing Use Cases and associated protocol requirements as embedded in Section 20.

Maximum Credit Threshold

Shall have the meaning defined in SMETS.

Maximum Meter Balance Threshold

Shall have the meaning defined in SMETS.

Message

A Command, Response or Alert.

Message Authentication

The process by which the receiver of a Message is provided with assurance that the sender is who they claim to be and that the Message is in the form originally sent.

Message Authentication Code (MAC)

The number incorporated in a Message to provide Message Authentication, as set out in Section 4.3.3.

Message Category

A grouping of Remote Party Messages.

Message Code

A 16 bit unsigned integer identifying the Use Case that the Message in question must conform to. Message Codes have the values specified in Section 15.

Message Identifier

Message Identifier shall be the concatenation of:

* Business Originator ID;
* Business Target ID;
* CRA Flag; and
* Originator Counter.

Message Series

Shall have the meaning defined in Section 7.2.11.1.

Message Template

A protocol-specific table defining the encoding of a Message.

Message Type

The Message Types are Command, Response or Alert.

Network Interface

A WAN Interface or HAN Interface.

Network Operator

In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the {networkOperator, digitalSignature, management} Trust Anchor Cell.

Object Identifier (OID)

An identifier used to name an object. Structurally, an OID consists of a node in a hierarchically-assigned namespace, formally defined using the ASN.1 standard.

Operating Sub GHz Channel

The Sub GHz Channel on which a Device is currently operating.

Organisation Certificate

Shall have the meaning set out in Section 12.

Originator Counter

Shall have the meaning defined in Section 4.3.1.2.

OTA Header

Shall have the meaning defined in Section 11.2.3.

OTA Upgrade Image

Shall have the meaning defined in Section 11.2.3.

OtherInfo

An input to the KDF with the meaning as specified in section 5.8.1 of *NIST Special Publication 800-56Ar2*.

Other User

A Remote Party which is not a Known Remote Party in relation to any Device, and so is always an Unknown Remote Party in any communication with a Device.

Outcome

The result of executing a Command, expressed as success or failure.

Payload

Part of the Message that provides the message-specific content.

Payment Mode

The information held on Smart Metering Equipment as described at sections 4 and 5 in SMETS.

Pending Private Key

A Private Key held on a Device for which a Device has not successfully received and processed a Device Certificate for the corresponding Public Key as defined in Section 13.5.

Plain Format

A Signature is a pair of integers, r and s. For the Elliptic Curve required by the GBCS, each can be represented as a 256 bit (or 32 octet) string. The Plain Format of a GBCS signature is the concatenation R || S where R is the 32 octet string representing r and S is the 32 octet string representing s. Thus, a GBCS Signature is an octet string of length 64.

Plaintext

An input to the Authenticated Encryption function and an output from the Authenticated Decryption function defined in *NIST Special Publication 800-38D*. Plaintext is the data whose Confidentiality is to be protected by Encryption. The encrypted form of the Plaintext is the Ciphertext.

PPMIDTS

The Prepayment Interface Device (PPMID) Technical Specifications in SMETS.

Polyphase

ESME containing three measuring elements suitable for a polyphase supply with up to three phases and neutral.

Premise(s)

The premise(s) which is / are being Supplied.

Prepayment Daily Read Log

Shall have the meaning defined in SMETS.

Prepayment Interface Device (PPMID)

A Device that provides a User Interface for Prepayment Mode related information and Commands.

Prepayment Token Decimal (PPTD)

Shall have the meaning defined in Section 14.1.

Prepayment Top Up

The addition of credit to an ESME (or, where it supports it, an SAPC) or GSME operating in prepayment mode.

Prepayment Top Up Token

Shall have the meaning defined in Section 14.1.

Private Digital Signing Key

A Private Key used for Digital Signing only.

Private Key

The key in a Public-Private Key Pair which must be kept secure by the entity to which it relates.

Private Key Cell

Shall have the meaning defined in Section 4.3.2.3. A Private Key Cell may be Current or Pending.

Private Key Agreement Key

A Private Key used for Key Agreement only.

