**Smart Metering Implementation Programme**

**Great Britain Companion Specification (GBCS)**

**Version 0.8**

**8 July 2014**

© Crown copyright 2014

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit [www.nationalarchives.gov.uk/doc/open-government-licence/](http://www.nationalarchives.gov.uk/doc/open-government-licence/) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

This document is also available from our website at [www.gov.uk/decc](http://www.gov.uk/decc).

**Version:** GBCS v0.8

**Issued:** 8 July 2014

**Enquiries to**:

Smart Metering Implementation Programme  
Department of Energy & Climate Change  
Orchard 3, Lower Ground Floor

1 Victoria Street

London, SW1H 0ET

Telephone: 0300 068 6659  
Email: [smartmetering@decc.gsi.gov.uk](mailto:smartmetering@decc.gsi.gov.uk)

Documentation Alignment

SMETS and CHTS

All references in this document to the second version of the Smart Metering Equipment Technical Specifications (SMETS) are to Version 1.57[[1]](#footnote-1). All references to the Communications Hub Technical Specifications (CHTS) are to Version 1.45.

Both these documents can be obtained here: <https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version>

DLMS Green and Blue Books

The DLMS User Association plans to publish the 8th edition of the Green Book in July 2014 and the 12th edition of the Blue Book in August 2014. In preparing this version of GBCS, the project team within DECC has had access to draft copies of these standards. These draft versions can be obtained from the DLMS User Association: <http://www.dlms.com>.

It is intended to check the alignment of GBCS v0.8 with the approved versions of the Green Book (DLMS UA 1000-2 Ed. 8.0) and Blue Book (DLMS UA 1000-1 Ed. 12.0) on their publication in July and August 2014.

ZigBee Smart Energy Profile

All references in this document to the ZigBee Smart Energy (ZSE) Profile Specification relate to 1.2a v0.9 draft (reference 14-0256 Rev 02: <http://zigbee.org/About/GBCSPartner.aspx>). The following documents are also referenced and are available from the same link:

* ZigBee Cluster Library (ZCL) Specification, reference 07-5123 Rev 04;
* ZigBee OTA Upgrade Cluster Specification, reference 09-5264 Rev 23;
* ZigBee Specification – 05-3474 Rev 20; and
* ZigBee Pro Stack Profile – 07-4855 Rev 05.

Please note that ZigBee Smart Energy Profile 1.2a v0.9 may be subject to minor amendment in accordance with the ZigBee development process prior to its publication as a standard (ZigBee Smart Energy Profile 1.2a v1.0).

Smart Energy Code

Where relevant, the contents of this version of GBCS align with the draft version of the Smart Energy Code (SEC) 4, which was issued for consultation in June 2014.

Table of Contents

[1 Introduction - informative 7](#_Toc392602235)

[2 Structure of the GB Companion Specification (GBCS) 8](#_Toc392602236)

[2.1 Normative Requirements 8](#_Toc392602237)

[2.2 Structure of the GB Companion Specification (GBCS) and its relationship to other documents - informative 8](#_Toc392602238)

[3 Scope and Terminology 10](#_Toc392602240)

[3.1 Introduction - informative 10](#_Toc392602241)

[3.2 Scope 10](#_Toc392602242)

[3.3 Terminology 11](#_Toc392602243)

[4 Security 13](#_Toc392602244)

[4.1 Introduction – informative 13](#_Toc392602245)

[4.2 Cryptographic Protections applying to all Messages 14](#_Toc392602246)

[4.3 Security for Remote Party Messages 14](#_Toc392602247)

[5 Remote Party Message Construction, Protection and Verification – informative 27](#_Toc392602248)

[5.1 Common Message Structures - informative 27](#_Toc392602249)

[5.2 Common Encryption and Decryption approach - informative 27](#_Toc392602250)

[5.3 Message Categories - informative 27](#_Toc392602251)

[5.4 Common Message Processing steps - informative 28](#_Toc392602252)

[5.5 Common processing stages and requirements for Devices operated through the DCC - informative 30](#_Toc392602253)

[6 Message Categories 34](#_Toc392602254)

[6.1 Introduction - informative 34](#_Toc392602255)

[6.2 Message Category SME.C 34](#_Toc392602256)

[6.3 Message Category SME.C.C 38](#_Toc392602257)

[6.4 Message Category SME.C.NC 39](#_Toc392602258)

[6.5 Message Category SME.C.PPMID-GSME 41](#_Toc392602259)

[6.6 Message Category SME.A 43](#_Toc392602260)

[6.7 Message Category SME.A.C 43](#_Toc392602261)

[6.8 Message Category SME.A.NC 44](#_Toc392602262)

[7 Message structure and DLMS COSEM / ZSE / ASN.1 requirements 46](#_Toc392602263)

[7.1 Introduction - informative 46](#_Toc392602264)

[7.2 Message Construction - general 46](#_Toc392602265)

[7.3 Device Requirements – DLMS COSEM 65](#_Toc392602266)

[7.4 Device requirements – ZSE - informative 67](#_Toc392602267)

[8 Encryption of Attributes in Remote Party Messages 80](#_Toc392602269)

[8.1 Approach - informative 80](#_Toc392602270)

[8.2 Common requirements 80](#_Toc392602271)

[8.3 Key Derivation Inputs 81](#_Toc392602276)

[8.4 AAD, Plaintext and Ciphertext 81](#_Toc392602277)

[8.5 Access to sensitive data – COSEM attribute access 82](#_Toc392602278)

[8.6 Access to sensitive data – ZSE attribute access 87](#_Toc392602279)

[9 Time Synchronisation and Future Dated Remote Party Messages 88](#_Toc392602280)

[9.1 Time synchronisation 88](#_Toc392602281)

[9.2 Future Dated Remote Party Messages 95](#_Toc392602283)

[10 ZSE Implementation 99](#_Toc392602284)

[10.1 Introduction - informative 99](#_Toc392602285)

[10.2 Tunnels 99](#_Toc392602286)

[10.3 GSME and GPF interactions 103](#_Toc392602287)

[10.4 GPF Structured Data Items 106](#_Toc392602288)

[10.5 Hand Held Terminal (HHT) interactions 110](#_Toc392602289)

[11 Downloading firmware images to Devices 114](#_Toc392602542)

[11.1 Introduction – informative 114](#_Toc392602543)

[11.2 Common Requirements 114](#_Toc392602544)

[11.3 CS05a Distribute Firmware to Communications Hub 117](#_Toc392602545)

[11.4 CS05b Distribute Firmware to ESME / GSME 118](#_Toc392602548)

[11.5 CS06 Activate Firmware 119](#_Toc392602551)

[12 Requirements for Certificates 124](#_Toc392602552)

[12.1 Requirements applicable to all Certificates 124](#_Toc392602553)

[12.2 Requirements applicable to Organisations’ Certificates only 125](#_Toc392602554)

[12.3 Requirements applicable to Certificates where RemotePartyRole = root or issuingAuthority 125](#_Toc392602555)

[12.4 Requirements applicable to Certificates where RemotePartyRole is neither root nor issuingAuthority 126](#_Toc392602556)

[12.5 Requirements applicable to Device Certificates 126](#_Toc392602557)

[12.6 Device processing of Certificates 126](#_Toc392602558)

[13 Managing Security Credentials on Devices 127](#_Toc392602560)

[13.1 Introduction - informative 127](#_Toc392602561)

[13.2 CS02a Provide Security Credential Details Command and Response 129](#_Toc392602562)

[13.3 CS02b Update Security Credentials Command, Response and Alert 141](#_Toc392602563)

[13.4 CS02c Issue Security Credentials 176](#_Toc392602572)

[13.5 CS02d Update Device Certificates on Device 181](#_Toc392602573)

[13.6 CS02e Provide Device Certificates from Device 186](#_Toc392602574)

[13.7 Pair-wise Authorisation of Devices 191](#_Toc392602575)

[13.8 GCS59 / 62 GPF Device Log Backup and Restore 206](#_Toc392602576)

[14 Apply Prepayment Top Up to an ESME or GSME 213](#_Toc392602577)

[14.1 Defined Terms 213](#_Toc392602578)

[14.2 Description - informative 213](#_Toc392602579)

[14.3 Common Requirements 214](#_Toc392602580)

[14.4 Applying a Prepayment Top Up to an ESME without consumer intervention 216](#_Toc392602581)

[14.5 Applying a Prepayment Top Up to a GSME without consumer intervention 218](#_Toc392602586)

[14.6 Applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on the ESME or GSME 219](#_Toc392602587)

[14.7 Applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on a PPMID 221](#_Toc392602592)

[14.8 Calculating and Verifying the UTRN Check Digit 223](#_Toc392602601)

[15 Message Codes 225](#_Toc392602602)

[16 Event / Alert Codes and related requirements 226](#_Toc392602603)

[16.1 Introduction – informative 226](#_Toc392602604)

[16.2 Event and Alert Codes 227](#_Toc392602605)

[16.3 Event Logs 227](#_Toc392602606)

[16.4 Requirements 227](#_Toc392602607)

[17 Remote Party Usage Rights 230](#_Toc392602608)

[17.1 Remote Party Access Rights to Attributes and Methods 230](#_Toc392602609)

[17.2 Remote Party Usage Rights to Use Cases 230](#_Toc392602610)

[18 Message Templates 231](#_Toc392603921)

[18.1 ZSE Message Templates 231](#_Toc392603922)

[18.2 DLMS COSEM Message Templates 231](#_Toc392603923)

[18.3 Illustrative command and response instantiation and DER encoding 237](#_Toc392603924)

[18.4 Cryptographic Test Vectors 246](#_Toc392603925)

[19 Use Cases 265](#_Toc392603926)

[19.1 Use Case Title 265](#_Toc392603927)

[19.2 Use Case-specific content 266](#_Toc392603928)

[19.3 ZSE specific content 267](#_Toc392603929)

[19.4 Embedded Use Cases 268](#_Toc392603930)

[20 Mapping Table 269](#_Toc392603931)

[21 Glossary 270](#_Toc392603932)

[22 Annex 1 – Additional DLMS Class 285](#_Toc392603933)

[22.1 Attribute description 285](#_Toc392603934)

[22.2 Method description 286](#_Toc392603935)

[23 Annex 2 - Counters and their use in transaction identification and Protection Against Replay protection - informative 288](#_Toc392603936)

[24 Annex 3 – ASN.1 modules - informative 292](#_Toc392603937)

[25 Annex 4 - Use of ZigBee in GBCS - informative 313](#_Toc392603938)

[25.1 Purpose 313](#_Toc392603939)

[25.2 GBCS requirements to use ZigBee 313](#_Toc392603940)

[25.3 GBCS requirements not to use ZigBee / vary from it 313](#_Toc392603941)

[26 Annex 5 - Use of DLMS COSEM in GBCS - informative 314](#_Toc392603942)

[26.1 Purpose 314](#_Toc392603943)

[26.2 GBCS requirements to use DLMS COSEM 314](#_Toc392603944)

[26.3 GBCS requirements not to use DLMS COSEM / vary from it 315](#_Toc392603945)

[27 Annex 6 - Deducing the UTRN Counter from the Truncated UTRN Counter – informative 316](#_Toc392603946)

# Introduction - informative

The second version of the Smart Metering Equipment Technical Specifications (SMETS2) requires that Gas Smart Metering Equipment (GSME), and Electricity Smart Metering Equipment (ESME) including variants, meet the requirements described in this Great Britain Companion Specification (GBCS).

The Communications Hub Technical Specifications (CHTS) requires that Communications Hubs meet the requirements described in this GBCS.

The HAN Connected Auxiliary Load Control Switches (HCALCS) Technical Specification (HCALCSTS) requires that HCALCS meet the requirements described in this GBCS.

The Prepayment Interface Device (PPMID) Technical Specifications (PPMIDTS) requires that PPMIDs meet the requirements described in this GBCS.

A draft version of this GBCS was notified to the European Commission on [date] in accordance with Directive 98/34/EC, as amended by Directive 98/48/EC.

# Structure of the GB Companion Specification (GBCS)

## Normative Requirements

Some sections of the GBCS are informative and others normative. Unless sections are marked ‘informative’ in the header, they shall be normative. Sub-sections of sections marked informative shall also be informative.

For defined terms (those capitalised), please see the Glossary at Section 21. Where terms are in courier new font, they are Abstract Syntax Notation One (ASN.1[[2]](#footnote-2)) specified structures defined in this document, or in IETF RFC 5912[[3]](#footnote-3). Definitions of such ASN.1 structures are not repeated in the Glossary.

## Structure of the GB Companion Specification (GBCS) and its relationship to other documents - informative

The whole of this Section 2.2 is informative. A number of documents specify what Devices should do and how they should do it, including:

* the Device Specifications (SMETS (including the IHDTS, HCALCSTS and PPMIDTS), and CHTS). These documents:
  + - * lay out minimum physical requirements and minimum functional capabilities for Devices;
      * specify that all Devices must use the ZSE protocol specifications; and
      * specify that Electricity Smart Metering Equipment (ESME) must additionally use DLMS COSEM protocol specifications.
* International Standards documents, including those which lay out what is required to use ZSE and DLMS COSEM protocols. However, the standards are flexible and could be used in many different ways to implement technically the minimum functional requirements of SMETS and CHTS;
* the end to end protocol that is defined in the GBCS deviates from the standard ZigBee SEP1.2 and DLMS COSEM protocols in some instances. Suppliers and the DCC are required to deploy Devices that are certified against those aspects of the GBCS that are fully compliant with the ZigBee and DLMS COSEM protocols. Certification is not required against those aspects of the GBCS where the ZigBee and DLMS COSEM protocols are actively dis-applied or modified.

For additional information on the level of the area that would not require certification please see Section 25 for ZigBee SEP1.2, and Section 26 for DLMS COSEM.

GB Smart Metering requires technical interoperability, and so requires a single, consistent, technical implementation of the capabilities laid out in SMETS and CHTS across all Devices, in so far as the network communications with Devices are concerned, be those communications over the Smart Metering Home Area Network (SMHAN) or Wide Area Network (WAN). The Devices in scope of this GBCS are:

* Electricity Smart Metering Equipment (ESME), including Polyphase, Twin Element, Auxiliary Load Control Switch (ALCS) and Boost Function variants thereof;
* Gas Smart Metering Equipment (GSME);
* Communications Hub (Communications Hub Function - CHF) and Communications Hub (Gas Proxy Function - GPF);
* Prepayment Interface Device (PPMID) and HAN Connected Auxiliary Load Control Switch (HCALCS); and
* Type 2 Devices, including In Home Displays (IHDs).

The purpose of this GBCS, and related documents, is to specify the single, consistent technical implementation in sufficient detail to achieve operational interoperability of Devices.

This GBCS refers out to International Standards, specifically those relating to DLMS COSEM, ZSE, ASN.1, NSA Suite B cryptography and X.509 related IETF RFCs. The GBCS does not duplicate what is laid out in such standards but rather provides references to them.

# Scope and Terminology

## Introduction - informative

This Section 3.1 is informative and summarises Section 3.

Section 3 introduces key terms used in the GBCS:

* Messages are how Devices communicate between themselves and with organisations remote from Consumers’ Premises. Such Messages are ‘end-to-end’ and ‘unicast’ in that:
  + - * they all identify the sender (e.g. a Supplier) and the intended recipient (e.g. an ESME); and
      * they are all intended for processing by the intended recipient, even though they may pass through intermediate Devices, such as a Communications Hub. Most Messages pass through Communications Hubs unaltered, save for any ‘wrapping’ information needed for transport purposes. The only exception is where a Communications Hub Device is the intended recipient or is the sender (in these cases the Message is processed by the CHF or GPF), or where covered by the Tapping Off Mechanism (Section 10);
* Messages are one of:
  + - * a Command to a Device or a corresponding Response;
      * an Alert from a Device; or
      * an information provision transaction (HAN Only Message) solely between Devices;
* Organisations (such as Suppliers and Network Operators) communicating with Devices are called Remote Parties;
* Messages to and from Remote Parties are called Remote Party Messages; and
* Messages solely between Devices are called HAN Only Messages.

Section 3 then:

* explains that the GBCS only covers the Messages needed for the minimum functionality laid out in the SMETS and CHTS;
* explains that the GBCS specifies how all such Messages are constructed and related processing performed; and
* notes that Type 2 Devices (e.g. IHDs) can only send or receive HAN Only Messages.

Section 3 also explains some technical terminology and technical conventions used in this GBCS.

## Scope

This Section 3.2 lays out the scope of the GBCS and introduces definitions relied upon in this GBCS.

A Message shall be of one the following:

* a Command;
* a Response to a Command;
* an Alert; or
* an information provision transaction (HAN Only Message).

A Message Instance shall be an instance of one of the Messages detailed in this GBCS.

The Device Specifications define the minimum functional capabilities required of Devices.

Except where those functional capabilities are internal to the Devices or are accessed via the Device’s User Interfaces, the minimum functional capabilities shall be invoked by, and / or result in, Messages being passed via the Devices’ Network Interfaces.

The GBCS is the technical specification, sufficient for the creation by the originator(s) and processing by the target(s), of each Message, where the Message is required in order to implement minimum functionality defined in the Device Specifications.

Specifically, the GBCS details the format, structure and associated processing for each of the Messages required to implement the Device Specifications’ minimum functionality.

There are two classifications of Message:

* HAN Only Message, where both the original sender and ultimate recipient are Devices within the same Smart Metering Home Area Network (SMHAN); and
* Remote Party Message, where either the original sender or the ultimate recipient is not a Device.

A Remote Party Message shall only be of one of the following:

* a Command;
* a Response to a Command; or
* an Alert.

Each Remote Party Message shall have a unique Message Code, which shall be as specified in Section 15.

Where a Remote Party is known to a Device by way of that Remote Party’s Security Credentials being stored on the Device (as specified in Section 4.3.2.5), the Remote Party is referred to as a Known Remote Party (KRP). Otherwise, it is referred to as an Unknown Remote Party (URP).

Commands requiring a Response to an Unknown Remote Party shall always be sent to the Device by the Device’s Access Control Broker (see Section 4.3.2.5).

For clarity, Type 2 Devices shall not be required to support any Remote Party Messages. Thus, provisions in this GBCS in relation to Remote Party Messages shall not apply to Type 2 Devices.

Remote Parties and Devices are collectively referred to in this GBCS as Smart Metering Entities.

## Terminology

### Numbers

Numbers within this GBCS are expressed in one of three ways, to avoid potential ambiguity:

* where a number has no prefix, it is a decimal number (base 10);
* the 0x prefix is used for hexadecimal numbers (base 16). For example, 0x10 equates to the decimal number 16; and
* the 0b prefix is for binary numbers (base 2). For example, 0b1010 equates to the decimal number 10.

### Bit numbering

Numbering of bits uses the ‘LSB 0’ bit numbering scheme, where the least significant bit is referred to as bit 0 and the most significant bit is referred to using the highest bit number.

### Octets and bytes - informative

The term ‘octet’ is used to refer to units of 8 bits of digital information, to avoid potential ambiguity with the term ‘byte’, and to align with protocol terminology.

### Tag and MAC - informative

In this GBCS:

* the word ‘tag’ is always used in the sense it is meant in encoding standards, such as A-XDR[[4]](#footnote-4) and Distinguished Encoding Rules (DER)[[5]](#footnote-5);
* ‘tag’ is never used to mean Authentication tag, in the cryptographic sense;
* ‘MAC’ is always used to mean Message Authentication Code, which is a cryptographic checksum on data. Thus, MAC is used instead of Authentication tag; and
* ‘MAC’ is never used to refer to Medium Access Control, as used in ‘MAC address’, which is a unique identifier assigned to network interfaces.

### Concatenation

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

For example:

X = 0xCAFE

Y = 0xBEEF

X || Y = 0xCAFEBEEF

### Encoding and length of variable length unsigned integers

Encoding(X) shall be the encoding of a variable size unsigned integer X as follows:

* if 0<X<128, then Encoding(X) is a single octet whose value is X; or
* if 128<= X <32,768, then Encoding(X) is a an octet string composed of the concatenation 0x82 || Y, where Y is two octets in length and has a value equal to the two’s complement representation of the value X; or
* if 32,768<= X <8,388,608, then Encoding(X) is a an octet string composed of the concatenation 0x83 || Y, where Y is three octets in length and has a value equal to the two’s complement representation of the value X.

Len(Encoding(X)) shall be the length in octets of Encoding(X), so shall be either 1 (X<128), 3 (128<= X <32768) or 4 (32,768<= X <8,388,608).

### ASN.1 terms

The GeneralizedTime ASN.1 type used in this GBCS shall be a UTC Time with a resolution of one second. See Section 46 of the ASN.1 specification for format.

# Security

## Introduction – informative

This Section 4.1 is informative and summarises Section 4.

Section 4.2 lays out security provisions that are common across Messages, specifically stating that:

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

Section 4.3 lays out security provisions that are common across Remote Party Messages, specifically:

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

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

The same requirements for security apply regardless of whether a Message is delivered by the Wide Area Network (WAN), SMHAN, Hand Held Terminal (HHT) or local interface. Note that, for Prepayment Top Up, there are a number of different Messages. The content of each particular Message will always be processed in the same way regardless of delivery mechanism. The governance and structures to ensure uniqueness of identifiers are set out in the Smart Energy Code (SEC) and SMETS, and are outside the scope of the GBCS.

A single Originator Counter can be used for the whole of a Remote Party Organisation (e.g. by that Party counting small enough time intervals). A separate counter per Device is not required.

The Supplementary Originator Counter as specified in Section 4.3.1.4 is required where the corresponding Response has to be cryptographically protected (by way of Encryption, a MAC, or both), to the Supplementary Remote Party. In all other cases, the Response is protected back to the Access Control Broker.

Smart Metering entities make extensive use of a range of Counters as part of the unique identification of Smart Metering Messages. Counters are also a key component used to support Protection Against Replay functionality. An overview of each of these counters and their use is included as Section 23.

## Cryptographic Protections applying to all Messages

Each Message shall have Cryptographic Protections to give assurance to the Message recipient(s) as to:

* the Message’s integrity; and
* the Authenticity of the party or parties creating or augmenting the Message.

The minimum set of such Cryptographic Protections is laid out in this GBCS.

This GBCS lays out the Cryptographic Protections for non-repudiation, where this quality is required for specific Messages, so for Critical Messages.

Where part of a Message is Confidential, that part shall have Cryptographic Protections to ensure both its Confidentiality and its integrity, as detailed in this GBCS.

For HAN Only Messages the Cryptographic Protections required by this GBCS shall be those provided by ZSE.

For clarity, the HAN Only Message Cryptographic Protections require that all Devices shall:

* be provisioned with the corresponding ZSE related Security Credentials; and
* be capable of performing the associated cryptographic operations.

## Security for Remote Party Messages

This Section 4.3 shall:

* apply only to Remote Party Messages;
* apply to all Remote Party Messages, regardless of the mechanism (i.e. across the WAN, SMHAN, HHT or User Interface) by which they are delivered to, or received from, the Device in question; and
* apply to the processing of Remote Party Messages by Remote Parties and Devices.

### Identifiers, Counters and Protection Against Replay

#### Identifiers

All Smart Metering Entities shall have an Entity Identifier which shall be an octet string of length 8. Each Entity Identifier shall be unique across GB Smart Metering.

Entity Identifiers shall be used in the Business Originator ID and Business Target ID fields of Remote Party Messages as shown in Table 4.3.1.1.

|  |  |  |
| --- | --- | --- |
| **Message Type** | **Business Originator ID** | **Business Target ID** |
| Command | Entity Identifier for the Known Remote Party which is requesting execution of this Command | Entity Identifier for the Device that the Remote Party wants to action the Command |
| Response | The Entity Identifier for the Device. This is always the same as the Business Target ID supplied in the corresponding Command | The Business Originator ID provided in the corresponding Command  For Commands to which the corresponding Response is intended for an Unknown Remote Party, the Business Originator ID in the Command shall always be that of the Access Control Broker |
| Alert | The Entity Identifier for the Device | The Entity Identifier for the Known Remote Party to which the Alert is to be addressed. Section 16 of this GBCS specifies which Known Remote Party role each type of Alert shall be addressed to |

Table 4.3.1.1: Entity Identifiers for Business Originator and Target ID fields

#### Originator Counter

Except where specified otherwise in the GBCS, a Remote Party Message shall include an Originator Counter, which shall be octet string of length 8 whose contents shall be set and read as an unsigned 64-bit integer. Responsibility for generating the Originator Counter shall be as shown in Table 4.3.1.2.

|  |  |
| --- | --- |
| **Message** | **Responsibility for generating the Originator Counter** |
| Command | The Known Remote Party identified by the Business Originator ID in the Command. |
| Response | The Originator Counter shall have the same value as in the corresponding Command. |
| Alert | The Device generating the Alert. |

Table 4.3.1.2: Responsibility for generating the Originator Counter

Where a Device is required to generate an Originator Counter, the Device shall ensure that the value it generates is strictly numerically greater than any previous Originator Counter value it has placed in any previous Message it has generated, and strictly numerically greater than any Supplementary Originator Counter it has placed in any previous Message it has generated.

Where a Remote Party is required to generate an Originator Counter, the Remote Party shall ensure that:

* the value it generates is strictly numerically greater than any previous Originator Counter value it has provided for use in any previous Command to the Device in question;
* the 32 least significant bits shall not all have the value 0b0 unless the Command is a Prepayment Top Up Command (see Section 14.3.6 for use of the Originator Counter as the UTRN Counter); and
* if the Command is a Prepayment Top Up then the 32 least significant bits shall all have the value 0b0.

#### Message Identifier

A Message Identifier shall be the concatenation:

Business Originator ID || Business Target ID || CRA Flag || Originator Counter

All Messages shall include a Message Identifier which shall be:

* constructed according to the requirements of this Section 4.3.1; and
* incorporated in the Message according to the requirements of Section 7.

#### Additional Counters and Identifiers

The following attributes shall be incorporated in Commands where (1) the Business Originator ID is set to be that of the Access Control Broker and (2) the Message Code is listed in the ‘Use Case reference’ worksheet of the Mapping Table as *‘Supplementary Remote Party Data required*’:

* Supplementary Remote Party ID, which shall be the Entity Identifier of the Remote Party requesting the creation of the Command by the Access Control Broker; and
* Supplementary Remote Party Counter, which shall be an octet string of length 8.

All Responses to such Commands shall incorporate:

* the same Supplementary Remote Party ID and Supplementary Remote Party Counter as the Command; and
* for those marked as ‘*Supplementary Originator Counter required in Response*’ in the ‘Use Case reference’ worksheet of the Mapping Table’, a Supplementary Originator Counter which shall be generated by the Device, shall be an octet string of length 8 whose contents shall be set and read as an unsigned 64-bit integer. The Device shall ensure that the value it generates is strictly numerically greater than any previous Originator Counter value it has placed in any previous Message it has generated, and strictly numerically greater than any Supplementary Originator Counter it has placed in any previous Message it has generated.

#### Protection Against Replay mechanisms

Where a Device supports one or more Remote Party Commands that are marked as requiring ‘Protection Against Replay’ in the Use Cases, the Device shall implement the requirements detailed in this Section 4.3.1.5.

For each Command that a Device supports, and that is marked as requiring ‘Protection Against Replay’ in its Use Case, the Device shall:

* have the capability to store an Originator Counter value for each Remote Party Role allowed to request immediate execution of that Command (the ‘Immediate Execution Counter’);
* have the capability to store a separate Originator Counter value for each Remote Party Role allowed to request future dated execution of that Command (the ‘Future Dated Counter’);
* have all Immediate Execution Counters and Future Dated Counters initially set to zero at manufacture;
* reject a Command Instance sent for immediate execution, where the Originator Counter in the Command Instance is not greater than the value of the Immediate Execution Counter held for that type of Command;
* reject a Command Instance for future dated execution, where the Originator Counter in the Command Instance is not greater than the value of the Future Dated Counter held for that type of Command at the point at which the Command Instance is received;
* having successfully verified a Command Instance for immediate execution, set the Immediate Execution Counter for that type of Command to the Originator Counter value in the successfully executed Command Instance; and
* having successfully verified the details of a Command Instance for future dated execution, set the Future Dated Counter for that type of Command to the Originator Counter value in the successfully verified and stored Command Instance.

As detailed in Section 13.3.5.10, a Device shall reset Immediate Execution Counters, Future Dated Counters and any caches of such counters for all Commands corresponding to a specific Remote Party Role, where:

* the Device successfully executes an Update Security Credentials Command Instance to replace Security Credentials related to that Remote Party Role, and
* that Update Security Credentials Command Instance specifies that Immediate Execution and Future Dated Counters should be reset.

In such cases, the Immediate Execution Counters and Future Dated Counters shall all be set to the Originator Counter value in the Update Security Credentials Command Instance.

Also as detailed in Section 13.3.5.10, caches related to such counters shall be cleared of all values, and then a value equating to the Originator Counter value in the Update Security Credentials Command Instance shall be placed in the cache. Any related flags in such caches shall record that this value is a floor value and does not relate to a Message Instance of that type being received.

### Security Credentials

#### Introduction – informative

A Device shall be able to process four kinds of Security Credential Document:

* its own Security Credential Documents, provided in the form of Device Certificates. Here the Device needs processing to cover (1) generating new Public-Private Key Pairs and so issuing Device Certificate Signing Requests, (2) storing its Device Certificates and (3) providing a copy of those Device Certificates on request;
* Security Credential Documents relating to Known Remote Parties, provided in the form of Organisation Certificates. For these, the Device needs to be capable of (1) storing, (2) replacing and (3) providing details of those it holds on request;
* Security Credential Documents relating to Unknown Remote Parties, provided in the form of Organisation Certificates. For these, the Device will receive them in a Command so that parts of the Response can be Encrypted. The Device does not need to store such Documents; and
* Security Credential Documents relating to Certification Authorities, provided in the form of Certification Authority Certificates. These are processed by the Device only when replacing Remote Parties’ Security Credential Documents.

Sections 8 and 13 cover the above functionality.

Section 13 covers requirements related to the structure and content of such Security Credential Documents, where such requirements are relevant to Device processing requirements.

This Section 4.3.2 covers requirements for the storage of such Security Credentials on Devices and their usage in verifying cryptographic protections on Command the Device receives.

#### Security Credential Documents

A Security Credential Document shall be either:

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

##### Device Certificate

A Device Certificate shall relate to only one Device and shall meet the requirements specified at Section 12. A Device Certificate shall either be used for Key Agreement or Digital Signing but not both. Device Certificates shall only be issued by Authorised Public Key Infrastructure (APKI) issuing Certificate Authorities. Where Security Credentials relating to a Device are incorporated in a Message, the Security Credentials shall be incorporated in the Message in the form of the Device Certificate.

##### Remote Party’s Certificate

A Remote Party Certificate shall be one of that Remote Party’s Organisation Certificates and so shall relate to only one Remote Party and shall meet the requirements specified at Section 12. As per Section 12, except where remotePartyRole = root a Remote Party Certificate shall either be used for Key Agreement or Digital Signing but not both. Remote Party Certificates shall only be issued by APKI authorised issuing Certificate Authorities. Where Security Credentials relating to a Remote Party are incorporated in a Message, the Security Credentials shall be incorporated in the Message in the form of the Remote Party’s Certificate.

##### Certification Authority Certificate

A Certification Authority Certificate shall relate to only one Certification Authority and shall meet the requirements specified at Section 12. A Certification Authority Certificate shall only be used by a Device for verifying Digital Signatures on Certificates. Where Security Credentials relating to a Certification Authority are incorporated in a Message, the Security Credentials shall be incorporated in the Message in the form of the Certification Authority’s Certificate.

#### Device Security Credentials

Where a Device is of deviceType that is gSME, eSME, communicationsHubCommunicationsHubFunction, or communicationsHubGasProxyFunction, that Device shall have the capacity to store and use securely four private keys:

* for Key Agreement, a Current Private Key and a Pending Private Key; and
* for Digital Signing, a Current Private Key and a Pending Private Key.

Where a Device is of deviceType that is type1HANConnectedAuxiliaryLoadControlSwitch or type1PrepaymentInterfaceDevice, that Device shall have the capacity to store and use securely two private keys:

* for Key Agreement, a Current Private Key; and
* for Digital Signing, a Current Private Key.

These stores shall be referred to as Private Key Cells.

Wherever one of a Device’s Private Keys is required to be used by a GBCS Cryptographic Protection process, only the relevant Current Private Key shall be used. A Device shall not use any Pending Private Key in any GBCS Cryptographic Protection.

Where a Device holds a Private Key that is to be used for Key Agreement, the corresponding Public-Private Key Pair shall have been generated according to the NSA’s ‘Suite B Implementer’s Guide to NIST SP 800-56Ar2’ using the ‘Key Pair Generation Using Extra Random Bits’ method.

Where a Device holds a Private Key that is to be used for Digital Signing, the corresponding Key Pair shall have been generated according to the NSA’s ‘Suite B Implementer’s Guide to FIPS 186-3 (ECDSA), February 3, 2010’[[6]](#footnote-6) using the ‘ECC Key Pair Generation Using Extra Random Bits’ method.

Where a Device supports the processing of Remote Party Messages, the Device shall:

* have two Trust Anchor Cells to store two Device Certificates relating to itself, with one Trust Anchor Cell for storing Device Certificates where keyUsage = keyAgreement and one for Device Certificates where keyUsage = digitalSignature;
* where those two Trust Anchor Cells are populated, ensure the Device Certificates have the following attributes:
  + - * both Device Certificates meet the requirements specified at Section 13;
      * both Device Certificates’ hwSerialNum fields have a value the same as the Devices’ Entity Identifier; and
      * each Device Certificate’s keyUsage field has the same value as the Trust Anchor Cell in which it is placed.

#### Remote Party Security Credentials

A Device shall only action a Remote Party Command where:

* the Known Remote Party identified by the Command has, according to the Security Credentials held on the Device, a Remote Party Role which, according to the Mapping Table for the Message Code in question, is allowed to request execution of the Command; and
* the Cryptographic Protections in the Command Instance received by the Device have been verified, in line with the requirements for a Command with the Message Code in question.

To enable this, Security Credentials relating to the Remote Parties in question:

* shall be held in Trust Anchor Cells on the Device; and
* shall act as the corresponding Trust Anchors.

#### Required Trust Anchor Cells and related Device requirements

The Trust Anchor Cells specified in Table 4.3.2.5 by TrustAnchorCellIdentifier are those required on each deviceType. Additionally:

* a GSME shall have a Trust Anchor Cell capable of storing Key Agreement Security Credentials for a PPMID; and
* a PPMID shall have a Trust Anchor Cell capable of storing Key Agreement Security Credentials for a GSME.

The types of Device and the corresponding value of deviceType shall be defined in ASN.1 notation by:

DeviceType ::= INTEGER {

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

CommunicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

Every Device shall:

* have storage allocated capable of holding Security Credentials as required by Table 4.3.2.5 for its Device type; and
* have all the Trust Anchor Cells, specified in Table 4.3.2.5 as being required for its Device type, populated with Security Credentials that comply with the requirements of this GBCS. Critically, root, recovery and accessControlBroker Trust Anchor Cells shall be populated with valid credentials for each of those three Remote Parties.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | |  | |  | Type of Device (✓= is required; empty = is not required) | | | | |  |
|  |  | |  | |  | ESME | GSME | CH (CHF) | CH (GPF[[7]](#footnote-7)) | HCALCS | PPMID |
|  | deviceType value(s) | | | | | 1 | 0 | 2 | 3 | 4 | 5 |
|  | **TrustAnchorCellIdentifier** | | | | |  |  |  |  |  |  |
| No | **remotePartyRole** | **keyUsage** | | **cellUsage** | |  |  |  |  |  |  |
| 1 | root | keyCertSign | | management | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 | recovery | digitalSignature | | management | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3 | supplier | digitalSignature | | management | | ✓ | ✓ |  | ✓ | ✓ |  |
| 4 | supplier | keyAgreement | | management | | ✓ | ✓ |  | ✓ |  |  |
| 5 | supplier | keyAgreement | | prePaymentTopUp | | ✓ | ✓ |  |  |  |  |
| 6 | networkOperator | digitalSignature | | management | | ✓ |  |  | ✓ |  |  |
| 7 | networkOperator | keyAgreement | | management | | ✓ |  |  | ✓ |  |  |
| 8 | accessControlBroker | digitalSignature | | management | |  |  | ✓ |  |  | ✓ |
| 9 | accessControlBroker | keyAgreement | | management | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 10 | transitionalCoS | digitalSignature | | management | | ✓ | ✓ |  | ✓ | ✓ |  |
| 11 | wanProvider | digitalSignature | | management | |  |  | ✓ |  |  |  |

Table 4.3.2.5: Requirements for Trust Anchor Cells by Device Type

A specific Trust Anchor Cell shall be identified in this GBCS using the notation {remotePartyRole, keyUsage, cellUsage}. For example {supplier, digitalSignature, management} shall refer to the Trust Anchor Cell that holds the Device’s Supplier Digital Signing Security Credentials, so including the Supplier’s:

* Entity Identifier;
* Remote Party Role; and
* Digital Signing Public Key.

Where a Device supports the processing of Remote Party Messages, that Device:

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

When verifying a Cryptographic Protection applied to a Command Instance it receives, a Device shall use the Remote Party Security Credentials that it holds at the time of Command processing.

Devices shall only be capable of replacing Remote Party Security Credentials on receipt of an Update Security Credentials Command specified in this GBCS.

#### 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 unencrypting encrypted data in Commands from the supplier and 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 by the Communications Hub (CHF) to verify the accessControlBroker’s signature on Commands addressed to the Communications Hub |
| 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 |

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

#### Mapping a Command to the Remote Party Security Credentials to be used in verifying the Command’s cryptographic protections

Except for the Security Credentials related Commands (see Section 13), a Device shall apply the requirements of this Section 4.3.2.7 to identify which of the Remote Party Public Keys that it holds are to be used to verify the cryptographic protections on a Command.

##### Message Authentication Codes

Where a Command is a Prepayment Top Up Command, the supplier MAC in that Command shall be verified using the Public Key in Trust Anchor Cell {**remotePartyRole** *supplier*, **keyUsage** *keyAgreement,* **cellUsage** *prePaymentTopUp*}, along with the Device’s Key Agreement Private Key.

All other MACs in Commands shall be verified using the Public Key in Trust Anchor Cell {**remotePartyRole** *accessControlBroker*, **keyUsage** *keyAgreement*, **cellUsage** *management*}, along with the Device’s Key Agreement Private Key.

##### Signature

Where a Command has a Digital Signature, the Device shall identify the Remote Party Role(s) which can legitimately sign the Command according to the message code identified in the Mapping Table.

If there is only one Remote Party Role so identified, then the signature shall be verified using the Public Key in Trust Anchor Cell {**remotePartyRole** *(the identified remote party role)*, **keyUsage** digitalSignature, **cellUsage** management}.

If there is more than one Remote Party Role so identified, the Device shall use the Business Originator ID in the Command to identify the Trust Anchor Cell(s) where:

* **keyUsage** = digitalSignature;
* **cellUsage** = management; and
* existingSubjectUniqueID = the Business Originator ID in the Command

If there is only one Trust Anchor Cell so identified, then the signature shall be verified using the Public Key in that Trust Anchor Cell.

If there is more than one Trust Anchor Cell so identified the Device shall attempt to verify the Digital Signature using each Trust Anchor Cell identified. These attempts shall be according to the following precedence, and attempts to verify shall cease when a signature verification succeeds:

1. supplier
2. wanProvider
3. networkOperator
4. accessControlBroker

For clarity, other Remote Party Roles on Devices are limited to Commands related to Security Credentials and so cannot have Trust Anchor Cells identified according to this Section 4.3.2.7.2.

#### Certification Path Validation

##### Access Control Broker requirements

Before it calculates the Access Control Broker to Device MAC (ACB-SMD MAC) in line with Section 6.2.3, the Access Control Broker shall undertake Certification Revocation List (CRL) Validation for any Organisation Certificate in a Command:

* either by using the algorithm specified in IETF RFC 5280[[8]](#footnote-8) Section 6.3; or
* by using functionality equivalent to the external behaviour resulting from that algorithm.

Only if the CRL Validation is successful shall the Access Control Broker calculate the ACB-SMD MAC. For clarity, the Access Control Broker shall never send a Message to a Device which contains any Certificate that has failed CRL Validation.

##### Device requirements

The requirements in this Section 4.3.2.8.2 shall apply only to Use Case CS02b (Update Security Credentials).

Where a Device has successfully completed all required Command Authenticity and Integrity checks on a Command of type covered by Use Case CS02b it has received, the Device shall undertake either:

* Certification Path Validation, including time checks; or
* Certification Path Validation, excluding time checks.

If the Device does not have Reliable Time (as defined in Use Cases GCS28 and ECS70 Set Clock) it shall always undertake Certification Path Validation, excluding time checks. Otherwise the validation to be undertaken shall be determined by the contents of the Remote Party Command Instance. For clarity, Device types which are not required to have a clock, shall always undertake Certification Path Validation, excluding time checks.

The Device shall undertake Certification Path Validation, including time checks:

* either by using the algorithm specified in IETF RFC 5280 Section 6.1; or
* by using functionality equivalent to the external behaviour resulting from that algorithm.

The Device shall undertake Certification Path Validation, excluding time checks:

* either by using the algorithm specified in IETF RFC 5280 Section 6.1 but not applying the check at 6.1.3 (a) (2) (‘the certificate validity period includes the current time’); or
* by using functionality equivalent to the external behaviour resulting from that algorithm where not applying the check that ‘the certificate validity period includes the current time’.

The ‘trust anchor’ information (with the meaning in IETF RFC 5280) shall be in the root Security Credentials held on the Device.

If the Device’s Certificate Path Validation does not confirm the required certification path validity, then the Device shall undertake no further processing of the Command, except for the issuance of a Response notifying that the Command was unsuccessful.

#### DLMS Client and Server

The Access Control Broker shall perform the role of DLMS COSEM client in relation to the DLMS COSEM Application Associations, and the Device shall perform the role of DLMS COSEM server.

### Cryptographic Primitives and their Usage

In relation to any Remote Party Message, Smart Metering Entities shall:

* use SHA-256, as specified in *FIPS* *180-4[[9]](#footnote-9)*, as the Hash function;
* use the AES-128 cipher, as specified in *FIPS 197[[10]](#footnote-10)*, as the block cipher primitive;
* use the Galois Counter Mode (GCM) mode of operation as specified in *NIST Special Publication 800-38D[[11]](#footnote-11)* ;
* use the GMAC technique, based on the use of AES-128, for the calculation of Message Authentication Codes (MACs), as specified in *NIST Special Publication 800-38D* (see above);
* use, as the Digital Signature technique, ECDSA (as specified in *FIPS PUB 186-4[[12]](#footnote-12)*) in combination with the curve P-256 (as specified in *FIPS PUB 186-4* at Section D.1.2.3) and SHA-256 as the Hash function. Within Messages, Signatures shall be in the Plain Format;
* use, to calculate the Shared Secret Z, the Static Unified Model, C(0e, 2s, ECC CDH) Key Agreement technique (as specified in *NIST Special Publication 800-56Ar2[[13]](#footnote-13)* save for the requirement to zeroize the Shared Secret) with:
  + - * the Single-step Key Derivation Function (KDF) based on SHA-256, as specified in *NIST Special Publication 800-56Ar2*; and
      * the P-256 curve for the elliptic curve operations.

Resulting DerivedKeyingMaterial (with its meaning in *NIST Special Publication 800-56Ar2*) shall only ever be used in relation to one Message Instance. Any Shared Secret that is not ‘zeroized’ shall be stored and used with the same security protections as Private Keys.

#### Scope of Cryptographic Protections

The fields that shall always contribute to MAC and Digital Signature are detailed in Section 7.2. Fields that vary across Messages are specified in Section 6, and in the relevant Use Cases. For clarity, a Message Instance may transit through multiple Smart Metering Entities before delivery to its target Device, and more than one Smart Metering Entity may be required to apply a Cryptographic Protection to that Message Instance. Thus, the scope of protection can only be across fields in the Message Instance as constructed at the point the protection is applied.

Where a Message has multiple Cryptographic Protections, the order in which the Smart Metering Entities apply these Cryptographic Protections is specified in this GBCS.

A Device verifying the Cryptographic Protections in such Messages shall undertake such verifications in the reverse sequence to that in which the Cryptographic Protections were applied. This order is also specified in this GBCS.

#### ECDSA per message secret number

When generating a Digital Signature, the Smart Metering Entity shall calculate the DSA Per-Message Secret Number ‘k’ with respect to ECDSA (with the meaning in Section 4.5 of *FIPS 186-4*) to be the SHA-256 hash of the concatenation of:

* the parts of the Message to be signed, as defined in Section 7.2.7; and
* the Private Key that the Smart Metering Entity will use in the Digital Signature generation.

If the value of k so calculated results in an ‘r’ or ‘s’ value of 0, where r and s have the meanings in the NSA’s ‘Suite B Implementor’s Guide to FIPS 186-3’, then a new value for k shall be calculated to be the SHA-256 hash of the concatenation of:

* the parts of the Message to be signed, as defined in Section 7.2.7;
* the Private Key that the Smart Metering Entity will use in the Digital Signature generation; and
* 0x00.

The addition of 0x00 to the concatenation shall be repeated until a value of k is generated that does not result in an ‘r’ or ‘s’ value of 0.

#### Calculating unique Shared Secret Keys for a Remote Party Message Instance

Where a Smart Metering Entity executes the KDF in relation to a Message Instance, the *OtherInfo* field, with the meaning in *NIST Special Publication 800-56Ar2*, shall be populated using the value of information provided in, or to be placed in, the originator-system-title, recipient-system-title and transaction-id fields of the Grouping Header, as per the requirements of Section 7.2.7.

The *OtherInfo* shall be in the Concatenation Format as defined in Section 5.8.1.2.1 of NIST Special Publication 800-56Ar2 and shall be the concatenation:

*AlgorithmID* || value of originator-system-title || length of transaction-id || value of transaction-id || value of recipient-system-title

where:

* *AlgorithmID* is that for AES-GCM-128 and so has a value 0x60857406080300, as specified by section 9.2.3.4.6.5 of the Green Book; and
* length of transaction-id has the value 0x09.

#### Calculating the Initialization Vector for GCM and GMAC

In relation to Remote Party Messages, Smart Metering Entities shall use a 96 bit Initialization Vector (IV) for the GCM and GMAC algorithms as defined in *NIST Special Publication 800-38D*. The IV shall be the concatenation

*FixedField* || *InvocationField*

where:

* *FixedField* = the Entity Identifier of the Smart Metering Entity that is creating, or has created, the Cryptographic Protection; and
* *InvocationField* = 0x00000000.

The DLMS COSEM Authentication Key (AK), as defined in the Green Book, shall not be present.

##### Other input parameters to MAC and Encryption / Decryption operations - informative

Other input parameters for MAC, Encryption and Decryption are not specified in this Section 4.3.3 because they vary dependent on a number of factors. These other input parameters are listed in tables of the same format as Table 4.3.3.4.1 and their values are specified in each part of the GBCS where such an operation is specified.

The template for such tables is the Table 4.3.3.4.1. Please note that this table does not contain any values as it is a template only.

| Input Parameter | Value | Note |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key |  |  |
| Public Key Agreement Key |  |  |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: |  |  |

Table 4.3.3.4.1: Template for other input parameters

##### Size of MAC

The bit length of the MAC shall be 96.

# Remote Party Message Construction, Protection and Verification – informative

Much of the content, processing and structure of Remote Party Messages is common across multiple Messages. The GBCS lays out such common requirements. This is to allow Use Cases to detail only those requirements that are specific to the Message(s) covered by that Use Case.

## Common Message Structures - informative

Parts of the structure and content of Remote Party Messages are common across multiple Remote Party Messages. These common parts of the structure and content are laid out in Section 7 of this GBCS. Section 7 also lays out specific requirements for DLMS COSEM and ZSE compliance for Devices compliant with this GBCS.

Note that Remote Party Messages in this GBCS are all constructed using aggregation structures. The GBCS does not allow for more granular message structures (e.g. for DLMS COSEM, individual set, get or action messages).

## Common Encryption and Decryption approach - informative

The content and processing of fields in relation to Confidentiality shall be common across all parts of Messages requiring such protections. Where specified in a Use Case, a Remote Party Message may contain one or more encrypted parts. For such requirements, the corresponding Authenticated Encryption and Authenticated Decryption shall always be undertaken using the approach laid out in Section 8.

Note that the GBCS does not require Encryption of the whole of a Message.

## Message Categories - informative

The content and processing of fields related to integrity, authenticity and non-repudiation varies according to whether:

* the Message is a Command, Response or Alert; and
* the Message is a Critical Message or not.

This leads to groupings which are referred to as Message Categories. Message Categories are structured in a hierarchical way, with the more generally applicable categories being at the tiers of the hierarchy with lower numbers. A category which is derived from another category (i.e. in a tier with a higher number) is called a subordinate Message Category. A category from which another category is derived (i.e. in a tier with a lower number) is called a superordinate Message Category. Figure 5.3 summarises the hierarchy.



Figure 5.3: Message Categories

Note that the ‘Command’ part of the hierarchy covers requirements for both the Command and the corresponding Response. Except in certain error cases (e.g. cryptographic processing failure), a Command always leads to a Response.

Section 6 is structured according to the hierarchy at Figure 5.3.

## Common Message Processing steps - informative

A common set of stages for Remote Party Message processing is used in this GBCS and the Use Cases, except for Variant Messages[[14]](#footnote-14). Variant Messages include Security Credentials and Prepayment Top Up related Messages.

The common set of stages for Commands is shown in Table 5.4a.

| **Name of Stage** | **Summary of the stage** | **Responsible Smart Metering Entity** |
| --- | --- | --- |
| 1. Command Construction | The Command is fully populated, apart from cryptographic fields | N/A  The entity undertaking this phase is not known to the Device  Although not apparent to the Device, the DSP’s Transform Service would normally undertake such construction for DCC managed Devices |
| 1. Command Cryptographic Protection I | This stage is only needed where a Remote Party, other than the Access Control Broker, is required to add Cryptographic Protection to the Command. So for digital signing of Critical Commands only | Known Remote Party |
| 1. Command Cryptographic Protection II | The Access Control Broker adds its Cryptographic Protection to the Message. This is by way of the ACB adding a MAC | Access Control Broker |
| 1. Command Authenticity and Integrity Verification | The Device undertakes the range of checks needed, including those to ensure authenticity of the sender and integrity of the Message.  This includes checking the Identifiers and Counter in the Command and verifying the Access Control Broker’s MAC | Device |

Table 5.4a: Common stages for Commands

That common set of stages for Responses is shown in Table 5.4b.

|  |  |  |
| --- | --- | --- |
| **Name of Stage** | **Summary of the stage** | **Responsible Smart Metering Entity** |

|  |  |  |
| --- | --- | --- |
| 1. Response Construction | The Response is fully populated by the Device, apart from cryptographic fields | Device |
| 1. Response Cryptographic Protection | The Device adds the required Cryptographic Protection to the Response | Device |
| 1. Response Recipient Verification | The Remote Party (Parties) can undertake the range of checks, including those to ensure authenticity of the sender and integrity of the Message | Remote Party named in the Response |

Table 5.4b: Common stages for Responses

That common set of stages for Alerts is shown in Table 5.4c.

|  |  |  |
| --- | --- | --- |
| **Name of Stage** | **Summary of the stage** | **Responsible Smart Metering Entity** |
| 1. Alert Construction | The Alert is fully populated by the Device, apart from cryptographic fields | Device |
| 1. Alert Cryptographic Protection | The Device adds the required cryptographic fields to the Alert | Device |
| 1. Alert Recipient Verification | The Remote Party (Parties) can undertake the range of checks, including those to ensure the authenticity of the sender and integrity of the Message | Remote Party named in the Alert |

Table 5.4c: Common stages for Alerts

The generic processing applied to Commands and their Responses (in relation to integrity, authenticity and non-repudiation) in a Message Category is summarised in Table 5.4d.



Table 5.4d: Generic Command and Response processing

The generic processing applied to Alerts in a Message Category is summarised in Table 5.4e.

Table 5.4e: Generic Alert processing

## Common processing stages and requirements for Devices operated through the DCC - informative

The sequence diagrams in the figures in this Section 5.5 illustrate the generic processing stages and common processing requirements, where a Device is operated via the DCC, for each of:

* SME.C.C: Critical Remote Party Command to a Device and the corresponding Remote Party Response (Figure 5.5a);
* SME.C.NC: non Critical Remote Party Command to a Device from a Known Remote Party and the corresponding Remote Party Response (Figure 5.5b);
* SME.A.C: Critical Alert from a Device (Figure 5.5c); and
* SME.A.NC: non Critical Alert from a Device (Figure 5.5d).

Note that only those parts of the sequence diagrams within yellow notes boxes are within the scope of the GBCS. The steps outside such boxes are provided for context and, where mandated, are mandated through mechanisms outside the GBCS, for example the Smart Energy Code.

For DCC managed Devices, the DSP would operate the services that provide (1) Access Control Broker, (2) Transform Service and (3) Transitional Change of Supplier. The CSPs would fulfil the role of WAN Provider.



Figure 5.5a: Sequence diagram for processing Critical Remote Party Commands and Responses



Figure 5.5b: Sequence diagram for processing non Critical Remote Party Commands and Responses



Figure 5.5c: Sequence diagram for processing Critical Remote Party Alerts



Figure 5.5d: Sequence diagram for processing non Critical Remote Party Alerts

# Message Categories

Requirements for the content and processing of fields in Remote Party Messages:

* related to integrity, Authenticity and non-repudiation; and
* common across groups of Remote Party Messages.

are laid out in this Section 6. Such groupings of Remote Party Messages are referred to as Message Categories.

Commands sent by a PPMID to a GSME and Responses to such Commands have requirements similar to Message Categories, and common requirements for this group of Messages are also laid out in this Section 6.

## Introduction - informative

Please see the Mapping Table for the mapping of Use Cases to the Message Categories in this Section 6.

## Message Category SME.C

### Definitions

The superordinate Message Category for SME.C is SME.

For a Message to be of Message Category SME.C it shall be a Command to a Device which is a Remote Party Message, or a Command from a PPMID to a GSME, or a Response to such Commands.

All SME.C Commands and any corresponding Response shall comply with the requirements of this Section 6.2 which covers:

* generation of a MAC by the Access Control Broker / PPMID and verification of that MAC by the Device; and
* validation by the Device of the Message Identifier.

### Processing Stages

The processing of each SME.C Command shall have the stages set out in Table 6.2.2a.

|  |  |
| --- | --- |
| **Stage** | **Responsible Smart Metering Entity** |

|  |  |
| --- | --- |
| 1. Command Construction | The entity undertaking this phase is not known to the Device |
| 1. Command Cryptographic Protection I | Known Remote Party |
| 1. Command Cryptographic Protection II | Access Control Broker / PPMID |
| 1. Command Authenticity and Integrity Verification | Device |

Table 6.2.2a: SME.C Command Processing Stages

For a Command, should any of the checks required in the Command Authenticity and Integrity Verification step fail, the Device shall take the steps laid out in Section 6.2.4.2. Otherwise the stages of processing set out in Table 6.2.2b shall be undertaken.

|  |  |
| --- | --- |
| **Stage** | **Responsible Smart Metering Entity** |
| 1. Response Construction | Device |
| 1. Response Cryptographic Protection | Device |
| 1. Response Recipient Verification | Remote Party named in the Response, or the PPMID named in the Response |

Table 6.2.2b: SME.C Response Processing Stages

#### Processing stages defined in the superordinate Message Category

There are no processing stages defined in the superordinate Message Category (SME).

#### Processing stages defined in subordinate Message Categories

There are no requirements for the following processing stages as they are wholly defined in subordinate Message Categories:

* Command Construction;
* Command Cryptographic Protection I;
* Response Construction;
* Response Cryptographic Protection; and
* Response Recipient Verification.

### Command Cryptographic Protection II

Requirements in this Section 6.2.3 for Command Cryptographic Protection II shall apply to Message Category SME.C and all subordinate categories.

For Remote Party Commands, the Access Control Broker shall calculate the Access Control Broker to Device Message Authentication Code (ACB-SMD MAC) using the parameters in Table 6.2.3a.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Access Control Broker’s |  |
| Public Key Agreement Key | Device’s | As identified by the Business Target ID in Message Identifier |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | Where a KRP Signature is present:  0x11 || Grouping Header || Command Payload|| 0x40 || KRP Signature  Where a KRP Signature is not present:  0x11 || Grouping Header || Command Payload || 0x00 |  |

Table 6.2.3a: Calculation of Access Control Broker to Device MAC

The ACB-SMD MAC for incorporation in the Command shall only be calculated once all fields of the Command are populated, as per requirements for the Command Construction and Command Cryptographic Protection I stages for the Message in question.

For HAN Only Commands from the PPMID to a GSME, the PPMID shall calculate the PPMID to GSME Message Authentication Code (PPMID-GSME MAC) using the parameters in Table 6.2.3b.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | PPMID’s |  |
| Public Key Agreement Key | GSME’s | As held by the PPMID in the GSME Trust Anchor Cell |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Command Payload || 0x00 |  |

Table 6.2.3b: Calculation of PPMID-GSME MAC

The PPMID-GSME MAC for incorporation in the Command shall only be calculated once all fields of the Command are populated, as per requirements for the Command Construction and Command Cryptographic Protection I stages for the Message in question.

### Command Authenticity and Integrity Verification

Requirements in this Section 6.2.4 shall apply to Message Category SME.C and all subordinate categories.

#### Checks to be undertaken

The Device shall undertake the checks set out in this Section 6.2.4.1 before undertaking any other processing of the Command.

##### Message Identifier Validation

To validate the Message Code and associated Message Structure, the Device shall verify that:

* the Message Code is for a Message that the Device is capable of processing, according to the associated Use Case; and
* the contents of the Message conform to the message formatting and structure requirements of this GBCS and the associated Use Case.

To validate the elements of Message Identifier within the Command Instance, whose structure is defined in Section 4.3.1.3, the Device shall verify that:

* the Business Target ID in the Command has the same value as the Device’s Entity Identifier;
* the Business Originator ID in the Command has the same value as the Entity Identifier held by the Device within a Trust Anchor Cell, where the Smart Metering Entity associated with that Trust Anchor Cell is allowed to request execution of a Command of this type, as specified by the Message Code in the Command and the Mapping Table (‘Use Case reference’ worksheet Message Code columns);
* if the Message is for immediate execution and the Message requires ‘Protection Against Replay’ according to the corresponding Use Case, the Originator Counter in the Command has a value that is greater than the value held by the Device for this type of Command in the corresponding Immediate Execution Counter; and
* if the Message is for future dated execution and the Message requires ‘Protection Against Replay’ according to the corresponding Use Case, the Originator Counter in the Command has a value that is greater than the value held by the Device for this type of Command in the Future Dated Counter.

##### ACB-SMD MAC Verification

To verify the ACB-SMD MAC in Remote Party Commands, the Device shall calculate a MAC using the parameters in Table 6.2.4.1.2 and ensure the MAC so calculated has the same value as the ACB-SMD MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Access Control Broker’s | As held by the Device in the Trust Anchor Cell {accessControlBroker, keyAgreement, management} |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | Where a KRP Signature is present:  0x11 || Grouping Header || Command Payload || 0x40 || KRP Signature  Where a KRP Signature is not present:  0x11 || Grouping Header || Command Payload || 0x00 |  |

Table 6.2.4.1.2: MAC calculation for ACB-SMD MAC verification

##### PPMID-GSME MAC Verification

To verify the PPMID-GSME MAC in HAN Only Commands from a PPMID to a GSME, the Device shall calculate a MAC using the parameters in Table 6.2.4.1.3 and ensure the MAC so calculated has the same value as the PPMID-GSME MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | GSME’s |  |
| Public Key Agreement Key | PPMID’s | As held by the GSME in the PPMID Trust Anchor Cell. |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Command Payload|| 0x00 |  |

Table 6.2.4.1.3: MAC calculation for PPMID-GSME MAC verification

#### Processing based on the outcome of checks

Should any of the checks, as required by this Section 6.2.4 Command Authenticity and Integrity Verification stage for this Message, fail then the Device shall:

* generate an entry in the Security Log recording failed Authentication;
* discard the Command without execution and without sending a Response; and
* send an Alert notifying the failed Authentication, constructed as specified in Section 6.7, populated with the relevant Alert Code from Section 16, to the Known Remote Party identified by the Security Credentials it holds in the Supplier role. If the Device is an ESME or a CHF, the Alert Payload shall be a DLMS COSEM Alert Payload. Otherwise, the Alert Payload shall be a GBZ Alert Payload.

Where all of the checks, as required of this Section 6.2.4 Command Authenticity and Integrity Verification stage for this Message, succeed the Device shall process the Command and produce a Response.

## Message Category SME.C.C

### Definitions

The superordinate Message Category for SME.C.C is SME.C.

For a Message to be of Message Category SME.C.C it shall be:

* a subordinate Message Category of Message Category SME.C;
* from or to a Remote Party; and
* a Critical Message.

A Device shall only be capable of processing the Critical Commands laid out in the GBCS.

All SME.C.C Commands and any corresponding Response shall comply both with the requirements for SME.C Messages and with the requirements of this Section 6.3 which covers:

* Digital Signing of the Command by the Known Remote Party;
* verification of the Digital Signature in the Command by the Device;
* Digital Signing of the Response by the Device; and
* verification of the Digital Signature in the Response by the Known Remote Party.

### Processing stages

#### Processing stages defined in the superordinate Message Category

There are no requirements additional to those of the superordinate Message Category (SME.C) for the Command Cryptographic Protection II stage.

#### Processing stages defined in subordinate categories

There are no requirements for the following processing stages as they are wholly defined in subordinate categories:

* Command Construction; and
* Response Construction.

### Command Cryptographic Protection I

Requirements in this Section 6.3.3 shall apply to Message Category SME.C.C and all subordinate categories.

The Remote Party originating the Command shall generate a Known Remote Party Signature (KRP Signature) for the Command.

The KRP Signature, for incorporation in the Command, shall only be generated once all fields of the Command Payload and Grouping Header are populated as per the requirements for the Command Construction stage, for the Message in question.

The KRP Signature shall be calculated across those fields of Grouping Header specified in Section 7.2.7 and all fields of the Command Payload, as specified in Section 7.2.7.

The Remote Party shall use its Private Digital Signing Key to generate the KRP Signature.

### Command Authenticity and Integrity Verification

Requirements in this Section 6.3.4 shall apply to Message Category SME.C.C and all subordinate categories.

The Device shall undertake the checks set out in this Section 6.3.4:

* only after all checks in Section 6.2.4.1 have been successfully completed; and
* before undertaking any other processing of the Command.

The Device shall use the Command Payload, Grouping Header and the Public Digital Signing Key of the Remote Party identified by the checks in Section 4.3.2.7.2 for Digital Signature verification of the KRP Signature.

The actions laid out in Section 6.2.4.2 shall then apply, as required by the success or failure of the Digital Signature verification.

### Response Cryptographic Protection

The Device creating the Response shall generate a Device Signature (SMD Signature) for the Response.

The SMD Signature, for incorporation in the Response, shall only be generated once all fields of the Response Payload and Grouping Header are populated, as per requirements for the Response Construction stage, for the Message in question.

The SMD Signature shall be calculated across those fields of Grouping Header specified in Section 7.2.7 and all fields of the Response Payload, as specified in Section 7.2.7.

The Device shall use its Private Digital Signing Key to generate the SMD Signature.

### Response Recipient Verification

A Remote Party may verify the SMD Signature in the Response by using the Response Body and the Public Digital Signing Key for the Device identified in the Response.

## Message Category SME.C.NC

### Definitions

For a Message to be of Message Category SME.C.NC, it shall be:

* a subordinate Message Category of Message Category SME.C;
* from or to a Remote Party; and
* not a Critical Message.

All SME.C.NC Commands and any corresponding Response shall comply both with the requirements for SME.C Messages and with the requirements of this Section 6.4 which covers:

* generation by the Device of a MAC for the Response; and
* verification of that MAC by the intended recipient of the Response.

### Processing stages

#### Processing stages defined in the superordinate Message Category

There are no requirements additional to those of the superordinate Message Category (SME.C) for the Command Cryptographic Protection II processing stage.

#### Processing stages defined in subordinate categories

There are no requirements for the following processing stages as they are wholly defined in subordinate categories:

* Command Construction; and
* Response Construction.

### Command Cryptographic Protection I

There are no additional requirements at the Command Cryptographic Protection I stage applicable to all Messages of Message Category SME.C.NC and any subordinate Message Category.

### Command Authenticity and Integrity Verification

There are no additional requirements at the Command Authenticity and Integrity Verification stage applicable to all Messages of Message Category SME.C.NC and any subordinate Message Category.

### Response Cryptographic Protection

Requirements in this Section 6.4.5 shall apply to Message Category SME.C.NC and all subordinate categories.

The Device shall calculate the Device to Known Remote Party MAC (SMD-KRP MAC) using the parameters in Table 6.4.5.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Known Remote Party’s | As held by the Device in the relevant Trust Anchor Cell {remotePartyRole, keyAgreement, management}. The relevant Cell will contain Business Originator ID as specified in Message Identifier. |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Response Payload || 0x00 |  |

Table 6.4.5: Calculation of Device to Known Remote Party MAC

The SMD-KRP MAC for incorporation in the Response shall only be calculated once all fields of the Response, except for the SMD-KRP MAC itself, are populated as per requirements for the Response Construction stage, for the Message in question.

### Response Recipient Verification

Requirements in this Section 6.4.6 shall apply to Message Category SME.C.NC and all subordinate categories.

The Remote Party, as identified by the Business Originator ID in the Response, may validate the SMD-KRP MAC in the Response by calculating a MAC using the parameters in Table 6.4.6 and comparing the MAC to the SMD-KRP MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Known Remote Party’s |  |
| Public Key Agreement Key | Device’s | As identified by the Business Target ID in Message Identifier |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Response Payload || 0x00 |  |

Table 6.4.6: MAC calculation for SMD-KRP MAC validation

## Message Category SME.C.PPMID-GSME

### Definitions

For a Message to be of Message Category SME.C.PPMID-GSME, it shall be:

* a subordinate Message Category of Message Category SME.C; and
* a Message between a PPMID and a GSME.

All SME.C.PPMID-GSME Commands and any corresponding Response shall comply both with the requirements for SME.C Messages and with the requirements of this Section 6.4 which covers:

* generation by the Device of a MAC for the Response; and
* verification of that MAC by the intended recipient of the Response.

### Processing stages

#### Processing stages defined in the superordinate Message Category

There are no requirements additional to those of the superordinate Message Category (SME.C) for the Command Cryptographic Protection II processing stage.

#### Processing stages defined in subordinate categories

There are no requirements for the following processing stages as they are wholly defined in subordinate categories:

* Command Construction; and
* Response Construction.

### Command Cryptographic Protection I

There are no additional requirements at the Command Cryptographic Protection I stage applicable to all Messages of Message Category SME.C.PPMID-GSME and any subordinate Message Category.

### Command Authenticity and Integrity Verification

There are no additional requirements at the Command Authenticity and Integrity Verification stage applicable to all Messages of Message Category SME.C.PPMID-GSME and any subordinate Message Category.

### Response Cryptographic Protection

Requirements in this Section 6.5.5 shall apply to Message Category SME.C.PPMID-GSME and all subordinate categories.

The GSME shall calculate the GSME to PPMID MAC (GSME-PPMID MAC) using the parameters in Table 6.5.5.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | PPMID’s | As held by the GSME in the PPMID Trust Anchor Cell |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Response Payload || 0x00 |  |

Table 6.5.5: Calculation of GSME-PPMID MAC

The GSME-PPMID MAC for incorporation in the Response shall only be calculated once all fields of the Response, except for the GSME-PPMID MAC itself, are populated as per requirements for the Response Construction stage, for the Message in question.

### Response Recipient Verification

Requirements in this Section 6.5.6 shall apply to Message Category SME.C.PPMID-GSME and all subordinate categories.

The PPMID, as identified by the Business Originator ID in the Response, shall validate the GSME-PPMID MAC in the Response by calculating a MAC using the parameters in Table 6.5.6 and comparing the MAC to the GSME-PPMID MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | PPMID’s |  |
| Public Key Agreement Key | GSME’s | As held by the PPMID in the GSME Trust Anchor Cell |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation : | 0x11 || Grouping Header || Response Payload || 0x00 |  |

Table 6.5.6: MAC calculation for GSME-PPMID MAC validation

## Message Category SME.A

### Definitions

The superordinate Message Category for SME.A is SME.

For a Message to be of Message Category SME.A it shall be an Alert from a Device which is addressed to a Remote Party.

There are no common requirements that shall be applied to all Messages of Message Category SME.A.

### Processing Stages

The processing of each SME.A Alert shall have the stages set out in Table 6.6.2:

|  |  |
| --- | --- |
| **Stage** | **Responsible Smart Metering Entity** |
| 1. Alert Construction | Device |
| 1. Alert Cryptographic Protection | Device |
| 1. Alert Recipient Verification | Remote Party named in the Alert. |

Table 6.6.2: SME.A Processing Stages

#### Processing stages defined in the superordinate Message Category

There are no processing stages defined in the superordinate Message Category (SME).

#### Processing stages defined in subordinate categories

There are no requirements for the following processing stages as they are wholly defined in subordinate categories:

* Alert Construction;
* Alert Cryptographic Protection; and
* Alert Recipient Verification.

## Message Category SME.A.C

### Definitions

For a message to be categorised as Message Category SME.A.C, it shall be:

* a subordinate Message Category of Message Category SME.A; and
* a Critical Message.

All SME.A.C Messages shall comply both with the requirements for SME.A Messages and with the requirements of this Section 6.7 which covers:

* Digital Signing of the Alert by the Device; and
* Verification of the Digital Signature in the Alert by the Remote Party.

### Processing stages

#### Processing stages defined in the superordinate Message Category

There are no processing stages defined in the superordinate Message Category (SME.A).

#### Processing stages defined in subordinate categories

There are no requirements for the Alert Construction processing stage as they are wholly defined in subordinate categories.

### Alert Cryptographic Protection

Requirements in this Section 6.7.3 shall apply to Message Category SME.A.C and all subordinate categories.

The Device creating the Alert shall generate a Device Signature (SMD Signature) for the Alert.

The SMD Signature, for incorporation in the Alert, shall only be generated once all fields of the Alert Payload and Grouping Header are populated, as per requirements for the Alert Construction stage for the Message in question.

The SMD Signature shall be calculated across those fields of Grouping Header and all fields of the Alert Payload, both as specified in Section 7.2.7.

The Device shall use its Private Digital Signing Key to generate the SMD Signature.

### Alert Recipient Verification

Requirements in this Section 6.7.4 shall apply to Message Category SME.A.C and all subordinate categories.

A Remote Party may verify the SMD Signature in the Alert by using the Alert Payload, Grouping Header and the Public Digital Signing Key for the Device, as identified in the Alert.

## Message Category SME.A.NC

### Definitions

For a Message to be of Message Category SME.A.NC it shall be:

* a subordinate Message Category of Message Category SME.A; and
* not a Critical Message.

All SME.A.NC Messages shall comply both with the requirements for SME.A Messages and with the requirements of this Section 6.8 which covers:

* generation by the Device of a MAC for the Alert and validation of that MAC by the intended recipient of the Alert.

### Processing stages

#### Processing stages defined in the superordinate Message Category

There are no processing stages defined in the superordinate Message Category (SME.A).

#### Processing stages defined in subordinate categories

There are no requirements for the Alert Construction processing stage as they are wholly defined in subordinate categories.

### Alert Cryptographic Protection

Requirements in this Section 6.8.3 shall apply to Message Category SME.A.NC and all subordinate categories.

The Device shall calculate the Device to Known Remote Party MAC (SMD-KRP MAC) using the parameters in Table 6.8.3.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Known Remote Party’s | As held by the Device in the relevant Trust Anchor Cell {remotePartyRole, keyAgreement, management}. The relevant Trust Anchor Cell will contain Business Originator ID as specified in Message Identifier. |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Alert Payload || 0x00 |  |

Table 6.8.3: Calculation of the Device to Known Remote Party MAC

The SMD-KRP MAC for incorporation in the Alert shall only be calculated once all fields of the Alert, except for the SMD-KRP MAC itself, are populated as per requirements for the Alert Construction stage, for the Message in question.

### Alert Recipient Verification

Requirements in this Section 6.8.4 shall apply to Message Category SME.A.NC and all subordinate categories.

The Remote Party, as identified by the Business Originator ID in the Alert, may validate the SMD-KRP MAC in the Alert by calculating a MAC using the parameters in Table 6.8.4 and comparing the MAC to the SMD-KRP MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Known Remote Party’s |  |
| Public Key Agreement Key | Device’s | As identified by the Business Originator ID in Message Identifier |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || Alert Payload || 0x00 |  |

Table 6.8.4: MAC calculation for SMD-KRP MAC verification

# Message structure and DLMS COSEM / ZSE / ASN.1 requirements

## Introduction - informative

This Section 7:

* defines the structure of Remote Party Messages containing DLMS COSEM, ASN.1 and GBZ Payloads. A GBZ Payload is a Payload containing one or more ZSE messages;
* defines the structure of Messages between a PPMID and a GSME on the same SMHAN; and
* lays out specific requirements for DLMS COSEM and ZSE compliance to which Devices shall adhere.

Note that Remote Party Messages all use an aggregation structure which allows for multiple, protocol-specific instructions within the same Message. The aggregation structures are used for all Messages, are based on xDLMS access service, general signing service and general ciphering service formats, and provide protections across all types of Message payload (be they DLMS COSEM, ZSE or security related).

The GBCS does not provide more granular Message structures (e.g. for DLMS COSEM, individual set, get or action messages).

SMETS and CHTS require that the Critical Commands mandated by them (and so those defined in the GBCS) are the only Critical commands allowed. Devices may implement additional non Critical features only.

It should be noted that:

* SMETS only requires DLMS COSEM certification on the ESME;
* any action that the Known Remote Party takes to remedy a failure will need to factor in that some of the instructions succeeded and others did not;
* in ASN.1 notation, the signature field in the general-signing service is a variable length OCTET STRING. When encoded, this means that the length of the signature needs to be incorporated before the actual signature value. The length is either 64 (0x40) if a signature is present or 0 (0x00) if signature is not present;
* these requirements are to ensure that all Devices behave consistently and in the way required by originating Remote Party requests, including in error states; and
* the WAN Provider may read CHF Operational Data and CHF Configuration Data, with their CHTS meanings, using mechanisms other than those defined in this GBCS.

## Message Construction - general

This Section 7.2 shall apply to Messages which are of a Message Category that is not ‘Variant’. For Messages of a Message Category that is ‘Variant’, this Section 7.2 shall only apply where explicitly stated in the Use Case, with the exception of Section 7.2.11 which shall apply to all Messages.

Except for elements detailed as being defined in the ZSE or ZCL specifications, the octet strings constructed in compliance with this Section 7 shall be in ‘big endian’ order according to IETF RFC 1700[[15]](#footnote-15). Elements detailed in this Section 7 as being defined in the ZSE or ZCL specifications, shall be serialised into the corresponding parts of octet strings as defined in the corresponding ZSE or ZCL specification.

### Commands

Whether a Command requires a KRP Signature is specified in the corresponding Message Category requirements in Section 6.

Where a KRP Signature is required, a Remote Party Command received by a Device shall be the concatenation:

MAC Header || Grouping Header || Command Payload || 0x40 || KRP Signature || ACB-SME MAC

Where a KRP Signature is not required, a Remote Party Command received by a Device shall be the concatenation:

MAC Header || Grouping Header || Command Payload || 0x00 || ACB-SME MAC

A HAN Only Command from a PPMID to a GSME shall be the concatenation:

MAC Header || Grouping Header || Command Payload || 0x00 || PPMID-GSME MAC

### Responses

Whether a Response requires an SMD Signature is specified in the corresponding Message Category requirements in Section 6.

Where a SMD Signature is required, a Remote Party Response shall be the concatenation:

Grouping Header || Response Payload || 0x40 || SMD Signature

Where a SMD Signature is not required, a Remote Party Response shall be the concatenation:

MAC Header || Grouping Header || Response Payload || 0x00 || SMD-KRP MAC

A HAN Only Response from a GSME to a PPMID shall be the concatenation:

MAC Header || Grouping Header || Response Payload || 0x00 || GSME-PPMID MAC

### Alerts

Whether an Alert requires an SMD Signature is specified in the corresponding Message Category requirements in Section 6.

Where a SMD Signature is required, a Remote Party Alert shall be the concatenation:

Grouping Header || Alert Payload || 0x40 || SMD Signature

Where a SMD Signature is not required, a Remote Party Alert shall be the concatenation:

MAC Header || Grouping Header || Alert Payload || 0x00 || SMD-KRP MAC

### Payload sequence and Break On Error

All Message Payloads - Command Payloads, Response Payloads and Alert Payloads - shall:

* only be constructed in the sequence specified in the corresponding Use Case;
* only be processed in the sequence specified in the corresponding Use Case; and
* be processed by a recipient Device on a Break On Error basis.

Where a Command Payload contains multiple instructions, processing of instructions shall cease at the point any one instruction fails. A ZSE command returning a status of ‘NOT\_FOUND’ shall not be treated as a failure. The corresponding element in the Response Payload shall detail that instruction's failure, and shall explicitly detail that all subsequent instructions also failed to execute. The specific result codes shall be as specified in the relevant ZSE / DLMS COSEM document, or in this GBCS where standard-based error codes do not exist. Where execution of instructions was not attempted due to the Break On Error requirement, the response shall return:

* for DLMS instructions, a Data-Access-Result / Action-Result of other-reason;
* for ZCL / ZSE instructions, a ZCL / ZSE status value of FAILURE (0x01).

### Message Construction – MAC Header

The required components of the MAC Header shall be populated with the values as per Table 7.2.5.[[16]](#footnote-16)

| **MAC Header** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | General-Ciphering | 0xDD | 1 | xDLMS APDU tag for General-Ciphering (221 in decimal) |
|  | transaction-id | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | originator-system-title | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | recipient-system-title | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | date-time | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | other-information | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | key-info | 0x00 | 1 | Key-info values are not present so encoded as 0x00 |
|  | ciphered-service |  |  |  |
|  | Length | Encoding(X) | Len(Encoding(X)) | X shall be the length in octets of the subsequent parts of the Message after this Length value. This includes the security header, the DLMS APDU being protected and the MAC |
|  | security header |  |  |  |
|  | security control byte (SC) | 0x11 | 1 | Bits 3..0 are security suite which is 0b0001 since Security Suite 1 is required  Bit 4 is set to 0b1 since Authentication of the APDU is required.  Bit 5 is set to 0b0 since the whole of an APDU is never encrypted  Bit 6 is set to 0b0 since messages with MACs are unicast  Bit 7 is set to 0b0 as per the Green Book |
|  | invocation counter (IC) | 0x00000000 | 4 | IC is always zero as specified in Section 8.4 |

Table 7.2.5: Required components of MAC Header

### Additional Authenticated Data (AAD) for the MAC calculation – informative

Terms in italics in this Section 7.2.6 shall have the meanings as specified in Green Book.

The Green Book requires that the AAD used as input to the MAC calculation is the concatenation of:

SC II AK II transaction-id II originator-system-title II recipient-system-title II date-time II other-information II information to be protected

The Green Book also requires that, for the elements contributing to AAD, only the values of the octet strings are included. The Green Book defines octet strings within the general-ciphering service in ASN.1 as:

*General-Ciphering ::= SEQUENCE*

*{*

*transaction-id OCTET STRING,*

*originator-system-title OCTET STRING,*

*recipient-system-title OCTET STRING,*

*date-time OCTET STRING,*

*other-information OCTET STRING,*

*key-info OPTIONAL,*

*ciphered-service OCTET STRING*

*}*

As stated in Table 7.2.5, in GBCS-compliant APDUs:

* SC takes the value 0x11; and
* the following octet strings in the general-ciphering service shall have zero length and so have no value:
  + - * transaction-id,
      * originator-system-title,
      * recipient-system-title,
      * date-time,
      * other-information.

As required by Section 4.3.3.4, AK is always absent.

Thus, the AAD to be used in MAC calculations that protect APDUs is the concatenation:

0x11 II information to be protected

### Message Construction - Grouping Header

The following shall be the required components of the Grouping Header and shall be populated with the values as per Table 7.2.7.

Where a Signature is required in a message, it shall be calculated using only those attributes marked ‘Yes’ in the ‘Input to the ECDSA calculation’ column of Table 7.2.7, in the sequence they appear in the table.

Thus, a KRP Signature or SMD Signature shall be calculated across the concatenation:

Business Originator ID || Business Target ID || Originator Counter || date-time (if present) Message Code || Supplementary Remote Party ID (if present) || Supplementary Remote Party Counter (if present) II Supplementary Originator Counter (if present) || Supplementary Remote Party Key Agreement Certificate (if present) || (information to be protected)

where (information to be protected) shall be:

* the Command Payload in a Command;
* the Response Payload in a Response; or
* the Alert Payload in an Alert.

| **Grouping Header** | | | | |
| --- | --- | --- | --- | --- |
| **Input to the ECDSA calculation** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
| No | General-Signing | 0xDF | 1 | xDLMS APDU tag for General-Signing (223 in decimal) |
|  | transaction-id |  |  |  |
| No | length | 0x09 | 1 | Length of Originator Counter plus 1 |
| Yes | value | CRA Flag || Originator Counter | 9 | CRA Flag shall be:  0x01 for Commands  0x02 for Responses  0x03 for Alerts |
|  | originator-system-title |  |  |  |
| No | length | 0x08 | 1 | Length of Entity Identifier |
| Yes | value | Business Originator ID | 8 |  |
|  | recipient-system-title |  |  |  |
| No | length | 0x08 | 1 | Length of Entity Identifier |
| Yes | value | Business Target ID | 8 |  |
|  | date-time |  |  |  |
| No | length | 0x00 where no date / time is required in this Message  0x0C where a date / time field is required | 1 | Where date-time is not required for a Message, it shall be a 0 octet string as per the DLMS specification  Where date-time is required for a Message, it shall be a 12 octet string as per the DLMS specification. See ‘date-timestamp in response’ column, ‘Use Case reference’ tab in Mapping Table |
| Yes | value | Either empty or a 12 character octet-string containing the date-time stamp for this Response | 0 or 12 |  |
|  | other-information |  |  |  |
| No | length | Encoding(X) | variable  Len(Encoding(X)) | X is length of other information octet string. X is 2 or 18 or 26 or variable |
| Yes | value | Message Code || Supplementary Remote Party ID || Supplementary Remote Party Counter || Supplementary Originator Counter || Supplementary Remote Party Key Agreement Certificate | 2 or 18 or 26 or variable | The Message Code shall always be present  In an Alert, Supplementary Remote Party ID shall be present, if it is required by Section 16  In a Command or Response, the Supplementary Remote Party ID, Supplementary Remote Party Counter and Supplementary Originator Counter, shall be present or not in line with the requirements of Section 4.3.1.4  Supplementary Remote Party Key Agreement Certificate shall only be present where (1) this is a Command, (2) the Response to it should contain encrypted attributes and (3) the Supplementary Remote Party ID is for a Remote Party which does not already have a Key Agreement Public Key on the Device. It may only be present in Commands marked as allowing it in the column ‘Key Agreement Certificate Potentially in Command?’ of the Use Case reference tab of the Mapping Table |
|  | Content |  |  |  |
| No | length | Encoding(X) | Len(Encoding(X)) | X is the length in octets of the Message Payload |

Table 7.2.7: Required components of Grouping Header

### Message Construction – ASN.1 Security Payloads

For Messages containing ASN.1 Security Payloads,, the Payloads shall be constructed as detailed in the Use Case for that Message Code (as defined by the Mapping Table).

### Message Construction – DLMS COSEM Payloads

For Messages containing DLMS COSEM payloads (as defined by the Message Code and Use Cases in Section 19):

* any Command Payload shall comply with the requirements of Table 7.2.9a and the associated Use Case;
* any Response Payload shall comply with the requirements of Table 7.2.9b and the associated Use Case; and
* any Alert Payload shall comply with the requirements of Table 7.2.9c and the associated Use Case.

| **DLMS COSEM Payloads – Commands** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | access-request | 0xD9 | 1 | xDLMS APDU tag for Access Request (217 in decimal) |
|  | long-invoke-id-and-priority | 0x20 || Least significant 24 bits of Originator Counter | 4 | Construction explained in rows below detailing bit (31..0) usage |
|  | (bits 0-23) invoke-id | Least significant 24 bits of Originator Counter |  |  |
|  | (bits 24 -27) reserved | 0b0000 |  | Fixed value |
|  | (bit 28) self-descriptive | 0b0 |  | Not-Self-Descriptive |
|  | (bit 29) processing-option | 0b1 |  | Break on Error |
|  | (bit 30) service-class | 0b0 |  | Unconfirmed |
|  | (bit 31) priority | 0b0 |  | Normal |
|  | date-time | 0x00 | 1 | A value for this element is not present so the length field is 0x00 |
|  | access-request-body |  |  |  |
|  | access-request-specification |  |  |  |
| *1* | *SEQUENCE OF* | *Use Case specific* | *1* | *The total number of gets, sets and actions in the Use Case (means that there will be less than 128 in total). This content is specified in each DLMS COSEM Use Case* |
| *2* | *Use Case Specific Content* | *Use Case specific* |  | *The list of Gets, Sets and Actions specific to the Use Case. This content is specified in each DLMS COSEM Use Case* |
|  | access-request-list-of-data |  |  |  |
|  | list-of-data |  |  |  |
| *3* | *SEQUENCE OF Data* | *Use Case specific* | *1* | *The total number of attributes in the list-of-data in the Use Case (means that there will be less than 128 in total). This content is specified in each DLMS COSEM Use Case* |
| *4* | *Use Case Specific Content* | *Use Case specific* | *Use Case set* | *Values of the attributes required by the Use Case. This content is specified in each DLMS COSEM Use Case* |

Table 7.2.9a: Required components of Command Payload

Elements marked in Table 7.2.9a as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 19).

| **DLMS COSEM Payloads – Responses** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | access-response | 0xDA | 1 | xDLMS APDU tag for Access Response (218 in decimal) |
|  | long-invoke-id-and-priority | 0x20 || Least significant 24 bits of Originator Counter | 4 |  |
|  | date-time | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | access-response-body |  |  |  |
|  | access-request -specification OPTIONAL | 0x00 | 1 | Not present so false (0x00) |
|  | access-response-list-of-data |  |  |  |
|  | list-of-data |  |  |  |
| *5* | *SEQUENCE OF Data* | *Use Case specific* | *1* | *The total number of attributes in the Response in the Use Case. This content is specified in each DLMS COSEM Use Case* |
| *6* | *Use Case Specific Content* | *Use Case specific* | *Use Case set* | *Values of the attributes required by the Use Case. This content is specified in each DLMS COSEM Use Case* |
|  | access-response-specification |  |  |  |
| *7* | *SEQUENCE OF CHOICE* | *Use Case specific* | *1* | *The total number of responses, including the 1 here and those in the Use Case* |
| *8* | *Use Case Specific Content* | *Use Case specific* | *Use Case set* | *Fields stating the result of each Gets, Sets and Actions specific to the Use Case.* |

Table 7.2.9b: Required components of Response Payload

Elements marked in Table 7.2.9b as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 19).

| **DLMS COSEM Payloads – Alerts** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | data-notification | 0x0F | 1 | xDLMS APDU tag for data-notification (15 in decimal) |
|  | long-invoke-id-and-priority | 0x20 || least significant 24 bits of Originator Counter | 4 |  |
|  | date-time | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | notification-body |  |  |  |
|  | structure | 0x02 | 1 |  |
| *1* | *SEQUENCE OF Data* | *0x02 unless there is Use Case specific data additional* | *1* | *The majority of Alerts do not contain any additional data. For Alerts without additional data, there is no corresponding Use Case (since there is no Use Case specific content).*    *Where an Alert does contain additional content, it has a specific Use Case. The additional content is specified in each such Use Case. In such cases, this field shall contain the total number of Data in the Use Case sequence plus the one in this template* |
|  | Data |  |  |  |
|  | Tag | 0x12 | 1 | Tag for LONG UNSIGNED |
|  | Value | Alert Code | 2 | The Alert Code for this Alert, shall be as defined in Section 16 |
|  | Data |  |  |  |
|  | Tag | 0x09 | 1 | Tag for octet-string |
|  | Length | 0x0C | 1 | Twelve characters long as DLMS date times are octet-string(12) |
|  | Value | Time Stamp | 12 | The time stamp for this Alert, shall be as defined in Section 16 |
| *2* | *Use Case Specific Additional Content* | *Use Case specific* | *Use Case* | *See Note at row 1, which means that, for most Alerts, there will be no Use Case specific content.* |

Table 7.2.9c: Required components of Alert Payload

Elements marked in Table 7.2.9c as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 19).

### Message Construction – GBZ Payloads

A GBZ Payload shall be a Payload containing one or more ZSE / ZCL commands. For clarity, this includes Payloads in HAN Only Commands between a PPMID and a GSME.

For Messages containing GBZ Payloads (as defined by the Mapping Table):

* any Command Payload shall comply with the requirements of Table 7.2.10a and the associated Use Case;
* any Response Payload shall comply with the requirements of Table 7.2.10b and the associated Use Case; and
* any Alert Payload shall comply with the requirements of Table 7.2.10c and the associated Use Case.

Each GBZ Use Case Specific Component shall comply with:

* Table 7.2.10d if the ZSE / ZCL command within it is not encrypted; or
* Table 7.2.10e if the ZSE / ZCL command within it is encrypted.

| **GBZ Payloads – Commands** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | Profile ID | 0x0109 | 2 | ZSE |
| *1* | *Total number of GBZ Use Case Specific Component(s)* | *See ‘Note’ column* | *1* | *This octet is to be interpreted as an 8 bit unsigned integer specifying the total number of GBZ Use Case Specific Component(s)* |
|  |  |  |  |  |
| *2* | *GBZ Use Case Specific Component(s)* | *Use Case specific* |  | *See Tables 7.2.10d and 7.2.10e* |

Table 7.2.10a: Required components of GBZ Command Payload

Elements marked in Table 7.2.10a as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 15).

| **GBZ Payloads – Response** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | Profile ID | 0x0109 | 2 | ZSE |
| *1* | *Total number of GBZ Use Case Specific Component(s)* | *See ‘Note’ column* | *1* | *This octet is to be interpreted as an 8 bit unsigned integer specifying the total number of GBZ Use Case Specific Component(s) in this Message* |
| *2* | *GBZ Use Case Specific Component(s)* | *Use Case specific* |  | *See Tables 7.2.10d and 7.2.10e* |

Table 7.2.10b: Required components of GBZ Response Payload

Elements marked in Table 7.2.10b as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 15).

| **GBZ Payloads – Alerts** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | Profile ID | 0x0109 | 2 | ZSE |
| *1* | *Total number of GBZ Use Case Specific Component(s)* | *See ‘Note’ column* | *1* | *This octet is to be interpreted as an 8 bit unsigned integer specifying the total number of GBZ Use Case Specific Component(s)* |
|  | Alert Code | See ‘Note’ column | 2 | The Alert Code for this Alert as defined in Section 16 |
|  | Timestamp | UTCTime | 4 | The *UTCTime*, with its ZCL meaning, at which this Alert was created |
| *2* | *GBZ Use Case Specific Component(s)* | *Use Case specific* |  | *See Tables 7.2.10d and 7.2.10e* |

Table 7.2.10c: Required components of GBZ Alert Payload

Elements marked in Table 7.2.10c as Use Case specific shall be populated according to the Use Case for the Message Code (see Section 15).

| **GBZ Use Case Specific Component without encrypted content** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | Extended Header Control Field | 0x00  Or  0x01 | 1 | 0x00 (if not the last GBZ Use Case Specific Component in this Message)  Or  0x01 (if the last GBZ Use Case Specific Component in this Message) |
|  | Extended Header Cluster ID | See ‘Note’ column | 2 | The Cluster ID of the ZSE / ZCL command contained in this GBZ Use Case Specific Component |
|  | Extended Header GBZ Command Length | See ‘Note’ column | 2 | These two octets shall be interpreted as a 16 bit unsigned integer specifying the total length on octets of the remainder of this GBZ Component (so excluding this and prior fields) |
|  | ZCL header | Use Case specific | 3 | These fields shall have the meaning specified in the ZSE / ZCL Specifications except for the Transaction Sequence Number. The Transaction Sequence Number shall be set to 0 for the first request-style ZSE / ZCL command in the Message and shall be incremented by one for every subsequent request-style ZSE / ZCL command frame in the Message. The corresponding response-style ZSE / ZCL command frame shall copy the Transaction Sequence Number from the request-style ZSE / ZCL command frame |
|  | ZCL payload | Use Case specific | Variable | These fields shall have the meaning specified in the ZSE / ZCL specifications |

Table 7.2.10d: Required components of GBZ Use Case Specific Component without encrypted content

| **GBZ Use Case Specific Component with encrypted content** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | Extended Header Control Field | 0x02  Or  0x03 | 1 | 0x02 (if not the last GBZ Use Case Specific Component in this Message)  Or  0x03 (if the last GBZ Use Case Specific Component in this Message) |
|  | Extended Header Cluster ID | See ‘Note’ column | 2 | The Cluster ID of the ZCL Command contained in this GBZ Use Case Specific Component |
|  | Extended Header GBZ Command Length | See ‘Note’ column | 2 | These two octets shall be interpreted as a 16 bit unsigned integer specifying the total length in octets of the remainder of this GBZ Component (so excluding this and prior fields but including the 2 octets of Additional Header) |
|  | Additional Header Control | 0x00 | 1 | Reserved for future extensibility |
|  | Additional Header Frame Counter | See ‘Note’ column | 1 | This octet is to be interpreted as an 8 bit unsigned integer. Its value shall be 0x00 for the first GBZ Use Case Specific Component with encrypted content in a Message. The value shall increase by one in each subsequent GBZ Use Case Specific Component with encrypted content in a Message |
|  | ZCL header | See ‘Note’ column | 3 | These fields shall have the meaning specified in the ZigBee Cluster Library |
|  | Length of Ciphered Information | See ‘Note’ column | 2 | These two octets shall be interpreted as a 16 bit unsigned integer specifying the total length in octets of the Ciphered Information |
|  | Ciphered Information | See ‘Note’ column | Variable | See Section 8.4 |

Table 7.2.10e: Required components of GBZ Use Case Specific Component with encrypted content

### Transfer of Large Remote Party Messages

All Devices which are not Type 2 Devices shall be capable of supporting the General Block Transfer (GBT) requirements of this Section 7.2.11.

#### GBT Terminology and Parameters[[17]](#footnote-17)

A GBT Message shall be an APDU constructed and processed as defined by this Section 7.2.11.

A GBT Message Series shall be the set of GBT Messages needed to exchange one complete Remote Party Message between a GBT Initiator and a GBT Recipient.

For a Remote Party Command sent using a GBT Message Series, the GBT Initiator shall be the Access Control Broker and the GBT Recipient shall be the target Device.

For a Remote Party Response or a Remote Party Alert sent using a GBT Message Series, the GBT Initiator shall be the sending Device and the GBT Recipient shall be the Access Control Broker.

A GBT Third Party shall be the Remote Party identified by:

* in a Remote Party Command, the value in the Business Originator ID field; and
* in a Remote Party Response or a Remote Party Alert, the value in the Business Target ID field.

GBT Streaming Window shall be the number of GBT Messages the GBT Initiator sends without receipt of a GBT Message (Acknowledgement), or since receipt of the most recent GBT Message (Acknowledgement).

GBT Streaming Window shall be:

* 63 where the GBT Message Series carries a Remote Party Response; and
* 5 where the GBT Message Series carries a Remote Party Command.

Maximum PDU Size shall be 1200 octets.

#### Remote Party Message size

Where a Remote Party Message exceeds the Maximum PDU Size, the GBT Initiator and the GBT Responder shall exchange the Remote Party Message in a GBT Message Series.

Where a Remote Party Message does not exceed the Maximum PDU Size, the GBT Initiator and the GBT Responder may exchange the Remote Party Message in a GBT Message Series.

#### GBT Message Structure

A GBT Message shall, if it is a GBT Message (Acknowledgement) or a GBT Message (Request Block Resend), be the concatenation:

Message Routing Header || GBT Header

A GBT Message shall, if it is neither a GBT Message (Acknowledgement) nor a GBT Message (Request Block Resend), be the concatenation:

Message Routing Header || GBT Header || GBT Block Data

where:

* Message Routing Header shall be structured and populated according to Table 7.2.11.5. Note that Message Routing Header (1) uniquely identifies the GBT Message Series, (2) identifies whether the GBT Message is being sent to or from the Device and (3) unambiguously ties all GBT Messages in the GBT Message Series to the single Remote Party Message being exchanged;
* GBT Header shall be structured and populated according to Table 7.2.11.6; and
* GBT Block Data shall be the part of the Remote Party Message, constructed as per Section 7.2.11.4, being carried in this GBT Message.

#### 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 bytes;
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 bytes; 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 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.

When a GBT Recipient receives a GBT Message with ‘block-number’ being an integer multiple of GBT Streaming Window for this GBT Message Series, it shall send a GBT Message (Acknowledgement).

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.