Protection Against Replay

An attribute defined in a Use Case specifying whether a recipient Device is required to implement the Protection Against Replay mechanisms, as defined in Section 4.3.1.5, for the Command covered by the Use Case.

Protocol Data Unit (PDU)

Information delivered as a unit among peer entities of networks containing control information, address information or data.

Provide Security Credentials Command

A Command of a type constructed according to either Section 13.2 or Section 13.9

Public Digital Signing Key

A Public Key used for Digital Signing only.

Public Key

The key in a Public-Private Key Pair which can be distributed to other parties.

Public Key Agreement Key

A Public Key used for Key Agreement only.

Public Key Security Credentials

Security Credentials which include a Public Key.

Public-Private Key Pair

Two mathematically related numbers that are used in Cryptographic Algorithms.

Recovery

In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the {recovery, digitalSignature, management} Trust Anchor Cell.

Reliable Time

The state of the Device clock such that is within 10 seconds of UTC, synchronised with the HAN time server and confirmed by Set Clock Command from the Remote Party whose security Credentials are stored in the {supplier, digitalSignature, management} Trust Anchor Cell.

Remote Party

An entity which is remote from a Device and is able to either send Messages to or receive Messages from a Device, whether directly or via a third party.

Remote Party Alert

Shall have the meaning defined in Section 7.2.3.

Remote Party Command

Shall have the meaning defined in Section 7.2.1.

Remote Party Message

A Message where either the sender(s) or recipient(s) are not Devices.

Remote Party Role

The role of a Remote Party in relation to which one or more Devices is capable of storing Security Credentials.

Replay Attack

A form of attack on a Communications Link in which a valid information transmission is repeated through interception and retransmission.

Response

A response to a Command received or sent over any interface.

Response Payload

The parts of a Response that are not related to Cryptographic Protections for integrity, authenticity or non-repudiation, as defined in Section 7.2.2.

Role

The entitlement of a party to execute one or more Commands.

Root

In the context of a specific Device, the entity whose Security Credentials are stored in the {root, keyCertSign, management} Trust Anchor Cell.

SAPC

Standalone Auxiliary Proportional Controller, as described in SMETS.

SAPCTS

The Standalone Auxiliary Proportional Controller (SAPC) Technical Specifications in SMETS.

Security Credential Document

Either a:

* Device’s Certificate; or a
* Remote Party’s Certificate; or a
* Certification Authority Certificate

Security Credentials

Information used to Authenticate a Device, Party or system.

Security Log

Data item described in the Technical Specifications.

Service Reference

Shall have the meaning as set out in Appendix AD of the Smart Energy Code.

SHA-256

The Hashing algorithm of that name approved by the NIST (see <http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html>).

Shared Secret

A number which is established by two parties through the Key Agreement technique specified in this GBCS and which can be used as input to a KDF.

Shared Secret Key

A number which is derived using the KDF specified in this GBCS.

Smart Energy Code (SEC)

The document of that name, as designated by the Secretary of State under Condition 22 of the DCC Licence.

Smart Metering Device to Known Remote Party MAC (SMD-KRP MAC)

A MAC generated by a Device in relation to a Response or Alert which can only be verified by the Known Remote Party which is the target of the Response or Alert.

Smart Metering Entity

An entity that is either a Device or a Remote Party.

Smart Metering Equipment Technical Specifications (SMETS)

A version of the Smart Metering Equipment Technical Specifications set out in Schedule 9 of the Smart Energy Code, including the ESMETS, GMSETS, HCALCSTS, PPMIDTS and SAPCTS.

Smart Metering Home Area Network (SMHAN)

The network enabling communications between the Devices recorded within a Communications Hub Function’s Device Log (as defined in CHTS).

SMD Signature

A Digital Signature generated by a Device.

Sub GHz

The range of radio frequencies catered for by the ZSE ‘Sub-GHz Cluster’.

Sub GHz Alert

An Alert which, in the column headed ‘0x02 CHF’ in Table 16.2, is required to be issued by a ‘Dual Band CH Only’. All such Alerts are generated by the CHF.