#### Message Routing Header

| **Message Routing Header** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | general-ciphering | 0xDD | 1 | Tag used is the same as for a normal DLMS General-Ciphering header |
|  | transaction-id |  |  |  |
|  | Length | 0x09 | 1 | Length of Originator Counter |
|  | Value | See ‘Note’ column | 9 | Shall be populated with the corresponding field from the Grouping Header in the Remote Party Message that is being carried in this GBT Message Series |
|  | originator-system-title |  |  |  |
|  | Length | 0x08 | 1 | Length of Entity Identifier |
|  | Value | Business Originator ID | 8 | If the GBT Message is sent from the Device, the value shall be the Entity Identifier of the Device.  If the GBT Message is sent to the Device, the value shall be the Entity Identifier of the GBT Third Party |
|  | recipient-system-title |  |  |  |
|  | Length | 0x08 | 1 | Length of Entity Identifier |
|  | Value | Business Target ID | 8 | If the GBT Message is sent to the Device, the value shall be the Entity Identifier of the Device.  If the GBT Message is sent from the Device, the value shall be the Entity Identifier of the GBT Third Party. |
|  | date-time | 0x00 | 1 | A value for this element is not needed so the length field is 0x00 |
|  | other-information |  |  |  |
|  | Length | 0x02 | 1 | Length of Message Code |
|  | Value | Message Code | 2 | Shall be populated with the corresponding field from the Grouping Header in the Remote Party Message that is being carried in this GBT Message Series |
|  | key-info | 0x00 | 1 | key-info values are not present so encoded as 0x00 |
|  | ciphered-service |  |  |  |
|  | Length | Encoding(X) | Len(Encoding(X)) | X shall be the length in octets of the subsequent parts of the GBT Message after this length value. |
|  | security header |  |  |  |
|  | security control byte (SC) | 0x01 | 1 | Specifies that no MAC field is present at the end of the APDU |
|  | invocation counter (IC) | 0x00000000 | 4 | IC is always zero |

Table 7.2.11.5: Message Routing Header

#### GBT Header

| **GBT Header** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **xDLMS Message Elements** | **Contents** | **Length (octets)** | **Note** |
|  | general-block-transfer | 0xE0 | 1 | xDLMS APDU tag for General-Block-Transfer |
|  | block-control |  |  |  |
|  | last-block (bit 7) | See ‘Note’ column | 1/8 | 0b0 if not the last GBT Message in this GBT Message Series the sender has to send, or  0b1 if this is the last GBT Message in this GBT Message Series the sender has to send |
|  | streaming (bit 6) | See ‘Note’ column | 1/8 | 0b1 if the sender has at least one more GBT Message in this GBT Message Series to send or  0b0 if this is the last GBT Message in this GBT Message Series the sender has to send |
|  | window (bits 5 – 0) | 0b11111 or  0b00101 | 5/8 | The value of GBT Streaming Window as required by Section 7.2.11.1. |
|  | block-number | See ‘Note’ column | 2 | GBT Initiator Block Number, if this GBS Message is sent by the GBT Initiator.  GBT Recipient Block Number, if this GBS Message is sent by the GBT Recipient. |
|  | block-number-ack | See ‘Note’ column | 2 | GBT Initiator Block Number Ack, if this GBS Message is sent by the GBT Initiator.  GBT Recipient Block Number Ack, if this GBS Message is sent by the GBT Recipient. |
|  | block-data |  |  |  |
|  | Length | Encoding(X) | Len(Encoding(X)) | X is the length in octets of the following parts of this APDU. |

Table 7.2.11.6: GBT Header

#### Illustrations – informative

GBT allows for the transport of Messages where the Message is greater than the Maximum PDU Size. A number of Use Cases can result in this larger Message size, either as a Command or a Response. There are no Alert Use Cases that result in the larger Message size.

GBT does not change any part of the Remote Party Message content that is being transported.

Example 1: A small Command with small Response – e.g. read MPAN.

Without GBT, the Command is:

MAC Header || Grouping Header || read MPAN Command Payload || 0x00 || ACB-SME MAC

and the Response is:

MAC Header || Grouping Header || read MPAN Response Payload || 0x00 || SMD-KRP MAC

GBT can be applied to this Use Case. The Command becomes:

Message Routing Header || GBT Header || MAC Header || Grouping Header || read MPAN Command Payload || 0x00 || ACB-SME MAC

and the Response becomes:

Message Routing Header || GBT Header || MAC Header || Grouping Header || read MPAN Response Payload || 0x00 || SMD-KRP MAC

Example 2: A large Command with small Response – e.g. set tariff on an ESME where the tariff is complex.

Without GBT, the Command is:

MAC Header || Grouping Header || set Tariff Command Payload || 0x40 || KRP Signature || ACB-SME MAC

For the purposes of example, assume this is divided into three blocks, so block-numbers 1, 2 and 3. Actual set tariff Commands will vary from this number of blocks.

The Command is transmitted as the GBT Message Series:

Message Routing Header || GBT Header || block 1

Message Routing Header || GBT Header || block 2

Message Routing Header || GBT Header || block 3

This is reconstructed at the ESME, by concatenating blocks 1, 2 and 3 to give:

MAC Header || Grouping Header || set Tariff Command Payload || 0x40 || KRP Signature || ACB-SME MAC

The Response would have the following structure:

Message Routing Header || GBT Header || Grouping Header || Response Payload || 0x40 || SMD Signature

It will be smaller than the Maximum PDU Size and so can be sent as a single APDU without any use of GBT.

Example 3: small Command with large Response – e.g. read half-hourly profile (Export)

The Command is:

MAC Header || Grouping Header || read half-hourly profile (Export) Command Payload || 0x00 || ACB-SME MAC

It will be smaller than the Maximum PDU Size and so can be sent as a single APDU without any use of GBT.

The ESME Response is:

MAC Header || Grouping Header || read half-hourly profile (Export) Response Payload || 0x00 || SMD-KRP MAC

Assuming that there are 75 blocks to send the GBT Message Series would, if no retries are needed, be as follows:

The ESME will send:

Message Routing Header || GBT Header || Block 1

…

Message Routing Header || GBT Header || Block 63

and wait for acknowledgement.

The Access Control Broker will construct and send that acknowledgement whose structure is:

Message Routing Header || GBT Header

When this acknowledgement is received by the ESME, the ESME will send:

Message Routing Header || GBT Header || Block 64

…

Message Routing Header || GBT Header || Block 75

When the whole Message is received by the Access Control Broker, the Response can then be reconstructed:

MAC Header || Grouping Header || read half-hourly profile (Export) Response Payload || 0x00 || SMD-KRP MAC

Once the response has been reconstructed, the MAC can be checked.

## Device Requirements – DLMS COSEM

### Introduction – informative

The DLMS COSEM server in the ESME (and CHF where a DLMS COSEM server is present) responds to requests for information, and also provides Alerts in response to events within the meter (e.g. push data at the end of billing period; Alert in the event of a tamper; disable supply when prepayment credit expires). To achieve this, a level of configuration is needed to ensure that the behaviour of the Device is as expected.

SMETS and CHTS require that the Critical Commands mandated by them (and so those defined in the GBCS) are the only Critical commands allowed. Devices may implement additional non Critical features only.

SMETS and CHTS only require DLMS COSEM support on the ESME.

DLMS COSEM objects (or functionality equivalent to them) are required to deliver the ESME functionality defined in the Use Cases in a consistent way but should not be accessible via the ESME’s HAN interface (i.e. it is internal functionality).

Constant values specified in Table 7.3.7a are fixed before operation and immutable save via a firmware upgrade. This is to ensure consistent functioning and guard against potential attacks.

### General Requirements

Except where explicitly required by this Section 7.3, a Device shall not expose any part of any DLMS COSEM object, either for the writing of an attribute or for the invocation of a method, that could, if used, constitute a Critical action.

For Devices which are not ESME or CHF (so where deviceType <> 1 or 2), the GBCS does not require the implementation of any DLMS COSEM objects.

All Devices which are ESME (so where deviceType = 1):

* shall implement all of the DLMS COSEM objects, attributes and methods detailed in ‘SMETS Required Objects’ tab of the table in Section 20, and expose the specified attributes and methods over its network interface; and
* shall have the constant values set for the DLMS COSEM attributes specified as requiring constant values in Table 7.3.7a, and shall ensure that such values cannot be amended, save via activation of new firmware.

### Application Associations

Any ESME or CHF shall communicate using pre-established Application Associations (AA). These shall be set at manufacture, and the Device shall reject all subsequent attempts to open or release Application Associations.

An ESME or CHF shall support the Application Associations in Table 7.3.7c. An ESME or CHF shall not support any additional Application Associations.

The Application Associations in Table 7.3.7c shall limit access to DLMS features by configuring the *object\_list* attribute to reflect the access granted to the role in ‘SMETS Required Objects’ tab of the table in Section 20. Any other methods and attributes of any class shall be made inaccessible by listing them in the *object\_list* attribute such that there is no access.

The Public AA shall only expose:

* the SAP Assignment object; and
* the DLMS COSEM Logical Device name object and object\_list with no objects listed other than the Association Logical Name (LN) Object (with its Blue Book meaning) and the SAP Assignment Object.

When a Message is received by the ESME or CHF, the Message shall be validated against the AA based on the Business Originator ID and the Message Code within the Grouping Header.

Other attributes in the Association LN Objects and the Security Setup Objects shall be set at manufacture in accordance with Tables 7.3.7d and 7.3.7e.

The ‘SAP Assignment’ object shall be configured at manufacture in accordance with Table 7.3.7f. The method associated  with the ‘SAP Assignment’ object shall not be accessible to any Application Association.

### Interface Classes and Objects

Devices shall support the version of Interface Classes shown as current in the Blue Book.

An ESME shall support the ‘Class 9000’ as detailed in Section 22 of this GBCS.

Unless explicitly required in a predetermined script or the SMETS ‘Required Objects’ tab of the Mapping Table, Class 3 objects shall not have a reset method that is accessible external to the Device.

Unless otherwise stated, Generic Profile objects with a non-zero attribute 4 shall capture the first entry at midnight UTC.

The ESME shall have the constant values set for the DLMS COSEM attributes specified as requiring constant values in Table 7.3.7a, and shall ensure that such values cannot be amended, save via activation of new firmware.

### Values normally negotiated when an AA is established

#### Conformance Block Contents

The conformance block shall be set according to Table 7.3.7g.

#### Other Items.

Other items for pre-establishing the Application Associations and other communication parameters shall be implemented as detailed in Table 7.3.7h.

#### Security Setup Objects

Security Setup Objects shall be limited to those listed in Table 7.3.7c.

Manufacturer specific attributes and methods for these objects shall not be accessible external to the Device.

The methods of the Security Setup objects shall not be accessible external to the Device. The attributes of the Security Setup objects shall be as specified in Table 7.3.7e.

Note that Security Credentials are updated as specified in Section 13.

### Scripts for operation of the meter

Scripts required for operation of the Device shall be as listed in Table 7.3.7b.

The Device shall ensure that the script table objects shall be read only. The Device shall ensure that a script table object entries shall only be executable by the corresponding Application Association specified in Table 7.3.7b.

The Device shall ensure that a script table object’s entries shall only be executable from an activity calendar, scheduler, or single action scheduler controlled by the corresponding Application Association application in Table 7.3.7b.

### DLMS Device Requirements Tables

Table 7.3.7a: Objects tab in embedded file

Table 7.3.7b: Scripts tab in embedded file

Table 7.3.7c: Application Associations tab in embedded file

Table 7.3.7d: Association LN Object Content tab in embedded file

Table 7.3.7e: Security Setup Object Content tab in embedded file

Table 7.3.7f: SAP Assignment Object content tab in embedded file

Table 7.3.7g: Conformance Content tab in embedded file

Table 7.3.7h: End to End Communications tab in embedded file



## Device requirements – ZSE - informative

This Section 7.4 sets out the optional features in the ZSE specification that shall be included for ESME, GSME and Communications Hub (CHF and GPF). Mandatory features in the ZSE specification are not detailed. The tables included in this Section 7.4 show a high level summary of features rather than a definitive list.  The Use Cases in Section 19 provide the definitive requirements for support.

### ESME

Single phase and three phase meters shall implement single instances of all the clusters in Table 7.4.1.

A Twin element meter shall implement single instances of all the clusters in Table 7.4.1 apart from the metering cluster, where two instances are required.

|  |  |  |
| --- | --- | --- |
| **ESME (single-element 1-phase; 3-phase) whole meter endpoint (ESI + metering) / ESME twin-element endpoints (2 instances ESI + metering)** | | |
| **Server clusters** | | |
| Cluster | Demand Response and Load Control | |
| Cluster | Device Management | |
|  | Attributes | |
|  |  | Low Medium Threshold |
|  |  | Medium High Threshold |
| Cluster | Metering | |
|  | Commands | |
|  |  | Change Supply |
|  |  | Credit Adjustment |
|  |  | Get Profile |
|  |  | Get Profile Response |
|  |  | GetSnapshot |
|  |  | Publish Snapshot |
|  | Attributes | |
|  |  | AmbientConsumptionIndicator |
|  |  | BillToDateDelivered |
|  |  | CurrentDayConsumptionDelivered |
|  |  | CurrentMonthConsumptionDelivered |
|  |  | CurrentNoTierBlockNSummationDelivered |
|  |  | CurrentSummationDelivered |
|  |  | CurrentSummationReceived |
|  |  | CurrentTierNBlockNSummationDelivered |
|  |  | CurrentTierNSummationDelivered |
|  |  | CurrentWeekConsumptionDelivered |
|  |  | Divisor |
|  |  | InstantaneousDemand |
|  |  | Multiplier |
|  |  | PreviousDayConsumption, PreviousDay{2..8}Consumption |
|  |  | PreviousMonthConsumption, PreviousMonth{2..13}Consumption |
|  |  | PreviousWeekConsumption, PreviousWeek{2..5}Consumption |
|  |  | SupplyStatus |
|  |  | UnitofMeasure |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Change Payment Mode |
|  |  | Select Available Emergency Credit |
|  | Attributes | |
|  |  | Accumulated Debt |
|  |  | Credit Remaining |
|  |  | Currency |
|  |  | CurrentDayCostConsumptionDelivered |
|  |  | CurrentMonthCostConsumptionDelivered |
|  |  | CurrentWeekCostConsumptionDelivered |
|  |  | CutOffValue |
|  |  | DebtAmount#1 |
|  |  | DebtAmount#2 |
|  |  | DebtAmount#3 |
|  |  | DebtRecoveryFrequency#1 |
|  |  | DebtRecoveryFrequency#2 |
|  |  | DebtRecoveryTopUpPercentage#3 |
|  |  | EmergencyCreditLimit |
|  |  | EmergencyCreditRemaining |
|  |  | EmergencyCreditThreshold |
|  |  | HistoricalCostConsumptionFormatting |
|  |  | LowCreditWarningLevel |
|  |  | OverallDebtCap |
|  |  | Payment Control Configuration |
|  |  | Prepayment Alarm Status |
|  |  | PreviousDayCostConsumptionDelivered, PreviousDay{2..8}CostConsumptionDelivered |
|  |  | PreviousMonthCostConsumptionDelivered, PreviousMonth{2..13}CostConsumptionDelivered |
|  |  | PreviousWeekCostConsumptionDelivered, PreviousWeek{2..5}CostConsumptionDelivered |
| Cluster | Price | |
|  | Commands | |
|  |  | PublishPriceMatrix |
|  | Attributes | |
|  |  | BlockNThreshold |
|  |  | Currency |
|  |  | NumberofBlockThresholdsInUse |
|  |  | Price Trailing Digit |
|  |  | PriceTierN |
|  |  | Standing Charge |
|  |  | ThresholdDivisor |
|  |  | ThresholdMultiplier |
|  |  | TierBlockMode |
|  |  | TierNBlockNPrice |
|  |  | UnitofMeasure |
| Cluster | TOU Calendar | |
|  | Commands | |
|  |  | GetDayProfiles |
|  |  | GetSeasons |
|  |  | GetSpecialDays |
|  |  | GetWeekProfiles |
|  | Attributes | |
|  |  | AuxSwitchNLabel |
| Cluster | Tunneling | |
| **Client clusters** | | |
| Cluster | Over-the-Air Bootload | |
| EmergencyCreditLimit | EmergencyCreditLimit | |

Table 7.4.1: ESME Device Requirements

### GSME

GSME shall implement single instances of all the clusters in Table 7.4.2.

|  |  |  |
| --- | --- | --- |
| **GSME endpoint** | | |
| **Server clusters** | | |
| Cluster | Basic | |
|  | Attributes | |
|  |  | HWVersion |
|  |  | ManufacturerName |
|  |  | ModelIdentifier |
| Cluster | Events | |
|  | Commands | |
|  |  | Clear Event Log Request |
|  |  | Clear Event Log Response |
|  |  | Get Event Log |
|  |  | Publish Event Log |
| Cluster | Metering | |
|  | Commands | |
|  |  | Change Supply |
|  |  | Credit Adjustment |
|  |  | GetSampledData |
|  |  | GetSnapshot |
|  |  | Publish Snapshot |
|  |  | SetSupplyStatus |
|  |  | SetUncontrolledFlowThreshold |
|  |  | StartSampling |
|  |  | Update CIN |
|  | Attributes | |
|  |  | BillToDateDelivered |
|  |  | CurrentMeterID |
|  |  | CurrentTierNSummationDelivered |
|  |  | CustomerIDNumber |
|  |  | Divisor |
|  |  | MeteringDeviceType |
|  |  | Multiplier |
|  |  | RemainingBatteryLifeinDays |
|  |  | SiteID |
|  |  | SupplyStatus |
|  |  | UnitofMeasure |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Change Debt |
|  |  | Change Payment Mode |
|  |  | Change Payment Mode Response |
|  |  | Consumer Top Up |
|  |  | Consumer Top Up Response |
|  |  | Credit Adjustment |
|  |  | Emergency Credit Setup |
|  |  | Get Debt Repayment Log |
|  |  | Get Prepay Snapshot |
|  |  | Get Top Up Log |
|  |  | Publish Debt Log |
|  |  | Publish Prepay Snapshot |
|  |  | Publish Top Up Log |
|  |  | Select Available Emergency Credit |
|  |  | Set Low Credit Warning Level |
|  |  | Set Maximum Credit Limit |
|  |  | Set Overall Debt Cap |
|  | Attributes | |
|  |  | Accumulated Debt |
|  |  | Credit Remaining |
|  |  | Currency |
|  |  | CurrentDayCostConsumptionDelivered |
|  |  | CurrentMonthCostConsumptionDelivered |
|  |  | CurrentWeekCostConsumptionDelivered |
|  |  | CutOffValue |
|  |  | DebtAmount#1 |
|  |  | DebtAmount#2 |
|  |  | DebtAmount#3 |
|  |  | DebtRecoveryFrequency#1 |
|  |  | DebtRecoveryFrequency#2 |
|  |  | DebtRecoveryTopUpPercentage#3 |
|  |  | EmergencyCreditLimit |
|  |  | EmergencyCreditRemaining |
|  |  | EmergencyCreditThreshold |
|  |  | HistoricalCostConsumptionFormatting |
|  |  | LowCreditWarningLevel |
|  |  | MaxCreditLimit |
|  |  | MaximumCreditPerTopUp |
|  |  | OverallDebtCap |
|  |  | Payment Control Configuration |
|  |  | Payment Control Configuration (10: Debt Configuration) |
|  |  | Payment Control Configuration (11: Emergency Debt Configuration) |
|  |  | Prepayment Alarm Status |
|  |  | PreviousDayCostConsumptionDelivered, PreviousDay{2..8}CostConsumptionDelivered |
|  |  | PreviousMonthCostConsumptionDelivered, PreviousMonth{2..13}CostConsumptionDelivered |
|  |  | PreviousWeekCostConsumptionDelivered, PreviousWeek{2..5}CostConsumptionDelivered |
| **Client clusters** | | |
| Cluster | Device Management | |
|  | Commands | |
|  |  | Publish Change of Supplier |
|  |  | Publish Change of Tenancy |
|  |  | Request New Password Response |
|  |  | SetEventConfiguration |
|  |  | Update CIN |
|  |  | Update SiteID |
| Cluster | Messaging | |
| Cluster | Over-the-Air Bootload | |
| Cluster | Price | |
|  | Commands | |
|  |  | Publish Block Period |
|  |  | PublishBillingPeriod |
|  |  | PublishBlockThresholds |
|  |  | PublishCalorificValue |
|  |  | PublishConversionFactor |
|  |  | PublishPriceMatrix |
|  |  | PublishTariffInformation |
| Cluster | TOU Calendar | |
| Cluster | Tunneling | |

Table 7.4.2: GSME Device Requirements

### Communications Hub

The Communications Hub shall implement single instances of all the clusters in Table 7.4.3a, Table 7.4.3b and Table 7.4.3c. The tables reflect the logical Devices on the Communications Hub:

* Gas Proxy Function:
  + - * ESI endpoint - for data that is stored on the Communications Hub via the Tapping Off Mechanism detailed in Section 10; and
      * Gas Mirror endpoint – for data that is mirrored from the GSME to the Communications Hub.
* Communications Hub Function – HAN network coordination functionality.

|  |  |  |
| --- | --- | --- |
| **GPF Gas ESI endpoint** | | |
| **Server clusters** | | |
| Cluster | Events | |
|  | Commands | |
|  |  | Clear Event Log Request |
|  |  | Clear Event Log Response |
|  |  | Get Event Log |
|  |  | Publish Event Log |
| Cluster | Messaging | |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Get Debt Repayment Log |
|  |  | Get Prepay Snapshot |
|  |  | Get Top Up Log |
|  |  | Publish Debt Log |
|  |  | Publish Prepay Snapshot |
|  |  | Publish Top Up Log |
| Cluster | Price | |
|  | Commands | |
|  |  | GetBillingPeriod |
|  |  | PublishBillingPeriod |
|  |  | PublishBlockThresholds |
|  |  | PublishCalorificValue |
|  |  | PublishConversionFactor |
|  |  | PublishPriceMatrix |
|  |  | PublishTariffInformation |
|  | Attributes | |
|  |  | BlockNThreshold |
|  |  | Calorific Value Trailing Digit |
|  |  | CalorificValue |
|  |  | CalorificValueUnit |
|  |  | ConversionFactor |
|  |  | ConversionFactorTrailingDigit |
|  |  | Currency |
|  |  | NumberofBlockThresholdsInUse |
|  |  | Price Trailing Digit |
|  |  | PriceTierN |
|  |  | Standing Charge |
|  |  | ThresholdDivisor |
|  |  | ThresholdMultiplier |
|  |  | TierBlockMode |
|  |  | TierNBlockNPrice |
|  |  | UnitofMeasure |
| Cluster | TOU Calendar | |
|  | Commands | |
|  |  | GetDayProfiles |
|  |  | GetSeasons |
|  |  | GetSpecialDays |
|  |  | GetWeekProfiles |
| **Client clusters** | | |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Get Debt Repayment Log |
|  |  | Get Prepay Snapshot |
|  |  | Get Top Up Log |
|  |  | Publish Debt Log |
|  |  | Publish Prepay Snapshot |
|  |  | Publish Top Up Log |

Table 7.4.3a: Communications Hub Device Requirements – GPF (ESI endpoint)

|  |  |  |
| --- | --- | --- |
| **GPF Gas mirror endpoint** | | |
| **Server clusters** | | |
| Cluster | Basic | |
|  | Attributes | |
|  |  | HWVersion |
|  |  | ManufacturerName |
|  |  | ModelIdentifier |
| Cluster | Device Management | |
|  | Commands | |
|  |  | Publish Change of Supplier |
|  | Attributes | |
|  |  | Provider Contact Details |
|  |  | Provider Name |
| Cluster | Metering | |
|  | Commands | |
|  |  | Credit Adjustment |
|  |  | GetSampledData |
|  |  | GetSampledDataResponse |
|  |  | GetSnapshot |
|  |  | Publish Snapshot |
|  |  | Update CIN |
|  | Attributes | |
|  |  | BillToDateDelivered |
|  |  | CurrentDayConsumptionDelivered |
|  |  | CurrentMeterID |
|  |  | CurrentMonthConsumptionDelivered |
|  |  | CurrentSummationDelivered |
|  |  | CurrentTierNSummationDelivered |
|  |  | CurrentWeekConsumptionDelivered |
|  |  | CustomerIDNumber |
|  |  | Divisor |
|  |  | MeteringDeviceType |
|  |  | Multiplier |
|  |  | PreviousDayConsumption, PreviousDay{2..8}Consumption |
|  |  | PreviousMonthConsumption, PreviousMonth{2..13}Consumption |
|  |  | PreviousWeekConsumption, PreviousWeek{2..5}Consumption |
|  |  | RemainingBatteryLifeinDays |
|  |  | SiteID |
|  |  | SupplyStatus |
|  |  | Uncontrolled Flow Divisor |
|  |  | Uncontrolled Flow Multiplier |
|  |  | Uncontrolled Flow Threshold |
|  |  | Uncontrolled Flow Threshold Unit of Measure |
|  |  | UnitofMeasure |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Change Payment Mode |
|  |  | Get Prepay Snapshot |
|  |  | Publish Prepay Snapshot |
|  | Attributes | |
|  |  | Accumulated Debt |
|  |  | Credit Remaining |
|  |  | Currency |
|  |  | CurrentDayCostConsumptionDelivered |
|  |  | CurrentMonthCostConsumptionDelivered |
|  |  | CurrentWeekCostConsumptionDelivered |
|  |  | CutOffValue |
|  |  | DebtAmount#1 |
|  |  | DebtAmount#2 |
|  |  | DebtAmount#3 |
|  |  | DebtRecoveryFrequency#1 |
|  |  | DebtRecoveryFrequency#2 |
|  |  | DebtRecoveryTopUpPercentage#3 |
|  |  | EmergencyCreditLimit |
|  |  | EmergencyCreditRemaining |
|  |  | EmergencyCreditThreshold |
|  |  | HistoricalCostConsumptionFormatting |
|  |  | LowCreditWarningLevel |
|  |  | MaxCreditLimit |
|  |  | MaximumCreditPerTopUp |
|  |  | OverallDebtCap |
|  |  | Payment Control Configuration |
|  |  | Payment Control Configuration (10: Debt Configuration) |
|  |  | Payment Control Configuration (11: Emergency Debt Configuration) |
|  |  | Prepayment Alarm Status |
|  |  | PreviousDayCostConsumptionDelivered, PreviousDay{2..8}CostConsumptionDelivered |
|  |  | PreviousMonthCostConsumptionDelivered, PreviousMonth{2..13}CostConsumptionDelivered |
|  |  | PreviousWeekCostConsumptionDelivered, PreviousWeek{2..5}CostConsumptionDelivered |
| **Client clusters** | | |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Change Payment Mode |
|  |  | Get Prepay Snapshot |
|  |  | Publish Prepay Snapshot |

Table 7.4.3b: Communications Hub Device Requirements – GPF (Gas Mirror endpoint)

|  |  |  |
| --- | --- | --- |
| **CHF remote communications endpoint** | | |
| **Server clusters** | | |
| Cluster | Events | |
|  | Commands | |
|  |  | Clear Event Log Request |
|  |  | Clear Event Log Response |
|  |  | Get Event Log |
|  |  | Publish Event Log |
| Cluster | Over-the-Air Bootload | |
| Cluster | Time | |
|  | Attributes | |
|  |  | LocalTime |
| Cluster | Tunneling | |
| **Client clusters** | | |
| Cluster | | Tunneling |

Table 7.4.3c: Communications Hub Device Requirements – Communications Hub Function

### Type 2 Devices

Table 7.4.4 sets out example requirements for Type 2 Devices

|  |  |  |
| --- | --- | --- |
| **Type 2 device (1-4 endpoints)** | | |
| Note that a Type 2 device may require multiple endpoints depending on which meters are installed | | |
| **Client clusters** | | |
| Cluster | Metering | |
|  | Commands | |
|  |  | Credit Adjustment |
|  |  | Get Profile |
|  |  | Get Profile Response |
|  |  | GetSampledData |
|  |  | GetSampledDataResponse |
|  |  | GetSnapshot |
|  |  | Publish Snapshot |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Change Payment Mode |
| Cluster | Price | |
|  | Commands | |
|  |  | PublishPriceMatrix |
| Cluster | TOU Calendar | |
|  | Commands | |
|  |  | GetDayProfiles |
|  |  | GetSeasons |
|  |  | GetSpecialDays |
|  |  | GetWeekProfiles |

Table 7.4.4: Type 2 Device - example requirements

### PPMID

PPMID shall implement single instances of all the clusters in Table 7.4.5.

|  |  |  |
| --- | --- | --- |
| **Type 1 device: PPMID** | | |
| **Server clusters** | | |
| Cluster | Tunneling | |
| **Client clusters** | | |
| Cluster | Metering | |
|  | Commands | |
|  |  | Change Supply |
|  |  | Credit Adjustment |
| Cluster | Prepayment | |
|  | Commands | |
|  |  | Consumer Top Up |
|  |  | Consumer Top Up Response |
|  |  | Select Available Emergency Credit |
| Cluster | Tunneling | |

Table 7.4.5: PPMID Requirements

### HCALCS

HCALCS shall implement single instances of all the clusters in Table 7.4.6.

|  |  |
| --- | --- |
| **Type 1 device: HCALCS** | |
| **Client clusters** | |
| Cluster | Demand Response and Load Control |

Table 7.4.6: HCALCS Device Requirements

# Encryption of Attributes in Remote Party Messages

In some Use Cases, some attributes are marked as Encrypted.

This Section 8 lays out requirements as to how such Encryption and related Decryption shall be undertaken.

## Approach - informative

Since ZSE and DLMS have differing data types to represent the same attribute of SMETS information, there are some differences in the format of the data that is encrypted. These differences are laid out in this Section 8. However, Encryption and Decryption use the same cryptographic AES GCM primitives in the same way in all cases, regardless of protocol. The usage is the same as that to generate MACs for Remote Party Message protection, and therefore as per the AES GCM approach laid out in the Green Book.

Encryption of SMETS attributes is required when:

* the Supplier reads the amounts held in Time Debt Register [1..2] and Payment Debt Register. Each of these is a single integer value;
* the Supplier reads the values held in the Active Import Register or Secondary Active Import Register. Each of these is a single integer value;
* a Known Party or an Unknown Party reads one or more entries from a Log (with each entry in the specific log having a Log specific structure), specifically:
  + - * the current or previous Supplier reads the Billing Data Log (excluding the export related parts), the Daily Read Log or the Prepayment Daily Read Log. Note that a previous Supplier is an Unknown Remote Party as far as the meter is concerned;
      * the Supplier, Network Operator, or an Unknown Remote Party reads the Daily Consumption Log or the Profile Data Log (Consumption parts);
* a Device sends an Alert containing a single entry from the Billing Data Log (excluding the export related parts).

## Common requirements

All Encryption shall be Authenticated Encryption which:

* shall use the cryptographic primitives, input value structures and cryptographic material specified in Section 4; and
* shall, for Key Agreement, use the Key Agreement key pair of the Device and the Remote Party which is accessing the data item.

A Device shall, where it stores a data item listed in the Mapping Table as Encrypted, only provide that data in a Remote Party Message in Encrypted form.

Where the Encrypted data item is within a Log, a Command requesting that data shall always have ‘from’ and ‘to’ date-times specified.

Where all the octets in the ‘from’ date-time are 0x00 (excluding the least significant 3 bytes in Blue Book octet string formatted date-times), the Device shall interpret the ‘from’ field as meaning from the oldest in the Log.

Where all the octets in the ‘to’ date-time are 0xFF (excluding the least significant 3 bytes in Blue Book octet string formatted date-times), the Device shall interpret the ‘to’ field as meaning to the newest in the Log.

Where the Encrypted data item in the Mapping Table is not in a Log, a Command requesting that data shall never have ‘from’ or ‘to’ date-times specified.

## Key Derivation Inputs

Where a Remote Party Message (1) contains Encrypted data items and (2) contains a Supplementary Remote Party ID, then the Encryption Remote Party shall be that identified by the Supplementary Remote Party ID. Otherwise, the Encryption Remote Party shall be the Remote Party identified in the Grouping Header of the Message.

If the Message is to include a Supplementary Originator Counter generated by the Device (see Section 4.3.1.4), then the Encryption Originator Counter shall be the Supplementary Originator Counter. Otherwise the Encryption Originator Counter shall be the Originator Counter with the value in the Grouping Header of the Message.

In relation to the Key Derivation Function requirements at Section 4.3.3, fields shall be populated as follows:

* ‘value of transaction-id’ shall be the concatenation 0x04 || Encryption Originator Counter. Note 0x04 ensures this value is not used in any other Key Derivation Function invocation save that related to this Encryption / Decryption; and
* for Encrypted data items in Responses and Alerts, ‘value of recipient-system-title’ shall be Encryption Remote Party and ‘value of originator-system-title’ shall be the Device’s Entity Identifier.

## AAD, Plaintext and Ciphertext

The Plaintext shall be set to the structure and content of the data item(s) as they would have been exposed on the Device’s HAN interface, if access to them were not constrained to be via Encrypted form by this Section 8.4.

AAD shall be set to security control byte (SC) which shall have the value of 0x31 (see Section 8.4.1).

The Invocation Counter (IC) shall have a value of 0x00000000.

The Authenticated Encryption MAC (AE MAC) shall be the MAC produced by applying Authenticated Encryption to AAD and Plaintext, as defined in *NIST Special Publication 800-38D*, with the values specified in this Section 8.4.

Authenticated Encryption (AE) Ciphertext shall be the Ciphertext produced by applying Authenticated Encryption to Plaintext, with the values specified in this Section 8.4.

Ciphered Information shall be the concatenation:

SC || IC || AE Ciphertext || AE MAC

### Meaning of SC - informative

The SC is set to 0x31 to reflect the following:

* Bits 3..0 are security suite which is 0b0001 since Security Suite 1 is required;
* Bit 4 is set to 0b1 since Authentication of the data is required;
* Bit 5 is set to 0b1 since Encryption of the data is required;
* Bit 6 is set to 0b0 since Messages containing the encrypted data are unicast; and
* Bit 7 is set to 0b0 as per the Green Book.

## Access to sensitive data – COSEM attribute access

Access to sensitive data items shall be via the *Data Protection* class, as specified in the Blue Book. The required OBIS codes and associated details for each attribute shall be as specified in the ‘SMETS required objects’ tab in the Mapping Table.

The Device shall only allow read access to attributes listed as Encrypted in the Mapping Table using the get\_protected\_attributes(data) method of the *Data Protection* class and not allow access to any other methods of such objects.

### Values of the *Data Protection* class attributes

The values of attributes 1, 3, 4 and 5 of an object of the *Data Protection* class shall be set on a Device at manufacture, and those values shall not be capable of amendment except by firmware upgrade. For each object of the *Data Protection* class:

* protection\_object\_list (attribute 3) shall be a single entry array containing one object\_definition. Within that single object\_definition: class\_id, logical\_name, attribute\_index, data\_index, restriction\_type and restriction\_value shall take values as per Table 7.3a;
* the value of protection\_parameters (attribute 4) shall be a single entry array containing one protection\_parameters\_element, which shall have the values specified in Table 8.5.1a;
* the value of required\_protection (attribute 5) shall be 0b01100000 (0x60) where the object exposes the get\_protected\_attributes(data) method, since Authenticated Encryption is required on the output of the method.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Type** | **Value** |
| protection\_type | Enum | (2) authenticate and encrypt |
| protection\_options | Structure |  |
| transaction\_id | octet-string | Empty string |
| originator\_system\_title | octet-string | Empty string |
| recipient\_system\_title | octet-string | Empty string |
| other\_information | octet-string | Empty string |
| key\_info | Structure |  |
| key\_info\_type: | Enum | (0) agreed\_key |
| key\_info\_options | CHOICE | agreed\_key\_options |
| agreed\_key\_info\_options | Structure |  |
| key\_parameters | octet-string | Empty string |
| key\_ciphered\_data | octet-string | Empty string |

Table 8.5.1a: Values of protection\_parameters\_element

### Parameters of the get\_protected\_attributes method

The protected\_attributes\_definition parameter of the get\_protected\_attributes method shall:

* be populated in the Command to the Device according to Table 8.5.2a; and
* be verified by the Device receiving the Command according to Table 8.5.2a;

The protection\_parameters part of the protected\_attributes\_response\_data returned by the get\_protected\_attributes method shall be populated by the Device according to Table 8.5.2b.

The value of protected\_attributes part of the protected\_attributes\_response\_data returned by the get\_protected\_attributes method shall be populated by the Device with Ciphered Information, calculated as per the requirements of Section 8.2. The tag for protected\_attributes shall be ‘octet-string’ (0x09) and the length shall be the length of Ciphered Information.

| **Field** | **Value** | **Device Validation** | **Note** |
| --- | --- | --- | --- |
| protected\_attributes\_definition |  |  |  |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x02 | Must have this value | 2 elements in the structure |
| object\_list |  |  | The first element in the protected\_attributes\_definition structure |
| Tag | 0x01 | Must have this value | Meaning ‘array’ |
| Length | 0x01 | Must have this value | 1 entry in the array |
| object\_definition |  |  | The 1 entry in the object\_list array |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x06 | Must have this value | 6 elements in the structure |
| class\_id |  |  |  |
| Tag | 0x12 | Must have this value | Meaning ‘long-unsigned’ |
| Value | See ‘Note’ column | Must be the same as the class\_id in attribute 3 of the Data Protection object being accessed | The class\_id of the object which is the source of the Encrypted data |
| logical\_name |  |  |  |
| Tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x06 | Must have this value | Logical\_name is always 6 octets long |
| Value | See ‘Note’ column | Must be the same as the logical\_name in attribute 3 of the Data Protection object being accessed | The logical\_name of the object which is the source of the Encrypted data |
| attribute\_index |  |  |  |
| Tag | 0x0F | Must have this value | Meaning ‘integer’ |
| Value | See ‘Note’ column | Must be the same as the attribute\_index in attribute 3 of the Data Protection object being accessed | The attribute\_index of the object which is the source of the Encrypted data |
| data\_index |  |  |  |
| Tag | 0x12 | Must have this value | Meaning ‘long-unsigned’ |
| Value | 0x0000 | Must have this value | Meaning the whole attribute is captured or set |
| Restriction |  |  |  |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x02 | Must have this value | 2 elements in the structure |
| EITHER |  | Must be present if this invocation is not to access a Log as defined in Section 1.2 | If this is not to access a Log as defined in Section 8.2 |
| restriction\_type |  |  |  |
| tag | 0x16 | Must have this value | Meaning ‘enum’ |
| value | 0x00 | Must have this value | Meaning ‘none’ |
| restriction\_value |  |  | Assumes that the CHOICE does not need encoding since the value of ‘restriction\_type’ defines the CHOICE [Note, there are no tags in the Blue Book for this CHOICE] |
| tag | 0x00 | Must have this value | Meaning ‘null-data’ |
| OR |  | Must be present if this invocation is to access a Log as defined in Section 1.2 | If this is to access a Log as defined in Section 8.2 |
| restriction\_type |  |  |  |
| tag | 0x16 | Must have this value | Meaning ‘enum’ |
| value | 0x01 | Must have this value | Meaning ‘restriction by date’ |
| restriction\_value |  |  | Assumes that the CHOICE does not need encoding since the value of ‘restriction\_type’ defines the CHOICE [Note, there are no tags in the Blue Book for this CHOICE] |
| tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x02 | Must have this value | 2 elements in the structure |
| from\_date |  |  | In the date-time format of the Blue Book |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x0C | Must have this value | Date-time is always 12 octets long |
| value | See ‘Note’ column |  | Log entries with a date-time stamp prior to this date-time shall not be returned. |
| to\_date |  |  | In the date-time format of the Blue Book |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x0C | Must have this value | Date-time is always 12 octets long |
| value | See ‘Note’ column |  | Log entries with a date-time stamp after this date-time shall not be returned. |
| protection\_parameters |  |  | The second element in the protection\_parameters\_element structure |
| Tag | 0x01 | Must have this value | Meaning ‘array’ |
| length | 0x01 | Must have this value | 1 entry in the array |
| protection\_parameters\_element |  |  | The 1 entry in the protection\_parameters array |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x02 | Must have this value | 2 elements in the structure |
| protection\_type |  |  | The first element in the protection\_parameters\_element |
| Tag | 0x16 | Must have this value | Meaning ‘enum’ |
| value | 0x02 | Must have this value | Meaning ‘authenticate and encrypt’ |
| protection\_options |  |  | The second element in the protection\_parameters\_element |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x05 | Must have this value | 5 elements in the structure |
| transaction\_id |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x09 | Must have this value | transaction\_id is always 9 octets in length |
| value | See ‘Note’ column |  | The concatenation 0x04 || the Originator Counter value part of the transaction\_id in the Grouping Header of this Command |
| originator\_system\_title |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x08 | Must have this value | Entity Identifier is always 8 octets in length |
| value | See ‘Note’ column |  | The Entity Identifier of the Encryption Remote Party |
| recipient\_system\_title |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x08 | Must have this value | Entity Identifier is always 8 octets in length |
| value | See ‘Note’ column | Must be the Device’s Entity Identifier | The Entity Identifier of the Device |
| other\_information |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x00 | Must have this value | Zero length since this string is empty |
| key\_info |  |  |  |
| tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x02 | Must have this value | 2 elements in the structure |
| key\_info\_type: |  |  |  |
| tag | 0x16 | Must have this value | Meaning ‘enum’ |
| value | 0x00 | Must have this value | Meaning ‘agreed\_key’ |
| key\_info\_options |  | CHOICE | Assumes that the CHOICE does not need encoding since the value of ‘restriction\_type’ defines the CHOICE [Note, there are no tags in the Blue Book for this CHOICE] |
| agreed\_key\_info\_options |  |  |  |
| tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x02 | Must have this value | 2 elements in the structure |
| key\_parameters |  |  |  |
| Tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x00 | Must have this value | Zero length since this string is empty. |
| key\_ciphered\_data |  |  |  |
| Tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x00 | Must have this value | Zero length since this string is empty |

Table 8.5.2a: values of protected\_attributes\_definition

| **Field** | **Value** | **Device Validation** | **Note** |
| --- | --- | --- | --- |
| protection\_parameters |  |  |  |
| Tag | 0x01 | Must have this value | Meaning ‘array’ |
| Length | 0x01 | Must have this value | 1 entry in the array |
| protection\_parameters\_element |  |  | The 1 entry in the protection\_parameters array |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x02 | Must have this value | 2 elements in the structure |
| protection\_type |  |  | The first element in the protection\_parameters\_element |
| Tag | 0x16 | Must have this value | Meaning ‘enum’ |
| Value | 0x02 | Must have this value | Meaning ‘authenticate and encrypt’ |
| protection\_options |  |  | The second element in the protection\_parameters\_element |
| Tag | 0x02 | Must have this value | Meaning ‘structure’ |
| Length | 0x05 | Must have this value | 5 elements in the structure |
| transaction\_id |  |  |  |
| Tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x09 | Must have this value | transaction\_id in is always 9 octets in length |
| Value | See note |  | The concatenation 0x04 || Encryption Originator Counter |
| originator\_system\_title |  |  |  |
| Tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| Length | 0x08 | Must have this value | Entity Identifier is always 8 octets in length |
| Value | See note |  | The Entity Identifier of the Device |
| recipient\_system\_title |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x08 | Must have this value | Entity Identifier is always 8 octets in length |
| value | See note | Must be the Device’s Entity Identifier | The Entity Identifier of the Encryption Remote Party |
| other\_information |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x00 | Must have this value | Zero length since this string is empty |
| key\_info |  | Structure |  |
| tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x02 | Must have this value | 2 elements in the structure |
| key\_info\_type: |  |  |  |
| tag | 0x16 | Must have this value | Meaning ‘enum’ |
| value | 0x00 | Must have this value | Meaning ‘agreed\_key’ |
| key\_info\_options |  | CHOICE | Assumes that the CHOICE does not need encoding since the value of ‘restriction\_type’ defines the CHOICE [Note, there are no tags in the Blue Book for this CHOICE] |
| agreed\_key\_info\_options |  |  |  |
| tag | 0x02 | Must have this value | Meaning ‘structure’ |
| length | 0x02 | Must have this value | 2 elements in the structure |
| key\_parameters |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x00 | Must have this value | Zero length since this string is empty |
| key\_ciphered\_data |  |  |  |
| tag | 0x09 | Must have this value | Meaning ‘octet-string’ |
| length | 0x00 | Must have this value | Zero length since this string is empty |

Table 8.5.2b: values of protection\_parameters

### Billing Data Log Alert – DLMS COSEM

‘Use Case Specific Additional Content’ within the Billing Data Log Alert shall be populated according to the Message Template for the Billing Data Log Alert in Section 18.2.

## Access to sensitive data – ZSE attribute access

Ciphered Information shall be used to populate each ‘GBZ Use Case Specific Component with encrypted content’ as specified in Section 7.2.10.

# Time Synchronisation and Future Dated Remote Party Messages

This Section 9 details how time synchronisation shall operate, and how future dated Remote Party Messages shall be processed by Devices. The latter applies only where a Command is specified in ‘Use Case reference’ tab in the Mapping Table, as ‘Capable of future dated invocation’.

Note that all references in the GBCS to time shall be to UTC date-time unless explicitly stated otherwise.

## Time synchronisation

Introduction – informativeSMETS requires that ESME and GSME have clocks and that, under normal operating circumstances, the time on those clocks is accurate to within 10 seconds.

CHTS requires that Communications Hubs have clocks and that, under normal operating circumstances, the time on those clocks is accurate to within 10 seconds.

Critical functionality on Communications Hubs can function predictably without reliance on time. Time setting mechanisms on Communications Hubs therefore are not constrained or specified in the GBCS. However, under normal operating circumstances, a Communications Hub will provide the time reference for all dependent Devices on the HAN.

Significant parts of ESME and GSME functionality are time-dependent for their correct and predictable functioning. This includes Critical functionality which can only be controlled by the Device’s Supplier with responsibility for that Device. Thus, time must be accurate in terms of alignment with the Supplier’s time on ESME and / or GSME. However, the accuracy requirements measured in seconds are smaller than end-to-end network latency for delivery of Commands to Devices.

This leads to a time synchronisation approach for ESME as specified in Section 9.1.3, and GSME as specified in Section 9.1.5.

That approach is:

* for the Supplier to send a Set Clock Command with the Supplier’s current time and a future time (reflecting a time tolerance) in the Command; and
* if, when the Device receives the Command, the Communications Hub’s time is within tolerance of the Supplier’s time, the Device aligns itself to the Communications Hub’s time and treats its time as Reliable. Otherwise the Device treats its time as Unreliable.

The time synchronisation for a GSME follows the same principles but tolerance needs to differ because a GSME is ‘sleepy’. ‘Sleepy’ means that its SMHAN radio will not be active most of the time and therefore the tolerance provided by the Supplier needs to reflect the extended latency.

### Common Requirements – Set Clock

Supplier Current Time shall be the Supplier’s time at the point the Supplier sends a Set Clock Command.

GSME and ESME shall maintain a record of its Time Status, which, for clarity, is not the same as the ZSE *TimeStatus* attribute. Time Status shall have one of the values in Table 9.1.1.

|  |  |
| --- | --- |
| **Value** | **Meaning** |
| Invalid | The Device has no meaningful time |
| Unreliable | The Device has a meaningful time but that time may not be accurate and needs to be affirmed / reaffirmed by the Supplier |
| Reliable | The Device has a meaningful time and that time has been affirmed by its Supplier |

Table 9.1.1: Time Status

### Device Requirements relating to the ZCL Time Cluster and its usage

All italicised terms in this Section 9.1.2 shall have the meanings defined in the *Time Cluster* specification within the ZigBee Cluster Library (ZCL) [075123r04ZB].

In relation to the ZCL *Time Cluster*, a Communications Hub shall:

* set the *Time* attribute to the *UTCTime* provided to it via its WAN interface, whenever such time information is available to it via its WAN interface;
* set the *Time* attribute to 0xFFFFFFFF whenever it does not have access to time information via its WAN interface; and
* always have *TimeStatus* attributes set as:
  + - * Attribute Bit Number 0 (Master) equal to 0b1 (master clock);
      * Attribute Bit Number 1 (Synchronised) equal to 0b0 (not synchronised);
      * Attribute Bit Number 2 (MasterZoneDst) equal to 0b0 (not master for Time Zone and DST); and
      * Attribute Bit Number 3 (Superseding) equal to 0b1 (time synchronization should be superseded).

In relation to the ZigBee Time Cluster, an ESME shall always have *TimeStatus* attributes set as:

* Attribute Bit Number 0 (Master) equal to 0b0 (not master clock);
* Attribute Bit Number 1 (Synchronised) equal to 0b0; and
* Attribute Bit Number 3 (Superseding) equal to 0b0 (time synchronization should not be superseded).

At power on of the clock, an ESME or GSME shall:

* set its Time Status as ‘Invalid’;
* attempt to synchronise time, using the Communications Hub’s Time Cluster; and
* where a valid *Time* (so not 0xFFFFFFFF) is provided by the Communications Hub before any Set Clock Command is received, set its time to the value of *Time* provided and set its Time Status to ‘Unreliable’.

ESME and GSME shall attempt to synchronise time, using the Communications Hub’s Time Cluster, once every 24 hour period in line with the SMETS requirement. ESME and GSME shall undertake the following processing dependent on the outcome of each attempted synchronisation:

* if a time of 0xFFFFFFFF is provided or if no time is received the Device shall set its Time Status to ‘Unreliable’;
* if the time provided by the Communications Hub differs from the Device’s time by more than 10 seconds, then the Device shall:
  + - * set its Time Status to ‘Unreliable’; and
      * if this results in a change to Time Status, the Device shall construct and issue an Alert with Alert Code 0x000C, meaning that its time would have been shifted by more than 10 seconds. If the Device is a GSME, the Alert Payload shall be a GBZ Alert Payload. If the Device is an ESME, the Alert Payload shall be a DLMS COSEM Alert Payload.
* if the time provided by the Communications Hub differs from the Device’s time by 10 seconds or less, then the Device shall adjust its time to the Communications Hub’s time.

Whenever an ESME or GSME attempts to synchronise time with the Communications Hub, and a time of 0xFFFFFFFF is provided or no time is received, the ESME or GSME shall retry the synchronisation after an elapsed period of 30 minutes, for a minimum of the lesser of three retries, or a retry resulting in a valid Time (so not 0xFFFFFFFF) being provided.

### ECS70 Set Clock on ESME

This Use Case covers the setting of the Clock by the Supplier on an ESME.

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.C |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | Yes |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.11 |
| SMETS Command | Set Clock |
| SMETS Data Item | N/A |
| Valid Target Device(s) | ESME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | DLMS COSEM |

Table 9.1.3: Use Case Cross References for ECS70 Set Clock on ESME

#### Pre-conditions

None.