Sub GHz Channel

One of the radio frequencies catered for by the ZSE ‘Sub-GHz Cluster’.

Sub GHz Channel Masks

Configuration settings to limit the Sub GHz frequencies that a Dual Band CH can switch to.

Sub GHz Available Channels

The subset of Sub GHz frequencies that could be used by Dual Band CH and so could be set in the Sub GHz Channel Masks, so as to comply with UK telecommunications regulations. This subset of Sub GHz frequencies is defined in Section 10.6.5.

Sub GHz Channel Change

The Dual Band CH action of changing its Operating Sub GHz Channel.

Sub GHz Channel Scan

A process undertaken by a Dual Band Communications Hub to identify the level of radio noise on each of the Sub GHz Channels that it is allowed to use by the Sub GHz Channel Masks. This is also referred to in the IEEE 802.15.4a 2007 standard as ‘active channel scan’ and in ZSE as ‘Energy Scan’.

Sub GHz End Device

A Device which is capable of operating on Sub GHz frequencies and which is not a Communications Hub.

Sub GHz GSME

A GSME that is capable of operating on Sub GHz frequencies.

Sub GHz Non-GSME Device

A Sub GHz End Device that is not a GSME.

Subject Unique ID

In the context of a Certificate, shall mean the value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-uniqueIdentifier.

Supplementary Originator Counter

Shall have the meaning defined in Section 4.3.1.4.

Supplementary Remote Party

The Remote Party identified by a Supplementary Remote Party ID.

Supplementary Remote Party ID

In relation to an Alert which has two recipient roles identified as required, the Entity Identifier of the recipient which is not the Supplier shall be the Supplementary Remote Party ID. In relation to a Command and the resulting Response, the Supplementary Remote Party ID shall be the Entity Identifier of the Remote Party requesting the creation of the Command by the Access Control Broker.

Supplementary Remote Party Counter

In relation to a Command and the resulting Response, a 64 bit integer specified by the Remote Party requesting the creation of the Command by the Access Control Broker.

Supply

The supply of gas to Premises for GSME and the supply of electricity to Premises for ESME and ‘Supplied’ shall be construed accordingly.

Supplier

A person authorised by licence to Supply gas to Premises for GSME and a person authorised by licence to Supply electricity to Premises for ESME. In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the {supplier, digitalSignature, management} Trust Anchor Cell.

Supplier Name

The name set in the name part of Contact Details, where that term has its SMETS meaning, and so the name of the Supplier.

Tag

The first element within a Message Header or part of a Message that provides identification of the Message or part of Message that follows.

Tapping Off Mechanism (TOM)

Shall have the meaning defined in Section 10.3.4.

Tariff

The structure of prices and other charges relating to a Supply.

Tariff Block Counter Matrix

Data item described in SMETS.

Technical Specifications

The document set comprising SMETS (incorporating the ESMETS, GSMETS, IHDTS, HCALCSTS, PPMIDTS and SAPCTS), and CHTS.

TOU

Time of Use.

Transitional Change of Supplier

In the context of a specific Device, the Known Remote Party whose Security Credentials are stored in the {transitionalCoS, digitalSignature, management} Trust Anchor Cell.

Trust Anchor (TA)

A Trust Anchor represents a Remote Party via a Public Key and associated data stored on a Device. A Trust Anchor is used by the Device in specified cryptographic operations to determine whether it should act on Remote Party Commands received.

Trust Anchor Cell

A data store on a Device capable of storing one Trust Anchor. Each Trust Anchor Cell is for a fixed and pre-specified KeyUsage, CellUsage and RemotePartyRole.

Trust Anchor Management Protocol (TAMP)

A range of IETF RFCs relate to Trust Anchor Management, including:

* [RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, ‘Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)’, [RFC 4210](http://tools.ietf.org/html/rfc4210), September 2005.
* [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, ‘Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile’, [RFC 5280](http://tools.ietf.org/html/rfc5280), May 2008.
* [RFC5914] Housley, R., Ashmore, S., and C. Wallace, ‘Trust Anchor Format’, [RFC 5914](http://tools.ietf.org/html/rfc5914), June 2010.
* [RFC5934] Housley, R., Ashmore, S., and C. Wallace, ‘Trust Anchor Management Protocol (TAMP)’, [RFC 5934](http://tools.ietf.org/html/rfc5934), August 2010.
* [RFC6024] Reddy, R. and C. Wallace, ‘Trust Anchor Management Requirements’, [RFC 6024](http://tools.ietf.org/html/rfc6024), October 2010.