#### Detailed Steps

The Command Payload shall be constructed as per Table 9.1.3.2a.

| **Class** | **OBIS Code** | **Attribute or Method?** | **Attribute / Method no.** | **Set, Get or Action** | **Attribute/Method name and Blue Book ref.** | **DLMS COSEM data types** | **Value (for Sets or Actions)** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 0-0:1.0.0.255 | A | 9 | Set | clock\_base | Enum | 5 | 5 shall mean radio controlled which shall be interpreted as controlled via the Communications Hub Time Cluster that is available over the ESME’s HAN interface |
| 8 | 0-0:1.0.0.255 | M | 5 | Action | preset\_adjusting\_time | structure{  preset\_time: octet-string,  validity\_interval\_start: octet-string,  validity\_interval\_end: octet-string} | {‘not specified’,  Supplier Current Time,  Supplier Current Time + Tolerance Period} | ‘not specified’ shall mean 0xFF in parts of preset\_time as required by the Blue Book. All times shall be formatted as octet-string according to section 4.1.6.1 of the Blue Book |
| 8 | 0-0:1.0.0.255 | M | 4 | Action | adjust\_to\_preset\_time | Integer | 0 |  |
| 8 | 0-0:1.0.0.255 | A | 2 | Get | time | Octet-string | Null | This get means that the resulting Time of the ESME shall be provided in the Response |
| 8 | 0-0:1.0.0.255 | A | 4 | Get | status | Unsigned | Null | This get means that the resulting Time Status of the ESME shall be provided in the Response |

Table 9.1.3.2a: Construction of Command Payload

In this Section 9.1.3.2, the object with OBIS code 0-0:1.0.0.255 shall be referred to as the *Clock* and italicised terms shall have their Blue / Green Book meaning.

On receipt of the Command, the ESME shall undertake processing in the following sequence:

1. the ESME shall undertake the ‘Command Authenticity and Integrity Verification’ processing required for Commands of type SME.C.C. If that fails, processing shall cease;
2. the ESME shall process the instructions in the *access-request-body* of the Command as follows:
3. when attribute 9 of the *Clock (clock\_base)* is set to ‘*radio controlled*’ (5), the ESME shall request the value of the Communications Hub Time from the Communications Hub via its ZigBee radio. If a time of 0xFFFFFFFF is provided or if no time is received:
4. if the current Time Status is set to ‘Reliable’, the ESME shall set bit 1 of attribute 4 (so setting *status* of Clock to be ‘*doubtful value*’ (Unreliable)); or
5. if the current Time Status is not set to ‘Reliable’, the ESME shall not change status.
6. the *preset\_adjusting\_time* method of the Clock shall be executed. Note this is to set parameters for the *adjust\_to\_present\_time* method.
7. the *adjust\_to\_present\_time* method of the Clock shall be executed as follows:
8. if the Communications Hub Time returned lies between *validity\_interval\_start* and *validity\_interval\_end*, then:
9. ESME *time* shall be updated to match Communications Hub Time;
10. the ESME shall unset bit 0 of attribute 4 (so setting *status* of the *Clock* not to be an ‘*invalid value*’); and
11. the ESME shall unset bit 1 of attribute 4 (so setting *status* of the *Clock* not to be a ‘*doubtful value*’);
12. if the Communications Hub Time returned lies before *validity\_interval\_start* (Supplier Current Time) or after *validity\_interval\_end* (Supplier Current Time + Tolerance)) and (bit 0 of attribute 4 of the *Clock* is unset), then:
13. time shall remain unchanged, since time is outside the *validity\_interval*; and
14. the ESME shall set bit 1 of attribute 4 (so setting status of *Clock* to be a ‘*doubtful value*’ (Unreliable))
15. the *get request* on the *time* and *status* attributes of the *Clock* shall be executed;
16. the ESME shall undertake the ‘Response Construction’ and ‘Response Cryptographic’ processing required for a Response of type SME.C.C.

On receipt of the Response, the recipient may undertake the ‘Response Recipient Processing’ for Responses of type SME.C.C.

The meaning of result attributes is as defined in the Green Book.

The meaning of the unsigned integer returned by the get request on attribute 4 of the Clock (status) is as per Table 9.1.3.2b.

|  |  |
| --- | --- |
| **Values in attribute 4 of the *Clock* object** | **Time Status Meaning** |
| Bit 0 is set (0x01) | Invalid |
| Bit 0 is unset and Bit 1 is set (0x10) | Unreliable |
| Bit 0 is unset and Bit 1 is unset (0x00) | Reliable |

Table 9.1.3.2b: Meaning of unsigned integer

### Time related object on ESME

Italicised terms in this Section shall have their Blue Book meaning.

An ESME shall have a *Data* object with *OBIS* code 0-0:94.44.100.255 where attribute 2 of that object:

* shall be a *double-long-unsigned* value;
* shall have a value set by the ESME to the number of seconds between 0 hours 0 minutes 0 seconds on 1st January 2000 UTC and the value of UTC time specified by attribute 2 of the *Clock* object with OBIS code 0-0:1.0.0.255;
* shall be the value recorded by the ESME in attribute 2 of any *Profile generic* object *entry* as the date-time stamp, at the time the *entry* is added;
* shall be the format recorded by the ESME in attribute 2 of any *Profile generic* object *entry* in other date-time fields.

Correspondingly:

* the *‘from\_value’* and *‘to\_value’* fields in the *selective access* structure, which are required by the GBCS when accessing attribute 2 of any *Profile generic* object directly, shall be *double-long-unsigned* attributes containing a date-time specified in seconds since 0 hours 0 minutes 0 seconds on 1st January 2000 UTC; and
* the *restricting\_object* field in the *selective access* structure shall be set with values of class\_id = 1; logical\_name = 0-0:94.44.100.255; attribute\_index = 2 and data\_index = 0.

The Blue Book requires that, for a *Data Protection* class object, *restriction\_by\_date* access has *from\_date* and *to\_date* specified as octet-string. Thus, where a Use Case requires that the contents of attribute 2 of a *Profile generic* object are returned in Encrypted form (and so accessed via a Data Protection object):

* the *from\_date* and *to\_date* fields in the Command shall be octet-strings formatted as per section 4.1.6.1 of the Blue Book; and
* the ESME shall undertake the conversion necessary to equate these values to *‘from\_value’* and *‘to\_value’* equivalents in accessingattribute 2 of any *Profile generic* object.

### GCS28 Set Clock on GSME

This Use Case covers the setting of time by the Supplier on a GSME.

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.C |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | Yes |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.11 |
| SMETS Command | Set Clock |
| SMETS Data Item | N/A |
| Valid Target Device(s) | GSME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 9.1.5: Use Case Cross References for GCS28 Set Clock on GSME

#### Pre-conditions

None.

#### Construction of Command

Set Clock Command Payloads shall be constructed according to the requirements of Section 9.1.5.4 and populated as specified in Table 9.1.5.2.

MAC Header, Grouping Header, KRP Signature and ACB-SMD MAC shall be populated as required for a Command of the SME.C.C Message Category.

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** |
| @SetTime.CommandPayload | SEQUENCE |  |  |
| validityIntervalStart | GeneralizedTime | The earliest time the Communications Hub can provide if the Command is to set Reliable Time | Mandatory |
| validityIntervalEnd | GeneralizedTime | The latest time the Communications Hub can provide if the Command is to set Reliable Time | Mandatory |

Table 9.1.5.2: @SetTime.CommandPayload population

#### Device processing of Command and Response handling

The GSME receiving a Set Clock Command shall undertake processing steps in the sequence defined in this Section 9.1.5.3.

The GSME shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of the SME.C.C Message Category;
2. request the now current Communications Hub Time. If the Communications Hub cannot supply a time that it has established as Reliable, it shall provide 0xFFFFFFFF. If this is sent, or no response is received, the GSME shall:
   1. if its current Time Status is set to ‘Reliable’, set Time Status to ‘Unreliable’, set deviceTimeStatus to unreliable, populate deviceTime with its current Time and process from step 5; or
   2. if its current Time Status is not set to ‘Reliable’, set deviceTimeStatus to be Time Status, populate deviceTime with its current Time and process from step 5.
3. if ((the Communications Hub Time < validityIntervalStart) or (Communications Hub Time > validityIntervalEnd)), set Time Status to ‘Unreliable’, and set deviceTimeStatus to unreliable, leave its Time unchanged, populate deviceTime with its current Time and process from step 5;
4. set its time to the Communications Hub Time, populate deviceTime with the corresponding value, and set deviceTimeStatus to reliable;
5. populate the Response Payload according to the requirements of Section 9.1.5.4 using the deviceTimeStatus and deviceTime values produced by the processing in this Section 9.1.5.3;
6. construct MAC Header, Grouping Header and apply the Response Cryptographic Protection required for a Response of the SME.C.NC Message Category, and
7. send the Response.

On receipt of the Response, the recipient may undertake the ‘Response Recipient Processing’ for Responses of type SME.C.C.

#### Set Clock Command and Response Payloads - structure **definition**

Each instance of @SetTime.CommandPayload and of @SetTime.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 9.1.5.4 which specifies the structure in Abstract Syntax Notation One (ASN.1) notation.

SetTime DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the period within which the Communications Hub’s time must lie

-- if this Command is successfully to set time

validityIntervalStart GeneralizedTime,

validityIntervalEnd GeneralizedTime

}

ResponsePayload ::= SEQUENCE

{

-- Specify the Device’s now current time

deviceTime GeneralizedTime,

-- Specify the Device’s now current Time Status

deviceTimeStatus DeviceTimeStatus

}

DeviceTimeStatus ::= INTEGER

{

reliable (0),

invalid (1),

unreliable (2)

}

END

## Future Dated Remote Party Messages

### Future Dated Commands for the Reading of Attributes - informative

Where future dated execution of a Command to read attributes is supported in a Use Case, this is achieved by setting values in a schedule stored on the Device. In such cases, the sequence of Messages is as follows:

* on receipt of a Command to update a schedule, the Device should attempt to Authenticate then execute the Command. The Device should then create a corresponding Response either indicating the schedule has been set or providing failure reasons; and
* when each trigger time in the schedule is reached (according to the Clock on the Device), the Device undertakes the required processing then creates and sends an Alert. One initial Command to set a schedule may generate many such Alerts.

In such circumstances, the Command and Response are specified in one Use Case, and the Alert is specified in a different Use Case.

Such future dated reading can be cancelled by sending a Command which resets the schedule values.

The only example of such a schedule is the Billing Calendar. The Alerts generated are Billing Calendar Alerts.

### Future Dated Commands for the Writing of Attributes

#### Introduction - informative

Only Commands marked ‘Capable of future dated invocation?’ in the Mapping Table can be future dated. Such Commands allow an attribute or group of attributes to be changed at a date-time in the future.

Where an attribute or group of attributes on a Device are capable of future dated updates, this is achieved by the Device having:

* a ‘current’ and a ‘next’ version of the group of attributes in question;
* an attribute for recording the date / time at which the ‘next’ version should be made ‘current’; and
* a method to set ‘current’ values equal to ‘next’ values.

This is the meaning of attributes with ‘Current’ and ‘Next’ post fixes in the ‘SMETS / CHTS Attribute / method’ column of the Mapping Table.

In such cases, the sequence of Messages to effect a future dated update would be:

1. a Command would be sent to the Device instructing that the attributes in question should be stored in the ‘next’ attributes and the activation date / time should be set (so overwriting previous ‘next’ values and any previous activation date / time);
2. only if the Command is Authenticated, would the Device attempt to execute the instructions in Command. Execution for such Commands means writing to ‘next’ values and setting activation date-times. If the activation date-times are in the past, the Device will also attempt to make the ‘next’ values ‘current’;
3. the Device would then create a Response. This Response would either confirm that the ‘next’ values and the activation date / time have been set (and so any previous future dated command with this Message Code has been over written), or would provide failure reasons. The ‘current’ values would be unaffected assuming the activation date / time is in the future; and
4. when the activation date / time is reached (according to the clock on the Device), the Device would attempt to make the ‘next’ values ‘current’. The Device would then send an Alert detailing success or failure.

Like all other Commands, future dated Commands cannot be modified once accepted by the Device. However, the time activated processing can be stopped from happening by sending a new Command of the same Message Type. This is because the new Command over writes the values from the old Command.

For example:

* a ‘cancellation’ can be effected by sending a new Command where the activation date / time in the new Command has a value that means ‘never’ to the Device; and
* a ‘modification’ can be effected by sending a new Command where the activation date-time and / or the ‘next’ values in the new Command are different than the old one.

Commands that are marked ‘Capable of future dated invocation?’ in the Mapping Table can also be invoked immediately, as specified in Section 9.2.2.3.

When there is a change of Supplier on a Device which is (1) after a future dated change is stored but (2) before it is activated, the processing at Section 13.3.5.10 will be undertaken at the point of update of Security Credentials. This ensures future dated commands from the old Supplier will not be actioned by the Device.

#### Effect on prior Commands of the same Message Code

On receipt of an Authenticated future dated Command, the Device shall over write all parts of any previously sent future dated Command of the same Message Code and, if the activation date-times for the instructions in the Command are in the past, the Device shall execute the instructions immediately.

#### Using a future dated Command to write Attributes immediately

Where a Command is marked ‘Capable of future dated invocation?’ in the Mapping Table, instructions within the Command shall be executed immediately after Authentication by the Device when:

* for DLMS COSEM Commands Payloads, activation date-time(s) have the value 0x0000000000000000008000FF;
* for ZSE Command Payloads, the activation date-time(s) have the value 0x00000000; and
* for ASN.1 Command Payloads, the activation date-time is not present.

#### Cancellation of future dated Commands for the writing of Attributes

Where a Command is marked ‘Capable of future dated invocation?’ in the Mapping Table, instructions within the Command shall never be executed by the Device when:

* for DLMS COSEM Commands Payloads, activation date-time(s) have the value 0xFFFFFFFFFFFFFFFFFF8000FF;
* for ZSE Command Payloads, the activation date-time(s) have the value 0xFFFFFFFF for any ZSE command other than PublishCalendar, PublishSpecialDays, PublishBlockThresholds, PublishPriceMatrix;
* for ZSE Command Payloads, the activation date-time(s) have the value 0xFFFFFFFE for the ZSE command PublishCalendar, PublishSpecialDays, PublishBlockThresholds, PublishPriceMatrix; and
* for ASN1 commands, the activation date-time has a value of 99991231235959Z.

For clarity, sending such a Command has the effect of ‘cancelling’ any previously sent future dated Command of the same Message Code that the Device has not already executed.

#### Reactions to Future Dated Commands

Subject to Command Authenticity and Integrity Verification as detailed in Section 6, where a Command is future dated:

* at time the Command is received, the Device shall send a Response to the Command confirming the Command’s receipt or a failure; and
* if the Command's details were successfully stored, the Device shall, at the time the future date is reached, process each of the instructions as specified in the Command in the sequence specified in that Command and then generate an Alert with an Alert Payload of the same type as the Payload type of the Command. Thus:
  + - * an ASN.1 Command Payload shall lead to an ASN.1 Alert Payload, which shall be as defined in Section 13;
      * a DLMS COSEM Command Payload shall lead to a DLMS COSEM Alert Payload, which shall be as defined in Table 7.2.9c, where the Use Case specific additional content contains the concatenation 0x09 || 0x0A Message Code || Originator Counter from the corresponding Command Payload. Note that 0x09 is the DLMS COSEM tag for octet-string and 0x0A is the length of the concatenation Message Code || Originator Counter; or
      * a GBZ Command Payload shall lead to a GBZ Alert Payload, shall be as defined in Table 7.2.10c, where the Use Case specific additional content contains the concatenation Message Code || Originator Counter from the corresponding Command.

# ZSE Implementation

Italicised terms in this Section 10 shall have their meaning in the ZCL / ZSE specifications.

## Introduction - informative

This Section 10 sets out specific requirements relating to the implementation of ZSE in Devices:

* Tunnels: requirements relating to Devices’ support for the *Tunneling Cluster*. This includes specific differences between GSME, HHT and other Devices, related to their use of the *Tunneling Cluster*. Note that all Devices except Type 2 Devices shall support the *Tunneling Cluster*, since this is the mechanism by which Remote Party Messages (and HAN Only Messages between a PPMID and a GSME) are transported over the HAN;
* GSME and GPF interactions (including the Tapping Off Mechanism): this includes requirements relating to the GPF maintaining a copy of GSME data items, where copies are not supported natively by ZSE mirroring;
* GPF structured data items: requirements relating to how structured data items on the GPF are updated by the GSME and resulting values on the GPF are calculated; and
* HHT interactions – requirements relating to HHT connection to the SMHAN, including specific *Tunneling Cluster* related requirements.

## Tunnels

### Overview – informative

All Remote Party Messages are carried across the SMHAN using the *Tunneling Cluster’s TransferData* command.

Type 2 Devices such as IHDs are not required to send or receive Remote Party Messages and so are not required to support the *Tunneling Cluster*.

Remote Party Messages to and from the GPF do not cross the SMHAN and so do not use the *Tunneling Cluster.*

All other types of Device need to be able to send and receive Remote Party Commands over the SMHAN and so, as specified in Section 10.2.2, shall support the *Tunneling Cluster*.

Section 10.2.2 lays out the associated requirements, across all Devices including those for the GSME and HHT.

GSME requirements are different than all other Devices since a GSME is a ‘sleepy’ Device. Additional GSME requirements are laid out in Sections 10.2.4 to 10.3.

HHT interactions also have specific requirements due to their function. These specific requirements are laid out in Section 10.5.

### Requirements for the Tunneling Cluster

Remote Party Messages and SME.C.PPMID-GSME Messages shall be transported over the SMHAN using the *Tunneling Cluster’s TransferData* command. Except where a *TransferData* command is to or from a GSME, the value of the *Data* field’s payload in the *TransferData* command shall be the Remote Party Message. Where a *TransferData* command is to or from a GSME, the *Data* field’s payload of the *TransferData* command shall take the values specified in Section 10.2.4.

Devices supporting the *Tunneling Cluster* as a *Server* shall have a *MaximumIncomingTransferSize* set to 1500 octets, in line with the ZSE default. All Devices supporting the *Tunneling Cluster* shall use this value in any *RequestTunnelResponse* command and any *RequestTunnel* command.

Devices shall set the value of the *ManufacturerCode* field in any *RequestTunnel* command to 0xFFFF (‘*not used’*).

The *ProtocolID* of all Remote Party Messages shall be 6 (‘*GB-HGRP’*). Devices shall set the value of the *ProtocolID* field in any *RequestTunnel* command to 6.

Devices shall set the value of the *FlowControlSupport* field in any *RequestTunnel* command to ‘*False’*.

All Devices except Type 2 Devices and GPFs shall support the *Tunneling Cluster* and, within that Cluster, the use of the protocol with a *ProtocolID* of 6(*GB-HGRP*).

An ESME, an HCALCS and a PPMID shall support the *Tunneling Cluster* as a *Server*.

A GSME and an HHT shall support the *Tunneling Cluster* as a *Client*.

A CHF shall support the *Tunneling Cluster* as a *Client* and as a *Server*.

A GPF shall support mirroring functionality. The *Basic Cluster Physical Environment* attribute shall be supported and shall have the value 0x01.

#### ESME, HCALCS and PPMID

When a Communications Hub has successfully established a shared secret key using *CBKE* with a Device of type ESME, HCALCS or PPMID, the CHF shall send a *RequestTunnel* command to the Device to request a tunnel association with the Device.

Where an ESME, a HCALCS or a PPMID remains in the CHF Device Log, the CHF shall send a *RequestTunnel* command to the Device whenever:

* 0xFFFF seconds have elapsed since receipt of the most recent *RequestTunnelResponse* command from that Device; or
* the CHF receives a Remote Party Message addressed to the Device but does not have a functioning tunnel association with the Device; or
* the CHF powers on.

Where the CHF receives a *RequestTunnelResponse* command from a Device with a *TunnelStatus* of 0x01 (*Busy*), the CHF shall send another *RequestTunnel* command three minutes later.

Where the CHF receives a *RequestTunnelResponse* command from a Device with a *TunnelStatus* of 0x02 (*No More Tunnel IDs*), the CHF shall send a *CloseTunnel* command for any *TunnelID* that may relate to an active tunnel association with that Device and, after receiving responses to all such commands, send another *RequestTunnel* command.

#### GSME

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

* send a request to the *ZigBee Gas ESI Endpoint* requesting the creation of a mirrored *Metering Cluster* using the *RequestMirror* command;
* configure the *ZigBee Gas Mirror Endpoint* to use the two way mirroring notification scheme ‘*Scheme B’* ; and
* send a *RequestTunnel* command to the CHF to request a tunnel association with the CHF*.*

For clarity, the GSME:

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

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

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

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

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

### GSME Tunnel Management – informative

Commands are sent from the Communications Hub via the tunnel to the GSME. Since the GSME is a ‘sleepy’ Device, a mechanism is needed for the GSME to request that Commands are sent to it by the CHF.

In common with the transport of all Remote Party Messages, the mechanism used is the *TransferData* command, but *TransferData* commands sent between a GSME and GPF need to distinguish between when:

* the GSME is sending a Remote Party Message, so an Alert or a Response or a GBT Message containing part of an Alert / Response;
* the GSME is asking the GPF to send it a Command, or a GBT Message containing part of a Command; and
* the GPF is sending the GSME a Command, or a GBT Message containing part of a Command.

To meet this need, the following sections specify additional structure in the first part of the *Data* parameter of the *TransferData* commands sent between GSME and GPF. Specifically the sending Device shall:

* where a Remote Party Message is being sent, set the *Data* parameter payload in a *TransferData* command to the concatenation:

Tunnel Manager Header || Remote Party Message

* where a Remote Party Message is not being sent (so when the GSME is requesting that a Message is sent), set the *Data* parameter payload in a *TransferData* command to the value of Tunnel Manager Header.

A mechanism is also required to notify the GSME that one or more Commands are available for retrieval from the CHF.

The ZSE specification has a flag called *Tunnel Message Pending* in the *Functional Flag Notification* definition. This flag is used to notify a GSME that the CHF has a Remote Party Message waiting to be transferred to the GSME. The flag is set on the first pending Command and is reset when all Remote Party Messages have been transferred to the GSME. The flag is available through the *ReadAttribute* or *MirrorAttributeResponse* command. The requirements for setting this flag are specified in Section 10.3.4. The Tunnel Manager Header identifies three different kinds of *TransferData* command usage:

* GET (the value 0x01): this is used by the GSME to retrieve waiting Message from the CHF;
* GET-RESPONSE (the concatenation 0x02 || number of Remote Party Messages remaining): this is used by the CHF to send a Remote Party Message to the GSME. It also indicates how many Remote Party Messages have yet to be retrieved; and
* PUT(the value 0x03): this is used by the GSME to send a Message via the CHF.

Where a Command is waiting on the CHF for the GSME to retrieve it, the following sequence shall apply:

1. the *Tunnel Message Pending* flag is set on the Communications Hub as detailed in Section 10.3.4;
2. the GSME turns on its HAN Interface and obtains the value of the *Tunnel Message Pending* flag; and
3. *Tunnel Message Pending* flag is set:
4. the GSME sends a *TransferData* command to the CHF with the GET structure in the Tunnel Manager Header. The Tunnel Manager Header is the only content in the *Data* field of this *TransferData* command;
5. the CHF sends a *TransferData* command to the GSME with the GET-RESPONSE structure in the Tunnel Manager Header and a Message in the remaining part of the *Data* field of the command. The GET-RESPONSE structure details how many more Messages are available for retrieval; and
6. the GET and GET-RESPONSE pattern repeats until all Messages have been transferred or the GSME decides to stop requesting Messages.

When the GSME wishes to send a Message, the GSME sends a *TransferData* command to the CHF with the PUT structure in the Tunnel Manager Header and the Message in the remainder of the *Data* field in the *TransferData* command.

### TransferData commands sent between GSME and GPF

When it wishes to send a Message, so an Alert or Response or GBT Message, a GSME shall send a *TransferData* command to the CHF with the value in the *Data* parameter payload of the *TransferData* command set to the concatenation:

0x03 || Message

When it wishes to retrieve a Message stored for it on a CHF, a GSME shall send a *TransferData* command to the CHF with the value in the *Data* field set to 0x01. When the CHF receives such a *TransferData* command from a GSME, the CHF shall send a *TransferData* command to the GSME with the value in the *Data* parameter payload set to:

* the concatenation

0x02 || (Number of Messages remaining for retrieval after this Message) || (Message addressed to the GSME)

where it has Messages for the GSME not yet downloaded by the GSME; or

* the concatenation 0x02 || 0x00, where it has no Messages for the GSME to retrieve, the 0x00 representing the number of Messages available to retrieve.

## GSME and GPF interactions

### Introduction - informative

The GSME is informed that Remote Party Commands are available for it to retrieve via *Tunnel Message Pending* flag on the GPF.

The GSME should, under normal operating circumstances, retrieve all Commands buffered for it when it turns its HAN Interface on. For example, if two Commands are buffered for it, the GSME should retrieve both Commands before turning its HAN Interface off.

However, in some circumstances, a GSME may chose not to retrieve all buffered Commands in a single session. In such cases, the GSME should retrieve each Command as soon as possible after that Command is received by the CHF.

Potential reasons for a GSME failing to retrieve all buffered Commands include:

* the GSME battery requires time to recover;
* the GSME is entering a ‘low battery’ mode and limiting the use of its radio; or
* a radio communications error.

Section 10.3 details actions the CHF may take where Commands, or GBT Messages containing parts of Commands, for a GSME are not retrieved by the GSME.

Commands addressed to a GSME must be processed by the GSME and, when successfully processed, any changed operational or configuration data must be made available to the GPF. The GPF then has updated information to provide to other Devices on the same SMHAN.

In ZSE terms, the GPF incorporates two distinct logical Devices, which are discoverable and addressed on different *endpoints*. Section 7 describes which *clusters* reside on which *endpoint*.

Figure 10.3.1 shows a simplified model of the Devices within the Communications Hub and their relation to the ZSE *endpoints*.



Figure 10.3.1: Communications Hub showing ZigBee endpoints

### GSME data residing on the *ZigBee Gas Mirror Endpoint* - informative

The *ZigBee* *Gas Mirror Endpoint* provides a ‘reflection’ of the data held by the GSME. A GSME is typically a battery-powered Device and its HAN Interface is mostly not turned on, making it unable to respond to other Devices. The GSME turns its HAN Interface on at regular intervals (e.g. 30 minutes) and pushes consumption data to the ZigBee *Gas Mirror Endpoint.* This provides other Devices on the same SMHAN with access to GSME consumption data at any time.

### GSME data residing on the *ZigBee Gas ESI Endpoint* - informative

The *ZigBee* *Gas ESI* *Endpoint* holds GSME data which is provided by a Remote Party, for example pricing. The *ZigBee* *Gas ESI Endpoint* makes this type of data available to Devices on the same SMHAN.

GSME data from a Remote Party is sent to the GSME in a Remote Party Command. Such a Command has to be validated by the GSME before any data in it is applied by the GSME. For example, a Command to change tariff must be rejected by the GSME if it fails authentication, and the data in the Command must not be applied in such circumstances.

If data in a Remote Party Command is accepted by the GSME, a mechanism is needed to provide the changed data to the *ZigBee Gas ESI Endpoint*. This is so that the *ZigBee Gas ESI* *Endpoint* can then provide that data to other Devices on the same SMHAN.

A mechanism is also needed to deal with a Response not being received from the GSME. The lack of a Response may indicate that the GSME and the *ZigBee Gas ESI* *Endpoint* do not contain the same value in one or more data items. If data items on the two are not synchronised, Devices on the SMHAN will display incorrect information.

There are several possible reasons why this lack of a Response may arise, not all of which mean that data is out of synchronisation:

* the Command has failed validation by the GSME and has been discarded;
* the Response has been lost due to a communications error; or
* a software error.

Figure 10.3.3 illustrates the data flows (A to G) from a Remote Party to the *ZigBee Gas ESI Endpoint*.

The Tapping Off Mechanism (TOM) supports the data flows illustrated in Figure 10.3.3, without the need for the GSME to transmit the contents of the original Remote Party Command back to the Communications Hub.

 Figure 10.3.3: Data Flows to ZSE Gas ESI Endpoint

### GSME Command retrieval and TOM Requirements

#### TOM Commands and Responses

A Command shall be a TOM Command if it is a Remote Party Command with one of the following Message Codes:

* 0x006B (GCS01a Set Tariff and Price on GSME);
* 0x0071 (GCS07 Send Message to GSME);
* 0x0072 (GCS09 Set Change of Tenancy date on GSME);
* 0x007C (GCS23 Set CV and Conversion Factor Value(s) on the GSME);
* 0x0088 (GCS44 Write Contact Details on GSME); or
* 0x00A3 (GCS01b Set Price on GSME).

A TOM Response shall be a Response to a TOM Command.

For clarity, neither a TOM Response nor a TOM Command may contain Encrypted data.

#### Processing of Commands addressed to a GSME

The CHF, GPF and GSME shall undertake the processing steps below following receipt of a Remote Party Command by the Communications Hub, where that Command is addressed to a GSME on the same SMHAN:

1. the CHF shall buffer the Command and instruct the GPF to set the *Tunnel Message Pending* flag to inform the GSME that the Command is awaiting retrieval. If the Command has been sent as multiple GBT Messages, the GPF *Tunnel Message Pending* flag shall only be set once all GBT Messages making up the Command have been received by the Communications Hub;
2. if 24 hours elapse after setting the GPF *Tunnel Message Pending* flag without the Command being retrieved by the GSME, the CHF may discard the Command. If the CHF discards a Command in this way, its shall notify the GPF and the GPF shall log the event in its Event Log and send an Alert with a GBZ Payload containing an Alert Code 0x009D;
3. when the GSME turns its HAN Interface on, it shall read the *Tunnel Message Pending* flag and retrieve the Command using the *TransferData* command as defined in Section 10.2.3. Each *TransferData* command received by the GSME shall result in the GSME sending a *DefaultResponse* command;
4. the CHF shall process the *DefaultResponse* commands it receives to establish when the Command has successfully been retrieved by the GSME, and shall provide an indication to the GPF accordingly. The GPF shall, when there are no further Commands or GBT Messages pending retrieval by the GSME, clear the *TunnelDataWaiting* flag;
5. if a Command is a TOM Command, the CHF shall retain a copy of the Command contents. For each such Command, the CHF shall start a response timer at the point where it has received *DefaultResponse* command(s) confirming the GSME has successfully retrieved the Command;
6. once a Command is successfully retrieved by the GSME, the GSME shall process the Command in line with the requirements of the GBCS. Note that (1) this processing shall result in the GSME attempting to send a Response to the Command or an Alert that it has received an invalid Command and (2) if sending a Response, the Response shall, as per the GBCS requirements, detail the success or failure of GSME processing for each instruction within the corresponding Command;
7. the GSME shall not, under normal operating conditions, delay sending the Response and shall, where possible, send it before turning its HAN Interface off;
8. on receipt of a Response that is a TOM Response, the CHF shall inspect the Response from the GSME. If the Response indicates successful execution of at least one elemental ZCL/ZSE command in the corresponding TOM Command, the CHF shall transfer a copy of the corresponding TOM Command contents and the TOM Response to the GPF, and shall clear the response timer for the Command;
9. on receipt of a TOM Response and the corresponding TOM Command contents, the GPF shall process the elemental ZCL/ZSE commands contained within the Command according to the *status* within the Response, updating data it holds accordingly. Once updated by the GPF, the GPF shall make this updated data available over the WAN and over the HAN to the Devices in the GPF’s Device Log;
10. if a Response to a TOM Command has not been received by the Communications Hub when the corresponding response timer reaches 6 hours:
    * + - the CHF may discard its copy of the TOM Command contents, clear the response timer and notify the GPF accordingly; and
        - on receipt of such a notification, the GPF shall log the event in its Event Log and send an Alert with a GBZ Payload containing an Alert Code 0x009E;
11. for clarity, the CHF shall relay all Remote Party Responses received on its HAN Interface through the WAN interface.

## GPF Structured Data Items

Underlined terms in this Section 10.4 shall have their meaning in the SMETS and / or CHTS.

### Introduction – informative

There are GPF requirements to store structured data items which do not have a direct one to one mapping in ZSE. These structured data items have to be constructed by the GPF.

### Structured Data Items

This Section 10.4.2 details how each structured data item shall be constructed by the GPF.

#### Daily Read Log

The GSME shall record the Daily Read Log data items at midnight UTC as defined in SMETS. In ZSE terms, the GSME shall take a *snapshot* of the relevant items. Note that the format and data of the *snapshot* taken is dependent upon the operating tariff. For example if the GSME tariff is ‘TOU only’, the snapshot shall not capture the block values.

The GSME shall use the *snapshot* *cause* ‘*General’* to identify the *snapshot* taken.

The GSME shall push the *snapshot* to the GPF using the *PublishSnapshot* command. It is not necessary for the GSME to report any attributes which duplicate those contained in the *snapshot*.

The GPF shall populate the relevant attributes upon receipt of the *PublishSnapshot* command, providing the command is received between midnight (UTC) and the next scheduled wake of the GSME.

The GPF shall store the data contained in the *PublishSnapshot* command in the GPF copy of the GSME Daily Read Log.

In the event of a communications outage, the GPF shall retrieve missing *snapshots* using the *GetSnapshot* command, with the UTC start time field populated based on the last received *snapshot* timestamp, if one has been received.

#### Prepayment Daily Read Log

If the GSME is operating in prepayment mode it shall record the Prepayment Daily Read Log data items at midnight UTC. In ZSE terms, the GSME shall take a *prepayment snapshot* of the relevant items. The format and data of the *prepayment snapshot* taken is defined in ZSE.

The GSME shall use the *snapshot cause* ‘*General’* to identify the *prepayment snapshot* taken.

The GSME shall push the *prepayment snapshot* to the GPF using the *PublishPrepaySnapshot* command.

The GPF shall populate the relevant attributes upon receipt of the *PublishPrepaySnapshot* command, providing the command is received between midnight (UTC) and the next scheduled wake of the GSME.

The GPF shall store the data contained in the *PublishPrepaySnapshot* command in the GPF copy of the GSME Prepayment Daily Read Log.

In the event of a communications outage, the GPF shall retrieve missing *prepayment snapshots* using the *GetPrepaySnapshot* command (and *GetPrepaySnapshot* notification flag) with the UTC start time field populated based on the last received *prepayment snapshot* timestamp, if one has been received.

#### Billing Data Log - informative

SMETS defines Billing Data Log as *‘a log capable of storing the following UTC date and time stamped entries:*

* *twelve entries comprising Tariff TOU Register Matrix, the Consumption Register and Tariff Block Counter Matrix;*
* *five entries comprising the value of prepayment credits;*
* *ten entries comprising the value of payment-based debt payments; and*
* *twelve entries comprising Meter Balance, Emergency Credit Balance, Accumulated Debt Register, Payment Debt Register and Time Debt Registers [1 … 2].’*

Requirements for each part are detailed separately in the following sections.

#### Billing Data Log - Tariff TOU Register Matrix, the Consumption Register and Tariff Block Counter Matrix

The GSME shall capture this *snapshot* at the following trigger points:

* End of Billing Cycle (snapshot cause “End of Billing Period” );
* Change of Payment Mode (snapshot cause “Change of Meter Mode”);
* Change of Tariff (snapshot cause ‘Change of Tariff Information’); and
* as specified in Section 13.3.5.10 (snapshot cause ‘Change of Supplier’).

When it next turns on its HAN Interface, the GSME shall push this *snapshot* to the GPF using the *PublishSnapshot* command.

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

In the event of a communications outage, the GPF shall retrieve missing *snapshots* using the *GetSnapshot* command (and the relevantnotification flag) with the UTC start time field populated based on the last received *snapshot* timestamp, if one has been received, or 0x0000 otherwise.

#### Billing Data Log - value of prepayment credits

A GSME shall support the *Top-up* *attribute set*.

A GPF shall mirror this *attribute set*.

Upon completion of processing of a valid prepayment top-up, the GSME shall push the latest five prepayment top-ups to the GPF using the *PublishTopup* command.

The GPF shall update the attributes of its *Top-up attribute set,* with the values held in the *PublishTopup* command.

*Note: There is no requirement for the GPF to mirror the ‘originating Device’ attributes of the Top-up attribute set.*

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.

#### Billing Data Log - payment-based debt payments

A GSME shall support the *Debt* attribute set.

A GPF shall mirror this attribute set.

The GSME shall push changed attributes in this set to the GPF. The GPF shall record all attributes related to each debt in the GPF copy of the GSME Billing Data Log.

Upon notification of a change of attributes within a particular debt’s attribute set, the GPF shall record all attributes related to that particular debt to the GPF copy of the Billing Data Log.

In cases of communications outages, the GPF shall request any outstanding debt payments by use of the *GetDebtRepaymentLog* command (and *GetDebtRepaymentLog* notification flag).

#### Billing Data Log - payment-based debt payments Meter Balance, Emergency Credit Balance, Accumulated Debt Register, Payment Debt Register and Time Debt Registers [1 … 2]

The GSME shall capture this snapshot at the following trigger points:

* End of Billing Cycle (snapshot cause ‘End of Billing Period’ );
* Change of Payment Mode (snapshot cause ‘Change of Meter Mode’);
* Change of Tariff (snapshot cause ‘Change of Tariff Information’); and
* as specified in Section 13.3.5.10 (snapshot cause ‘Change of Supplier’)..

When it next turns on its HAN Interface, the GSME shall push this *snapshot* to the GPF using the *PublishPrepaySnapshot* command.

The GPF shall store the data contained in the *PublishPrepaySnapshot* command in the GPF copy of the GSME Billing Data Log.

In the event of a communications outage, the GPF shall retrieve missing *snapshots* using the *GetPrepaySnapshot* command (and *GetPrepaySnapshot* notification flag) with the UTC start time field populated based on the last received snapshot timestamp, if one has been received.

#### GPF Profile Data Log

The GPF shall create the GPF Profile Data Log from the consumption information pushed by the GSME each half hour.

The GSME shall, on each half hour, record the following information and push to the GPF:

* total consumption value (with units of m3);
* total consumption today (with units of kWh); and
* total cost of consumption today (with units of Currency Unit);

Upon receipt of the pushed data, the GPF shall calculate the consumption with units of m3 over the previous half hour by subtracting its previously recorded total consumption value from the total consumption value now sent.

The resulting value shall be stored in the GPF Profile Data Log.

In the event that there are missing values in the GPF Profile Data Log, the GPF shall interrogate the GSME Profile Data Log using the *GetSampledData (SampleID 1)* command and the *StayAwake* notification flagto retrieve missing values.

#### GPF Daily Gas Consumption Log

The GPF shall create the GPF Daily Gas Consumption Log based on the values pushed from the GSME. The last total consumption value pushed from the GSME each UTC day shall be time stamped and stored in the GPF Daily Gas Consumption Log.

In the event of communications outages resulting in the final daily value being missed, the GPF shall retrieve the value from the GSME Profile Data Log using the *GetSampledData (SampleID 0)* command and *StayAwake* notification flag.

#### Historical Attributes

A GSME shall support:

* the *Historical Cost Consumption Information* attribute set, measured in Currency Units; and
* the *Alternative Historical Consumption* attribute set, measured in kWh.

A GPF shall mirror the attribute sets listed above.

As per Section 10.4.2.8, the GSME shall, on each half hour, record the following information and push to the GPF:

* total consumption value (with units of m3);
* total consumption today (with units of kWh); and
* total cost of consumption today (with units of Currency Unit);

Using the ‘total consumption today’ value, the GPF shall update the attributes of the mirrored *Alternative Historical Consumption* attribute set.

Using the ‘total cost of consumption today’ value, the GPF shall update the attributes of the mirrored *Historical Cost Consumption Information* attribute set.

In exception circumstances, the GPF shall request the GSME to push the historical data sets using the ‘*Push Historical Metering Data Attribute Set*‘ and ‘*Push Historical Prepayment Data Attribute Set’* notification flags.

## Hand Held Terminal (HHT) interactions

### Introduction - informative

An HHT allows for delivery of Remote Party Messages to and from the SMHAN. This is as an alternative delivery route to the Communications Hub’s WAN connection. It is intended for one-off configuration of Devices, for example at installation. Hence, there are time outs to ensure usage is limited in this way.

This Section 10.5 specifies requirements related to:

* how a connection is made between an HHT and a Communications Hub; and
* how Remote Party Messages are then to be transferred to and from the HHT.

### Establishing a connection between an HHT and a Communications Hub - informative

The ZSE specification defines an *Inter-PAN Communications* mechanism. This mechanism is used to establish an initial secure link between the HHT and the Communications Hub, with the security being provided by ZSE’s *CBKE*. Once this secure link is established:

* the HHT uses the link to send its Entity Identifier and *Install Code* to the Communications Hub;
* the Communications Hub adds these details to the CHF’s Device Log (so allowing the HHT to *join* the SMHAN); and
* the HHT then *joins* the SMHAN and so can exchange Remote Party Messages within the Communications Hub, and the Communications Hub can relay them to / from the specified Device(s) on the HAN.

Both the *Inter-PAN Communications* and *joining* to the SMHAN use the CBKE mechanism that is defined in ZSE.

*Inter-PAN Communications* shall only be available for 60 minutes from power on of the Communications Hub. So, if needed, *Inter-PAN Communications* can be enabled by power cycling the Communications Hub.

The *Inter-PAN Communications* mechanism defined by ZSE requires the HHT to specify the Communications Hub that it wishes to link to. There may be multiple Communications Hubs available to the HHT to connect to via *Inter-PAN Communications.*

There are a number of options to provide the HHT with information sufficient to identify uniquely the Communications Hub it is to link to, including:

* the installer manually reading the GPF’s Entity Identifier (which is the IEEE address of the Communications Hub’s SMHAN radio) printed on the Hub, and confirming / selecting this on the HHT; or
* the installer using a scanner on the HHT to read the GPF’s Entity Identifier.

Two illustrative connection scenarios are provided in the following two sections

#### Illustration 1: Installer manually chooses network - informative

1. the Communications Hub opens inter-PAN communication for 60 minutes after power on;
2. the HHT is powered on;
3. the HHT performs an active scan using the *Beacon Request* mechanism;
4. the HHT displays the IEEE addresses returned in the *Beacons* from all neighbouring *PAN Coordinators*. Note that the GBCS requires the *Extended PAN ID* to be set to the Communications Hub’s HAN Interface’s IEEE address. This is the same as the GPF Entity Identifier, which is printed on the Communications Hub in line with CHTS;
5. the installer (who knows the Consumer’s Communications Hub’s ZigBee IEEE address as the GPF Entity Identifier is printed on the Communications Hub) picks the desired IEEE address;
6. the HHT initiates *Inter-PAN CBKE* with the Communications Hub;
7. the Communications Hub responds to the *Inter-PAN CBKE;*
8. if *Inter-PAN CBKE* completes successfully:
   * + - The HHT sends its Install Code and Entity Identifier to the Communications Hub in a command secured using the shared symmetric key (the *APS link key*) produced by the *Inter-PAN CBKE* process; then
       - The Communications Hub adds the HHT to the CHF Device Log; and then
       - The HHT then *joins* to SMHAN.
9. otherwise, no link is established.

#### Illustration 2: HHT uses barcode scan - informative

1. the Communications Hub opens inter-PAN communication for 60 minutes after power on;
2. the HHT is powered on;
3. the HHT optically scans the GPF Entity Identifier printed on the target Communications Hub;
4. the HHT performs an active scan using the *Beacon Request* mechanism;
5. when a Beacon returns an IEEE address equal to the scanned GPF Entity Identifier, the HHT initiates *Inter-PAN CBKE* with the Communications Hub so identified;
6. the Communications Hub responds to the *Inter-PAN CBKE;*
7. if *Inter-PAN CBKE* completes successfully:
   * + - the HHT sends its Install Code and Entity Identifier to the Communications Hub in a command secured using the shared symmetric key (the *APS link key*) produced by the *Inter-PAN CBKE* process; then
       - the Communications Hub adds the HHT to the CHF Device Log; and then
       - the HHT then *joins* to SMHAN.
8. otherwise, no link is established.

### WAN proxy operation - informative

The HHT has to be capable of holding Remote Party Messages, to which the appropriate Remote Party Message protection has already been applied, and has to be capable of exchanging such Messages.

The Communications Hub must therefore be able to maintain two effective ‘WAN’ interfaces; the real one via the WAN network interface and a ‘logical WAN’ via the connection to the HHT.

The Communications Hub shall send any Responses and Alerts through both its WAN interface and the link to the HHT, if present. Whilst this may result in apparent unsolicited Responses at the Remote Party which have to be dealt with, it ensures the earliest possible reconciliation of Commands destined for Smart Metering Equipment.

#### HHT and CHF – Device Requirements

As per Section 10.2.2, in all interactions between an HHT and a Communication Hub:

* the HHT shall support the *Tunneling Cluster* as a *Client*; and
* the Communication Hub shall support the *Tunneling Cluster* as a *Server*.

The Communication Hub shall only allow *Inter-PAN Communications* for 60 minutes from any power on of the Communication Hub. For clarity, this is the period during which an HHT can establish a connection, not the period of use of any connection.

At power on, a Communication Hub shall remove any Devices of type HHT (so a Device with device\_type = 0x7E with its DLMS COSEM class\_id 104 meaning) from the CHF Device Log.

To exchange Remote Party Messages, the Communication Hub and HHT shall only use the *TransferData* command.

The Communications Hub shall always set *nwkExtendedPANId* to be the Entity Identifier of the GPF, which is always the Communication Hub’s IEEE address for its HAN Interface.

#### HHT and CHF – establishing communications

Prior to being able to exchange Messages, the HHT and Communication Hub shall undertake the following steps:

1. the HHT shall identify the Communication Hub and initiate the *CBKE* process, as specified in the ZSE specification;
2. the Communication Hub shall not respond to any such request if more than 60 minutes has elapsed since the Communication Hub’s most recent power on, or if there is a Device of type HHT already in the CHF’s Device Log. Otherwise, the Communication Hub shall respond to the *CBKE* request;
3. if CBKE does not succeed, processing shall cease. Otherwise, processing shall continue from step 4;
4. using the *APS link key* established through *CBKE* to secure the commands:
5. the HHT shall send a *RequestTunnel* command to the Communication Hub, with contents as per Section 10.2.2*;*
6. the Communication Hub shall send a *RequestTunnelResponse* command in response;
7. if *TunnelStatus* in the response is not 0x00 (‘*success’*), processing by the HHT shall cease. Otherwise the HHT shall send a *TransferData* command with the *TunnelID* parameter set to the *TunnelID* provided in the *RequestTunnelResponse* command and the *Data* parameter payload set to the concatenation:

0x01 || Entity Identifier of the HHT || 16 octet *Install Code* of the HHT

1. on receipt of the *TransferData* command, the Communication Hub shall:

* add the HHT’s Entity Identifier to the CHF Device log, recording the Device as being of type HHT, so with a device\_type of 0x7E with its DLMS COSEM class\_id 104 meaning;
* permit joining of the SMHAN for either (1) 240 seconds or (2) until the HHT has joined the SMHAN, whichever is the earlier; and
* start a timer. When that timer reaches 0xFFFF seconds, the CHF shall remove the HHT from its Device Log, remove the HHT from the SMHAN and close any open tunnels to the HHT.

1. having added the HHT to its Device Log, the CHF shall send a *Default Response* to the HHT and close the tunnel to the HHT;
2. on receipt of the *Default Response*, the HHT shall, if that *Default Response* contains a *Status Code* of 0x00 (‘*success*’), attempt to *join* the SMHAN;
3. if the *joining* is successful, the HHT shall send a *RequestTunnel* command to the CHF, with contents as per Section 10.2.2*;*
4. the CHF shall process the *RequestTunnel* command and send a *RequestTunnelResponse* command in response;
5. if *TunnelStatus* in the *RequestTunnelResponse* command is not 0x00 (‘*success’*), processing by the HHT shall cease. Otherwise the HHT and CHF may now exchange Messages using the *TransferData* command.

Note that steps 1 to 4.e) above use *Inter-PAN Communications*; the remaining steps use the standard ZigBee SMHAN communications.

Once the HHT has *joined* the SMHAN, any Messages received by the CHF from the HHT in the *Data* parameter payload of a *TransferData* command, shall be forwarded to the relevant Device on the SMHAN as if they were received via the Communication Hub’s WAN interface.

Whilst the HHT is in the CHF’s Device Log and *joined* to the SMHAN, any Responses received by the CHF from any SMHAN Device shall be provided to the HHT using the *TransferData* command. Such Responses shall also be sent over the Communication Hub’s WAN interface, if available.

Once the HHT usage on the SMHAN is complete, the HHT should send a *CloseTunnel* command to the Communications Hub. On receipt of such a *CloseTunnel* command from an HHT, the Communications Hub shall process that command as per the ZSE specification and shall:

* remove the HHT from its Device Log; and
* remove the HHT from the SMHAN.

# Downloading firmware images to Devices

## Introduction – informative

Compared to other Smart Metering messages, firmware images are large. Further, each image is likely to be applicable to a significant number of Devices. Thus, an end-to-end, unicast Message to each affected Device, with each message containing a copy of the image, is not efficient from a WAN perspective.

This leads to the approach for firmware update process being separated into two stages:

* distribution of the image to end Devices without any activation of that image; and
* a separate and subsequent ‘activation’ Command to each Device.

The Distribute Firmware Command is not a Critical Command (since it does not affect the operating firmware) and does not need to be unicast.

The Activate Firmware Command is a Critical Command and so must be unicast – as it must be digitally signed and be for one, and only one specified Device. Further, the Activate Command must apply to one, and only one, image and that image must have originated from the same party that signs the Activate Firmware Command (that is, the party responsible for that Device). To meet these requirements:

* the Activate Firmware Command is of type SME.C.C and so the Signature and MAC on the Command shall have been verified by the Device prior to the Hash validation (see next bullet); and
* a Device receiving an Activate Firmware Command shall calculate a Hash over the Manufacturer Image it holds and ensure the Hash so calculated matches that in the Activate Firmware Command, before the Device attempts to activate the corresponding Manufacturer Image.

The GBCS does not constrain the mechanisms used by Device manufacturers to ensure that only valid Manufacturer Images are activated on Devices manufactured by them. The GBCS does require that the manufacturer information related to a Manufacturer Image is made available, so that the Upgrade Image and the ZigBee Over-The-Air (OTA) Header can be provided when requesting distribution of an image.

In common with other Messages, the GBCS shall not constrain the mechanisms by which the firmware Messages are transported to the Communications Hub. The GBCS constrains HAN transport mechanisms to those provided by ZSE.

## Common Requirements

### Transport of firmware images

Italicised terms in this Section 11.2.1 shall have the meanings defined in ZigBee Document 09-5264-23.

For ESME and GSME firmware image distribution, the ZigBee Over-The-Air (OTA) mechanisms shall be used for transport of the image over the HAN. The ESME / GSME firmware image delivered to the Communications Hub shall comply with ZigBee OTA format requirements.

Communications Hub firmware images shall not be transported over the HAN and so ZigBee OTA structures shall not be required.

Every Communications Hub shall be configured to act as the single OTA Server on its HAN.

ESME and GSME shall be configured to act as an OTA Client. The ESME shall use the ‘*Image Notify’[[18]](#footnote-18) command* sent by the OTA Server to inform it that a new firmware image is available. The GSME shall use the notification flags mechanism whereby a flag shall be set by the OTA Server to inform it that a new firmware image is available when requested.

The Communications Hub shall:

* as required by CHTS, have the capability to store one GSME OTA Upgrade Image and one ESME OTA Upgrade Image; and
* overwrite an image with a subsequently delivered image for the same Device type unless:
  + - * the subsequently delivered image has Force Replace = 0x00; and
      * the Communications Hub has sent at least one *Image Block Response* *Command* relating to the already stored image but has not received a corresponding *Upgrade End Request* *Command[[19]](#footnote-19)*.

In such circumstances the Communications Hub shall not overwrite the currently stored image.

Whenever the OTA Server issues an *Upgrade End Response Command* to an OTA Client, the *UpgradeTime* parameter shall always have the value 0xFFFFFFFF[[20]](#footnote-20).

The OTA Server shall not issue *Image Block Response Commands* with WAIT\_FOR\_DATA status.

Contrary to Section 6.13 of ZigBee Document 09-5264-19, the OTA Client shall not activate the OTA Image except as specified in Use Case CS06.

### Construction of Upgrade Image

For an ESME or GSME firmware image, the Authorising Remote Party shall be the Supplier for the target Device.

For a Communications Hub firmware image, the Authorising Remote Party shall be the WAN Provider for the target Device.

Upgrade Image shall be the concatenation:

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

where:

* Manufacturer Image shall contain the firmware image the Device is to apply and any manufacturer specific data needed. For clarity, the GBCS shall not constrain the structure or contents of Manufacturer Image;
* Force Replace shall be a single octet where Force Replace = 0x00 shall mean do not force the replacement of the currently stored image, and
* Authorising Remote Party Signature shall be calculated across the Manufacturer Image using the Authorising Remote Party’s Private Digital Signing Key.

### Construction of OTA Upgrade Image

OTA Upgrade Image shall be the concatenation:

OTA Header || Upgrade Image

where OTA Header shall be populated according to Table 11.2.3. For clarity, there shall be no other sub-elements present.

|  |  |  |  |
| --- | --- | --- | --- |
| **OTA Header** | | | |
| **ZigBee OTA Message Element** | **Contents** | **Length (octets)** | **Note** |
| OTA upgrade file identifier | 0x0BEEF11E | 4 | Fixed by ZigBee OTA specification |
| OTA Header version | 0x0100 | 2 | Specified by current version of ZigBee OTA specification |
| OTA Header length | 0x003C | 2 | The length of ZigBee OTA Header which is decimal 60 |
| OTA Header Field control | 0x0004 | 2 | Detailing what is / is not present in ZigBee OTA Header |
| Manufacturer code | ZSE assigned identifier for the Manufacturer of the target Device | 2 | So this identifies the manufacturer producing the Manufacturer Image |
| Image type | Manufacturer specific | 2 | As per the ZigBee OTA specification, this is to differentiate products from the same manufacturer |
| File version | Manufacturer specific | 4 | As per the ZigBee OTA specification, this is to differentiate release and build numbers for the product in question |
| ZigBee Stack version | 0x0002 | 2 | ZigBee PRO |
| OTA Header string | Manufacturer specific | 32 | May be blank but is not required to be used in Device processing of the firmware image |
| Total Image size (including header) | The length in octets of OTA Upgrade Image | 4 | Contents to be interpreted as an unsigned integer |
| Minimum hardware version | Manufacturer specific | 2 |  |
| Maximum hardware version | Manufacturer specific | 2 |  |

Table 11.2.3: Population of the OTA Header

The OTA Header shall uniquely identify a firmware image.

### Construction of Manufacturer Image Hash

Manufacturer Image Hash shall be a Hash calculated across the whole Manufacturer Image file that is provided to the Authorising Remote Party.

### Verification of the authenticity of the Upgrade Image

The Device shall verify Upgrade Image by verifying the Authorising Remote Party Signature using Manufacturer Image and the Authorising Remote Party’s Public Key. For clarity, this shall be the only ECDSA verification required by the GBCS and this is not the ZSE ECDSA Signature sub-element.

For an ESME or GSME receiving an Upgrade Image, the Authorising Remote Party’s Public Key shall be that held by the Device in the {supplier, digitalSignature, management} Trust Anchor Cell.

For a Communications Hub receiving an Upgrade Image, the Authorising Remote Party’s Public Key shall be that held by the Device in the {wanProvider, digitalSignature, management} Trust Anchor Cell.

### Construction of Firmware Distribution Receipt Alert

If the Device is an ESME or a Communications Hub, the ‘Alert Payload’ fields shall be populated according to Section 7.2.9.

If the Device is a GSME, the ‘Alert Payload’ fields shall be populated according to Section 7.2.10.

In all cases, the Device shall:

* populate the Use Case Specific Additional Content with the concatenation

0x0940 || the calculated Manufacturer Image Hash

* populate the Alert Code field with 0x001C (failure), or 0x0072 (success).

### Activation of firmware images

The Activate Firmware Command shall be of type SME.C.C.

A Device receiving such a Command shall undertake the verifications required of a SME.C.C Command.

If all such SME.C.C verifications succeed, the Device shall then calculate Manufacturer Image Hash over the Manufacturer Image it holds and compare that with the Manufacturer Image Hash specified in the Activate Firmware Image Command (see Use Case CS06 in Section 11.5 for details of the Activate Firmware Command Payload construction).

If the two Hashes match, the Device shall attempt to activate the firmware image.

If the two Hashes do not match, the Device shall not attempt to activate the firmware image.

The Device shall issue a relevant Activate Firmware Image Response detailing the success or failure (see Use Case CS06 in Section 11.5 for details of the Activate Firmware Command Payload construction).

## CS05a Distribute Firmware to Communications Hub

This Use Case covers the distribution of an Upgrade Image that is intended for a Communications Hub to that Communications Hub.

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | None – this is a Variant Message |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | No |
| SEC User Gateway Services Schedule (Service Request) Reference | N/A (this Command is not available as part of the User Gateway Services Schedule ) |
| SMETS Command | Receive Firmware |
| SMETS Data Item | N/A |
| Valid Target Device(s) | Communications Hub |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | WAN Provider |
| Valid Response Recipient role(s) (only for Messages authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | CSP Specific |

Table 11.3: Use Case Cross References for CS05a Distribute Firmware to Communications Hub

### Pre-conditions

None.

### Detailed Steps

The Upgrade Image shall be constructed according to Section 11.2.2.

The Upgrade Image shall be transported to the Communications Hub.

The Communications Hub shall verify the Upgrade Image according to Section 11.2.5, verify the Upgrade Image is suitable for this Communications Hub, and update its Event Log with the outcome of that verification.

If the verification is successful, the Communications Hub shall construct and send a Firmware Distribution Receipt Response, according to Section 11.2.6 and shall store the Manufacturer Image contained within the Upgrade Image.

If the verification is not successful, the Communications Hub shall discard the upgrade image and construct and send a Firmware Distribution Receipt Alert, according to Section 11.2.6.

On receipt of a Firmware Distribution Receipt Response, the WAN Provider may verify the cryptographic protection as specified in Section 6.8.3.

Additionally, the WAN Provider may verify that the Manufacturer Image received is that intended by comparing the Manufacturer Image Hash in the Firmware Distribution Receipt Response, with the Hash which it calculates over the Manufacturer Image provided.

## CS05b Distribute Firmware to ESME / GSME

This Use Case covers the distribution of an OTA Upgrade Image that is intended for a GSME or ESME to that GSME or ESME.

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | None – this is a Variant Message |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | No |
| SEC User Gateway Services Schedule (Service Request) Reference | 11.1 |
| SMETS Command | Receive Firmware |
| SMETS Data Item | N/A |
| Valid Target Device(s) | ESME / GSME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | CSP Specific to Communications Hub; ZigBee OTA from Communications Hub to ESME / GSME |

Table 11.4: Use Case Cross References for CS05b Distribute Firmware to ESME / GSME

### Pre-conditions

None.

### Detailed Steps

Italicised terms in this Section 11.4.2 shall have the meaning specified in ZSE.

The OTA Upgrade Image shall be populated according to Section 11.2.3.

The OTA Upgrade Image shall be transported to the Communications Hub through which the Device communicates.

The Communications Hub shall update its OTA Cluster to reflect availability of the OTA Upgrade Image, once the image is received by the Communications Hub.

The Communications Hub, as OTA Server, shall indicate availability of an OTA Upgrade Image differently for ESME and GSME:

* for ESME, the Communications Hub shall send a ZSE *Image Notify* command; and
* for GSME, the Communications Hub shall set a *Notification Flag*.

The ESME / GSME shall download an OTA Upgrade Image when it is aware of the availability of a suitable OTA Upgrade Image using the *QueryNextImage* and *Image Block/Page* commands specified in the *OTA Cluster* specification[[21]](#footnote-21).

The ESME / GSME shall verify the Upgrade Image contained within the OTA Upgrade Image according to Section 11.2.5, and update its Event Log with the outcome of that verification.

If the verification is successful, the ESME / GSME shall construct and send a Firmware Distribution Receipt Alert, according to Section 11.2.6, and shall store the Manufacturer Image contained within the OTA Upgrade Image.

If the verification is not successful, the Device shall discard the OTA Upgrade Image, and send a Firmware Verification Failed Alert, as detailed in Section 11.3.2.

On receipt of a Firmware Distribution Receipt Alert, the Supplier may verify the cryptographic protection as specified in Section 6.8.3.

Additionally, the Supplier may verify that the Manufacturer Image received by the Device is that intended by comparing the Manufacturer Image Hash in the Firmware Distribution Receipt Response, with the Hash which it calculates over the Manufacturer Image provided.

## CS06 Activate Firmware

This Use Case covers the activation of a Firmware Image.

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command, Response and Alert (if future dated) |
| Message Type Category | SME.C.C |
| Capable of future dated invocation? | Yes |
| Protection Against Replay Required? | No |
| SEC User Gateway Services Schedule (Service Request) Reference | N/A for Communications Hub (this Command is not available as part of the User Gateway Services)  11.3 for ESME and GSME |
| SMETS Command | Activate Firmware |
| SMETS Data Item | Firmware Version |
| Valid Target Device(s) | ESME / GSME / CHF / GPF |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier for ESME / GSME  WAN Provider for CHF / GPF |
| Valid Response Recipient role(s) (only for Messages authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 11.5: Use Case Cross References for CS06 Activate Firmware

### Pre-conditions

None.

### Detailed Steps

#### Construction of Command

Activate Firmware Command Payloads shall be constructed according to the requirements of Section 11.5.2.3 and populated as specified in Table 11.5.2.1.

MAC Header, Grouping Header, KRP Signature and ACB-SMD MAC shall be populated as required for a Command of the SME.C.C Message Category.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @ActivateFirmware.CommandPayload | SEQUENCE |  |  |  |
| manufacturerImageHash | OCTET STRING | The Manufacturer Image Hash of the image to be activated. | Mandatory | An octet-string of length 32 interpreted as the Manufacturer Image Hash of the Manufacturer Image that is to be activated |
| executionDateTime | GeneralizedTime | The date-time at which the Command is to be executed, if future dated | Optional |  |

Table 11.5.2.1: @ActivateFirmware.CommandPayload population

#### Device processing of Command and Response handling

The Device receiving an Activate Firmware Command shall undertake processing steps in the sequence defined in this Section 11.5.2.2.

The Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of the SME.C.C Message Category;
2. if executionDateTime is present then the Device shall:
   * + - record manufacturerImageHash, originatorCounter and executionDateTime;
       - construct and send a Response where executionOutcome is not present. Grouping Header is constructed and Response Cryptographic Protection is applied as required for a Response of the SME.C.C Message Categories; and
       - at the date-time specified in executionDateTime, undertake the processing from step 3.

If executionDateTime is not present then the Device shall continue processing from step 3 immediately;

1. if the Device does not have a stored Manufacturer Image then set activateImageResponseCode to noImageHeld and process from step 5;
2. calculate Manufacturer Image Hash. If the calculated value does not equal manufacturerImageHash then the Device shall set activateImageResponseCode to hashMismatch and process from step 5;
3. attempt to activate Manufacturer Image. If the activate fails then the Device shall set activateImageResponseCode to activationFailure ;
4. set activateImageResponseCode to success ;
5. populate the executionOutcome according to the requirements of Section 11.5.2.3 using the activateImageResponseCode value produced by the processing in this Section 11.5.2.2, the value of originatorCounter from the Command and the version of firmware now in operation to populate firmwareVersion;
6. construct Grouping Header and apply the Response Cryptographic Protection required for a Response / Alert of the SME.C.C / SME.A.C Message Categories respectively. In such an Alert, the Message Code shall be that for a Generic Critical Alert; and
7. send the Response if executionDateTime was not present in the Command or send the Alert if executionDateTime was not present in the Command.

On receipt of the Response, the recipient may undertake the ‘Response Recipient Verification’ for Responses of type SME.C.C. or for Alerts of type SME.A.C, dependent upon the Message received.

#### Activate Firmware Command, Response and Alert Payloads - structure **definition**

Each instance of @ActivateFirmware.CommandPayload and of @ActivateFirmware.ResponsePayload and of @ActivateFirmware.AlertPayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 11.5.2.3 which specifies the structure in ASN.1 notation.

ActivateFirmware DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the hash of the Manufacturer Image to be activated

manufacturerImageHash OCTET STRING,

-- the Originator Counter as in the Grouping Header of the Command

originatorCounter INTEGER (0..9223372036854775807),

-- the date-time at which the Command is to execute, if future dated

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

}

AlertPayload ::= SEQUENCE

{

-- specify the Alert Code

alertCode INTEGER(0..4294967295),

-- specify the date-time of execution

executionDateTime GeneralizedTime,

-- the Originator Counter as in the Grouping Header of the corresponding Command

originatorCounter INTEGER (0..9223372036854775807),

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

executionOutcome ExecutionOutcome

}

ExecutionOutcome ::= SEQUENCE

{

-- Specify whether the activation was successful or not

activateImageResponseCode ActivateImageResponseCode,

-- Specify the Device’s now current firmware version

firmwareVersion OCTET STRING

}

ActivateImageResponseCode::= INTEGER

{

success (0),

noImageHeld (1),

hashMismatch (2),

activationFailure (3)

}

END

# Requirements for Certificates

This Section 12 lays out requirements as to structure and content to which all valid authorised Certificates shall comply, in so far as those requirements affect the processing carried out by Devices. All terms in this section shall, where not defined in the GBCS, have the meanings in IETF RFC 5759[[22]](#footnote-22) and IETF RFC 5280.

## Requirements applicable to all Certificates

All Security Credential Documents that are successfully authorised within the APKI for use by Devices within the scope of this GBCS shall:

* be compliant with IETF RFC 5759 and so with IETF RFC 5280. In adherence with the requirements of IETF RFC5759, all Security Credential Documents shall:
  + - * contain the authorityKeyIdentifier extension, except where the Security Credential Document is self-signed;
      * contain the keyUsage extension which shall be marked as critical;
* be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
* only contain public keys of types that are explicitly allowed within the GBCS. This means all public keys shall be elliptic curve public keys on the NIST P-256 curve;
* only contain public keys in uncompressed form which shall be elliptic curve points in uncompressed form as detailed in Section 2.2 of IETF RFC 5480[[23]](#footnote-23);
* only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
* contain a serialNumber of no more than 8 octets in length;
* contain a subjectKeyIdentifier which shall be marked as non-critical;
* contain a certificatePolicies extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Devices shall interpret this extension;
* contain an authorityKeyIdentifier in the form [0] KeyIdentifier which shall be marked as non-critical, except where the Security Credential Document is self-signed. Note this exception only applies where RemotePartyRole as specified in the X520OrganizationalUnitName field = root;
* only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280. Thus KeyIdentifiers shall always be 8 octets in length;
* contain an IssuerName which is identical to the Security Credential Document’s signer's SubjectName; and
* have a valid notBefore field consisting of the time of issue encoded and a valid notAfter as per IETF RFC 5280 Section 4.1.2.5.

## Requirements applicable to Organisations’ Certificates only

All Organisations’ Certificates that are Authorised for use by Devices within the scope of this GBCS shall:

* have a fixed expiration date in the notAfter field which shall not be GeneralizedTime value of 99991231235959Z;
* contain a non-empty subject field which shall contain a unique X.500 Distinguished Name (DN), which shall be the unique trading name of the Organisation, and an X520OrganizationalUnitName whose value shall be set to the RemotePartyRole that this Certificate allows the subject of the Certificate to perform; and
* contain a single Public Key except where the RemotePartyRole = root. Where the RemotePartyRole = root, the Certificate shall contain two public keys. The second public key shall be referred to as the Contingency Key[[24]](#footnote-24) and shall be present in the WrappedApexContingencyKey extension with the meaning of IETF RFC 5934[[25]](#footnote-25). The Contingency Key shall be Encrypted as per the requirements of Section 13.3.5.8.1.

## Requirements applicable to Certificates where RemotePartyRole = root or issuingAuthority

All Remote Parties’ Certificates that:

* are Authorised within the APKI for use by Devices within the scope of this GBCS; and
* have a X520OrganizationalUnitName whose value is either root or issuingAuthority

shall:

* have a keyUsage with a value of keyCertSign and cRLSign. For clarity, Devices are not required to use the associated Public Keys in relation to the cRLSign keyUsage;
* where X520OrganizationalUnitName = issuingAuthority:
  + - * contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID(s) valid for usage in GB Smart Metering;
      * contain the basicConstraints extension, with values cA=True, and pathLen=1. This extension shall be marked as critical;
* where X520OrganizationalUnitName = root:
  + - * contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for anyPolicy; and
      * contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

## Requirements applicable to Certificates where RemotePartyRole is neither root nor issuingAuthority

All Remote Parties’ Certificates that:

* are Authorised within the APKI for use by Devices within the scope of this GBCS; and
* have a X520OrganizationalUnitName whose value is not root and is not issuingAuthority

shall:

* contain a subjectUniqueID whose value shall be the 8 octet Entity Identifier of the subject of the Certificate;
* have a keyUsage with a value of only one of digitalSignature or keyAgreement; and
* contain a single policyIdentifier in the certificatePolicies extension that refers to the OID applicable to the environment the Certificate has been issued in.

## Requirements applicable to Device Certificates

All Device Certificates that are Authorised within the APKI for use by Devices within the scope of this GBCS shall:

* not have a well-defined expiration date and so the notAfter field shall be assigned the GeneralizedTime value of 99991231235959Z;
* have an empty SubjectName;
* have a keyUsage with a value of only one of digitalSignature or keyAgreement;
* contain a single policyIdentifier in the certificatePolicies extension that refers to the OID applicable to the environment the Device Certificate has been issued in;
* contain a SubjectAlternativeName extension which shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-HardwareModuleName) as defined in IETF RFC 4108[[26]](#footnote-26). The hwSerialNum field shall be set to the Device’s Entity Identifier. In adherence to IETF RFC 5280, SubjectAlternativeName shall be marked as critical; and
* contain a single Public Key.

## Device processing of Certificates

In relation to Certificates, Devices shall:

* accept unexpected (not required by the GBCS) certificate extensions and shall ignore silently non-critical unrecognized certificate extensions;
* in adherence with the requirements of IETF RFC 5280, reject any certificate containing unrecognized critical certificate extensions; and
* reject any certificate containing either policy mappings or name constraints.

# Managing Security Credentials on Devices

## Introduction - informative

This Section 13 includes the Use Cases related to the management of Security Credentials on Devices in terms of the relevant Commands, Responses and Alerts:

* 13.2 - CS02a Provide Security Credential Details Command and Response;
* 13.3 - CS02b Update Security Credentials Command, Response and Alert;
* 13.4 - CS02c Issue Security Credentials;
* 13.5 - CS02d Update Device Certificates on Device;
* 13.6 - CS02e Provide Device Certificates from Device;
* 13.7 - Pair-wise Authorisation of Devices (covered by various Join / Unjoin Use Cases); and
* 13.8 - GPF Device Log Backup and Restore (GCS59 and GCS62).

### Device Security Credentials - informative

In terms of processing relating to a Device’s own Security Credentials:

* the Command to Devices for issuing Device Certificate Signing Requests (and therefore generate new Public-Private Key Pairs) is covered in Section 13.4;
* the Command to Devices for the Device to replace its current Device Certificate with a new Device Certificate resulting from a Device Certificate Signing Request is covered in Section 13.5, as are the related requirements for the capability to store such Documents; and
* the Command to a Device to provide a copy of its currently held Device Certificates is covered Section 13.6.

### Remote Party Security Credentials - informative

This Section 13.1.2 summarises the GBCS requirements in relation to storing, replacing and providing details of Remote Party Security Credentials. The use of such credentials to control access to Device functions is detailed in other sections of the GBCS and in relevant Use Cases.

A Remote Party Security Credential is a Public Key Certificate which securely binds together the Remote Party’s identity with a Public Key along with related information, including what that Public Key can be used for and over what time period it is valid. The corresponding Private Key should be securely controlled solely by the Remote Party and known only to that Remote Party.

The purpose of storing each Remote Party Public Key (and related details) on a Device is so that each Public Key can act as a ‘Trust Anchor’ for the Device. The Device uses these Trust Anchors to check cryptographically whether Remote Party Messages can be trusted or not (and so whether it should act on them or not). Thus, all of a Device’s Trust Anchors must be populated.

Trust Anchors need to be capable of being replaced during a Device’s operational life for a number of reasons including:

* the Certificate’s expiry (Organisation Certificates will only be valid for a fixed period of time);
* the Known Party transferring control to a different organisations (for example on Change of Supplier);
* the cryptographic algorithms, or parameters such as key length, needing to be changed;
* the Known Party having lost the use of the corresponding Private Key; or
* there being concerns that someone other than the Known Party has use of, or may have use of, the corresponding Private Key.

Thus, an ‘Update Security Credentials Command’ must be supported by all Devices that rely on Remote Party Security Credentials to act as Trust Anchors. Related, all such Devices need to support a ‘Provide Security Credential Details’ Command, so that Remote Parties can be sure which Devices need to have credentials replaced.

However, if these Trust Anchors could be replaced without proper protections, attackers could take over control of Devices or the Devices could be rendered inoperable. Thus, a Device needs to do thorough checks before applying an Update Security Credentials Command. The checks that the Device can and must do vary dependent on the reasons for the change. Thus, Section 13.2.1 lays out a number of different checks and the circumstances in which corresponding Commands may be issued. Broadly the following checks are carried out by the Device:

* is the Command properly formed?
* is the Command for the Device that it has been delivered to, and is the Command one that it has not processed previously?
* are the Remote Parties apparently authorising the Command allowed to authorise it?
* was the Command Authorised by the Remote Parties that it appears to be Authorised by?
* were the Certificates in the payload of the Command issued by properly Authorised parties, specifically by Certification Authorities Authorised (by ‘root’ under the APKI) to issue GB Smart Metering Certificates?

Only when a Device has successfully undertaken all five sets of checks should it action the Update Security Credentials Command.

Other Critical Commands only have to complete the first four categories of check.

### Trust Anchor Management (TAMP) - informative

The GBCS does not specify a fully compliant TAMP solution due to the limited processing and networking capability of Devices. However, it does incorporate checks that are functionally derived from relevant checks in IETF RFC 5934.

The GBCS only permits a restricted subset of ‘IETF RFC 5934 like’ functionality:

* replacement of Trust Anchors is required (and specified in this Use Case) but their addition, change or removal is not allowed;
* status queries are supported (and are specified in this Section 13.1.3); and
* community related functions are not supported.

## CS02a Provide Security Credential Details Command and Response

### Description

This section covers the creation, validation and processing of (i) Provide Security Credential Details Commands and (ii) Responses to such Commands.

### Use Case Cross References

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | Variant Message and is not a Critical Command |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | No |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.24 |
| Valid Target Device(s) | ESME / GSME / GPF / CHF / HCALCS / PPMID |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier  Network Operator  Access Control Broker  Transitional Change of Supplier  WAN Provider  Recovery |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 13.2.2: Use Case Cross References for Provide Security Credential Details Command and Response

### Common Requirements

#### Summary - informative

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

#### The ‘Provide Security Credential Details’ Command and Response

This Section 13.2.3.2 summarises the structure of the Provide Security Credential Details Command.

If protected by an Access Control Broker MAC as per Section 13.2.4.2, a Provide Security Credential Details Command shall be the concatenation:

MAC Header || Grouping Header || @ProvideSecurityCredentialDetails.Command || 0x00 || ACB-SME MAC

If protected by a KRP Signature as per Section 13.2.4.2, a Provide Security Credential Details Command shall be the concatenation:

Grouping Header || @ProvideSecurityCredentialDetails.Command || 0x40 || KRP Signature

If an SMD Signature is required as per Section 13.2.4.5, a Provide Security Credential Details Response shall be the concatenation:

Grouping Header || @ProvideSecurityCredentialDetails.Response || 0x40 || SMD Signature

If an SMD Signature is not required as per Section 13.2.4.5, a Provide Security Credential Details Response shall be the concatenation:

MAC Header || Grouping Header || @ProvideSecurityCredentialDetails.Response || 0x00 || SMD-KRP MAC

Where:

* @ProvideSecurityCredentialDetails.Command and Response shall each be an octet string containing the DER encoding of the populated ASN.1 structure (as laid out in Section 13.2.3.3);
* 0x40 is the length in octets of Signature when a SMD or KRP Signature is present, and 0x00 is the length in octets of Signature when a SMD or KRP Signature is not present;
* KRP Signature and ACB-SMD MAC are as defined in Section 13.2.4.2;
* SMD Signature and SMD-KRP MAC are as defined in Section 13.2.4.5; and
* MAC Header and Grouping Header are as defined in Section 7.2.

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

Each instance of @ProvideSecurityCredentialDetails.Command and of @ProvideSecurityCredentialDetails.Response shall be an octet string containing the DER[[27]](#footnote-27) encoding of the populated structure defined in this Section 13.2.3.3 which specifies the structure in Abstract Syntax Notation One (ASN.1) notation[[28]](#footnote-28).

ProvideSecurityCredentialDetails DEFINITIONS ::= BEGIN

Command ::= SEQUENCE

{

-- Identify which of the Public Keys on the Device is to be used in verifying the Signature or MAC

-- (so defining the nature of the verification by way of the KeyUsage parameter held on the

-- Device for the Public Key so identified).

authorisingRemotePartyTACellIdentifier TrustAnchorCellIdentifier,

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

remotePartyRolesCredentialsRequired SEQUENCE OF RemotePartyRole

}

Response ::= SEQUENCE OF RemotePartyDetails

RemotePartyDetails ::= SEQUENCE

{

-- Which Remote Party do these details relate to?

remotePartyRole RemotePartyRole,

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

statusCode StatusCode,

-- What is the current Update Security Credentials Protection Against Replay number on the Device for this role, where there is such a number for this role?

currentSeqNumber SeqNumber OPTIONAL,

-- What are the details held on the Device for each of the Cells related to this role? The list shall have between one and

-- three entries (e.g. there will be one if role is transitional change of supplier; there may be three if role is supplier)

trustAnchorCellsDetails SEQUENCE OF TrustAnchorCellContents OPTIONAL

}

SeqNumber ::= INTEGER (0..9223372036854775807)

TrustAnchorCellContents ::= SEQUENCE

{

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. This will be absent except where used to refer to the Supplier Key Agreement Key.

-- This Key is used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions.

trustAnchorCellUsage CellUsage DEFAULT management,

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

existingSubjectUniqueID OCTET STRING,

-- The APKI requirements mean that KeyIdentifier attributes will all be 8 byte SHA-1 Hashes.

-- existingSubjectKeyIdentifier shall be set accordingly based on the contents of the Trust Anchor Cell

existingSubjectKeyIdentifier OCTET STRING

}

TrustAnchorCellIdentifier ::= SEQUENCE

{

-- Which Remote Party Role does this Cell relate to?

trustAnchorCellRemotePartyRole RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. This may be absent except where use to refer to the Supplier Key

-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions

trustAnchorCellUsage CellUsage DEFAULT management

}

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

RemotePartyRole ::= INTEGER

{

-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake

-- processing. Note that most Devices will only support processing in relation to a subset of these.

root (0),

recovery (1),

supplier (2),

networkOperator (3),

accessControlBroker (4),

transitionalCoS (5),

wanProvider (6),

issuingAuthority (7), -- Devices will receive such Certificates but they do not

-- need to store them over an extended period

-- The ‘other’ RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from

-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid

-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is bought in to operation

other (127)

}

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

KeyUsage ::= BIT STRING

{

-- Define valid uses of Public Keys.

digitalSignature (0),

contentCommitment (1), -- not valid for GBCS compliant transactions

keyEncipherment (2), -- not valid for GBCS compliant transactions

dataEncipherment (3),

keyAgreement (4),

keyCertSign (5),

cRLSign (6),

encipherOnly (7),

decipherOnly (8) -- not valid for GBCS compliant transactions

}

-- The GBCS only allows for a constrained set of Trust Anchor Cell operations and so the list of possible outcomes

-- is more limited than in IETF RFC 5934. The list below is that more constrained subset

StatusCode ::= ENUMERATED {

success (0),

-- trustAnchorNotFound indicates that details of a trust anchor were requested, but the referenced trust anchor

-- is not represented on the Device

trustAnchorNotFound (25),

other (127)}

END

### Provide Security Credential Details from a Device – Processing Steps

This Section 13.2.4 lays out the requirements relating to the construction, protection and Authentication of the Provide Security Credentials Command, and the construction, protection and Authentication of the corresponding Response.

#### Command Construction

The Remote Party constructing the Command shall populate Grouping Header according to the requirements of Section 7.2.6.

@ProvideSecurityCredentialDetails.Command shall have the structure defined in Section 13.2.3.3, and the Remote Party constructing the Command shall populate with values according to Table 13.2.4.1.

The Remote Party constructing the Command shall populate Command Length once it has fully populated @ProvideSecurityCredentialDetails.Command, based on the length of the octet string so constructed.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @ProvideSecurityCredentialDetails.Command ::= | SEQUENCE |  |  |  |
| authorisingRemotePartyTACellIdentifier | SEQUENCE |  | Mandatory | This structure identifies which Public Key on the Device is to be used in checking the Command’s cryptographic protection . 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 |
| trustAnchorCellRemotePartyRole | INTEGER | recovery (1) ,  supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) | Mandatory if authorisingRemotePartyTACellIdentifier  present | The role of the Party applying the Command’s cryptographic protection |
| trustAnchorCellKeyUsage | BIT STRING | digitalSignature (0) ,  keyAgreement (4) | Mandatory if authorisingRemotePartyTACellIdentifier present | Where the Command’s cryptographic protection is a digital signature (digitalSignature) or a MAC (keyAgreement). The value shall be digitalSignature unless trustAnchorCellRemotePartyRole = accessControlBroker |
| trustAnchorCellUsage | INTEGER | management(0) | DEFAULT management | Must be absent or set to ‘management’ since the prePaymentTopUp key pair cannot be used in relation to this command |
| remotePartyRolesCredentialsRequired | SEQUENCE OF |  |  |  |
| RemotePartyRole | INTEGER | root (0) ,  recovery (1) ,  supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) | Mandatory to have at least one | List the Remote Party Role(s) for which credential details are required |

Table 13.2.4.1: Attribute values for Provide Security Credentials Command

#### Command Cryptographic Protection

If the Access Control Broker is undertaking this step to apply a MAC, then the Access Control Broker shall undertake the steps in Section 13.2.4.2.1 otherwise:

* the Remote Party originating the Command shall generate a Signature for the Command and set KRP Signature accordingly;
* the Signature, for incorporation in the Command, shall only be generated once all fields of the Grouping Header || @ProvideSecurityCredentialDetails.Command are populated as per the requirements for the Command Construction stage; and
* the Remote Party shall use its Private Digital Signing Key to generate the Signature.

##### Access Control Broker MAC

If the Access Control Broker is undertaking this step to apply a MAC, then the Access Control Broker shall calculate a MAC using the parameters in Table 13.2.4.2.1 and set ACB-SMD MAC to the value so calculated.

|  |  |  |
| --- | --- | --- |
| **Input Parameter** | **Value** | **Note** |
| To calculate the Shared Secret (‘Z’) input to the KDF: | | |
| Private Key Agreement Key | Access Control Broker’s |  |
| Public Key Agreement Key | Device’s | As identified by the Business Target ID in Message Identifier |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  |  |  |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || @ProvideSecurityCredentialDetails.Command || 0x00 |  |

Table 13.2.4.2.1: Calculation of Access Control Broker MAC for Provide Security Credentials command

#### Command Authenticity and Integrity Verification

The Device shall undertake processing according to the requirements of this section before undertaking any other processing of the Command.

The checks should be carried out in the order specified. The Device shall cease checking at the point that any one check fails.

The checks required are shown in Table 13.2.4.3.

|  |  |  |
| --- | --- | --- |
| **Check Number** | **Criteria that shall be tested by the Device** | **How the Device shall test the Criteria** |
| 1.1 | The Message is for the Device | The value in the Business Target ID field of the Message Identifier part of the Command Instance must be equal to the Device’s Entity Identifier |
| 1.2 | The Message Code is for Provide Security Credentials | The value in the Message Code field of the Command Instance must be equal to 0x0008 |
| 2.1 | The Command was protected cryptographically using the Private Key corresponding to the Remote Party Public Key held in the Trust Anchor Cell identified by authorisingRemotePartyTACellIdentifier | As specified in Section 13.2.4.3.1 |

Table 13.2.4.3: Provide Security Credentials Command authenticity and integrity verification

Should any of the checks detailed in this Section 13.2.4.3 fail then the Device shall:

* generate an entry in the Security Log recording failed Authentication;
* discard the Command without execution and without sending a Response; and
* send an Alert notifying the failed Authentication, constructed as specified in Section 6.2.4.2, populated with the relevant Alert Code from Section 16 , to the Known Remote Party identified by the Security Credentials it holds in the {supplier, management, digitalSignature} Trust Anchor Cell.

Where all of the checks detailed in this Section 13.2.4.3 succeed the Device shall process the Command and produce a Response.

##### Command Authenticity and Integrity Verification

The Device shall undertake the following checks until either all are successful or one has failed.

1. If trustAnchorCellUsage is present it has a value of management else this test shall fail.

2. If trustAnchorCellKeyUsage = keyAgreement then

((trustAnchorCellRemotePartyRole = accessControlBroker) and (the MAC calculated by the Device according to Table 13.2.4.3.1 equates to ACB-SMD MAC)

else

((trustAnchorCellKeyUsage = digitalSignature) and (the Device shall use the Public Key in the Trust Anchor Cell identified by authorisingRemotePartyTACellIdentifier to verify that KRP Signature is the Digital Signature across Grouping Header || @ProvideSecurityCredentialDetails.Command)

else

3. This test shall fail.

|  |  |  |
| --- | --- | --- |
| **Input Parameter** | **Value** | **Note** |
| To calculate the Shared Secret (‘Z’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Access Control Broker’s | As held by the Device in Trust Anchor Cell {accessControlBroker, keyAgreement, management} |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || @ProvideSecurityCredentialDetails.Command || 0x00 |  |

Table 13.2.4.3.1: Calculation of MAC for Provide Security Credential Details Command

#### Response Construction

The Device shall populate Grouping Header according to the requirements of Section 7.2.6.

The @ProvideSecurityCredentialDetails.Response shall have the structure defined in Section 13.2.3.3, and the Device shall populate with values according to Table 13.2.4.4.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @ProvideSecurityCredentialDetails.Response ::= | SEQUENCE OF |  |  |  |
| SEQUENCE |  |  |  |  |
| remotePartyRole | INTEGER | root (0) ,  recovery (1) ,  supplier (2) ,  networkOperator (3) ,  accessControlBroker (4) ,  transitionalCoS (5) ,  wanProvider (6) , | Mandatory if SEQUENCE is present | The role to which the credentials in this SEQUENCE relate |
| statusCode | ENUMERATED | success (0) ,  trustAnchorNotFound (25) ,  other (127) | Mandatory if SEQUENCE is present | Whether the Device can supply the details |
| currentSeqNumber | INTEGER | The corresponding Counter value | Present if statusCode=0 | The Protection Against Replay number held by the Device for this role’s use of the Update Security Credentials Command |
| trustAnchorCellsDetails | SEQUENCE OF |  | At least one in the SEQUENCE OF must be present if statusCode=0 |  |
| SEQUENCE |  |  |  |  |
| trustAnchorCellKeyUsage | BIT STRING | digitalSignature (0) ,  keyAgreement (4) ,  keyCertSign (5) | Mandatory if SEQUENCE is present | To what use can the public key in this Cell be put |
| trustAnchorCellUsage | INTEGER | prePaymentTopUp(1) | DEFAULT management (0) | Only needs to be present for the {supplier, keyAgreement, prePaymentTopUp} Cell |
| existingSubjectUniqueID | OCTET STRING | Entity Identifier in this Cell | Mandatory if SEQUENCE is present | See Section 12.4 |
| existingSubjectKeyIdentifier | OCTET STRING | Key Identifier of the key in this Cell | Mandatory if SEQUENCE is present |  |

Table 13.2.4.4: Attribute values for Provide Security Credentials Response

#### Response Cryptographic Protection

If the Command that triggered this Response was protected by a MAC then the Device shall calculate a MAC using the parameters in Table 13.2.4.5 and set SMD-KRP MAC to the value so calculated.

|  |  |  |
| --- | --- | --- |
| **Input Parameter** | **Value** | **Note** |
| To calculate the Shared Secret (‘Z’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Access Control Broker’s | As held by the Device in {accessControlBroker, keyAgreement, Management} |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || @ProvideSecurityCredentialDetails.Response || 0x00 |  |

Table 13.2.4.5: Calculation of MAC for Provide Security Credential Details Response

Otherwise:

* the Device creating the Response shall generate a Signature for the Response and set SMD Signature to the value calculated;
* the Signature, for incorporation in the Response, shall only be generated once all fields of the Grouping Header || Length || @ProvideSecurityCredentialDetails.Response are populated, as per requirements for the Response Construction stage; and
* the Device shall use its Private Digital Signing Key to generate the Signature.

#### Response Recipient Cryptographic Verification

If the Response contains a MAC, the Access Control Broker can verify that MAC by calculating a MAC according to the parameters in Table 13.2.4.6 and checking that the MAC so calculated equates to that in the Response.

|  |  |  |
| --- | --- | --- |
| **Input Parameter** | **Value** | **Note** |
| To calculate the Shared Secret (‘Z’) input to the KDF: | | |
| Private Key Agreement Key | Access Control Broker’s |  |
| Public Key Agreement Key | Device’s | As identified by Business Originator ID in the Message Identifier |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  |  |  |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Grouping Header || @ProvideSecurityCredentialDetails.Response || 0x00 |  |

Table 13.2.4.6: Calculation of MAC for Provide Security Credential Details Response Verification

## CS02b Update Security Credentials Command, Response and Alert

### Description

This Section 13.3 covers the creation, validation and processing of:

* Update Security Credentials Commands;
* Responses to such Commands; and
* Alerts resulting from the future dated execution of such Commands.

The Update Security Credentials Command shall be:

* used solely to replace Remote Party Security Credentials held in Trust Anchor Cells on Devices;
* supported by any Device that can process Remote Party Messages; and
* the only Command that Devices are capable of accepting for replacement of Remote Party Security Credentials, once the tamper seal is applied to the Device.

### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Response / Alert |
| Message Type Category | Variant Message and is Critical |
| Capable of future dated invocation? | Yes |
| Protection Against Replay Required? | The Protection Against Replay mechanisms for Update Security Credentials are specified in Section 13.3. The Protection Against Replay mechanisms of other sections of the GBCS do not apply. |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.15, 6.23, 8.5, 6.21 |
| SMETS Command | Update Security Credentials |
| SMETS Data Item | Security Credentials |
| Valid Target Device(s) | ESME / GSME / GPF / CHF / HCALCS / PPMID |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier  Network Operator  Access Control Broker  Transitional Change of Supplier  WAN Provider  Recovery |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 13.3.2: Use Case Cross References for Update Security Credentials Command

### Command, Response and Alert Structure

#### The Update Security Credentials Command

This Section 13.3.3.1 summarises the structure of the Update Security Credentials Command, which depends on credentialsReplacementMode and the deviceType of the Device.

If credentialsReplacementMode = anyByContingency or anyExceptAbnormalRootByRecovery then an Update Security Credential Details Command shall be the concatenation:

Grouping Header || @UpdateSecurityCredentials.CommandPayload || 0x40 || KRP Signature

If credentialsReplacementMode = accessControlBrokerByACB and deviceType is not communicationsHubCommunicationsHubFunction then an Update Security Credentials Command shall be the concatenation:

MAC Header || Grouping Header || @UpdateSecurityCredentials.CommandPayload || 0x00 || ACB-SMD MAC

In all other cases, the Update Security Credentials Command shall either be the concatenation:

MAC Header || Grouping Header || @UpdateSecurityCredentials.CommandPayload || 0x40 || KRP Signature|| ACB-SMD MAC

In these Command structures:

* @UpdateSecurityCredentials.CommandPayload shall be an octet string containing the DER encoding of the populated ASN.1 structure (as laid out in Section 13.3.5.11);
* Grouping Header shall be constructed as specified in Section 7.2.7 with Business Originator ID being the Entity Identifier of the Known Remote Party which generated KRP Signature, and with Business Originator Counter being that of the same Known Remote Party;
* KRP Signature shall be generated as specified in Section 6.3.3;
* ACB Grouping Header shall be constructed as specified in Section 7.2.7 with Business Originator ID being the Entity Identifier of the Access Control Broker and Business Originator Counter being that of the Access Control Broker;
* MAC Header shall be constructed as specified in Section 7.2.5; and
* ACB-SMD MAC shall be calculated as specified in Section 6.2.3.

#### The Update Security Credentials Response

An Update Security Credentials Response shall be the concatenation:

Grouping Header || @UpdateSecurityCredentials.ResponsePayload || 0x40 || SMD Signature

where:

* @UpdateSecurityCredentials.ResponsePayload shall be an octet string containing the DER encoding of the populated ASN.1 structure (as laid out in Section 13.3.5.11);
* Grouping Header in the Response shall be constructed as specified in Section 7.2.7 with Business Target ID being the Entity Identifier specified in the corresponding Command’s Grouping Header; and
* SMD Signature shall be generated as specified in Section 6.3.5.

#### The Update Security Credentials Alert

An Update Security Credentials Alert shall be the concatenation:

Grouping Header || @UpdateSecurityCredentials.AlertPayload || 0x40 || SMD Signature

where:

* @UpdateSecurityCredentials.AlertPayload shall be an octet string containing the DER encoding of the populated ASN.1 structure (as laid out in Section 13.3.5.11);
* Grouping Header in the Alert shall be constructed as specified in Section 7.2.7 with Business Target ID being the Entity Identifier specified in the corresponding Command’s Grouping Header;
* the Message Code being that for a Generic Critical Alert; and
* SMD Signature shall be generated as specified in Section 6.3.5.

#### The Update Security Credentials Command, Response and Alert - informative

The @UpdateSecurityCredentials.CommandPayload structure has four parts:

* authorisingRemotePartyControl: which includes details of what kind of credential replacement this Command is, which Remote Parties are authorising it and information to support Protection Against Replay protections;
* replacements: which is a list of new Certificates the Device is to store details from, along with which Trust Anchor Cell each set of details is to be stored in on the Device;
* certificationPathCertificates: which is a list of Certification Authority Certificates the Device will need to use in checking that the replacement Certificates were properly issued; and
* executionDateTime: which, if present, specifies the date-time at which the certificates in the CommandPayload are to be used to replace the credentials currently in use on the Device. If this field is not present, the Command shall be executed immediately. If this field has the value equivalent to ‘never’ (which is '99991231235959Z') the certificate replacement will never happen. This is to allow cancellation of future dated Commands. Note that future dating is not supported where certificates are being replaced in exception conditions.

The @UpdateSecurityCredentials.Response structure contains, for immediate execution commands, a list detailing the success of failure of each of the replacements, including details of the parties affected. For future dated commands, @UpdateSecurityCredentials.AlertPayload structure contains the list detailing the success, or failure, of each of the replacements, including details of the parties affected.

Section 13.3.5.11 contains narrative for each of the parts of these ASN.1 structures.

Section 18.3 provides an illustrative instantiation of @UpdateSecurityCredentials.CommandPayload and its corresponding DER encoding.

### Updating Security Credentials on a Device – Processing Steps

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

#### 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 | rootBySupplier (0) ,  rootByWanProvider (1) ,  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, rootBySupplier is where a new root 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. root 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) | Mandatory if authorisingRemotePartyTACellIdentifier  present | KRP Signature is a digital signature |
| trustAnchorCellUsage | INTEGER | management(0) | DEFAULT management | Must be absent or set to ‘management’ 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, sequence 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 didn’t 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 |
| otherRemotePartySpecialistFloorSeqNumber | 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 has chosen to use a separate key agreement Key Pair in relation to prepayment top ups to the Device and this is a replacement of the corresponding certificate |
| certificationPathCertificates | SEQUENCE OF Certificate | The list of certificates needed for Certification Path Validation | At least one Certificate must be present since root will never directly sign any end entity certificate | 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 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

#### Command Authenticity and Integrity Verification

The Device shall undertake processing according to the requirements of Section 13.3.5.1.

Should any of the checks detailed in Section 13.3.5.1 fail then the Device shall:

* generate an entry in the Security Log recording failed Authentication;
* discard the Command without execution and without sending a Response; and
* send an Alert notifying the failed Authentication, constructed as specified in Section 6.2.4.2 of the GBCS, populated with the relevant Alert Code according to Section 16, to the Known Remote Party identified by:
  + - * the Trust Anchor Cell {supplier, digitalSignature, management} if the Device’s deviceType is not communicationsHubCommunicationsHubFunction; or
      * the Trust Anchor Cell {wanProvider, digitalSignature, management} if the Device’s deviceType is communicationsHubCommunicationsHubFunction.

Where all of the checks detailed in Section 13.3.5.1 succeed the Device shall process the Command and produce a Response.

#### Command Processing

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

If executionDateTime is present then the Device shall:

* record against the remotePartyRole (as specified in authorisingRemotePartyControl ), authorisingRemotePartyControl, replacements; and executionDateTime;
* construct a Response where executionOutcome is not present according to the requirements of Section 13.3.4.4; and
* at the date-time specified in executionDateTime, undertake the processing of Section 13.3.4.3.1 then construct an Alert according to the requirements of Section 13.3.4.5.

If executionDateTime is not present then the Device shall:

* undertake the processing of Section 13.3.4.3.1; and
* construct a Response where executionOutcome is present according to the requirements of Section 13.3.4.4.

##### replacements Processing

For each of the targetTrustAnchorCell in replacements, the Device shall:

* record the entityIdentifier and subjectKeyIdentifier currently held in that targetTrustAnchorCell;
* attempt to replace the contents of that targetTrustAnchorCell using the corresponding certificate in TrustAnchorReplacement; and
* if the contents of the replacement are successfully applied, undertake the processing required by Section 13.3.5.10 in relation to the RemotePartyRole for that targetTrustAnchorCell.

#### Response Construction

The @UpdateSecurityCredentials.ResponsePayload shall have the structure defined in Section 13.3.5.11, and the Device shall populate the executionOutcome, where present with values according to Table 13.3.4.4.