Twin Element

ESME containing two measuring elements.

Type 2 Device

A Device that is not required to have a Device Log, with its SMETS meaning.

Unauthorised

Not Authorised.

Unique Transaction Reference Number (UTRN)

A 20 decimal digit number that is used to convey a Prepayment Top-Up Remote Party Command to an ESME / GSME / SAPC (where it supports such functionality).

Unknown Remote Party (URP)

In the context of a specific Device, a Remote Party whose Security Credentials are not stored on that Device.

Update Security Credentials Command

A Command of a type constructed according to either Section 13.3 or Section 13.10.

Upgrade Image

Shall have the meaning defined in Section 11.2.2.

Use Case

The structure, format and processing of a Message.

User

Shall have the meaning as set out in Section A of the Smart Energy Code

User Interface

An interface for providing local human interaction with Devices which supports input and visual output.

User Interface Command

A Remote Party Command that is entered through the User Interface.

UTC

Coordinated Universal Time.

UTRN Check Digit

Shall have the meaning defined in Section 14.1.

UTRN Counter Cache

Shall have the meaning defined in Section 14.1.

Variant Message

A Message that does not fall in to any of the Message Categories defined in Section 6.

Wide Area Network (WAN) Interface

A component of a Communications Hub that is capable of sending and receiving information via the Wide Area Network Provider.

Wide Area Network (WAN) Provider

The organisation providing communications over the WAN Interface of the Communications Hub. Consequently, in the context of a specific Communications Hub, the Known Remote Party whose Security Credentials are stored in the {wanProvider, digitalSignature, management} Trust Anchor Cell.

ZigBee Cluster Library (ZCL)

The ZigBee Cluster Library Specification reference document as defined in the ‘Documentation Alignment’ Section of this GBCS.

ZigBee PRO/2007 Layer PICS and Stack Profiles

The ZigBee PRO/2007 Layer PICS and Stack Profiles reference document as defined in the ‘Documentation Alignment’ Section of this GBCS.

ZigBee Specification

The ZigBee Specification reference document as defined in the ‘Documentation Alignment’ Section of this GBCS.

ZigBee Smart Energy (ZSE) Profile (SEP)

The ZigBee Smart Energy (ZSE) Profile Specification reference document as defined in the ‘Documentation Alignment’ Section of this GBCS.

Schedule 9 ‘ESME Technical Specifications’ version 5.x

These changes have been drafted against ESMETS v5.0

These changes will be applied to the next Sub-Version of the ESMETS v5.x series at the time the modification is implemented. These will also be applied to the next Sub-Version of any subsequent SMETS series introduced on or before the modification is implemented.

## Amend Section 5.5.6 as follows:

**5.5.6 Load limiting**

ESME shall be capable of determining when the *Active Power Import [INFO](5.7.5.4)* is above, for the *Load Limit Period(5.7.4.19)*, the *Load Limit Power Threshold(5.7.4.20)* and on such an occurrence ESME shall be capable of:

1. generating an entry to that effect in the *Event Log(5.7.5.16)*;
2. generating and sending an Alert to that effect via its HAN Interface and its User Interface;
3. counting the number of such occurrences in the *Load Limit Counter(5.7.5.18)*; and
4. Disabling the Supply in circumstances where the *Load Limit Supply State(5.7.4.22)* is configured to require Disablement, and then:
5. immediately Arming the Supply such that it can be Enabled as set out in *Section 5.6.2.5* and generating and sending an Alert to this affect via its HAN Interface;
6. prior to the *Load Limit Restoration Period*(*5.7.4.21*) elapsing,

* Disabling the Supply if ESME is in Prepayment Mode, and either:
* it is not in a Non-Disablement Period and the *Meter Balance [INFO](5.7.5.22*) is below, or falls below, the *Disablement Threshold [INFO]*(*5.7.4.15)* and, if Emergency Credit is activated, the *Emergency Credit Balance [INFO](5.7.5.15)* is, or falls to, zero; or
* a Non-Disablement Period ends and the *Meter Balance [INFO](5.7.5.22*)is below the *Disablement Threshold [INFO](5.7.4.15)* and, if Emergency Credit is activated, the *Emergency Credit Balance [INFO](5.7.5.15)* is zero.
* then placing the Supply in such a state whereby Supply will be Armed where the *Meter Balance [INFO]*(*5.7.5.22*) rises above the *Disablement Threshold [INFO](5.7.4.15)*.

1. after the *Load Limit Restoration Period*(*5.7.4.21*) has elapsed, unless:

* ESME is in Prepayment Mode;
* ESME is not in a Non-Disablement Period; and
* the *Meter Balance [INFO](5.7.5.22)* is below the *Disablement Threshold [INFO](5.7.4.15)*; and
* if Emergency Credit is activated, the *Emergency Credit Balance [INFO](5.7.5.15)* is zero,

then:

* enabling the Supply, and setting the *Load Limit Supply State*(*5.7.4.22*) to unchanged; and
* displaying any such change in the *Supply State [INFO](5.7.5.32)* on its User Interface and generating and sending an Alert indicating the change in state via its HAN Interface.

## Amend Section 5.25.1 as follows:

***5.25.1.1 Activate Boost Period***

A Command to:

1. cause the ALCS specified in *Boost Function Control [n](5.26.2.1)* to close; and
2. cause the APC specified in *Boost Function Control [n](5.26.2.1)* to be set to their maximum output level

for a quarter, half, three quarters, one, two, three, four, five, six, seven or eight hours and, at the end of that period, for each Auxiliary Controller affected, to have its output state set to that specified in the *Auxiliary Controller Calendar [INFO](5.7.4.2)*; or, where there is no corresponding calendar setting, to cause the ESME:

1. to open each such ALCS; and
2. to leave each such APC at its maximum output level.

ESME shall only be capable of executing this Command if no Boost Period is currently active.

Where there are any APC specified in *Boost Function Control [n](5.26.2.1)*, ESME shall only be capable of executing this Command if there is no APC [n] Limit Period active for any such APC.

***5.25.1.2 Cancel Boost Period***

A Command to cause the ALCS and APC specified in *Boost Function Control [n](5.26.2.1)* to revert to normal operation in accordance with the *Auxiliary Controller Calendar [INFO](5.7.4.2)* or, where there is no corresponding calendar setting, to cause the ESME:

1. to open each such ALCS; and
2. to leave each such APC at its maximum level.

ESME shall only be capable of executing this Command if a Boost Period is active.

In executing the Command, ESME shall be capable of generating an entry in the *Boost Function Event Log(5.26.3.1)* to the effect that the active Boost Period has been cancelled.

***5.25.1.3 Extend Boost Period***

A Command to cause the ALCS specified in *Boost Function Control [n*](*5.26.2.1*) to remain closed, and the APC specified in *Boost Function Control [n]*(*5.26.2.1*) to be set to their maximum output level, for an additional quarter, half, three quarters, one, two, three, four, five, six or seven hours, and then for each Auxiliary Controller affected, to have its output state set to that specified in the *Auxiliary Controller Calendar [INFO](*5.7.4.2*)*, or, where there is no corresponding calendar setting, to cause the ESME:

1. to open each such ALCS; and
2. to leave each such APC at its maximum output level.

ESME shall only be capable of executing this Command if a Boost Period is active, and where there are any APC specified in *Boost Function Control [n](5.26.2.1)*, if there is no APC [n] Limit Period in force for any of those APC. In executing the Command ESME shall be capable of limiting any active Boost Period to a maximum of 8 hours.

1. In some cases where p < 512, this result may be negative. How negative binary numbers are represented in the calculation is an implementation decision, and not a matter for the GBCS since there is no impact on interoperability. [↑](#footnote-ref-1)