#### Alert Construction

The @UpdateSecurityCredentials.AlertPayload shall have the structure defined in Section 13.3.4, and the Device shall populate the executionOutcome, with values according to Table 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 | rootBySupplier (0) ,  rootByWanProvider (1) ,  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 |  | OPTIONAL | The resulting changes to any replay counters 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 counter values changed on the Device |
| otherRemotePartyFloorSeqNumber | INTEGER | The corresponding 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 has chosen to use a separate key agreement Key Pair in relation to prepayment top ups to the Device and this is a replacement of the corresponding certificate |
| statusCode | ENUMERATED | success (0) ,  badCertificate (5) ,  noTrustAnchor (10) ,  insufficientMemory (17) ,  contingencyPublicKeyDecrypt (22) ,  trustAnchorNotFound (25) ,  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 13.3.4.4: Attribute values for executionOutcome

### Common Requirements

#### Update Security Credentials Command Verification

The Device shall undertake the checks set out in this Section 13.3.5.1 before undertaking any other processing of the Command. The checks should be carried out in the order specified. Checking shall cease at the point that any one check fails. The checks required are shown in Table 13.3.5.1.

| **Check Number** | **Criteria that must be tested by the Device** | **How the Device shall test the Criteria** |
| --- | --- | --- |
| 1.1 | The Message is for the Device | The value of the Business Target ID in the Grouping Header in Command Instance must be equal to the Device’s Entity Identifier |
| 1.2 | The Message Code is for Update Security Credentials | The value in the Message Code field of the Grouping Header must be equal to the value specified in Table 13.3.5.2 for the CredentialsReplacementMode specified in CommandPayload. |
| 1.3 | If executionDateTime is present the Command is to replace Supplier Security Credentials. | If executionDateTime is present then credentialsReplacementMode must either supplierBySupplier  or supplierByTransCoS |
| 1.4 | The Device has not already actioned this Command. | As specified in Section 13.3.5.3 |
| 2.1 | The targetTrustAnchorCells all exist on a Device of this type | As specified in Section 13.3.5.4 |
| 2.2 | The credentialsReplacementMode is one that can be Authorised by the Remote Party / Parties authorising the Command | As specified in Section 13.3.5.5 |
| 2.2 | The replacements specified are all allowed in this credentialsReplacementMode. | As specified in Section 13.3.5.6 |
| 2.3 | The keyUsage in each of the replacement certificates provided is consistent with the target Trust Anchor Cells identified in replacements | As specified in Section 13.3.5.7 |
| 3.1 | The Cryptographic Protections are valid | As specified in Section 13.3.5.8 |

Table 13.3.5.1: Update Security Credentials Command authenticity and integrity verification

#### Message Code Validation

| **CredentialsReplacementMode** | **Message Code** |
| --- | --- |
| rootBySupplier | 0x0100 |
| rootByWanProvider | 0x0101 |
| supplierBySupplier | 0x0102 |
| networkOperatorByNetworkOperator | 0x0103 |
| accessControlBrokerByACB | 0x0104 |
| wanProviderByWanProvider | 0x0105 |
| transCoSByTransCoS | 0x0106 |
| supplierByTransCoS | 0x0107 |
| anyExceptAbnormalRootByRecovery | 0x0108 |
| anyByContingency | 0x0109 |

Table 13.3.5.2: Message Code validation against CredentialsReplacementMode

#### Preventing Replay of Commands

The Protection Against Replay mechanisms for the Update Security Credentials Command shall be that specified in this Section 13.3.5.3 (which is different than that for other GBCS Commands).

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

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

* (authorisingRemotePartyTACellIdentifier is populated in the Command) and (the authorisingRemotePartySeqNumber is strictly numerically greater than the Highest Prior Sequence Number the Device has recorded for the RemotePartyRole identified in authorisingRemotePartyTACellIdentifier)

else

* (the authorisingRemotePartySeqNumber is strictly numerically greater than the Highest Prior Sequence Number the Device has recorded for the accessControlBroker)

#### Required Trust Anchor Cells by Device Type

The Trust Anchor Cells specified in Section 4.3.2.5 are those required on each Device type and so are the only valid targetTrustAnchorCells.

The Device shall ensure that all targetTrustAnchorCells specified in the Command Instance are valid for the type of Device it is, according to the requirements of Section 4.3.2.5. A Command containing any invalid targetTrustAnchorCells shall not be processed any further by the Device.

#### Valid credentialsReplacementMode by Remote Party Roles authorising the Command

A Command containing a certain credentialsReplacementMode is only Authorised using certain types of Public-Private Key Pairs in certain ways. The Command identifies the Public Key corresponding to the Private Key used by the authorising Remote Party in the authorisingRemotePartyTACellIdentifier structure. Table 13.3.5.5 lists the only Authorised combinations. All other combinations represent Commands not properly Authorised and shall be rejected by a Device.

|  | **authorisingRemotePartyTACellIdentifier** | | |
| --- | --- | --- | --- |
|  | **RemotePartyRole** | **KeyUsage** | **CellUsage** |
| **credentialsReplacementMode** |  |  |  |
| rootBySupplier | supplier | digitalSignature | management |
| rootByWanProvider | wanProvider | digitalSignature | management |
| supplierBySupplier | supplier | digitalSignature | management |
| networkOperatorByNetworkOperator | networkOperator | digitalSignature | management |
| accessControlBrokerByACB, only if authorisingRemotePartyTACellIdentifier is present | accessControlBroker | digitalSignature | management |
| wanProviderByWanProvider | wanProvider | digitalSignature | management |
| transCoSByTransCoS | transitionalCoS | digitalSignature | management |
| supplierByTransCoS | transitionalCoS | digitalSignature | management |
| anyExceptAbnormalRootByRecovery | recovery | digitalSignature | management |
| anyByContingency | recovery | digitalSignature | management |

Table 13.3.5.5: Valid credentialsReplacementMode by Remote Party Roles authorising the Command

#### Valid credentialsReplacementMode by the targetTrustAnchorCells specified in the Command

A Command containing a certain credentialsReplacementMode can only validly replace the Security Credentials in a certain subset of Trust Anchor Cells. The Command identifies the Cells that are to have credentials replaced in each targetTrustAnchorCell within each TrustAnchorReplacement in replacements.

Table 13.3.5.6 below lists the only valid targetTrustAnchorCell combinations for each credentialsReplacementMode. All other combinations are invalid. A Command containing any invalid combinations shall not be processed any further by the Device

|  | **targetTrustAnchorCell** | | |
| --- | --- | --- | --- |
|  | **RemotePartyRole** | **KeyUsage** | **CellUsage** |
| **credentialsReplacementMode** |  |  |  |
| rootBySupplier | root | keyCertSign | management |
| rootByWanProvider | root | keyCertSign | management |
| supplierBySupplier | supplier | any valid for GBCS | any valid for GBCS |
| networkOperatorByNetworkOperator | networkOperator | any valid for GBCS | any valid for GBCS |
| accessControlBrokerByACB | accessControlBroker | any valid for GBCS | any valid for GBCS |
| wanProviderByWanProvider | wanProvider | any valid for GBCS | any valid for GBCS |
| transCoSByTransCoS | transitionalCoS | digitalSignature | management |
| supplierByTransCoS | supplier | any valid for GBCS | any valid for GBCS |
| anyExceptAbnormalRootByRecovery | any valid for GBCS | any valid for GBCS | any valid for GBCS |
| anyByContingency | any valid for GBCS | any valid for GBCS | any valid for GBCS |

Table 13.3.5.6: Valid credentialsReplacementMode by the targetTrustAnchorCells specified in the Command

#### Valid usage of Certificates against the targetTrustAnchorCells specified in the Command

[Note: Each of the ‘end entity’ Certificates in the Command must have the same keyUsage as the Trust Anchor Cell it is to be applied to.]

For each instance of the TrustAnchorReplacement structure in the Command, the keyUsage in replacementCertificate shall be equal to targetTrustAnchorCell.KeyUsage. Where this check fails for any one or more of the TrustAnchorReplacement instances, the Command shall not be actioned by the Device.

[Note: Save for supplier and network operator roles, each of the ‘end entity’ Certificates in the Command must have the same RemotePartyRole as the Trust Anchor Cell it is to be applied to.]

For each instance of the TrustAnchorReplacement structure in the Command where (targetTrustAnchorCell.RemotePartyRole <> supplier) and (targetTrustAnchorCell.RemotePartyRole <> networkOperator), the RemotePartyRole in replacementCertificate shall be equal to targetTrustAnchorCell.RemotePartyRole. Where this check fails for any one or more of the TrustAnchorReplacement instances, the Command shall not be actioned by the Device.

Notes:

* mismatches between RemotePartyRole in the certificate and the target Trust Anchor Cell are admissible for supplier and networkOperator only, and are needed (see Section 4.3.2.5); and
* CellUsage is simply a selector to allow a different Key Agreement key pair to be used for Prepayment Top Ups. However, that use of a different Key Pair is not mandated and so validation is not required; any valid supplier Key Agreement certificate may be used in this Trust Anchor Cell.

#### Verifying the CryptographicProtections

In verifying Cryptographic Protections pursuant to this Section 13.3.5.8.1:

* KRP Signature shall be verified according to the requirements in Section 4.3.2.7.2; and
* ACB-SMD MAC shall be verified according to the requirements in Section 6.2.4.1.2.

If credentialsReplacementMode = anyByContingency then KRP Signature shall be verified using the public key established according to the requirements of Section 13.3.5.8.1.

If credentialsReplacementMode = <> anyByContingency then KRP Signature shall be verified using the public key identified as per Section 4.3.2.7.2.

If credentialsReplacementMode = accessControlBrokerByACB and deviceType is not communicationsHubCommunicationsHubFunction then ACB-SMD MAC shall be verified as per Section 6.2.4.1.2.

##### 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, digitalSignature, 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.

#### 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 13.3.5.9.1 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;
* 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}) 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 <> anyByContingency) and (replacements does include a targetTrustAnchorCell of {root, keyCertSign}) 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.

If (credentialsReplacementMode = anyByContingency) and (replacements does include a targetTrustAnchorCell of {root, keyCertSign}) 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} as the root for Certification Path Validation.

##### Validation of new root Certificate against current root Security Credentials

The Device shall:

* identify the Certificate in replacements that corresponds to the targetTrustAnchorCell of {root, keyCertSign}. The Certificate shall be referred to as NewWithNew; then
* identify the Certificate in certificationPathCertificates that has the same subjectKeyIdentifier as the NewWithNew Certificate. The Certificate shall be referred to as NewWithOld. If no such Certificate is found, the Section 13.3.5.9.1 check fails else:
* undertake Certification Path Validation on NewWithOld according to the requirements of Section 4.3.2.8. If the Certification Path Validation fails, the Section 13.3.5.9.1 check fails else:
* use the Public Key in NewWithNew to verify the digital signature in NewWithNew. If the digital signature verification fails, the Section 13.3.5.9.1 check fails.

#### Required Processing on Change of Remote Party Control

If:

* the targetTrustAnchorCell is {supplier, digitalSignature, management}; and
* the Entity Identifier in the targetTrustAnchorCell is changed by the replacement; and
* the Device is an ESME or a GSME,

then the Device shall:

* set the Supplier Name which it displays to the X.500 Distinguished Name in the subject field of the certificate that was used to populate the targetTrustAnchorCell; and
* add an entry in the Billing Data Log (with the entry added having the same content as is required on Set Payment Mode Or Tariff change); and
* reset the Tariff Block Counter Matrix.

If the targetTrustAnchorCell is {root, keyCertSign, management} and there are any future dated Update Security Credentials or Activate Firmware Commands held on the Device that have not yet executed, and so the executionDateTime is in the future, then the Device shall set each executionDateTime to '99991231235959Z'.

If the targetTrustAnchorCell is not {root, keyCertSign, management} and there are any future dated Update Security Credentials or Activate Firmware Commands held on the Device that:

* include replacements for this remotePartyRole; and
* have not yet executed, and so the executionDateTime is in the future:

then the Device shall set each executionDateTime to '99991231235959Z'.

If:

* the targetTrustAnchorCell is {supplier, digitalSignature, management} or {root, keyCertSign, management}; and
* the Entity Identifier in the targetTrustAnchorCell is changed by the replacement

then the Device shall set the execution date-time of any other future dated Commands, that are held on the Device but not yet executed, to ‘never’, as detailed in Section 9.2. If the deviceType of the Device is gSME then the Device shall also delete any future dated data items that are pending activation.

If:

* remotePartyRole of targetTrustAnchorCell and that of authorisingRemotePartyControl is supplier; and
* keyUsage of targetTrustAnchorCell is digitalSignature

then the Device shall:

* set all Immediate Execution Counters and Future Dated Counters to the value in newRemotePartyFloorSeqNumber;
* clear all values from the UTRN Counter Cache; and
* place a single value in the UTRN Counter Cache. If newRemotePartySpecialistFloorSeqNumber is present and the seqNumberUsage in that newRemotePartySpecialistFloorSeqNumber is prepaymentTopUp then that value shall be the 32 most significant bits of the seqNumber in the newRemotePartySpecialistFloorSeqNumber. Otherwise the value shall be the 32 most significant bits of the newRemotePartyFloorSeqNumber.

If (remotePartyRole of authorisingRemotePartyControl is not supplier) but (targetTrustAnchorCell is {supplier, digitalSignature, management}) then there should be an instance of otherRemotePartySeqNumberChanges where remotePartyRole is supplier in the Command. Using the values in that instance of otherRemotePartySeqNumberChanges or the values zero if there is no such instance, the Device shall:

* set all Immediate Execution Counters and Future Dated Counters to the value in otherRemotePartyFloorSeqNumber;
* clear all values from the UTRN Counter Cache; and
* place a single value in the UTRN Counter Cache. If newRemotePartySpecialistFloorSeqNumber is present and the seqNumberUsage in that newRemotePartySpecialistFloorSeqNumber is prepaymentTopUp then that value shall be the 32 most significant bits of the seqNumber in the newRemotePartySpecialistFloorSeqNumber. Otherwise the value shall be the 32 most significant bits of the otherRemotePartyFloorSeqNumber.

#### 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, digitalSignature, management) Trust Anchor Cell

plaintextSymmetricKey [0] IMPLICIT OCTET STRING OPTIONAL,

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

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

-- Identify which of the Public Keys on the Device is to be used in checking KRP Signature

-- ‘authorisingRemotePartyTACellIdentifier’ can only be omitted when

-- the access control broker is updating its own credentials. 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 newTrustAnchorFloorSeqNumber must be included

-- and will be the value used to prevent replay of Update Security Credentials Commands for the

-- new controlling Remote Party.

newRemotePartyFloorSeqNumber [4] IMPLICIT SeqNumber OPTIONAL,

-- Some Commands on the Device may use a different Originator Counter sequence for Protection Against Replay. At this

-- version of the GBCS, the only example is the Prepayment Top Up Command on ESME and GSME. The

-- SpecialistSeqNumber structure allows such Counters to also be reset on change of control.

newRemotePartySpecialistFloorSeqNumber [5] IMPLICIT SEQUENCE OF SpecialistSeqNumber OPTIONAL,

-- In some cases, one party acting in one Remote Party Role may be replacing certificates for a different Remote Party Role.

-- In some cases, sequence 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..9223372036854775807)

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 subjectUniqueID 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 subjectUniqueID in the subject field of the certificate in this TrustAnchorReplacement

replacingSubjectUniqueID OCTET STRING,

-- The subjectKeyIdentifier in the certificate in this TrustAnchorReplacement

replacingSubjectKeyIdentifier OCTET STRING

}

TrustAnchorCellIdentifier ::= SEQUENCE

{

-- Which Remote Party Role does this Cell relate to?

trustAnchorCellRemotePartyRole RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. It will be absent except where used to refer to the Supplier Key

-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up

-- transactions

trustAnchorCellUsage CellUsage DEFAULT management

}

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

RemotePartyRole ::= INTEGER

{

-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake

-- processing. Note that most Devices will only support a subset of these.

root (0),

recovery (1),

supplier (2),

networkOperator (3),

accessControlBroker (4),

transitionalCoS (5),

wanProvider (6),

issuingAuthority (7), -- Devices will receive such Certificates but they do not need to store

-- them over an extended period

-- The ‘other’ RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from

-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid

-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is brought in to operation

other (127)

}

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

KeyUsage ::= BIT STRING

{

-- Define valid uses of Public Keys held by Devices in their Trust Anchor Cells.

digitalSignature (0),

contentCommitment (1), -- not valid for GBCS compliant transactions

keyEncipherment (2), -- not valid for GBCS compliant transactions

dataEncipherment (3), -- not valid for GBCS compliant transactions

keyAgreement (4),

keyCertSign (5),

cRLSign (6),

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

CredentialsReplacementMode ::= INTEGER

{

-- Define the valid combinations as to which Remote Party Roles can replace which kinds of Trust Anchors.

-- Normal operational replacement modes

rootBySupplier (0),

rootByWanProvider (1),

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),

-- contingencyPublicKeyDecrypt indicates that the update could not be processed because an error occurred while

-- decrypting the contingency public key.

contingencyPublicKeyDecrypt (22),

-- trustAnchorNotFound indicates that a change to a trust anchor was requested, but the referenced trust anchor

-- is not represented in the Trust Anchor Cell.

trustAnchorNotFound (25),

-- 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

#### 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 credentials (in which case it should be omitted) |
| authorisingRemotePartySeqNumber | Always required |
| newRemotePartyFloorSeqNumber | If the Command is to effect a change of control, then newTrustAnchorFloorSeqNumber should be included. It can be present in all other situations |
| newRemotePartySpecialistFloorSeqNumber | Only required on Change of Supplier where the new Supplier has decided to use a different sequence of Originator Counters for prepayment top ups. |
| otherRemotePartySeqNumberChanges | Should be present if one role (e.g. recovery, transitionalCoS) is changing credentials for another role or roles (e.g. supplier). In such cases, this should be present to set Protection Against Replay counters for that other role or roles |

Table 13.3.5.12: Requirements for AuthorisingRemotePartyControl elements

## CS02c Issue Security Credentials

### Description

This section covers the creation, validation and processing of (i) Issue Security Credentials Commands and (ii) Responses to such Commands.

### Use Case Cross References

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.C |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | Yes |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.17 |
| Valid Target Device(s) | ESME / GSME / GPF / CHF |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier (for Devices other than CHF)  WAN Provider (for CHF Devices only) |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | None |
| Valid initiating Device type(s) [HAN Only Messages] | None |
| Protocol | ASN.1 |

Table 13.4.2: Use Case Cross References for Issue Security Credential Details Command and Response

### Construction of Commands

Issue Security Credentials Command Payloads shall be constructed as specified in Section 13.4.7 and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of Message Category SME.C.C.

### Device processing of Commands and Response handling

The Device receiving an Issue Security Credentials Command shall undertake processing steps in the sequence defined in this Section 13.4.4.

In processing an Issue Security Credentials Command, the Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of Message Category SME.C.C. The Security Credentials used to verify Cryptographic Protection I shall be:
   * + - those held in the {wANProvider, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType equals communicationsHubCommunicationsHubFunction;
       - those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType does not equal communicationsHubCommunicationsHubFunction;
2. validate that the value of keyUsage in CommandPayload is either digitalSignature only or keyAgreement only. If this validation fails then the Device shall set issueCredentialsResponseCode to invalidKeyUsage, and process from step 6;
3. generate a Private-Public Key Pair and store the Private Key so generated in the Pending Private Key Cell determined by the value of keyUsage in CommandPayload. If the step fails then the Device shall set issueCredentialsResponseCode to keyPairGenerationFailed, and process from step 6;
4. with the ASN.1 terms in this step (that are not defined in this Section 13.4.4) having the meaning of IETF RFC 2986[[29]](#footnote-29); generate a CertificationRequest which:
   * + - complies with the requirements of IETF RFC2986 and IETF RFC 5912;
       - is DER encoded, in line with the recommendation of IETF RFC 5967[[30]](#footnote-30);
       - has subjectPublicKey set to the bit string representation of the Public Key generated in step 3;
       - incorporates an extensionRequest identified by id-ce-keyUsage which shall contain the keyUsage value specified in CommandPayload;
       - incorporates an extensionRequest identified by id-ce-subjectAltName which shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-HardwareModuleName) as defined in IETF RFC 4108. The hwSerialNum field shall be set to the Device’s Entity Identifier; and
       - has the signature generated using the Private Key generated in step 3;
5. if the generation of CertificationRequest is not successful then the Device shall set issueCredentialsResponseCode to cRProductionFailed;
6. create a Response according to the requirements of Section 13.4.7, apply the Response Cryptographic Protection required for a Response of Message Category SME.C.C, and send the Response.

### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of Message Category SME.C.C. The issueCredentialsResponseCode field, where present in the Response, may be decoded according to the ASN.1 definitions at Section 13.4.6.

### Issue Security Credentials Command and Response payloads – structure definition

Each instance of @IssueSecurityCredentials.CommandPayload and of @IssueSecurityCredentials.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.4.6 which specifies the structure in Abstract Syntax Notation One (ASN.1) notation.

IssueSecurityCredentials DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the keyUsage to which the generated key-pair will be put, if subsequently authorised

keyUsage KeyUsage

}

ResponsePayload ::= CHOICE

{

-- if the Command was successful, provide the generated Certification Request. CertificationRequest shall

-- be as defined in ASN.1 by IETF RFC 5912. For reference, it is in the section headed ‘ASN.1 Module for RFC 2986’

certificationRequest CertificationRequest,

-- if the Command was unsuccessful, detail the failure

issueCredentialsResponseCode IssueCredentialsResponseCode

}

-- KeyUsage is only repeated here for ease of reference. It is defined in IETF 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), -- not valid for this Use Case

cRLSign (6), -- not valid for this Use Case

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

IssueCredentialsResponseCode::= INTEGER

{

invalidKeyUsage (1),

keyPairGenerationFailed (2),

cRProductionFailed (3)

}

END

### Constructing the @IssueSecurityCredentials.CommandPayload and of @IssueSecurityCredentials.ResponsePayload

@IssueSecurityCredentials.CommandPayload shall have the structure defined in Section 13.4.6, and the Remote Party constructing the Command shall populate with values according to Table 13.4.7a.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @IssueSecurityCredentials.CommandPayload | SEQUENCE |  |  |  |
| keyUsage | BIT STRING | Either digitalSignature (0) only,  Or keyAgreement (4) only | Mandatory | Only one or the other is valid |

Table 13.4.7a: @IssueSecurityCredentials.CommandPayload population

@IssueSecurityCredentials.ResponsePayload shall have the structure defined in Section 13.4.6, and the Device constructing the Response shall populate with values according to Table 13.4.7b.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @IssueSecurityCredentials.ResponsePayload | CHOICE |  |  |  |
| certificationRequest | See IETF RFC 5912 | The Certification Request produced according to the requirements of Section 13.4.4. | Mandatory | Mandatory if certificationRequest successfully produced |
| issueCredentialsResponseCode | INTEGER | Shall be populated according to the processing defined in Section 13.4.4 | Mandatory | Mandatory if certificationRequest is not successfully produced |

Table 13.4.7b: @IssueSecurityCredentials.ResponsePayload population

## CS02d Update Device Certificates on Device

### Description

This Section 13.5 covers the creation, validation and processing of (i) Update Device Certificates on Device, Commands and (ii) Responses to such Commands.

### Use Case Cross References

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.C |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | Yes |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.15 |
| Valid Target Device(s) | ESME / GSME / GPF / CHF |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier (for Devices other than CHF)  WAN Provider (for CHF Devices only) |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | None |
| Valid initiating Device type(s) [HAN Only Messages] | None |
| Protocol | ASN.1 |

Table 13.5.2: Use Case Cross References for Update Device Certificate on Device, Command and Response

### Construction of Commands

Update Device Certificate on Device Command Payloads shall be constructed as specified in Section 13.5.7, and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of Message Category SME.C.C.

### Device processing of Commands and Response handling

The Device receiving an Update Device Certificate on Device Command shall undertake processing steps in the sequence defined in this Section 13.5.4.

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

1. undertake Command Authenticity and Integrity Verification as required for a Command of Message Category SME.C.C. The Security Credentials used to verify Cryptographic Protection I shall be:
   * + - those held in the {wANProvider, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType equals communicationsHubCommunicationsHubFunction; or
2. those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType does not equal communicationsHubCommunicationsHubFunction.establish the values of keyUsage, subjectPublicKey and hwSerialNum in certificate in the CommandPayload. If any of the values cannot be established then the Device shall set updateDeviceCertResponseCode to invalidCertificate, and process from step 9;
3. validate that hwSerialNum established at step 2 is the Device’s Entity Identifier. If this validation fails then the Device shall set updateDeviceCertResponseCode to wrongDeviceIdentity, and process from step 9;
4. validate that keyUsage established at step 2 is either digitalSignature only or keyAgreement only. If this validation fails then the Device shall set updateDeviceCertResponseCode to invalidKeyUsage, and process from step 9;
5. validate that the Device holds a Pending Private Key for the keyUsage as established at step 2. If this validation fails then the Device shall set updateDeviceCertResponseCode to noCorrespondingKeyPairGenerated, and process from step 9;
6. validate that subjectPublicKey established at step 2 is the bit string representation of the Public Key corresponding to the Pending Private Key identified at step 5. If this validation fails then the Device shall set updateDeviceCertResponseCode to wrongPublicKey, and process from step 9;
7. store certificate. If this step fails then the Device shall set updateDeviceCertResponseCode to certificateStorageFailed, and process from step 9;
8. set the Current Private Key to have the value of the Pending Private Key for the keyUsage established at step 2. If this step fails then the Device shall set updateDeviceCertResponseCode to privateKeyChangeFailed, and process from step 9;
9. set updateDeviceCertResponseCode to success; and
10. create a Response according to the requirements of Section 13.5.7, apply the Response Cryptographic Protection required for a Response of Message Category SME.C.C, and send the Response.

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

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

### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of the relevant Message Category. The updateDeviceCertResponseCode field may be decoded according to the ASN.1 definitions at Section 13.5.6.

If this was a change of digitalSignature certificate, the public key to be used to verify the Device’s signature is dependent on the value of updateDeviceCertResponseCode. If updateDeviceCertResponseCode is success then the Private Key used for Signing will have changed. If updateDeviceCertResponseCode is other than success, the Private Key used for Signing will not have changed.

### Update Device Certificate on Device Command and Response payloads – structure definition

Each instance of @UpdateDeviceCertificateonDevice.CommandPayload and of @UpdateDeviceCertificateonDevice.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.5.6, which specifies the structure in ASN.1 notation.

UpdateDeviceCertificateonDevice DEFINITIONS ::= BEGIN

CommandPayload ::= Certificate

-- provide the certificate which the Device is to store

-- the ASN.1 specification of certificate shall be as defined in IETF RFC 5912 for IETF RFC 5280

ResponsePayload ::= UpdateDeviceCertResponseCode

-- if the Command was unsuccessful, detail the failure; otherwise respond with success

UpdateDeviceCertResponseCode::= INTEGER

{

success (0),

invalidCertificate (1),

wrongDeviceIdentity (2),

invalidKeyUsage (3),

noCorrespondingKeyPairGenerated (4),

wrongPublicKey (5),

certificateStorageFailed (6),

privateKeyChangeFailed (7)

}

END

### Constructing the @UpdateDeviceCertificateonDevice.CommandPayload and @UpdateDeviceCertificateonDevice.ResponsePayload

@UpdateDeviceCertificateonDevice.CommandPayload shall have the structure defined in Section 13.5.6, and the Remote Party constructing the Command shall populate with values according to Table 13.5.7a.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @UpdateDeviceCertificateonDevice.CommandPayload |  |  |  |  |
| Certificate | See IETF RFC 5912 | A new Device Certificate that the Device is to process | Mandatory |  |

Table 13.5.7a: @UpdateDeviceCertificateonDevice.CommandPayload population

@UpdateDeviceCertificateonDevice.ResponsePayload shall have the structure defined in Section 13.5.6, and the Device constructing the Response shall populate with values according to Table 13.5.7b.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @UpdateDeviceCertificateonDevice.ResponsePayload |  |  |  |  |
| UpdateDeviceCertResponseCode | INTEGER | Shall be populated according to the processing defined in Section 13.5.4 | Mandatory |  |

Table 13.5.7b: @UpdateDeviceCertificateonDevice.ResponsePayload population

## CS02e Provide Device Certificates from Device

### Description

This section covers the creation, validation and processing of (i) Provide Device Certificates from Device Commands and (ii) Responses to such Commands.

### Use Case Cross References

|  |  |
| --- | --- |
| **Cross Reference** | **Value** |
| Grouping | Remote Party Message |
| Message Type | Command & Response |
| Message Type Category | Variant Message |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | No |
| SEC User Gateway Services Schedule (Service Request) Reference | 6.24 |
| Valid Target Device(s) | ESME / GSME / GPF / CHF |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier (for Devices other than CHF)  WAN Provider (for CHF Devices only) |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | None |
| Valid initiating Device type(s) [HAN Only Messages] | None |
| Protocol | ASN.1 |

Table 13.6.2: Use Case Cross References for Provide Device Certificates from Device Command and Response

### Construction of Commands

Provide Device Certificates from Device Command Payloads shall be constructed as specified in Section 13.6.7 and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of Message Category SME.C.C.

### Device processing of Commands and Response handling

The Device receiving a Provide Device Certificates from Device Command shall undertake processing steps in the sequence defined in this Section 13.6.4.

In processing a Provide Device Certificates from Device Command, the Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of Message Category SME.C.C, except that Cryptographic Protection II shall not be verified. The Security Credentials used to verify Cryptographic Protection I shall be:
   * + - those held in the {wANProvider, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType equals communicationsHubCommunicationsHubFunction; or
       - those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if the target Device’s deviceType does not equal communicationsHubCommunicationsHubFunction;
2. validate that keyUsage in CommandPayload is either digitalSignature only or keyAgreement only. If this validation fails then the Device shall set provideDeviceCertResponseCode to invalidKeyUsage, and process from step 5;
3. confirm that the Device holds a certificate which (1) is for the keyUsage identified at step 2, (2) contains in hwSerialNum a value equal to the Device’s Entity Identifier and (3) contains in subjectPublicKey the bit string representation of the Public Key corresponding to the Current Private Key for this keyUsage. If this validation fails then the Device shall set provideDeviceCertResponseCode to noCertificateHeld, and process from step 5;
4. retrieve the certificate identified in step 3. If this step fails then the Device shall set provideDeviceCertResponseCode to certificateRetrievalFailure, and process from step 5;
5. create a Response according to the requirements of Section 13.6.7, apply the Response Cryptographic Protection required for a Response of Message Category SME.C.C, and send the Response.

### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of the Message Category SME.C.C. The provideDeviceCertResponseCode field may be decoded according to the ASN.1 definitions at Section 13.6.6.

### Provide Device Certificates from Device Command and Response payloads – structure definition

Each instance of @ProvideDeviceCertificateFromDevice.CommandPayload and of @ProvideDeviceCertificateFromDevice.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.6.6 which specifies the structure in ASN.1 notation.

ProvideDeviceCertificateFromDevice DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the KeyUsage of the Certificate to be returned

keyUsage KeyUsage

}

ResponsePayload ::= CHOICE

{

-- if the Command was successful, provide the certificate

certificate Certificate,

-- if the Command was unsuccessful, detail the failure

provideDeviceCertResponseCode ProvideDeviceCertResponseCode

}

-- KeyUsage is only repeated here for ease of reference. 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), -- not valid for this Use Case

cRLSign (6), -- not valid for this Use Case

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

ProvideDeviceCertResponseCode::= INTEGER

{

invalidKeyUsage (1),

noCertificateHeld (2),

certificateRetrievalFailure (3)

}

END

### Constructing the @ProvideDeviceCertificateFromDevice.CommandPayload and @ProvideDeviceCertificateFromDevice.ResponsePayload

@ProvideDeviceCertificateFromDevice.CommandPayload shall have the structure defined in Section 13.6.6 and the Remote Party constructing the Command shall populate with values according to Table 13.6.7a.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @ProvideDeviceCertificateFromDevice.CommandPayload | SEQUENCE |  |  |  |
| keyUsage | BIT STRING | Either digitalSignature (0) only,  Or keyAgreement (4) only | Mandatory | Only one or the other is valid |

Table 13.6.7a: @ProvideDeviceCertificateFromDevice.CommandPayload population

@ProvideDeviceCertificateFromDevice.ResponsePayload shall have the structure defined in Section 13.6.6, and the Device constructing the Response shall populate with values according to Table 13.6.7b.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @ProvideDeviceCertificateFromDevice.ResponsePayload | CHOICE |  |  |  |
| Certificate | See IETF RFC 5912 | The Device Certificate provided pursuant to Section 13.6.4 | Mandatory | Mandatory if certificate successfully produced |
| provideDeviceCertResponseCode | INTEGER | Shall be populated according to the processing defined in Section 13.5.4 | Mandatory | Mandatory if certificate is not successfully produced |

Table 13.6.7b: @ProvideDeviceCertificateFromDevice.ResponsePayload population

## Pair-wise Authorisation of Devices

### Introduction to pair-wise Authorisation of Devices - informative

#### The role of pair-wise Authorisation - informative

This Section 13.7 includes the Use Cases related to the Authorisation (and the removal of Authorisation) for pair-wise, secure application layer interaction between two Devices on the same SMHAN. It also covers the related Use Cases for backing up and restoring the GPF Device Log.

The process of authorising two Devices to communicate is referred to as ‘Joining’[[31]](#footnote-31). Removal of such authorisation is referred to as ‘Un-joining’. Correspondingly, Remote Party Commands are specified in this Section 13.7 for instructing Devices that they are to ‘Join’ or ‘Unjoin’.

In line with the SMETS and CHTS Device Log requirements, two Devices on a HAN must only be capable of interacting at the application layer if they are currently Joined. They must not be capable of interacting if (1) they have never been Joined or (2) they have been Unjoined.

The application layer interactions between Devices on the same SMHAN must conform to the Device Based Access Controls (DBAC) as defined in Section 13.7.3. For example, an ESME must not be capable of processing an ‘Enable Supply’ Command from an IHD or an HCALCS.

It is a precondition of Joining that both Devices have been ‘White-listed’ on to the HAN (as per Use Case ‘CCS01 Add Device to CHF Device log’) so that they are able to communicate over the HAN at the network layer (and so have network access). The GPF may be configured to be in the CHF’s Device Log at manufacture. A Device on a white-list can be removed from the white-list. It must then be unable to communicate over the HAN, and so unable to interact at the application layer with any Devices to which it was ‘Joined’.

In SMETS terminology:

* the CHF’s Device Log holds the list of currently white-listed Devices on the SMHAN; and
* the Device Log on an ESME, GSME, GPF or Type 1 Device holds the Entity Identifiers, Device Types and related Security Credentials of other Devices on the HAN to which the Device is currently Joined (and so Authorised to interact with at an application layer).

The process of white-listing a Device and its subsequently obtaining network access establishes a shared secret key between the Device and the Communications Hub. The Gas Proxy Function, which is part of the Communications Hub, uses this shared secret key, combined with a Device being entered in to its Device Log, for application layer authorisation.

IHDs and other Type 2 Devices are not required to have a Device Log (as defined in SMETS). They are required to store security and related details of the Devices to which they are Joined as required by ZSE however (otherwise they would be cryptographically unable to understand the information being sent to them by the Joined Devices).

IHDs and other Type 2 Devices can only read application layer information from Devices to which they are Joined (either by requesting the information from the Device or by receiving information published by the Device). When a PPMID is joined to a GPF the PPMID can only read information from the GPF to which it is Joined.

When other types of Device are Joined (e.g. HCALCS, PPMID), they can also exchange Commands and Responses at the application layer. For example, an ESME that is Joined to an HCALCS can send a Command to the HCALCS to turn its switch on and the HCALCS can send a Response saying whether it has done that. A PPMID can send an ‘enable supply’ Command to an ESME etc.

#### The joining sequence – informative

There are three types of Join:

* Join Method B: this is a Join involving a Type 2 Device or a GPF;
* Join Method C: this is a Join between a GSME and a PPMID; and
* Join Method A: this is any Join which is not covered by Method B or C.

Except for Method C, all Joins use the ZSE cryptography which requires exchange of messages between the two Devices to establish the shared secret that the two Devices will need to use. Method C uses the cryptography of Section 4 of this GBCS.

Only certain combinations of Devices can be validly ‘Joined’. Table 13.7.1.2 summarises valid combinations:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Device Name |  | ESME | GSME | Comms Hub (CHF) | Comms Hub (GPF) | HCALCS | PPMID | Type 2 (IHD or CAD) |
|  | **deviceType** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| ESME | **0** | Not permitted |  |  |  |  |  |  |
| GSME | **1** | Not permitted | Not permitted |  |  |  |  |  |
| Comms Hub (CHF) | **2** | Not permitted | Not permitted | Not permitted |  |  |  |  |
| Comms Hub (GPF) | **3** | Not permitted | Method B | Not permitted | Not permitted |  |  |  |
| HCALCS | **4** | Method A | Not permitted | Not permitted | Not permitted | Not permitted |  |  |
| PPMID | **5** | Method A | Method C | Not permitted | Method B | Not permitted | Not permitted |  |
| Type 2 (IHD or CAD) | **6** | Method B | Not permitted | Not permitted | Method B | Not permitted | Not permitted | Not permitted |

Table 13.7.1.2: Permitted Joins

A Method A Join always involves an ESME and therefore any HAN exchanges required by a Method A Join shall always be instigated by the ESME involved. In this context the ESME is referred to as the methodAInitiator, since it initiates Method A Joins.

The additional step with a Method A Join is that the other Device must first be sent a Join Command detailing the ESME with which it is allowed to Join. On receipt, the Device should add the ESME details to its Device Log and send a Response accordingly. If, subsequently, the Device is asked to undertake key establishment, it must check that the requesting Device is in its Device Log.

Only one Device in a Method B Join is remotely instructed. Thus, the HAN exchanges required by a Method B Join shall always be instigated by the Device receiving such a Command. From Table 13.7.1.2, this is always a GSME or ESME except where a GPF is to Join to a PPMID, IHD or CAD. Thus, the sequence of a Method B Join is that the ESME / GSME / GPF:

* is sent a Join Command containing the Entity Identifier of the Device to which it is to Join and that other Device’s DeviceType;
* verifies the cryptographic protection on the Command and checks to make sure it is well formed and valid;
* updates its Device Log to include details of the new Device;
* for an ESME[[32]](#footnote-32), undertakes the key establishment process with the specified Device, as per the ZSE 1.2 specification. The constraint that Key Establishment has to involve the ZSE Trust Centre shall not be applied by Devices; and
* creates and sends a Response detailing the success or otherwise of its actions.

A Method C join does not require exchange of Messages between the two Devices for the establishment of the shared secret. Thus the sequence of a Method C Join is that each of the GSME and PPMID:

* is sent a Join Command containing the Entity Identifier of the Device to which it is to Join, that other Device’s DeviceType and Key Agreement Certificate;
* verifies the cryptographic protection on the Command and does checks to make sure it is well formed and valid;
* updates its Device Log to include details of the new Device;
* checks there is a well-formed Device Certificate in the Command;
* optionally calculates the shared secret using the Device Certificate of the other Device (which is provided in the Command); and
* creates and sends a Response detailing the success or otherwise of its actions.

#### The format of Message Payloads - informative

In common with other GBCS Remote Messages related to the management of Security Credentials, the payloads of Commands and Responses defined in this Section 13.7.1.3 are specified using ASN.1, with DER encoding to be applied to Command and Response payloads.

### Device Requirements

All Devices shall:

* support the ZSE Key Establishment Cluster as specified in Annex C of the ZSE cluster;
* support ‘Crypto Suite 2’ as defined in the ZSE specification; and
* use ‘Crypto Suite 2’ when undertaking any associated Key Establishment process.

Devices shall not apply any restrictions on the types of Devices used in any associated Key Establishment process, except for those specified in the GBCS. Specifically, the ZSE constraint requiring Trust Centre involvement shall not be applied (where ‘Trust Centre’ has the meaning defined in ZSE).

An ESME shall be configured to be a ZSE ‘Router’, as defined in ZSE so that communications between the ESME and Devices Joined to the ESME are not reliant on availability of the Communications Hub.

Pursuant to the requirements in the SMETS and the CHTS requirement, Devices shall only communicate at an application layer with other Devices that are currently in their Device Log and are permitted by Device Based Access Controls (DBAC) as defined at Section 13.7.3. Such communications shall always be secured using the shared secrets established pursuant to Sections 13.7.4.

Application layer communications within the scope of the DBAC requirement are HAN Only Messages, including provision of information to a PPMID or Type 2 Device. Note that HAN Only Messages between a PPMID and GSME have a structure that is specified in this GBCS in the corresponding Use Cases, and those relate only to Add Credit and Activate Emergency Credit Commands and the corresponding Responses.

Each entry in a non CHF Device Log shall contain the Entity Identifier of the Authorised Device and its deviceType.

The Entity Identifier of a Device with DeviceType of communicationsHubGasProxyFunction shall be the EUI 64-bit identifier of the ZigBee radio interface installed in the Communications Hub.

### Device Based Access Control

In relation to information and functionality within SMETS, a Device shall, when it is a recipient of a Command or request for information from another Device on its SMHAN, only attempt to action that Command when:

* the sending Device’s Entity Identifier is in the recipient Device’s Device Log;
* the ZSE cryptographic protection on the Message is authenticated using the Shared Secret / Shared Secret Key established with the sending Device; and
* the Command or request for information is explicitly allowed by a cell in Tables 13.7.3a and 13.7.3b, in terms of the DeviceType of the sending (client) and receiving (service) Device. The receiving Device shall determine the sending Device’s DeviceType by reference to its Device Log entry for that sending Device.

Where a Device is a recipient of a Command or request for information from another Device on its SMHAN that does not meet the access requirements of this Section 13.7.3, it shall:

* generate an entry in the Security Log recording failed Authentication;
* discard the Command or request for information without execution and without sending a Response; and
* send an Alert notifying the failed Authentication, constructed as specified in Section 6.2.4.2, populated with the relevant Alert Code from Section 16, to the Known Remote Party identified by the Security Credentials it holds in the Supplier role.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Device Name | Server / recipient | ESME | GSME | Comms Hub (GPF) | HCALCS | PPMID | Type 2 (IHD or CAD) |
| Client / sender | DeviceType | 0 | 1 | 3 | 4 | 5 | 6 |
| ESME | 0 | - | - | - | 5.6.4.1  5.6.4.2  5.6.4.3 | - | - |
| GSME | 1 | - | - | - | - | - | - |
| Comms Hub (GPF) | 3 | - | Request for Information | - | - | - | - |
| HCALCS | 4 | 8.5.2.1 | - | - | - | - | - |
| PPMID | 5 | 7.5.5.1  7.5.5.2  7.5.5.3  Request for Information | 7.5.4.1  7.5.4.2 | Request for Information | - | - | - |
| Type 2 (IHD or CAD) | 6 | Request for Information | - | Request for Information | - | - | - |

Table 13.7.3a: Permitted Access by DeviceType, with Commands shown by SMETS reference

|  |  |  |
| --- | --- | --- |
| **SMETS Ref** | **SMETS Command Name** | **ZSE Ref** |
| 5.6.4.1 | Cancel Control HAN Connected Auxiliary Load Control Switch | Cancel Load Control Event |
| 5.6.4.2 | Request a HAN Connected Auxiliary Load Control Switch State Change | Load Control Event |
| 5.6.4.3 | Write Configuration Data to an HCALCS | Demand Response and Load Control Cluster: WriteAttributes |
| 8.5.2.1 | Request Control of a HAN Connected Auxiliary Load Control Switch | Get Scheduled Events |
| 7.5.5.1 | Request Emergency Credit Activation | Select Available Emergency Credit |
| 7.5.5.2 | Request to Add Credit | Consumer Top Up |
| 7.5.5.3 | Request to Enable ESME Supply | Change Supply |
| 7.5.4.1 | Request Emergency Credit Activation | Select Available Emergency Credit |
| 7.5.4.2 | Request to Add Credit | Consumer Top Up |

Table 13.7.3b: Mapping of Table 13.7.3a command references to SMETS names and ZSE

### Use Case Requirements

This Section 13.7.4 details requirements which shall be complied with for all Join or Unjoin related Use Cases.

#### Use Cases covered

The types of Join Device related Messages, the Grouping names used in this Section 13.7.4, the associated Message Category and the valid recipient deviceType for each shall be as specified in Table 13.7.4.1[[33]](#footnote-33). The SEC User Gateway Services Schedule (Service Request) Reference for all Join Use Cases shall be 8.7, and for Unjoin Use Cases shall be 8.8.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Message Code** | **Use Case Name** | **Valid recipient deviceType** | **Grouping** | **Message Category** |
| 0x000D | CS03A1 Method A Join (Meter) | eSME | Join Device | SME.C.C |
| 0x00AB | CS03A2 Method A Join (non Meter) | type1HANConnectedAuxiliaryLoadControlSwitch  type1PrepaymentInterfaceDevice | Join Device | SME.C.C |
| 0x000E | CS03B Method B Join | gSME  eSME  communicationsHubGasProxyFunction | Join Device | SME.C.NC |
| 0x00AF | CS03C Method C Join | gSME  type1PrepaymentInterfaceDevice | Join Device | SME.C.C |
| 0x000F | CS04AC Method A or C Unjoin | gSME  eSME  communicationsHubGasProxyFunction  type1HANConnectedAuxiliaryLoadControlSwitch  type1PrepaymentInterfaceDevice | Unjoin Device | SME.C.C |
| 0x0010 | CS04B Method B Unjoin | gSME  eSME  communicationsHubGasProxyFunction | Unjoin Device | SME.C.NC |
| 0x0013 | CS07 Read Device Join Details | gSME  eSME  communicationsHubGasProxyFunction type1HANConnectedAuxiliaryLoadControlSwitch  type1PrepaymentInterfaceDevice |  | SME.C.NC |

Table 13.7.4.1: Join Device related Commands, Grouping and Message Categories

#### Join Device Command and Response Processing

##### Construction of Commands

‘Join Device’ Command Payloads shall be constructed as specified in Section 13.7.4.5.2 and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of the relevant Message Category.

For a Command (1) which complies with either Use Case ‘CS03B Method A Join (non Meter)’ or Use Case ‘CS03A2 Method C Join‘ and (2) where the Device to which it is addressed has a deviceType equal to type1PrepaymentInterfaceDevice, the Access Control Broker’s Digital Signing Private Key shall be used in generating the KRP Signature.

##### 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 Section 13.4.7, 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. The Security Credentials used to verify Cryptographic Protection 1 shall be:
   * + - those held in the {accessControlBroker, digitalSignature, management} Trust Anchor Cell, if deviceType equals type1PrepaymentInterfaceDevice; or
       - those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if deviceType does not equal type1PrepaymentInterfaceDevice;
2. verify the joinMethodAndRole as specified in Section 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;
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.

##### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of the relevant Message Category. The joinResponseCode field in the Response may be decoded according to the ASN.1 definitions at Section 13.7.4.5.1.

#### ‘Unjoin Device’ Command and Response Processing

##### Construction of Commands

‘Unjoin Device’ Command Payloads shall be constructed as specified in Section 13.7.4.6.2 and Cryptographic Protection I and Cryptographic Protection II shall be applied as required for a Command of the relevant Message Category.

For a Command where the Device to which it is addressed has a deviceType equal to type1PrepaymentInterfaceDevice, the Access Control Broker’s Digital Signing Private Key shall be used in generating the KRP Signature.

##### Device processing of Commands and Response handling

The Device receiving an ‘Unjoin Device’ Command shall undertake processing steps in the sequence defined in this Section 13.7.4.3.2.

In processing an ‘Unjoin Device’ Command, the Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of this Message Category. The Security Credentials used to verify Cryptographic Protection 1 shall be:
   * + - those held in the {accessControlBroker, digitalSignature, management} Trust Anchor Cell, if deviceType equals type1PrepaymentInterfaceDevice; or
       - those held in the {supplier, digitalSignature, management} Trust Anchor Cell, if deviceType does not equal type1PrepaymentInterfaceDevice;
2. set unjoinResponseCode to success;
3. verify the otherDeviceEntityIdentifier matches an Entity Identifier currently recorded in its Device Log. If it does not then set unjoinResponseCode to otherDeviceNotInDeviceLog and process from step 5; otherwise process from step 4;
4. delete all information from the entry in its Device Log that has the same Entity Identifier as otherDeviceEntityIdentifier along with all shared cryptographic material related to that entry. If the deletion does not succeed, set unjoinResponseCode to otherFailure; and
5. Create a Response according to the requirements of Section 13.7.4.6.2, apply the Response Cryptographic Protection required for a Response of the relevant Message Category, and send the Response.

##### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of the relevant Message Category. The unjoinResponseCode field in the Response may be decoded according to the ASN.1 definitions at Section 13.7.4.6.1.

#### ‘CS07 Read Device Join Details’ Command and Response Processing

##### Construction of Commands

‘CS07 Read Device Join Details’ Command Payloads shall be constructed as specified in Section 13.7.4.7 and Cryptographic Protection II shall be applied as required for a Command of the SME.C.NC Message Category.

##### Device processing of Commands and Response handling

The Device receiving a ‘CS07 Read Device Join Details’ Command shall undertake processing steps in the sequence defined in this Section 13.7.4.4.2.

In processing a ‘CS07 Read Device Join Details’ Command, the Device shall:

1. undertake Command Authenticity and Integrity Verification as required for a Command of the SME.C.NC Message Category;
2. set readLogResponseCode to success;
3. attempt to read the Entity Identifier and deviceType for each of the entries in its Device Log. If the reading does not succeed for all entries, set readLogResponseCode to readFailure; otherwise populate deviceLogEntries using the data read from its Device Log; and
4. create a Response according to the requirements of Section 13.7.4.7, apply the Response Cryptographic Protection required for a Response of the SME.C.NC Message Category, and send the Response.

##### Response Processing

Response Recipient Verification may be undertaken as specified in this GBCS for a Response of the SME.C.NC Message Category. The readLogResponseCode and deviceLogEntries fields in the Response may be decoded according to the ASN.1 definitions at Section 13.7.4.7.

#### Component Requirements – Join

##### Join Command and Response payloads – structure definition

Each instance of @JoinDevice.CommandPayload and of @JoinDevice.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.7.4.5.1 which specifies the structure in ASN.1 notation.

JoinDevice DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify which type of joining is being authorised and,

-- for Method A Joins, the role the Device is to play

joinMethodAndRole JoinMethodAndRole,

-- specify the Entity Identifier of the Device which is to be Joined with

otherDeviceEntityIdentifier OCTET STRING,

-- specify the DeviceType of that other Device

otherDeviceType DeviceType,

-- provide the other Device’s Key Agreement certificate, if and only if this

-- is a join between a gSME and a type1PrepaymentInterfaceDevice.

-- Certificate shall be as defined in IETF RFC 5912

otherDeviceCertificate Certificate OPTIONAL

}

-- detail whether the Command successful executed or, if it didn’t,

-- what the failure reason was

ResponsePayload ::= JoinResponseCode

JoinMethodAndRole ::= INTEGER

{

-- methodB is to be used where the other Device is a Type 2 Device or GPF.

-- methodC is used where the Devices involved are a GSME and a PPMID.

-- methodA is used otherwise.

-- methodAInitiator is used where the Device this Command is targeted at

-- should initiate the Key Agreement process

-- methodAResponder is used where the Device this Command is targeted at

-- should respond in the Key Agreement process, but shall not initiate it

methodAInitiator (0),

methodAResponder (1),

methodB (2),

methodC (3)

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

JoinResponseCode::= INTEGER

{

success (0),

invalidMessageCodeForJoinMethodAndRole (1),

invalidJoinMethodAndRole (2),

incompatibleWithExistingEntry (3),

deviceLogFull (4),

writeFailure (5),

keyAgreementNoResources (6),

keyAgreementUnknownIssuer (7),

keyAgreementUnsupportedSuite (8),

keyAgreementBadMessage (9),

keyAgreementBadKeyConfirm (10),

invalidOrMissingCertificate (11)

}

END

##### Constructing the @JoinDevice.CommandPayload and of @JoinDevice.ResponsePayload

@JoinDevice.CommandPayload shall have the structure defined in Section 13.7.4.5.1, and the Remote Party constructing the Command shall populate with values according to Table 13.7.4.5.2a.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @JoinDevice.CommandPayload | SEQUENCE |  |  |  |
| joinMethodAndRole | INTEGER | methodAInitiater (0),  methodAResponder (1),  methodB (2),  methodC (3) |  | See Section 13.7.4.5.3 for valid values |
| otherDeviceEntityIdentifier | OCTET STRING | Entity Identifier | Mandatory | The Entity Identifier of the Device which is to be entered in this Device’s Device Log |
| otherDeviceType | INTEGER | gSME (0),  eSME (1),  communicationsHubCommunicationsHubFunction (2),  communicationsHubGasProxyFunction (3),  type1HANConnectedAuxiliaryLoadControlSwitch (4),  type1PrepaymentInterfaceDevice (5),  type2 (6) | Mandatory | The DeviceType of the Device which is to be entered in this Device’s Device Log |
| otherDeviceCertificate | Certificate | The Key Agreement Certificate currently in use by the other Device. | OPTIONAL | The other Device’s Key Agreement certificate, which shall only be present if and only if this is a join between a gSME and a type1PrepaymentInterfaceDevice.  Certificate shall be as defined in IETF RFC 5912. |

Table 13.7.4.5.2a: @JoinDevice.CommandPayload population

@JoinDevice.ResponsePayload shall have the structure defined in Section 13.7.4.5.1, and the Remote Party constructing the Command shall populate with values according to Table 13.7.4.5.2b.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @JoinDevice.ResponsePayload |  |  |  |  |
| JoinResponseCode | INTEGER | Shall be populated according to the processing defined in Section 13.7.4.2.2 | Mandatory |  |

Table 13.7.4.5.2b: @JoinDevice.ResponsePayload population

##### Verification of joinMethodAndRole

The Device shall first verify the joinMethodAndRole specified in the Command Payload against the Message Code specified in the Grouping Header of the Command according to Table 13.7.4.5.3a. If the check fails JoinResponseCode in the Response shall be set to the value invalidMessageCodeForJoinMethodAndRole and no further verification checks in this Section 13.7.4.5.3a shall be undertaken.

| **Message Code** | **Use Case Name** | **Valid joinMethodAndRole** |
| --- | --- | --- |
| 0x000D | CS03A1 Method A Join (Meter) | methodAInitiator |
| 0x00AB | CS03B Method A Join (non Meter) | methodAResponder |
| 0x000E | CS03A2 Method B Join | methodB |
| 0x00AF | CS03C Method C Join | methodC |

Table 13.7.4.5.3a: Valid deviceMethod and joinMethodAndRole against Message Code

The Device receiving a Join Device Command shall verify joinMethodAndRole against its own DeviceMethod and the DeviceType specified in the otherDeviceType parameter of the Command according to the requirements of the remainder of this Section 13.7.4.5.3.

If joinMethodAndRole is methodB then the Device’s verification of joinMethodAndRole shall be successful if there is a cell identified by its own DeviceMethod,and the value of otherDeviceType (as identified in the Command) of a type defined in Table 13.7.4.5.3b, and that cell contains ‘success’. Otherwise, the verification shall fail and JoinResponseCode in the Response shall be set to the value invalidJoinMethodAndRole.

|  |  |  |  |
| --- | --- | --- | --- |
|  | otherDeviceType | | |
|  | **communicationsHub**  **GasProxyFunction** | **type1PrepaymentInterfaceDevice** | **type2** |
| DeviceType of Device to which the Command is addressed |  |  |  |
| gSME | Success | - | - |
| eSME | - | - | Success |
| communicationsHubGasProxyFunction | - | Success | Success |

Table 13.7.4.5.3b: joinMethodAndRole is methodB

If joinMethodAndRole is methodAInitiator then the Device’s verification of joinMethodAndRole shall be successful if there is a cell identified by its own DeviceType, and the value of otherDeviceType (as identified in the Command) of a type defined in Table 13.7.4.5.3c, and that cell contains ‘success’. Otherwise, the verification shall fail and JoinResponseCode in the Response shall be set to the value invalidJoinMethodAndRole.

|  |  |  |
| --- | --- | --- |
|  | otherDeviceType | |
|  | **type1HANConnected**  **AuxiliaryLoadControlSwitch** | **type1Prepayment**  **InterfaceDevice** |
| DeviceType of Device to which the Command is addressed |  |  |
| eSME | Success | Success |

Table 13.7.4.5.3c: joinMethodAndRole is methodB

If joinMethodAndRole is methodAResponder then the Device’s verification of joinMethodAndRole shall be successful if there is a cell identified by its own DeviceType,and the value of otherDeviceType (as identified in the Command) of a type defined in Table 13.7.4.5.3d, and that cell contains ‘success’. Otherwise, the verification shall fail and JoinResponseCode in the Response shall be set to the value invalidJoinMethodAndRole.

|  |  |
| --- | --- |
|  | otherDeviceType |
|  | **eSME** |
| DeviceType of Device to which the Command is addressed |  |
| type1HANConnectedAuxiliaryLoadControlSwitch | Success |
| type1PrepaymentInterfaceDevice | Success |

Table 13.7.4.5.3d: joinMethodAndRole is methodAResponder

If joinMethodAndRole is methodC then the Device’s verification of joinMethodAndRole shall be successful if there is a cell identified by its own DeviceType and the value of otherDeviceType (as identified in the Command) in Table 13.7.4.5.3e and that cell contains ‘success’. Otherwise, the verification shall fail and JoinResponseCode in the Response shall be set to the value invalidJoinMethodAndRole.

|  |  |  |
| --- | --- | --- |
|  | otherDeviceType | |
|  | **type1PrepaymentInterfaceDevice** | **gSME** |
| DeviceType of Device to which the Command is addressed |  |  |
| gSME | Success | - |
| type1PrepaymentInterfaceDevice | - | Success |

Table 13.7.4.5.3e: joinMethodAndRole is methodB

##### 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. 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.

##### Undertaking Key Establishment with the other Device

The Device shall initiate, and attempt to complete, Key Establishment according to the ZSE requirements. The initiating Device shall wait a minimum of two seconds before timing out any key establishment operation.

Should there be errors that result in that process not completing, the Device shall set joinResponseCode to the value specified by Table 13.7.4.5.5.

| **GBZ Response Code[[34]](#footnote-34)** | **Value of** joinResponseCode |
| --- | --- |
| NO\_RESOURCES | keyAgreementNoResources |
| UNKNOWN\_ISSUER | keyAgreementUnknownIssuer |
| UNSUPPORTED\_SUITE | keyAgreementUnsupportedSuite |
| BAD\_MESSAGE | keyAgreementBadMessage |
| BAD KEY\_CONFIRM | keyAgreementBadKeyConfirm |

Table 13.7.4.5.5: joinResponseCode mapping to GBZ Responses

#### Component Requirements – Unjoin

##### Unjoin Command and Response payloads – structure definition

Each instance of @UnjoinDevice.CommandPayload and of @UnjoinDevice.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.7.4.6.1 which specifies the structure in ASN.1 notation.

UnjoinDevice DEFINITIONS ::= BEGIN

CommandPayload ::= OtherDeviceEntityIdentifier

-- specify the Entity Identifier of the Device for which authorisation

-- is to be removed

OtherDeviceEntityIdentifier ::= OCTET STRING

ResponsePayload ::= UnjoinResponseCode

-- detail whether the Command successful executed or, if it didn’t,

-- what the failure reason was

UnjoinResponseCode::= INTEGER

{

success (0),

otherDeviceNotInDeviceLog (1),

otherFailure (2)

}

END

##### Constructing the @UnjoinDevice.CommandPayload and of @UnjoinDevice.ResponsePayload

@UnjoinDevice.CommandPayload shall have the structure defined in Section 13.7.4.6.1, and the Remote Party constructing the Command shall populate with values according to Table 13.7.4.6.2a.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @UnjoinDevice.CommandPayload |  |  |  |  |
| OtherDeviceEntityIdentifier | OCTET STRING | Entity Identifier | Mandatory | The Entity Identifier of the Device which is to be removed from this Device’s Device Log |

Table 13.7.4.6.2a: @UnjoinDevice.CommandPayload population

@UnjoinDevice.ResponsePayload shall have the structure defined in Section 13.7.4.6.1, and the Remote Party constructing the Command shall populate with values according to Table 13.7.4.6.2b.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @UnjoinDevice.ResponsePayload |  |  |  |  |
| unjoinResponseCode | INTEGER | success (0), (0),  otherDeviceNotInDeviceLog (1), (1),  otherFailure (2) (2) | Mandatory | Shall be populated according to the processing defined in Section 13.7.4.3 |

Table 13.7.4.6.2b: @UnjoinDevice.ResponsePayload population

### 

#### CS07 Read Device Join Details Command and Response payloads – structure definition

Each instance of @ReadDeviceLog.CommandPayload and of @ReadDeviceLog.ResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.7.4.7 which specifies the structure in ASN.1 notation.

ReadDeviceLog DEFINITIONS ::= BEGIN

CommandPayload ::= NULL

ResponsePayload ::= SEQUENCE

{

-- detail whether the Command successful

readLogResponseCode ReadLogResponseCode,

-- if it was, return the Log Entries

deviceLogEntries SEQUENCE OF DeviceLogEntry OPTIONAL

}

DeviceLogEntry ::= SEQUENCE

{

deviceIndentifier OCTET STRING,

deviceType DeviceType

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

ReadLogResponseCode::= INTEGER

{

success (0),

readFailure (1)

}

END

## GCS59 / 62 GPF Device Log Backup and Restore

### Introduction to GPF Device Log Backup and Restore - informative

#### The role of pair-wise authorisation - informative

This Section 13.8 includes the Use Cases related to the backing up and restoring of the GPF's Device Log. This is to cater for situation where the existing Communications Hub fails and has to be replaced.

In summary:

* a GPF sends an Alert whenever its Device Log changes. That Alert contains the contents of the GPF's Device Log after the change has been made; and
* the Restore GPF Device Log Command shall contain the same structure of Device Log contents. If successful, the Command will place those contents in to the GPF's Device Log and will have triggered the processing required to authorise the specified Devices application layer interaction with the GPF, where required.

#### The format of Message Payloads - informative

In common with other GBCS Remote Messages related to the management of Security Credentials, the Payloads of Alerts, Commands and Responses defined in this Section 13.8 are specified using ASN.1, with DER encoding to be applied to Command and Response payloads.

Each entry in a GPF Device Log shall contain the Entity Identifier of the Authorised Device and its deviceType.

### GCS62 GPF Backup Device Log Alert

#### Description

This Section 13.8.2 covers the creation, validation and processing of Alerts resulting from changes to the GPF Device Log. One such Alert shall be generated each time that the GPF Device Log changes, regardless of the trigger for that change.

#### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Alert |
| Message Type Category | SME.A.NC |
| Capable of future dated invocation? | N/A |
| Protection Against Replay Required? | N/A |
| SEC User Gateway Services Schedule (Service Request) Reference | 8.12 |
| CHTS Command | N/A |
| CHTS Data Item | GPF Device Log |
| Valid Initiating Device(s) | GPF |
| Valid Business Target role(s) for Alert | Access Control Broker |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 13.8.2.2: Use Case Cross References for GPF Device Log Backup Alert

#### Construction of Alerts

GPF Device Log Backup Alert Payloads shall be constructed according to the requirements of Section 13.8.4.1 and populated as specified in Table 13.8.2.3.

MAC Header, Grouping Header and SMD-KRP MAC shall be populated as required for an Alert of the SME.A.NC Message Category, with the Message Code being specific to this Alert Use Case. Note that the Business Target ID in the Grouping Header shall always contain the Entity Identifier of the Access Control Broker.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @GPFDeviceLog.BackupAlertPayload | SEQUENCE |  |  |  |
| alertCode | INTEGER | 0x0071 | Mandatory | Fixed value specifying that this is a GPF Device Log Backup Alert |
| backupDateTime | GeneralizedTime | The date-time at which this Alert was created | Mandatory | This is based on the Device’s own clock |
| deviceLogEntries | SEQUENCE OF |  | OPTIONAL | There may be 0, 1 or many entries in the Log. The following two fields will be repeated as many times as there are Device Log Entries |
| deviceEntityIdentifier | OCTET STRING | Entity Identifier | Mandatory | The Entity Identifier of the Device to which this entry relates. |
| deviceType | INTEGER | type1PrepaymentInterfaceDevice (5),  type2 (6) | Mandatory | The DeviceType of the Device to which this entry relates. These are the only valid entries for the GPF Device Log. |

Table 13.8.2.3: @GPFDeviceLog.BackupAlertPayload population

#### Processing of Alerts

SMD-KRP MAC may be verified by the Access Control Broker as per Section 6.8.3.

### GCS59 GPF Device Log Restore

#### Description

This section covers the creation, validation and processing of Commands to restore the GPF Device Log, and the creation and validation of the corresponding Response.

#### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.NC |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | Yes |
| SEC User Gateway Services Schedule (Service Request) Reference | 8.12 |
| CHTS Command | Restore GPF Device Log |
| CHTS Data Item | GPF Device Log |
| Valid Target Device(s) | GPF |
| Valid Business Originator role(s) for Command | Access Control Broker |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | ASN.1 |

Table 13.8.3.2: Use Case Cross References for GPF Device Log Restore

#### Construction of Command

GPF Device Log Restore Command Payloads shall be constructed according to the requirements of Section 13.8.4.1 and populated as specified in Table 13.8.3.3.

MAC Header, Grouping Header, KRP Signature and ACB-SMD MAC shall be populated as required for a Command of the SME.C.C Message Category.

| **Attribute name** | **Data Type** | **Value (blank cells mean the command specific value is derived by the encoding process)** | **Mandatory, OPTIONAL or DEFAULT value** | **Notes** |
| --- | --- | --- | --- | --- |
| @GPFDeviceLog.RestoreCommandPayload | SEQUENCE |  |  |  |
| deviceLogEntries | SEQUENCE OF |  | OPTIONAL | There may be 0, 1 or many entries in the Log. The following two fields will be repeated as many times as there are Device Log Entries. Note that there would be no effect if the Command had no deviceLogEntries. |
| deviceEntityIdentifier | OCTET STRING | Entity Identifier | Mandatory as part of each entry that is present | The Entity Identifier of the Device to which this entry relates. |
| deviceType | INTEGER | type1PrepaymentInterfaceDevice (5),  type2 (6) | Mandatory as part of each entry that is present | The DeviceType of the Device to which this entry relates. These are the only valid entries for the GPF Device Log. Note that the GSME does not need to be in the GPF’s Device Log, since the GPF only receives information from the GSME. |

Table 13.8.3.3: @GPFDeviceLog.RestoreCommandPayload population

#### Device processing of Command and Response handling

The GPF receiving a GPF Device Log Restore Command shall undertake processing steps in the sequence defined in this Section 13.8.3.4. The Device shall undertake Command Authenticity and Integrity Verification as required for a Command of this Message Category, and then, if successful, for each DeviceLogEntry in deviceLogEntries, shall:

1. set deviceLogEntry in the corresponding ResponseOutcome to the values of this DeviceLogEntry in deviceLogEntries;
2. set joinResponseCode in the corresponding ResponseOutcome to success;
3. if the deviceEntityIdentifier matches an Entity Identifier currently recorded in its Device Log, compare deviceType in that log entry with otherDeviceType. If the Device types match then the addition is successful and processing of this DeviceLogEntry shall cease; otherwise the Device shall set joinResponseCode to incompatibleWithExistingEntry and processing of this DeviceLogEntry shall cease;
4. check if there is capacity for an additional entry in its Device Log. If there is not, the Device shall set joinResponseCode to deviceLogFull and processing of this DeviceLogEntry shall cease; and
5. attempt to create a new Device Log entry using deviceEntityIdentifier and deviceType. If that entry is not successfully created, the Device shall set joinResponseCode to writeFailure and processing of this DeviceLogEntry shall cease.

Once all DeviceLogEntry in deviceLogEntries have been processed, the GPF shall populate the Response Payload according to the requirements of Section 13.8.4.1 using the ResponseOutcomes produced by the processing in this Section 13.8.3.4, construct MAC Header, Grouping Header and apply the Response Cryptographic Protection required for a Response of the SME.C.NC Message Category, and send the Response.

### Common Requirements

#### GPF Device Log Backup Alert, Restore Command and Restore Response Payloads – structure definition

Each instance of @GPFDeviceLog.BackupAlertPayload, @GPFDeviceLog.RestoreCommandPayload and of @GPFDeviceLog.RestoreResponsePayload shall be an octet string containing the DER encoding of the populated structure defined in this Section 13.8.4.1 which specifies the structure in ASN.1 notation.

GPFDeviceLog DEFINITIONS ::= BEGIN

BackupAlertPayload ::= SEQUENCE

{

-- specify the Alert Code

alertCode INTEGER(0..4294967295),

-- specify the date-time of the backup

backupDateTime GeneralizedTime,

-- detail the entries in the Device Log now that the change has been made

deviceLogEntries SEQUENCE OF DeviceLogEntry

}

RestoreCommandPayload ::= SEQUENCE

{

-- list the Device Log entries that are to be added

deviceLogEntries SEQUENCE OF DeviceLogEntry

}

DeviceLogEntry ::= SEQUENCE

{

-- specify the Entity Identifier of the Device

deviceEntityIdentifier OCTET STRING,

-- specify the DeviceType of that Device

deviceType DeviceType

}

RestoreResponsePayload ::= SEQUENCE

{

-- for each DeviceLog Entry, detail whether the Command successfully executed or, if it didn’t, what the failure reason was

restoreOutcomes SEQUENCE OF RestoreOutcome

}

RestoreOutcome ::= SEQUENCE

{

deviceLogEntry DeviceLogEntry,

joinResponseCode JoinResponseCode

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

JoinResponseCode::= INTEGER

{

success (0),

invalidMessageCodeForJoinMethodAndRole (1),

invalidJoinMethodAndRole (2),

incompatibleWithExistingEntry (3),

deviceLogFull (4),

writeFailure (5),

keyAgreementNoResources (6),

keyAgreementUnknownIssuer (7),

keyAgreementUnsupportedSuite (8),

keyAgreementBadMessage (9),

keyAgreementBadKeyConfirm (10),

invalidOrMissingCertificate (11)

}

END

# Apply Prepayment Top Up to an ESME or GSME

## Defined Terms

The following terms used in this Section 14 shall have the meanings defined in this Table 14.1.

|  |  |
| --- | --- |
| **Defined Term** | **Meaning** |
| Currency Unit | Shall be either GB Pound or European Central Bank Euro |
| Maximum Vend | Shall be the maximum value of any single Pre-payment Top Up entered locally. Its value shall be interpreted by the Device in Currency Units (whole currency units only) |
| Maximum Prepayment Credit | Shall be the maximum total credit value recorded on the ESME / GSME. Its value shall be interpreted by the Device in Currency Units (whole currency units only) |
| Highest UTRN Counter | The highest numerical value of any UTRN Counter in the UTRN Counter Cache |
| Prepayment Token Decimal (PPTD) | Shall have the meaning specified in Section 14.3.1 |
| Prepayment Top Up Token (PTUT) | Shall have the meaning specified in Section 14.3.2 |
| Unique Transaction Reference Number (UTRN) | Shall have the meaning specified in Section 14.3.3 |
| UTRN Check Digit | Shall be the 20th digit of the UTRN |
| UTRN Counter Cache | Shall be an array of 100 entries, each entry containing an unsigned integer of 32 bits in length and an associated flag to indicate whether the UTRN Counter represented by the integer relates to a locally entered Prepayment Top Up, a network delivered Prepayment Top Up or has been set as a floor value on execution of an Update Security Credentials Command.  The array shall be arranged as a circular buffer such that, when full, further writes shall cause the lowest numerical value entry to be overwritten |
| UTRN Counter | The 32 most significant bits of the Originator Counter |

Table 14.1: Meanings of Defined Terms

## Description - informative

This section covers the application of a Prepayment Top Up, that has been purchased for a particular ESME or GSME, to that ESME or GSME.

It covers four options:

* applying a Prepayment Top Up to an ESME without consumer intervention;
* applying a Prepayment Top Up to a GSME without consumer intervention;
* applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on the ESME or GSME; and
* applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on a PPMID.

Some requirements are common to all four options. Accordingly, this Section 14 is split in to five sub sections:

* an initial sub-section covering requirements common to all four options; and
* four subsequent sub sections covering one option in each sub-section.

By way of context:

* any Prepayment Top Up Message is a Remote Party Command in GBCS terms (because it is from a Remote Party to a GSME or ESME). The means of delivery (typing in on meter, typing in on PPMID, sending over WAN, etc.) does not affect this classification;
* as a Remote Party Command, it must result in the GSME or ESME generating a Response back to the Remote Party who issued it (so the Supplier), unless there is an Authentication failure (in which case the Supplier has to be sent an Alert), as per SMETS and CHTS;
* because the ranges are exclusive, the Originator Counter in Prepayment Top Up transactions cannot collide with the Originator Counter in any other transaction; and
* there is no requirement to include the Device’s ID explicitly in the locally entered transaction, so a PPMID joined to more than one Smart Meter will need to allow the Consumer to pick which Smart Meter the Prepayment Top Up is for.

## Common Requirements

### Construction of the PPTD

The PPTD shall be a 19 decimal digit integer. The most significant two digits of the PPTD shall always be between 73 and 96, which shall be constructed and represented according to the requirements of this Section 14.3.1.

The decimal representation of the PPTD shall be the result of the addition of 7,394,156,990,786,306,048 to the decimal representation of the PTUT.

### Construction of the PTUT

The PTUT shall be an unsigned 64 bit integer (so 8 octets), which shall be constructed and represented according to the requirements of this Section 14.3.2.

The bits within the PTUT shall be numbered from 63 for the most significant bit through to 0 for the least significant bit.

The bits of the PTUT shall be set to the values in Table 14.3.2.

| **PTUT component** | **Value** | **Bits** | **Note** |
| --- | --- | --- | --- |
| PTUT Lead | 0b000 | 63-61 | Fixed Value |
| PTUT Sub Class | 0b0000 | 60-57 | Fixed value |
| PTUT Value Class | 0b00 if PTUT Value is to be interpreted as multiples of 1/100 of Currency Unit;  OR  0b01 if PTUT Value is to be interpreted as multiples of Currency Unit. | 56-55 | If Currency Unit is set to GB Pounds on the ESME or GSME, 0b00 means PTUT Value will be interpreted as GB Pennies; and 0b01 means PTUT Value will be interpreted as GB Pounds. |
| PTUT Value | The quantum of the PTUT expressed as an unsigned binary number of 13 bits in length, so with leading binary zeros where required. | 54-42 | Thus, the maximum value is either:  £81.91 if PTUT Value Class =0b00; or  £8,191.00 if PTUT Value Class =0b01. |
| PTUT Truncated Originator Counter | Bits 41-32 of the Originator Counter | 41-32 | Used for Protection Against Replay purposes when the transaction is entered locally. |
| PTUT Supplier MAC | See Section14.3.4 | 31-0 |  |

Table 14.3.2: Values of PTUT bits

### Construction of the Unique Transaction Reference Number (UTRN)

The Unique Transaction Reference Number (UTRN) shall be a 20 decimal digit which shall be the 19 decimal digits of the PPTD with a 20th decimal digit which shall be appended after the least significant digit of the 19 decimal digit representation of PPTD. This 20th decimal digit shall be the UTRN Check Digit. The UTRN Check Digit shall be calculated according to the requirements of Section 14.8.

### Construction of the PTUT Supplier MAC

The PTUT Supplier MAC shall only be calculated once the 32 most significant bits of PTUT (bits 63-32 of the PTUT) have been populated as per the requirements of Section 14.3.2.

The Remote Party, whose Security Credentials are stored against the Supplier role of the target Device, shall calculate a MAC using the parameters in Table 14.3.4 then setting the PTUT Supplier MAC to be the 32 least significant bits of the 128 bit MAC produced by the MAC calculation.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Supplier’s Prepayment Top Up Key Agreement Key [which the Supplier may elect to be different than the Key Agreement Key they use for other interactions with the Device] |  |
| Public Key Agreement Key | Device’s |  |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Message Identifier || 32 most significant bits of the PTUT |  |

Table 14.3.4: Calculation of the PTUT Supplier MAC

### Validating the PTUT Supplier MAC

To validate the PTUT Supplier MAC, the Device shall calculate the MAC using the parameters in Table 14.3.5, then ensure the 32 least significant bits of the 128 bit MAC produced by the MAC calculation has the same value as the PTUT Supplier MAC.

| **Input Parameter** | **Value** | **Note** |
| --- | --- | --- |
| To calculate the Shared Secret (‘*Z*’) input to the KDF: | | |
| Private Key Agreement Key | Device’s |  |
| Public Key Agreement Key | Supplier’s Prepayment Top Up Key Agreement Key |  |
| The other input to the KDF (‘*OtherInfo*’) shall be calculated according to the requirements of Section 4.3.3.3. | | |
|  | | |
| As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and: | | |
| Additional Authenticated Data shall be the concatenation: | 0x11 || Message Identifier || 32 most significant bits of the PTUT |  |

Table 14.3.5: Validation of the PTUT Supplier MAC

### Checking the UTRN Counter against the UTRN Counter Cache

The Device shall set the UTRN Counter to be the 32 most significant bits of the Originator Counter.

The Device shall check that the UTRN Counter is strictly numerically greater than the numerically lowest value in the UTRN Counter Cache, and is not equal to any value in the UTRN Originator Counter Cache.

### 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 and whose flag shall be set to record this Prepayment Top Up either as a network delivered Prepayment Top Up or as a locally entered Prepayment Top Up, as appropriate.

### Validating the Maximum Credit Values

#### Maximum Vend

The Device shall ensure that the top-up value specified by PTUT Value Class and PTUT Value does not exceed the Device’s Maximum Vend parameter.

#### Maximum Prepayment Credit

The Device shall ensure that the top-up value specified by PTUT Value Class and PTUT Value when added to the Device’s Credit Balance does not exceed the Device’s Maximum Prepayment Credit parameter.

### Validating the PTUT Sub-Class

The Device shall ensure that the value specified by PTUT Sub-Class is of value 0b0000.

## Applying a Prepayment Top Up to an ESME without consumer intervention

This Use Case CS01a covers the application of a Prepayment Top Up that has been bought for an ESME to that ESME, in the case where the consumer does not enter any details on Devices in their premises, except for the additional processing defined in this section.

### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |

|  |  |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | SME.C.NC but with additional cryptographic processing specified in Sections 14.3.4 and 14.3.5 |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | The Protection Against Replay mechanisms for Prepayment Top Ups are specified in Section 14.3.6. The Protection Against Replay mechanisms specified elsewhere in the GBCS do not apply |
| SEC User Gateway Services Schedule (Service Request) Reference | 2.2 |
| SMETS Command | Add Credit |
| SMETS Data Item | Meter Balance |
| Valid Target Device(s) | ESME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the ESME) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | DLMS COSEM |

Table 14.4.1: Use Case Cross References for Prepayment Top Up to an ESME without consumer intervention

### Pre-conditions

None.

### Detailed Steps

The Device shall undertake the checks set out in this Section 14.4.3 in the sequence laid out:

* only once all checks in Section 6.2.4.1.1 have been successfully completed; and
* before undertaking any other processing of the Command.

If any of the checks specified in this Section 14.4.3 fail, the Device shall not carry out further checks, and the requirements of Section 6.2.4.2 shall apply. Otherwise, processing shall continue as per the requirements of Section 6.2.4.1.2. Where that check is successful, processing shall continue as below.

#### Verifying against the maximum credit values

The Device shall carry out the checks specified in Section 14.3.8.1 and Section 14.3.8.2.

#### Verifying the Originator Counter

The Device shall verify the Originator Counter against the UTRN Counter Cache according to Section 14.3.6.

#### Validating the PTUT Supplier MAC

The Device shall validate the PTUT Supplier MAC according to Section 14.3.5.

### Response Construction

At the Response Construction stage, the Device shall first update the UTRN Counter Cache according to Section 14.3.7, and shall then populate the Response according to the requirements of Use Case CS01a.

## Applying a Prepayment Top Up to a GSME without consumer intervention

### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |

|  |  |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | See Table 14.4.1 |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | See Table 14.4.1 |
| SEC User Gateway Services Schedule (Service Request) Reference | N/A |
| SMETS Command | Add Credit |
| SMETS Data Item | Meter Balance |
| Valid Target Device(s) | GSME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the ESME) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | GBZ |

Table 14.5.1: Use Case Cross References for Prepayment Top Up to a GSME without consumer intervention

### Pre-conditions

None.

### Detailed Steps

The Device shall undertake the checks set out in this Section 14.5.3 in the sequence laid out:

* only once all checks in Section 6.2.4.1.1 have been successfully completed; and
* before undertaking any other processing of the Command.

#### Verifying against the maximum credit values

The Device shall carry out the checks specified in Section 14.3.8.1 and Section 14.3.8.2.

#### Verifying the Originator Counter

The Device shall verify the Originator Counter against the UTRN Counter Cache according to Section 14.3.6.

#### Validating the PTUT Supplier MAC

The Device shall validate the PTUT Supplier MAC according to Section 14.3.5.

If any of the checks specified in this Section 14.5.3 fail, the requirements of Section 6.2.4.2 shall apply. Otherwise, processing shall continue as per the requirements of Section 6.2.4.1.2.

### Response Construction

At the Response Construction stage, the Device shall first update the UTRN Counter Cache according to Section 14.3.7 and shall then populate the Response according to the requirements of Use Case CS01b.

## Applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on the ESME or GSME

This Use Case covers the application of a Prepayment Top Up that has been bought for a GSME or ESME to that GSME or ESME in the case where the consumer enters the corresponding UTRN on the GSME or ESME.

### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Response |
| Message Type Category | This is a Variant Message type. The Command shall be the UTRN constructed in accordance with Section 14.3.3. The Command includes cryptographic protections as specified in Sections 14.3.4 and 14.3.5. The Response shall be of Message Type Category SME.C.NC. An Alert as specified in SMETS for locally entered commands is not required |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | See Table 14.4.1 |
| SEC User Gateway Services Schedule (Service Request) Reference | N/A |
| SMETS Command | Add Credit |
| SMETS Data Item | Meter Balance |
| Valid Target Device(s) | ESME or GSME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [HAN Only Messages] | N/A |
| Protocol | Outside of protocols since entered via User Interface |

Table 14.6.1: Use Case Cross References for Prepayment Top Up through consumer UTRN entry

### Pre-conditions

None.

### Detailed Steps

#### Detailed Steps/Sequence

The Device shall undertake the validation checks set out in this Section 14.6.3.1 before undertaking any other processing of the Command. The validation checks shall be undertaken in the sequence laid out. Should a validation check fail, subsequent validation checks shall not be undertaken by the Device.

Should any of the checks fail (save for the optional UTRN Check Digit verification), the requirements of Section 6.2.4.2 shall apply.

##### Verifying the UTRN Check Digit

The Device:

* may validate the 20th digit (the UTRN Check Digit) as specified at Section 14.8 (Calculating and Verifying the UTRN Check Digit); and
* shall disregard the 20th decimal digit to determine PPTD prior to undertaking any subsequent checks.

##### Using the PPTD to calculate the PTUT

PTUT shall take the value of PPTD minus 7,394,156,990,786,306,048.

The Device shall interpret the resulting unsigned integer according to Table 14.6.3.1.2.

| **PTUT component** | **Bits** |
| --- | --- |
| PTUT Sub Class | 60-57 |
| PTUT Value Class | 56-55 |
| PTUT Value | 54-42 |
| PTUT Truncated Originator Counter | 41-32 |
| PTUT Supplier MAC | 31-0 |

Table 14.6.3.1.2: Interpretation of the PTUT

##### Verifying PTUT subclass category

The Device shall carry out the checks specified in Section 14.3.9.

##### Verifying against the maximum credit values

The Device shall carry out the checks specified in Section 14.3.8.1 and Section 14.3.8.2.

##### Deriving the Originator Counter[[35]](#footnote-35)

The Originator Counter shall be derived by:

1. creating four 32 bit signed integer variables p, q, r and s;
2. setting p = the numeric value of the 10 least significant bits of Highest UTRN Counter;
3. setting q = (the numeric value Highest UTRN Counter) – p;
4. setting r = the numeric value of PTUT Truncated Originator Counter;
5. if r < (p – 29) then setting s = (r + 210) else if r > (p + 29) then setting s = (r – 210) else setting s = r;
6. setting Originator Counter equal to ((q+s)\*232)

##### Verifying the Originator Counter

The Device shall verify the Originator Counter against the UTRN Counter Cache according to Section 14.3.6.

##### Deriving the Message Identifier

The Device shall derive the Message Identifier by:

* setting the Business Originator ID to the Entity Identifier in the Key Agreement Security Credentials it holds for the Trust Anchor Cell with Remote Party Role as supplier and cell usage of prePaymentTopUp;
* setting the Business Target ID to its own Entity Identifier; and
* setting Message Identifier to the concatenation Business Originator ID || Business Target ID || Originator Counter.

##### Validating the PTUT Supplier MAC

The Device shall validate the PTUT Supplier MAC according to Section 14.3.5.

### Response Construction

The Device shall first update the UTRN Counter Cache according to Section 14.3.7.

Where the Device is an ESME, the Device shall construct, and send via its HAN interface, a Response message complying with the requirements of Use Case CS01a, using a Message Identifier as specified in Section 14.6.3.1.7, and where the Originator Counter is as derived by the calculations in Section 14.6.3.1.5.

Where the Device is a GSME, the Device shall construct, and send via its HAN interface, a Response message complying with the requirements of Use Case CS01b, using Message Identifier as specified in Section 4.3.1.3, Message Identifierand where the Originator Counter is as derived by the calculations in Section 14.6.3.1.5.

## Applying a Prepayment Top Up to an ESME or GSME with consumer entry of a numeric code on a PPMID

This Use Case covers the application of a Prepayment Top Up that has been bought for a specific GSME or ESME to that GSME or ESME in the case where the consumer enters the corresponding UTRN on a PPMID on the same SMHAN.

### Use Case Cross References

| **Cross Reference** | **Value** |
| --- | --- |
| Grouping | Remote Party Message |
| Message Type | Command and Responses |
| Message Type Category | The Command and Response requirements are specifically as detailed in this Section 14.7 |
| Capable of future dated invocation? | No |
| Protection Against Replay Required? | See Table 14.4.1 |
| SEC User Gateway Services Schedule (Service Request) Reference | N/A |
| SMETS Command | Add Credit |
| SMETS Data Item | Meter Balance |
| Valid Target Device(s) | ESME or GSME |
| Valid Business Originator role(s) for Command invocation (and so, for DLMS COSEM Commands, which Application Association is to be used for delivery of the Command to the Device) [Remote Party Messages Only] | Supplier |
| Valid Response Recipient role(s) (only for Messages Authorised by the Access Control Broker on behalf of parties not known to the Device) [Remote Party Messages Only] | N/A |
| Valid initiating Device type(s) [SMHAN Only Messages] | N/A |
| Protocol | See this Section 14.7 |

Table 14.7.1: Use Case Cross References for Prepayment Top Up through PPMID entry

### Pre-conditions

None.

### Detailed Steps

#### Detailed Steps / Sequence

##### Verifying the UTRN check digit

The PPMID may validate the 20th digit (the UTRN Check Digit) as specified at Section 14.8 (Calculating and Verifying the UTRN Check Digit). Where this check fails, the PPMID shall cease processing the Command and shall inform the consumer of the failure of the check digit.

##### Command Construction by the PPMID

Where the target Device is a GSME, the PPMID shall construct the Command according to the requirements of Use Case PCS01.

Where the target Device is an ESME, the PPMID shall construct a GBZ Consumer Top Up command.

In all cases:

* the value of the TopUp Code, with its GBZ meaning, shall be set to be a VisibleString whose value is the 20 digit UTRN; and
* the value of the Originating Device, with its GBZ meaning, shall be 0x02 (IHD).

##### HAN 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 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 GBZ cryptographic processes to establish whether the Command was authentically issued by the 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.

If the Command was authentically issued by the PPMID within the Device Log, the ESME / GSME shall apply the requirements of Section 6.2.4.2.

If the Command was authentically issued by the PPMID within the Device Log, the ESME / GSME shall comply with the requirements of Section 14.6.3 (but excluding requirements in Sections 14.6.3.1.1, save that the ESME / GSME shall disregard the 20th digit before undertaking any further steps), and so process the contents of the Command accordingly.

##### HAN Only Response Construction and Issue

Where the ESME / GSME successfully creates a Remote Party Response to its Supplier, as per the requirements in Section 14.6.4, the ESME / GSME shall also:

* where the Device is a GSME, construct the HAN Only Response according to the requirements of Use Case PCS01 and send it to the PPMID; or
* where the Device is an ESME, construct a GBZ Consumer Top Up command, and send it to the PPMID.

In all cases the value of the Source of Top up, with its GBZ meaning, shall be 0x02 (IHD).

## Calculating and Verifying the UTRN Check Digit

The UTRN Check Digit shall be calculated from the 19 decimal digit representation of the PTUT by a process equivalent to the following (Verhoeff’s) Algorithm[[36]](#footnote-36):

* setting an interim digit (referred to as IntDig) to have a value of zero;
* setting an index (referred to as K) to have a value of four;
* repeating the following steps with another index (referred to as J) taking the nineteen values of the integers from 1 to 19 in succession;
  + - * setting CurDig to the value of the Jth digit of the 19 decimal digits of the PTUT, where the first digit is the most significant (leftmost as written) and the nineteenth digit the least significant;
      * setting a third index (referred to as L) to the value in Table 14.8a using K as the Row Index and CurDig as the Column Index;
      * if the value of K is less than 7, setting K to the value of K+1, otherwise setting K to zero;

1. setting IntDig to the value in Table 14.8b using IntDig as the Row Index and L as the Column Index;

* setting IntDig to the value in row 1 of Table 14.8c using the value of IntDig as the Column Index; and
* setting the UTRN Check Digit to the value of IntDig.

The UTRN Check Digit may be verified by undertaking exactly the same calculation on the 19 most significant digits of the UTRN, and comparing the result (the final value of *IntDig*, which would be used to set the UTRN Check Digit) to the 20th decimal digit which is the UTRN Check Digit.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Column Index | | | | | | | | | |
|  |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Row | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Index | 1 | 1 | 5 | 7 | 6 | 2 | 8 | 3 | 0 | 9 | 4 |
|  | 2 | 5 | 8 | 0 | 3 | 7 | 9 | 6 | 1 | 4 | 2 |
|  | 3 | 8 | 9 | 1 | 6 | 0 | 4 | 3 | 5 | 2 | 7 |
|  | 4 | 9 | 4 | 5 | 3 | 1 | 2 | 6 | 8 | 7 | 0 |
|  | 5 | 4 | 2 | 8 | 6 | 5 | 7 | 3 | 9 | 0 | 1 |
|  | 6 | 2 | 7 | 9 | 3 | 8 | 0 | 6 | 4 | 1 | 5 |
|  | 7 | 7 | 0 | 4 | 6 | 9 | 1 | 3 | 2 | 5 | 8 |

Table 14.8a: Setting a third index

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Column Index | | | | | | | | | |
|  |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Row | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Index | 1 | 1 | 2 | 3 | 4 | 0 | 6 | 7 | 8 | 9 | 5 |
|  | 2 | 2 | 3 | 4 | 0 | 1 | 7 | 8 | 9 | 5 | 6 |
|  | 3 | 3 | 4 | 0 | 1 | 2 | 8 | 9 | 5 | 6 | 7 |
|  | 4 | 4 | 0 | 1 | 2 | 3 | 9 | 5 | 6 | 7 | 8 |
|  | 5 | 5 | 9 | 8 | 7 | 6 | 0 | 4 | 3 | 2 | 1 |
|  | 6 | 6 | 5 | 9 | 8 | 7 | 1 | 0 | 4 | 3 | 2 |
|  | 7 | 7 | 6 | 5 | 9 | 8 | 2 | 1 | 0 | 4 | 3 |
|  | 8 | 8 | 7 | 6 | 5 | 9 | 3 | 2 | 1 | 0 | 4 |
|  | 9 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Table 14.8b: Setting IntDig using IntDig as a Row Index

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Column Index | | | | | | | | | |
| Row |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Index | 1 | 1 | 2 | 6 | 7 | 5 | 8 | 3 | 0 | 9 | 4 |

Table 14.8c: Setting IntDig using IntDig as a Column Index

# Message Codes

Message Codes shall be 2 octets in length and shall take the values specified in the ‘Use Case reference’ tab in the Mapping Table.

For Messages specified by this GBCS, the most significant bit of the Message Code shall be 0b0.

# Event / Alert Codes and related requirements

## Introduction – informative

This Section 16 sets out how Events and Alerts are handled. SMETS and CHTS define when Events occur and whether these Events are logged (in an Event Log) and additionally sent as an Alert via the HAN / WAN.

Table 16.2 defines Event Codes for events defined in SMETS and CHTS. It also indicates whether, as per SMETS and CHTS, there is a corresponding Alert issued over the Device’s network interface (containing the relevant Event Code). It is important to note that not all Event Codes have a corresponding Alert. Where Alert Code is used elsewhere in this document, it equates to Event Code in Table 16.2.

Alerts sent over the SMHAN are not subject to the same message categorisation as those sent over the WAN. An Alert sent over the SMHAN is a native ZSE message.

### Types of Alert

There are two Alert types. All have the same Grouping Header but different payloads as set out below:

* Alert type 1 - Payload comprises Alert Code and Timestamp only (two sub-types: DLMS and ZigBee); and
* Alert type 2 - Payload comprises Alert Code, Timestamp and Use Case specific data as defined in Table 16.2 or main body of document (three sub-types: ASN1, DLMS and ZigBee).

Table 16.2 sets out the Alert type for each Alert Code. Examples of Use Case specific data include Billing Data Logs and content relating to future dated Commands (e.g. Message ID)

Table 16.2 sets out whether Alerts are mandated, mandatory conditional or non-mandated:

* Mandated - Alerts that Devices must support;
* Mandated conditional – Devices must support at least one from the specified group (e.g. there are seven Alerts in ‘mandated – conditional group 1’, Devices must support at least one of these seven); and
* Non-mandatory – no requirement for Devices to support, but where implemented Alert Codes shall have the meaning shown in Table 16.2.

### Alert Construction

Alert construction is described in the GBCS in a number of places, including:

* Section 7.2.3 details common Message construction for all Alert types;
* Section 7.2.9 details Message construction for Alerts with DLMS COSEM Payloads. Table 7.2.9c details the required components of the Alert;
* Section 7.2.10 details Message construction for Alerts with ZSE Payloads. Table 7.2.10c details the required components of the Alert;
* Sections 11.2 and 13.3 detail the Message Construction for the Alerts with ASN1 Payload; and
* Section 9.2.2 details the Message Construction for future dated Alerts.

### Event Behaviour

Detail on Event behaviour can be found in SMETS and CHTS using the relevant SMETS and CHTS reference in Table 16.2.

## Event and Alert Codes

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



Table 16.2: Event and Alert Codes

## Event Logs

Only GSME, ESME, CHF and GPF have Event Logs. The requirement set out in Table 16.2 to log entries into Event Logs only applies to GSME, ESME, CHF and GPF as follows:

* Event Log (GSME, ESME, CHF and GPF);
* Security Event Log (GSME, ESME, CHF and GPF);
* Power Event Log (ESME); and
* ALCS Event Log (ESME).

Use Cases to read logs (all) and clear logs (event logs only) are detailed in the Mapping Table.

## Requirements

Event / Alert codes shall be 2 octets in length and shall take the values specified in Table 16.2. As per the Device Specifications, all Alerts, Event Log entries and Security Log entries shall contain a UTC date time stamp, in addition to the Event / Alert code. Non-Critical Alerts can be configured to be sent / not to be sent using the relevant Commands and Responses defined in Use Cases ECS25a, ECS25b and GCS20 (all configurable Alerts can be configured in a single Message). The relevant DCC User needs to ensure that Critical Alerts are always configured on.

As specified in Table 16.2 by way of ‘x’ in a cell, deviceType (and for ESME, variant of ESME) shall determine which Alerts a device shall issue and which Event Log and Security Log entries it shall record. Where deviceType = 0x04 (HCALCS) or 0x05 (PPMID), this Section 16 only requires the sending of Alerts, since neither Device type is required to have either an Event Log or a Security Log.

Where an Alert Instance and a Log entry have the same trigger in a Device, the Device shall record the same UTC date time stamp and the same Event / Alert code in both.

The Remote Party to which an Alert containing a specific Event Code is addressed shall be determined by the Remote Party Role as specified in Table 16.2. Where the Remote Party Role is stated as Supplier or WAN Provider, the Alert shall be addressed:

* to the WAN Provider if deviceType = 0x02 (CHF); and
* to the Supplier for all other deviceType values.

Where a Use Case is specified in Table 16.2 the corresponding Alert shall be constructed according to the specified Use Case. Where no Use Case is specified the Alert shall be constructed according to Section 7.

Where an Alert has two recipient roles identified, the Device shall place the Entity ID of the Supplier in the Business Target ID field and the Entity ID of the other recipient in the Supplementary Remote Party ID field.

For any Event Log entries relating to Event Codes 0x0061 and 0x0062, the Device shall record the commands input on the User Interface by including the User Interface Command Code in the Event Log entry as defined in Table 16.4.

| **User Interface Command Code** | **User Interface Command (from SMETS)** | **GSME** | **ESME** | **ESME with ALCS** | **ESME with Boost Function** |
| --- | --- | --- | --- | --- | --- |
| 0x0001 | Activate Boost Period |  |  |  | x |
| 0x0002 | Activate Emergency Credit [PIN] | x | x |  |  |
| 0x0003 | Activate ESME Emergency credit |  |  |  |  |
| 0x0004 | Activate GSME Emergency credit |  |  |  |  |
| 0x0005 | Add Credit | x | x |  |  |
| 0x0006 | Add Credit to ESME |  |  |  |  |
| 0x0007 | Add Credit to GSME |  |  |  |  |
| 0x0008 | Allow Access to User Interface | x | x |  |  |
| 0x0009 | Arm Supply | x | x |  |  |
| 0x000A | Cancel Boost Period |  |  |  | x |
| 0x000B | Check for HAN Interface Commands | x |  |  |  |
| 0x000C | Disable Privacy PIN Protection [PIN] | x | x |  |  |
| 0x000D | Enable ESME Supply |  |  |  |  |
| 0x000E | Enable Supply [PIN] | x | x |  |  |
| 0x000F | Extend Boost Period |  |  |  | x |
| 0x0010 | Initiate Pairing of Type 2 Device [PIN] | x | x |  |  |
| 0x0011 | Initiate Unpairing of Type 2 Device [PIN] | x | x |  |  |
| 0x0012 | Set Privacy PIN [PIN] | x | x |  |  |
| 0x0013 | Test Auxiliary Load Control Switch 1 |  |  | x |  |
| 0x0014 | Test Auxiliary Load Control Switch 2 |  |  | x |  |
| 0x0015 | Test Auxiliary Load Control Switch 3 |  |  | x |  |
| 0x0016 | Test Auxiliary Load Control Switch 4 |  |  | x |  |
| 0x0017 | Test Auxiliary Load Control Switch 5 |  |  | x |  |
| 0x0018 | Test Valve | x |  |  |  |
| 0x0019 | Reset Remaining Battery Capacity | x |  |  |  |
| 0x001A | Find and Join SMHAN | x | x | x | x |

Table 16.4: User Interface Command Codes by Device

For any Event Log entries relating to Event Codes 0x0054 and 0x0055, the Device shall record the Commands received on the Network Interface by including the Message Code in the Event Log.

# Remote Party Usage Rights

## Remote Party Access Rights to Attributes and Methods

Access rights to attributes and methods shall be enforced by the Device as per the requirements in the ‘SMETS required objects’ tab in the Mapping Table. ‘R’ shall mean that the Remote Party Role shall have read access to the attribute. ‘W’ shall mean that the Remote Party Role shall have write access to the attribute. ‘A’ shall mean that the Remote Party Role shall be able to invoke the method. There shall be no other access to these attributes and methods allowed by the Device.

Encryption of attributes whenever transiting the HAN Interface shall be enforced by the Device as per the requirements in the ‘SMETS required objects’ tab in the Mapping Table. ‘Y’ in the column headed ‘Encrypted’ shall mean that the Encryption shall always be applied to the corresponding attribute as it crosses the HAN Interface.

## Remote Party Usage Rights to Use Cases

Access rights to Use Cases shall be enforced by the Device as per the requirements in the Use Case Access Permissions table in each Use Case (see Table 19.4). In that table, ‘A’ shall mean that the Remote Party Role has shall have access to the Use Case. There shall be no other access allowed by the Device. Remote Party roles align to the Trust Anchor Cells in Section 4.3.2.5. The Access Control Broker controls access for Unknown Remote Parties.

# Message Templates

## ZSE Message Templates

Message Templates for GBZ Use Cases are detailed in the embedded Use Cases, Section 19.4. These Message Templates are derived from the Mapping Table, and shall be complied with in the construction and population of all such Messages.

## 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

### Encoding

Italicised terms in this Section 18.2.1 shall have their DLMS COSEM meaning.

The Blue Book definition of attribute 2 of *Profile Generic* objects may be interpreted as requiring ‘*entry’* to be a *structure* containing a single choice from the DLMS data types. The GBCS interprets it as meaning that ‘*entry’* is a *structure* that can contain multiple choices of DLMS data types. These choices vary between instances of Profile Generic object. To identify these different structures, the naming convention ‘entry\_nameOfStructure’ is used.

The GBCS uses the *compact-array* data type in attribute 2 of *Profile Generic* objects. Table 18.2.1 details the derivation of the *contents-description* element within the *compact-array structure* for the structures used in the *Profile Generic* objects required by this GBCS. These encodings are reflected in the DLMS COSEM Message Templates.

| ***Structure definition*** | ***Tag*** | ***Number of entries (structures and arrays only)*** | ***Tag of entries in array*** | ***contents-description for compact-array*** |
| --- | --- | --- | --- | --- |
| entry\_dlValueLogEntry::= structure { | 0x02 | 0x02 |  | 0x1302020606 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| dlValue: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_enumValueLogEntry::= structure { | 0x02 | 0x02 |  | 0x1302020616 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| enumValue: enum | 0x16 |  |  |  |
| } |  |  |  |  |
| entry\_eventLogEntry12::= structure { | 0x02 | 0x03 |  | 0x130203061209 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| logCode: long-unsigned, | 0x12 |  |  |  |
| otherInformation: octet-string(12) | 0x09 |  |  |  |
| } |  |  |  |  |
| entry\_powerLogEntry::= structure { | 0x02 | 0x03 |  | 0x130203061206 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| logCode: long-unsigned, | 0x12 |  |  |  |
| otherInformation: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_eventLogEntry8::= structure { | 0x02 | 0x03 |  | 0x130203061209 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| logCode: long-unsigned, | 0x12 |  |  |  |
| otherInformation: octet-string(8) | 0x09 |  |  |  |
| } |  |  |  |  |
| entry\_securityLogEntry::= structure { | 0x02 | 0x02 |  | 0x1302020612 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| logCode: long-unsigned | 0x12 |  |  |  |
| } |  |  |  |  |
| entry\_billingCalendarLogEntry::= structure{ | 0x02 | 0x07 or 0x09 |  | 0x1302070606013006010806010806010806010806 (single element) or 0x130209060606013006010406010806010806010806010806 (twin element) |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| activeImportRegisterValue: double-long-unsigned, | 0x06 |  |  |  |
| secondaryActiveImportRegisterValue: double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x06 |  |  |  |
| tariffTOURegisterValues: array double-long-unsigned, | 0x01 | 0x30 | 0x06 |  |
| secondaryTariffTOURegisterValues: array double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x01 | 0x04 | 0x06 |  |
| tariffTOUBlock1RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock2RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock3RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock4RegisterValues: array double-long-unsigned | 0x01 | 0x08 | 0x06 |  |
| } |  |  |  |  |
| entry\_billingCalendarOnSetModeOrTariffLogEntry::= structure{ | 0x02 | 0x0D or 0x0F |  | 0x13020D0606013006010806010806010806010806060606060606 (single element) or 0x13020F060606013006010406010806010806010806010806060606060606 (twin element) |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| activeImportRegisterValue: double-long-unsigned, | 0x06 |  |  |  |
| secondaryActiveImportRegisterValue: double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x06 |  |  |  |
| tariffTOURegisterValues: array double-long-unsigned, | 0x01 | 0x30 | 0x06 |  |
| secondaryTariffTOURegisterValues: array double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x01 | 0x04 | 0x06 |  |
| tariffTOUBlock1RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock2RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock3RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock4RegisterValues: array double-long-unsigned | 0x01 | 0x08 | 0x06 |  |
| emergencyCreditBalanceValue: double-long-unsigned, | 0x06 |  |  |  |
| meterBalanceValue: double-long-unsigned, | 0x06 |  |  |  |
| paymentDebtRegisterValue: double-long-unsigned, | 0x06 |  |  |  |
| timeDebtRegisters1Value: double-long-unsigned, | 0x06 |  |  |  |
| timeDebtRegisters2Value: double-long-unsigned, | 0x06 |  |  |  |
| accumulatedDebtRegisterValue: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_boostFunctionLogEntry::= structure { | 0x02 | 0x02 |  | 0x1302020606 |
| boost\_start: double-long-unsigned, | 0x06 |  |  |  |
| boost\_end: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_prepaymentReadLogEntry::= structure { | 0x02 | 0x07 |  | 0x13020706060606060606 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| emergencyCreditBalanceValue: double-long-unsigned, | 0x06 |  |  |  |
| meterBalanceValue: double-long-unsigned, | 0x06 |  |  |  |
| paymentDebtRegisterValue: double-long-unsigned, | 0x06 |  |  |  |
| timeDebtRegisters1Value: double-long-unsigned, | 0x06 |  |  |  |
| timeDebtRegisters2Value: double-long-unsigned, | 0x06 |  |  |  |
| accumulatedDebtRegisterValue: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_registerReadLogEntry::= structure{ | 0x02 | 0x07 or 0x09 |  | 0x1302070606013006010806010806010806010806 (single element) or 0x130209060606013006010406010806010806010806010806 (twin element) |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| activeImportRegisterValue: double-long-unsigned, | 0x06 |  |  |  |
| secondaryActiveImportRegisterValue: double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x06 |  |  |  |
| tariffTOURegisterValues: array double-long-unsigned, | 0x01 | 0x30 | 0x06 |  |
| secondaryTariffTOURegisterValues: array double-long-unsigned, [[MAY NOT BE PRESENT]] | 0x01 | 0x04 | 0x06 |  |
| tariffTOUBlock1RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock2RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock3RegisterValues: array double-long-unsigned, | 0x01 | 0x08 | 0x06 |  |
| tariffTOUBlock4RegisterValues: array double-long-unsigned | 0x01 | 0x08 | 0x06 |  |
| } |  |  |  |  |
| entry\_activeImportLogEntry ::= structure { | 0x02 | 0x03 or 0x02 |  | 0x130203060606 (twin element) or 0x1302020606 (single element) |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| primaryValue: double-long-unsigned, | 0x06 |  |  |  |
| secondaryValue: double-long-unsigned [[MAY NOT BE PRESENT]] | 0x06 |  |  |  |
| } |  |  |  |  |
| entry\_twoDlValueLogEntry::= structure { | 0x02 | 0x03 |  | 0x130203060606 |
| timestamp: double-long-unsigned, | 0x06 |  |  |  |
| dlValue: double-long-unsigned, | 0x06 |  |  |  |
| dlValue2: double-long-unsigned | 0x06 |  |  |  |
| } |  |  |  |  |

Table 18.2.1a: derivation of the *contents-description* element within the *compact-array structure*

## Illustrative command and response instantiation and DER encoding

### Illustrative @UpdateSecurityCredentials.Command instantiation and its DER encoding - informative

supplierUpdatingAllSupplierCertificates in Table 18.3.1a is an ASN.1 structured value assignment. This specific example is where a Device’s Supplier is instructing the Device to replace both the Supplier Digital Signing and Key Agreement credentials on the Device, and resetting Protection Against Replay counters. In business terms, an example of this would be at Change of Supplier.

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

| **ASN.1** | **Notes** |
| --- | --- |
| supplierUpdatingAllSupplierCertificates Command ::=  {authorisingRemotePartyControl  {credentialsReplacementMode *supplierBySupplier,*  authorisingRemotePartyTACellIdentifier  {trustAnchorCellRemotePartyRole *supplier*,  trustAnchorCellKeyUsage { *digitalSignature*}},  authorisingRemotePartySeqNumber *123456789*,  newRemotePartyFloorSeqNumber *987654321*}  replacements  {{replacementCertificate *'0A7C8E9F123456789ABCDEF01234'H*,  targetTrustAnchorCell  {trustAnchorCellRemotePartyRole *supplier*,  trustAnchorCellKeyUsage { *digitalSignature*}}}  {replacementCertificate *'0B34269F123456789ABCDEF01234'*H,  targetTrustAnchorCell  {trustAnchorCellRemotePartyRole *supplier*,  trustAnchorCellKeyUsage {*keyAgreement*}}}}  certificationPathCertificates {*'FFAABB9F123456789ABCDEF01234'*H }} | This message is for the Supplier replacing supplier credentials  The public key to be used to check the signature on this message is the supplier digital signing key currently held by the Device.  This is the existing supplier’s counter, so greater than any this supplier has used  This is the new supplier’s counter, which the Device should use if the Command is successful  The new supplier’s digital signing certificate …  … which is to be placed in the Device’s supplier, digital signature Trust Anchor Cell  The new supplier’s key agreement certificate…  which is to be placed in the Device’s supplier, key agreement Trust Anchor Cell  The Certificate for the CA which issued the new supplier’s certificates. The Device will use this to check that the new supplier certificates were properly issued. |

Table 18.3.1a: Illustrative @UpdateSecurityCredentials.Command instantiation – ASN.1 structure

The message sent to the Device would contain the DER encoding of the above ASN.1 value assignment. This DER encoding is laid out and explained in Table 18.3.1b. For these purpose, the Certificate is simply shown as an OCTET STRING.

| **Component** | **Value** | **Notes** |
| --- | --- | --- |
| Payload SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x64 | 100 octet length follows |
| contents =: |  |  |
| authorisingRemotePartyControl AuthorisingRemotePartyControl SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x18 | Length of authorisingRemotePartyControl |
| contents =: |  |  |
| credentialsReplacementMode CredentialsReplacementMode INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 |  |
| length = | 0x01 |  |
| contents =: | 0x02 | Representing supplierBySupplier |
| authorisingRemotePartyTACellIdentifier TrustAnchorCellIdentifier SEQUENCE: |  |  |
| tag = [2] constructed; | 0xA2 | Tag for authorisingRemotePartyTACellIdentifier |
| length = | 0x07 | Length of authorisingRemotePartyTACellIdentifier |
| contents =: |  |  |
| trustAnchorCellRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 | 1 octet length INTEGER |
| contents =: | 0x02 | Representing supplier RemotePartyRole |
| trustAnchorCellKeyUsage KeyUsage BIT STRING: |  |  |
| tag = [UNIVERSAL 3] primitive; | 0x03 | Tag for BIT STRING |
| length = | 0x02 | 2 octet length BIT STRING |
| contents =: | 0x0780 | Representing digitalSignature |
| authorisingRemotePartySeqNumber SeqNumber INTEGER: |  |  |
| tag = [4] primitive; | 0x84 | Tag for INTEGER |
| length = | 0x04 | 4 octet length INTEGER |
| contents =: | 0x075bcd15 | The old supplier’s Protection Against Replay counter in hex |
| newRemotePartyFloorSeqNumber SeqNumber INTEGER: |  |  |
| tag = [5] primitive; | 0x85 | Tag for INTEGER |
| length = | 0x04 | 4 octet length INTEGER |
| contents =: | 0x3ade68b1 | The new supplier’s Protection Against Replay counter in hex |
| replacements SEQUENCE OF: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x38 | Length of replacements |
| contents =: |  |  |
| TrustAnchorReplacement SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x19 | Length of first TrustAnchorReplacement |
| contents =: |  |  |
| replacementCertificate Certificate OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x0e | Length of certificate |
| contents =: | 0x0a7c8e9f123456789abcdef01234 | New supplier’s digitalSignature certificate |
| targetTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x07 | Length of targetTrustAnchorCell |
| contents =: |  |  |
| trustAnchorCellRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 | 1 octet length INTEGER |
| contents =: | 0x02 | Representing supplier RemotePartyRole |
| trustAnchorCellKeyUsage KeyUsage BIT STRING: |  |  |
| tag = [UNIVERSAL 3] primitive; | 0x03 | Tag for BIT STRING |
| length = | 0x02 | 2 octet length BIT STRING |
| contents =: | 0x0780 | Representing digitalSignature |
| TrustAnchorReplacement SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x19 | Length of second TrustAnchorReplacement |
| contents =: |  |  |
| replacementCertificate Certificate OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x0e | Length of certificate |
| contents =: | 0x0b34269f123456789abcdef01234 | New supplier’s keyAgreement certificate |
| targetTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x07 | Length of targetTrustAnchorCell |
| contents =: |  |  |
| trustAnchorCellRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 | 1 octet length INTEGER |
| contents =: | 0x02 | Representing supplier RemotePartyRole |
| trustAnchorCellKeyUsage KeyUsage BIT STRING: |  |  |
| tag = [UNIVERSAL 3] primitive; | 0x03 | Tag for BIT STRING |
| length = | 0x02 | 2 octet length BIT STRING |
| contents =: | 0x0308 | Representing keyAgreement |
| certificationPathCertificates SEQUENCE OF: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x10 | Length of certificationPathCertificates |
| contents =: |  |  |
| Certificate OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x0e | Length of certificate |
| contents =: | 0xffaabb9f123456789abcdef01234 | CA certificate for new supplier |

Table 18.3.1b: Illustrative @UpdateSecurityCredentials.Command instantiation – DER encoding

### Illustrative @UpdateSecurityCredentials.Response instantiation and its DER encoding - informative

supplierUpdatingAllSupplierCertificatesResponse in Table 18.3.2a is an ASN.1 structured value assignment. This specific example is where a Device is responding successfully to a Command.

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

| **ASN.1** | Notes |
| --- | --- |
| supplierUpdatingAllSupplierCertificatesResponse Response ::=  {credentialsReplacementMode *supplierBySupplier*,  remotePartySeqNumberChanges  {{otherRemotePartyRole *supplier*,  otherRemotePartyFloorSeqNumber *987654321*}  },  replacementOutcomes  {  {affectedTrustAnchorCell  trustAnchorCellRemotePartyRole *supplier*,  trustAnchorCellKeyUsage { *digitalSignature*}},  statusCode *success*,  existingSubjectUniqueID '*123456789ABCDEF0*'H,  existingSubjectKeyIdentifier '*1234567890123456*'H,  replacingSubjectUniqueID '*FEDCBA9876543210*'H,  replacingSubjectKeyIdentifier '*ABCDEABCDEABCDEA*'H},  {affectedTrustAnchorCell  {trustAnchorCellRemotePartyRole *supplier*,  trustAnchorCellKeyUsage { *keyAgreement*}},  statusCode *success*,  existingSubjectUniqueID *'123456789ABCDEF0*'H,  existingSubjectKeyIdentifier *'0987654321098765*'H,  replacingSubjectUniqueID *'FEDCBA9876543210*'H,  replacingSubjectKeyIdentifier *'FEDCBFEDCBFEDCBF*'H}}} | The corresponding Command was for the Supplier replacing supplier credentials  This is the new supplier’s counter, which the Device will now use for Protection Against Replay in relation to the supplier role  This outcome is for the supplier digital signing store  The old supplier’s Entity Identifier  The KeyIdentifier for the old supplier’s digital signing key  The new supplier’s Entity Identifier  The KeyIdentifier for the old supplier’s digital signing key  This outcome is for the supplier key agreement store |

Table 18.3.2a: Illustrative @UpdateSecurityCredentials.Response instantiation – ASN.1 structure

The message sent by the Device would contain the DER encoding of the above ASN.1 value assignment. This DER encoding is laid out and explained in Table 18.3.2b.

| **Component** | **Value** | **Notes** |
| --- | --- | --- |
| Response SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x7E | Length 126 |
| content = |  |  |
| credentialsReplacementMode CredentialsReplacementMode INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 |  |
| content = | 0x02 | Value for supplierBySupplier |
| remotePartySeqNumberChanges SEQUENCE OF: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x0B |  |
| content = |  |  |
| RemotePartySeqNumberChange SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x09 |  |
| content = |  |  |
| otherRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 |  |
| content = | 0x02 | Value for supplier |
| otherRemotePartyFloorSeqNumber SeqNumber INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x04 |  |
| content = | 0x3ade68b1 | The new supplier’s Protection Against Replay counter in hexadecimal |
| replacementOutcomes SEQUENCE OF: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x6C | Length of 108 |
| content = |  |  |
| ReplacementOutcome SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x34 | Length of 52 |
| content = |  |  |
| affectedTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x07 |  |
| content = |  |  |
| trustAnchorCellRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 |  |
| content = | 0x02 | Value for supplier |
| trustAnchorCellKeyUsage KeyUsage BIT STRING: |  |  |
| tag = [UNIVERSAL 3] primitive; | 0x03 | Tag for BIT STRING |
| length = | 0x02 |  |
| content = | 0x0780 | Tag for digitalSignature |
| statusCode StatusCode ENUMERATED: |  |  |
| tag = [UNIVERSAL 10] primitive; | 0x0A | Tag for ENUMERATED |
| length = | 0x01 |  |
| content = | 0x00 | Value for success |
| existingSubjectUniqueID OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | 8 octet length of Entity Identifier |
| content = | 0x123456789abcdef0 |  |
| existingSubjectKeyIdentifier OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | length of KeyIdentifier |
| content = | 0x1234567890123456 | KeyIdentifier |
| replacingSubjectUniqueID OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | 8 octet length of Entity Identifier |
| content = | 0xfedcba9876543210 |  |
| replacingSubjectKeyIdentifier OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | length of KeyIdentifier |
| content = | 0xABCDEABCDEABCDEA | KeyIdentifier |
| ReplacementOutcome SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x34 |  |
| content = |  |  |
| affectedTrustAnchorCell TrustAnchorCellIdentifier SEQUENCE: |  |  |
| tag = [UNIVERSAL 16] constructed; | 0x30 | Tag for SEQUENCE |
| length = | 0x07 |  |
| content = |  |  |
| trustAnchorCellRemotePartyRole RemotePartyRole INTEGER: |  |  |
| tag = [UNIVERSAL 2] primitive; | 0x02 | Tag for INTEGER |
| length = | 0x01 |  |
| content = | 0x02 | Value for supplier |
| trustAnchorCellKeyUsage KeyUsage BIT STRING: |  |  |
| tag = [UNIVERSAL 3] primitive; | 0x03 | Tag for BIT STRING |
| length = | 0x02 |  |
| content = | 0x0308 |  |
| statusCode StatusCode ENUMERATED: |  |  |
| tag = [UNIVERSAL 10] primitive; | 0x0A | Tag for ENUMERATED |
| length = | 0x01 |  |
| content = | 0x00 | Value for success |
| existingSubjectUniqueID OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | 8 octet length of Entity Identifier |
| content = | 0x123456789abcdef0 |  |
| existingSubjectKeyIdentifier OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | length of KeyIdentifier |
| content = | 0x0987654321098765 | KeyIdentifier |
| replacingSubjectUniqueID OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | 8 octet length of Entity Identifier |
| content = | 0xfedcba9876543210 |  |
| replacingSubjectKeyIdentifier OCTET STRING: |  |  |
| tag = [UNIVERSAL 4] primitive; | 0x04 | Tag for OCTET STRING |
| length = | 0x08 | length of KeyIdentifier |
| content = | 0xFEDCBFEDCBFEDCBF | KeyIdentifier |

Table 18.3.2b: Illustrative @UpdateSecurityCredentials.Response instantiation – DER encoding

## Cryptographic Test Vectors

This Section 18.4 provides cryptographic calculations in relation to a number of sample messages. The sample messages’ contents align with the corresponding Message Templates in Section 18.2. To undertake cryptographic calculations, a number of details about the Smart Metering Entities involved are also required, not least Key Pairs, Entity Identifiers and Originator Counters. This section specifies and uses sample values of such attributes.

### Cryptographic Calculations

Create details for three Smart Metering Entities with associated Keys and shared secrets:

An Entity called SupplierA:

|  |  |
| --- | --- |
| --With an Entity ID: | 0x12:34:56:78:9A:BC:DE:F0 |
| --With a current Originator Counter: | 0x00:00:00:00:00:00:00:01 |
| --Digital Signing Private key : | 0x3A:6B:2E:AA:0D:9F:25:A9:E4:55:98:3F:EB:5B:B9:47:52:81:21:91:1B:F3:B7:6B:E5:66:1C:89:DB:F2:4B:26 |
| --Digital Signing Public key : | 0x76:62:8E:1C:84:EF:79:35:54:8A:E5:D6:2C:7B:B3:AD:28:96:4C:F7:94:F0:38:7A:69:7E:EC:19:CD:D9:8F:46:0A:4D:5E:19:08:7E:F7:21:6E:D8:9C:29:83:1A:6E:E8:38:C8:DE:88:EF:34:F1:1D:3F:41:F3:6D:80:B2:A5:D5 |
| --Key Agreement Private key : | 0x3D:9D:FB:33:2E:B4:D6:D6:06:D7:47:18:55:3E:5E:61:B3:92:B0:FC:4C:90:CE:6A:A4:CE:DA:81:7E:80:11:B1 |
| --Key Agreement Public key : | 0xEF:F2:1D:5D:D6:74:EE:C6:E0:87:40:70:3B:52:25:52:CB:B7:4F:FC:A1:15:36:C5:37:C3:C8:06:E4:14:3C:8F:B2:E7:CA:3E:73:06:CB:46:DB:E4:BD:59:9C:C4:A3:1F:78:8C:2F:B7:A9:B9:BC:97:BE:98:C8:1E:F1:82:1A:30 |
| --The shared secret calculated with DeviceA is : | 0x15:45:AD:F2:75:DC:8E:57:AB:E4:71:E9:F0:C1:20:C2:FA:DD:5B:12:51:AF:B7:BD:AB:25:3C:80:1B:41:11:CE |

An Entity called Access Control Broker:

|  |  |
| --- | --- |
| --With an Entity ID: | 0xAB:AB:AB:AB:AB:AB:AB:AB |
| --With a current Originator Counter: | 0x10:00:00:00:00:00:00:01 |
| --Key Agreement Private key : | 0xE4:A6:CF:B4:31:47:1C:FC:AE:49:1F:D5:66:D1:9C:87:08:2C:F9:FA:77:22:D7:FA:24:B2:B3:F5:66:9D:BE:FB |
| --Key Agreement Public key : | 0x29:2F:97:FE:C1:B3:0C:38:49:B8:06:D9:04:46:E4:A0:37:D6:D1:78:01:97:96:E7:6E:52:55:BD:C3:A0:8E:34:6F:9F:6E:6E:7E:8F:6A:4D:55:96:2D:2F:2D:0E:16:CF:F2:7B:F3:F9:25:FA:7D:BA:FD:15:A8:B1:DC:69:58:94 |
| --The shared secret calculated with DeviceA is : | 0x9A:AC:F2:E6:D5:1B:D5:FF:8F:37:BF:36:80:19:A6:91:CB:5B:2F:CB:7B:5F:03:0A:00:06:36:47:B2:0E:13:FE |

An Entity called DeviceA:

|  |  |
| --- | --- |
| --With an Entity ID: | 0xFF:FF:FF:FF:FF:FF:FF:FE |
| --With a current Originator Counter: | 0x20:00:00:00:00:00:00:01 |
| --Digital Signing Private key : | 0xFC:9B:B7:73:E6:C8:35:0A:DB:40:51:AC:91:3C:A4:70:CF:42:2D:8A:53:DE:8C:88:1D:BF:FE:B4:0B:A4:70:51 |
| --Digital Signing Public key : | 0x86:FB:5E:B3:CA:05:07:22:6B:E7:19:70:58:B9:EC:04:1D:3A:37:58:D9:D9:C9:19:02:AC:A3:39:1F:4E:58:AE:F1:3A:FF:63:CC:4E:F6:89:42:B9:B9:49:04:DC:1B:89:0E:DB:EA:BD:16:B9:92:11:06:24:96:8E:89:4E:56:0E |
| --Key Agreement Private key : | 0xFB:9F:4C:02:B7:AB:F8:B0:DA:BA:02:7E:0B:C8:1B:8D:D2:09:68:3B:1C:88:93:EE:45:3F:AD:F3:A8:0F:73:E5 |
| --Key Agreement Public key : | 0x2D:B4:5A:3F:21:88:94:38:B4:2C:8F:46:4C:75:29:2B:AC:F5:FD:DB:5D:A0:B4:92:50:1B:29:9C:BF:E9:2D:8F:DB:90:FC:8F:F4:02:61:29:83:8B:1B:CA:D1:40:2C:AE:47:FE:7D:80:84:E4:09:A4:1A:FC:E1:6D:63:57:9C:5F |
| --The shared secret calculated with AccessControlBroker is : | 0x9A:AC:F2:E6:D5:1B:D5:FF:8F:37:BF:36:80:19:A6:91:CB:5B:2F:CB:7B:5F:03:0A:00:06:36:47:B2:0E:13:FE |
| --The shared secret calculated with SupplierA is : | 0x15:45:AD:F2:75:DC:8E:57:AB:E4:71:E9:F0:C1:20:C2:FA:DD:5B:12:51:AF:B7:BD:AB:25:3C:80:1B:41:11:CE |

Create a Critical Command from SupplierA to Device A: ECS04b Reset Meter Balance on the ESME:

|  |  |
| --- | --- |
| --GBCS Message Category: | SME.C.C |
| --GBCS Message Type: | Command |
| --CRA Flag: | 0x01 |
| --Originator Counter: | 0x00:00:00:00:00:00:00:01 |
| --Business Originator ID: | 0x12:34:56:78:9A:BC:DE:F0 |
| --Business Target ID: | 0xFF:FF:FF:FF:FF:FF:FF:FE |
| --Date Time: | 0x |
| --Other Info: | 0x00:B3 |
| --Message Content: | 0xD9:20:00:00:01:00:03:03:00:70:00:00:13:0A:00:FF:02:03:00:70:00:00:13:0A:01:FF:02:03:00:70:00:00:13:0A:02:FF:02:03:05:00:00:00:00:05:00:00:00:00:05:00:00:00:00 |
| --The originator’s Private Signing Key: | 0x3A:6B:2E:AA:0D:9F:25:A9:E4:55:98:3F:EB:5B:B9:47:52:81:21:91:1B:F3:B7:6B:E5:66:1C:89:DB:F2:4B:26 |
| --The Message parts used in Signing: | 0x01:00:00:00:00:00:00:00:01:12:34:56:78:9A:BC:DE:F0:FF:FF:FF:FF:FF:FF:FF:FE:00:B3:D9:20:00:00:01:00:03:03:00:70:00:00:13:0A:00:FF:02:03:00:70:00:00:13:0A:01:FF:02:03:00:70:00:00:13:0A:02:FF:02:03:05:00:00:00:00:05:00:00:00:00:05:00:00:00:00 |
| --The per message secret number: | 28321578986444545792209120900555608833352738719916097837081350912149044905275 |
| --The resulting Signature in Plain Format: | 0x85:AE:39:D4:5D:5C:73:A4:40:70:DF:71:C7:A0:97:6B:AF:60:A3:62:6E:6D:08:D1:67:AA:7C:F4:AB:83:93:B0:B4:13:E9:1D:3E:79:FD:6C:CC:93:F4:5D:B0:A2:0B:E5:26:4B:5C:E9:BA:56:A2:47:00:72:78:4D:D1:A1:17:52 |
| --The Grouping Header: | 0xDF:09:01:00:00:00:00:00:00:00:01:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:B3:35 |
| --All of the Message parts covered by the general-signing structure | 0xDF:09:01:00:00:00:00:00:00:00:01:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:B3:35:D9:20:00:00:01:00:03:03:00:70:00:00:13:0A:00:FF:02:03:00:70:00:00:13:0A:01:FF:02:03:00:70:00:00:13:0A:02:FF:02:03:05:00:00:00:00:05:00:00:00:00:05:00:00:00:00:40:85:AE:39:D4:5D:5C:73:A4:40:70:DF:71:C7:A0:97:6B:AF:60:A3:62:6E:6D:08:D1:67:AA:7C:F4:AB:83:93:B0:B4:13:E9:1D:3E:79:FD:6C:CC:93:F4:5D:B0:A2:0B:E5:26:4B:5C:E9:BA:56:A2:47:00:72:78:4D:D1:A1:17:52 |
| --The KDF OtherInfo: | 0x60:85:74:06:08:03:00:12:34:56:78:9A:BC:DE:F0:09:01:00:00:00:00:00:00:00:01:FF:FF:FF:FF:FF:FF:FF:FE |
| --The per message secret symmetric key: | 177594815140134193685548970760141301611 |
| --The Initialization Vector: | 0x12:34:56:78:9A:BC:DE:F0:00:00:00:00 |
| --The Additional Authenticated Data: | 0x11:DF:09:01:00:00:00:00:00:00:00:01:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:B3:35:D9:20:00:00:01:00:03:03:00:70:00:00:13:0A:00:FF:02:03:00:70:00:00:13:0A:01:FF:02:03:00:70:00:00:13:0A:02:FF:02:03:05:00:00:00:00:05:00:00:00:00:05:00:00:00:00:40:85:AE:39:D4:5D:5C:73:A4:40:70:DF:71:C7:A0:97:6B:AF:60:A3:62:6E:6D:08:D1:67:AA:7C:F4:AB:83:93:B0:B4:13:E9:1D:3E:79:FD:6C:CC:93:F4:5D:B0:A2:0B:E5:26:4B:5C:E9:BA:56:A2:47:00:72:78:4D:D1:A1:17:52 |
| --The resulting MAC: | 0x43:0C:DE:EA:CC:82:97:09:44:71:CF:92 |
| --The MAC Header excluding the Security Header | 0xDD:00:00:00:00:00:00:82:00:A9 |
| --The Security Header fields: | 0x11:00:00:00:00 |
| --The resulting Message: | 0xDD:00:00:00:00:00:00:82:00:A9:11:00:00:00:00:DF:09:01:00:00:00:00:00:00:00:01:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:B3:35:D9:20:00:00:01:00:03:03:00:70:00:00:13:0A:00:FF:02:03:00:70:00:00:13:0A:01:FF:02:03:00:70:00:00:13:0A:02:FF:02:03:05:00:00:00:00:05:00:00:00:00:05:00:00:00:00:40:85:AE:39:D4:5D:5C:73:A4:40:70:DF:71:C7:A0:97:6B:AF:60:A3:62:6E:6D:08:D1:67:AA:7C:F4:AB:83:93:B0:B4:13:E9:1D:3E:79:FD:6C:CC:93:F4:5D:B0:A2:0B:E5:26:4B:5C:E9:BA:56:A2:47:00:72:78:4D:D1:A1:17:52:43:0C:DE:EA:CC:82:97:09:44:71:CF:92 |

And get a Critical Response to SupplierA from Device A: ECS04b Reset Meter Balance on the ESME:

|  |  |
| --- | --- |
| --GBCS Message Category: | SME.C.C |
| --GBCS Message Type: | Response |
| --CRA Flag: | 0x02 |
| --Originator Counter: | 0x00:00:00:00:00:00:00:01 |
| --Business Originator ID: | 0xFF:FF:FF:FF:FF:FF:FF:FE |
| --Business Target ID: | 0x12:34:56:78:9A:BC:DE:F0 |
| --Date Time: | 0x |
| --Other Info: | 0x00:B3 |
| --Message Content: | 0xDA:20:00:00:01:00:00:03:00:00:00:03:03:00:03:00:03:00 |
| --The originator’s Private Signing Key: | 0xFC:9B:B7:73:E6:C8:35:0A:DB:40:51:AC:91:3C:A4:70:CF:42:2D:8A:53:DE:8C:88:1D:BF:FE:B4:0B:A4:70:51 |
| --The Message parts used in Signing: | 0x02:00:00:00:00:00:00:00:01:FF:FF:FF:FF:FF:FF:FF:FE:12:34:56:78:9A:BC:DE:F0:00:B3:DA:20:00:00:01:00:00:03:00:00:00:03:03:00:03:00:03:00 |
| --The per message secret number: | 48814838122802850934537136292612629832407092209107840231664691912455948374928 |
| --The resulting Signature in Plain Format: | 0x01:99:E9:84:CE:C7:5D:DC:A7:F1:DD:F6:E5:3E:2E:67:35:2A:2B:E3:8A:4B:66:F8:ED:59:66:06:FA:B9:83:FF:30:0C:AA:76:DE:88:CE:D9:D5:63:A5:C0:3E:8F:3A:7C:00:07:80:F3:F2:06:1C:61:1E:9A:A0:B1:8B:46:0D:77 |
| --The Grouping Header: | 0xDF:09:02:00:00:00:00:00:00:00:01:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:B3:12 |
| --All of the Message parts covered by the general-signing structure | 0xDF:09:02:00:00:00:00:00:00:00:01:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:B3:12:DA:20:00:00:01:00:00:03:00:00:00:03:03:00:03:00:03:00:40:01:99:E9:84:CE:C7:5D:DC:A7:F1:DD:F6:E5:3E:2E:67:35:2A:2B:E3:8A:4B:66:F8:ED:59:66:06:FA:B9:83:FF:30:0C:AA:76:DE:88:CE:D9:D5:63:A5:C0:3E:8F:3A:7C:00:07:80:F3:F2:06:1C:61:1E:9A:A0:B1:8B:46:0D:77 |
| --The resulting Message: | 0xDF:09:02:00:00:00:00:00:00:00:01:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:B3:12:DA:20:00:00:01:00:00:03:00:00:00:03:03:00:03:00:03:00:40:01:99:E9:84:CE:C7:5D:DC:A7:F1:DD:F6:E5:3E:2E:67:35:2A:2B:E3:8A:4B:66:F8:ED:59:66:06:FA:B9:83:FF:30:0C:AA:76:DE:88:CE:D9:D5:63:A5:C0:3E:8F:3A:7C:00:07:80:F3:F2:06:1C:61:1E:9A:A0:B1:8B:46:0D:77 |

Supplier A has now increased its Originator Counter by 1.

Create a non-Critical Command from SupplierA to Device A: ECS12 Set Change of Tenancy date on ESME:

|  |  |
| --- | --- |
| --GBCS Message Category: | SME.C.NC |
| --GBCS Message Type: | Command |
| --CRA Flag: | 0x01 |
| --Originator Counter: | 0x00:00:00:00:00:00:00:02 |
| --Business Originator ID: | 0x12:34:56:78:9A:BC:DE:F0 |
| --Business Target ID: | 0xFF:FF:FF:FF:FF:FF:FF:FE |
| --Date Time: | 0x |
| --Other Info: | 0x00:22 |
| --Message Content: | 0xD9:20:00:00:02:00:01:02:00:01:00:00:5E:2C:03:02:02:01:09:0C:07:DF:01:05:FF:00:00:00:00:80:00:FF |
| --The Grouping Header: | 0xDF:09:01:00:00:00:00:00:00:00:02:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:22:20 |
| --All of the Message parts covered by the general-signing structure | 0xDF:09:01:00:00:00:00:00:00:00:02:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:22:20:D9:20:00:00:02:00:01:02:00:01:00:00:5E:2C:03:02:02:01:09:0C:07:DF:01:05:FF:00:00:00:00:80:00:FF:00 |
| --The KDF OtherInfo: | 0x60:85:74:06:08:03:00:12:34:56:78:9A:BC:DE:F0:09:01:00:00:00:00:00:00:00:02:FF:FF:FF:FF:FF:FF:FF:FE |
| --The per message secret symmetric key: | 323267885984686097664772256155520506945 |
| --The Initialization Vector: | 0x12:34:56:78:9A:BC:DE:F0:00:00:00:00 |
| --The Additional Authenticated Data: | 0x11:DF:09:01:00:00:00:00:00:00:00:02:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:22:20:D9:20:00:00:02:00:01:02:00:01:00:00:5E:2C:03:02:02:01:09:0C:07:DF:01:05:FF:00:00:00:00:80:00:FF:00 |
| --The resulting MAC: | 0xD7:48:D3:F8:7C:97:64:E4:2D:68:1C:11 |
| --The MAC Header excluding the Security Header | 0xDD:00:00:00:00:00:00:54 |
| --The Security Header fields: | 0x11:00:00:00:00 |
| --The resulting Message: | 0xDD:00:00:00:00:00:00:54:11:00:00:00:00:DF:09:01:00:00:00:00:00:00:00:02:08:12:34:56:78:9A:BC:DE:F0:08:FF:FF:FF:FF:FF:FF:FF:FE:00:02:00:22:20:D9:20:00:00:02:00:01:02:00:01:00:00:5E:2C:03:02:02:01:09:0C:07:DF:01:05:FF:00:00:00:00:80:00:FF:00:D7:48:D3:F8:7C:97:64:E4:2D:68:1C:11 |

And get a non-Critical Response to SupplierA from Device A: ECS12 Set Change of Tenancy date on ESME:

|  |  |
| --- | --- |
| --GBCS Message Category: | SME.C.NC |
| --GBCS Message Type: | Response |
| --CRA Flag: | 0x02 |
| --Originator Counter: | 0x00:00:00:00:00:00:00:02 |
| --Business Originator ID: | 0xFF:FF:FF:FF:FF:FF:FF:FE |
| --Business Target ID: | 0x12:34:56:78:9A:BC:DE:F0 |
| --Date Time: | 0x |
| --Other Info: | 0x00:22 |
| --Message Content: | 0xDA:20:00:00:02:00:00:01:00:01:02:00 |
| --The Grouping Header: | 0xDF:09:02:00:00:00:00:00:00:00:02:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:22:0C |
| --All of the Message parts covered by the general-signing structure | 0xDF:09:02:00:00:00:00:00:00:00:02:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:22:0C:DA:20:00:00:02:00:00:01:00:01:02:00:00 |
| --The KDF OtherInfo: | 0x60:85:74:06:08:03:00:FF:FF:FF:FF:FF:FF:FF:FE:09:02:00:00:00:00:00:00:00:02:12:34:56:78:9A:BC:DE:F0 |
| --The per message secret symmetric key: | 102613665902023293907968102748610736248 |
| --The Initialization Vector: | 0xFF:FF:FF:FF:FF:FF:FF:FE:00:00:00:00 |
| --The Additional Authenticated Data: | 0x11:DF:09:02:00:00:00:00:00:00:00:02:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:22:0C:DA:20:00:00:02:00:00:01:00:01:02:00:00 |
| --The resulting MAC: | 0xDF:27:D0:FE:42:DD:ED:6D:C5:DC:F3:F6 |
| --The MAC Header excluding the Security Header | 0xDD:00:00:00:00:00:00:40 |
| --The Security Header fields: | 0x11:00:00:00:00 |
| --The resulting Message: | 0xDD:00:00:00:00:00:00:40:11:00:00:00:00:DF:09:02:00:00:00:00:00:00:00:02:08:FF:FF:FF:FF:FF:FF:FF:FE:08:12:34:56:78:9A:BC:DE:F0:00:02:00:22:0C:DA:20:00:00:02:00:00:01:00:01:02:00:00:DF:27:D0:FE:42:DD:ED:6D:C5:DC:F3:F6 |

### Example Messages Produced

|  |  |  |  |
| --- | --- | --- | --- |
| ECS04b Reset Meter Balance on the ESME (Message Category: SME.C.C) | |  | |
|  |  |  | |
| **Command Message Structure** |  |  | |
| **Name** | **Encoded Content** | **Encoded Length** | |
| MAC Header (general-ciphering) |  |  | |
| \_\_\_\_tag | 0xDD | 1 | |
| \_\_\_\_contents | 0x000000000000 | 6 | |
| \_\_\_\_ciphered-service |  |  | |
| \_\_\_\_\_\_\_\_length | 0x8200A9 | 3 | |
| \_\_\_\_\_\_\_\_security header |  |  | |
| \_\_\_\_\_\_\_\_security control byte (SC) | 0x11 | 1 | |
| \_\_\_\_\_\_\_\_invocation counter (IC) | 0x00000000 | 4 | |
| Grouping Header (general-signing) |  |  | |
| \_\_\_\_tag | 0xDF | 1 | |
| \_\_\_\_transaction-id |  |  | |
| \_\_\_\_\_\_\_\_length | 0x09 | 1 | |
| \_\_\_\_\_\_\_\_value (CRA FLAG) | 0x01 | 1 | |
| \_\_\_\_\_\_\_\_value (Originator Counter) | 0x0000000000000001 | 8 | |
| \_\_\_\_originator-system-title |  |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | 1 | |
| \_\_\_\_\_\_\_\_value | 0x123456789ABCDEF0 | 8 | |
| \_\_\_\_recipient-system-title |  |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | 1 | |
| \_\_\_\_\_\_\_\_value | 0xFFFFFFFFFFFFFFFE | 8 | |
| \_\_\_\_date-time |  |  | |
| \_\_\_\_\_\_\_\_length | 0x00 | 1 | |
| \_\_\_\_other-information |  |  | |
| \_\_\_\_\_\_\_\_Length | 0x02 | 1 | |
| \_\_\_\_\_\_\_\_Message Code | 0x00B3 | 2 | |
| \_\_\_\_content |  |  | |
| \_\_\_\_\_\_\_\_length | 0x35 | 1 | |
| access-request |  |  | |
| \_\_\_\_tag | 0xD9 | 1 | |
| \_\_\_\_long-invoke-id-and-priority |  |  | |
| \_\_\_\_\_\_\_\_configuration | 0x20 | 1 | |
| \_\_\_\_\_\_\_\_invoke-id | 0x000001 | 3 | |
| \_\_\_\_date-time | 0x00 | 1 | |
| \_\_\_\_access-request-body |  |  | |
| \_\_\_\_access-request-specification |  |  | |
| \_\_\_\_SEQUENCE OF | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_Request number 1 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-request-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_cosem-method-descriptor |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_class-id | 0x0070 | 2 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_instance-id | 0x0000130A00FF | 6 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_method-id | 0x02 | 1 | |
| \_\_\_\_\_\_\_\_Request number 2 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-request-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_cosem-method-descriptor |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_class-id | 0x0070 | 2 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_instance-id | 0x0000130A01FF | 6 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_method-id | 0x02 | 1 | |
| \_\_\_\_\_\_\_\_Request number 3 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-request-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_cosem-method-descriptor |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_class-id | 0x0070 | 2 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_instance-id | 0x0000130A02FF | 6 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_method-id | 0x02 | 1 | |
| \_\_\_\_access-request-list-of-data |  |  | |
| \_\_\_\_SEQUENCE OF | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_Parameter for request number 1 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_Names |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x05 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Value | 0x00000000 | 4 | |
| \_\_\_\_\_\_\_\_Parameter for request number 2 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_Names |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x05 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Value | 0x00000000 | 4 | |
| \_\_\_\_\_\_\_\_Parameter for request number 3 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_Names |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x05 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Value | 0x00000000 | 4 | |
| \_\_\_\_signature-length | 0x40 | 1 | |
| \_\_\_\_signature-content | 0x85AE39D45D5C73A44070DF71C7A0976BAF60A3626E6D08D167AA7CF4AB8393B0B413E91D3E79FD6CCC93F45DB0A20BE5264B5CE9BA56A2470072784DD1A11752 | 64 | |
| \_\_\_\_mac-content | 0x430CDEEACC8297094471CF92 | 12 | |
| Response Message Structure |  |  | |
|  |  |  | |
| **Name** | **Encoded Content** | **Encoded Length** | |
| Grouping Header (general-signing) |  |  | |
| \_\_\_\_tag | 0xDF | 1 | |
| \_\_\_\_transaction-id |  |  | |
| \_\_\_\_\_\_\_\_length | 0x09 | 1 | |
| \_\_\_\_\_\_\_\_value (CRA FLAG) | 0x02 | 1 | |
| \_\_\_\_\_\_\_\_value (Originator Counter) | 0x0000000000000001 | 8 | |
| \_\_\_\_originator-system-title |  |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | 1 | |
| \_\_\_\_\_\_\_\_value | 0xFFFFFFFFFFFFFFFE | 8 | |
| \_\_\_\_recipient-system-title |  |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | 1 | |
| \_\_\_\_\_\_\_\_value | 0x123456789ABCDEF0 | 8 | |
| \_\_\_\_date-time |  |  | |
| \_\_\_\_\_\_\_\_length | 0x00 | 1 | |
| \_\_\_\_other-information |  |  | |
| \_\_\_\_\_\_\_\_Length | 0x02 | 1 | |
| \_\_\_\_\_\_\_\_Message Code | 0x00B3 | 2 | |
| \_\_\_\_content |  |  | |
| \_\_\_\_\_\_\_\_length | 0x12 | 1 | |
| access-response |  |  | |
| \_\_\_\_tag | 0xDA | 1 | |
| \_\_\_\_long-invoke-id-and-priority |  |  | |
| \_\_\_\_\_\_\_\_configuration | 0x20 | 1 | |
| \_\_\_\_\_\_\_\_invoke-id | 0x000001 | 3 | |
| \_\_\_\_date-time | 0x00 | 1 | |
| \_\_\_\_access-request-specification | 0x00 | 1 | |
| \_\_\_\_access-response-list-of-data |  |  | |
| \_\_\_\_SEQUENCE OF | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_Response for request number 1 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x00 | 1 | |
| \_\_\_\_\_\_\_\_Response for request number 2 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x00 | 1 | |
| \_\_\_\_\_\_\_\_Response for request number 3 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x00 | 1 | |
| \_\_\_\_access-response-specification |  |  | |
| \_\_\_\_SEQUENCE OF | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_Result for request number 1 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-response-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_result | 0x00 | 1 | |
| \_\_\_\_\_\_\_\_Result for request number 2 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-response-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_result | 0x00 | 1 | |
| \_\_\_\_\_\_\_\_Result for request number 3 |  |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-response-action | 0x03 | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_result | 0x00 | 1 | |
| \_\_\_\_signature-length | 0x40 | 1 | |
| \_\_\_\_signature-content | 0x0199E984CEC75DDCA7F1DDF6E53E2E67352A2BE38A4B66F8ED596606FAB983FF300CAA76DE88CED9D563A5C03E8F3A7C000780F3F2061C611E9AA0B18B460D77 | 64 | |
| ECS12 Set Change of Tenancy date on ESME | | |  | |
| Command Message Structure |  | |  | |
|  |  | |  | |
| **Name** | **Encoded Content** | | **Encoded Length** | |
| MAC Header (general-ciphering) |  | |  | |
| \_\_\_\_tag | 0xDD | | 1 | |
| \_\_\_\_contents | 0x000000000000 | | 6 | |
| \_\_\_\_ciphered-service |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x54 | | 1 | |
| \_\_\_\_\_\_\_\_security header |  | |  | |
| \_\_\_\_\_\_\_\_security control byte (SC) | 0x11 | | 1 | |
| \_\_\_\_\_\_\_\_invocation counter (IC) | 0x00000000 | | 4 | |
| Grouping Header (general-signing) |  | |  | |
| \_\_\_\_tag | 0xDF | | 1 | |
| \_\_\_\_transaction-id |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x09 | | 1 | |
| \_\_\_\_\_\_\_\_value (CRA FLAG) | 0x01 | | 1 | |
| \_\_\_\_\_\_\_\_value (Originator Counter) | 0x0000000000000002 | | 8 | |
| \_\_\_\_originator-system-title |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | | 1 | |
| \_\_\_\_\_\_\_\_value | 0x123456789ABCDEF0 | | 8 | |
| \_\_\_\_recipient-system-title |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | | 1 | |
| \_\_\_\_\_\_\_\_value | 0xFFFFFFFFFFFFFFFE | | 8 | |
| \_\_\_\_date-time |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x00 | | 1 | |
| \_\_\_\_other-information |  | |  | |
| \_\_\_\_\_\_\_\_Length | 0x02 | | 1 | |
| \_\_\_\_\_\_\_\_Message Code | 0x0022 | | 2 | |
| \_\_\_\_content |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x20 | | 1 | |
| access-request |  | |  | |
| \_\_\_\_tag | 0xD9 | | 1 | |
| \_\_\_\_long-invoke-id-and-priority |  | |  | |
| \_\_\_\_\_\_\_\_configuration | 0x20 | | 1 | |
| \_\_\_\_\_\_\_\_invoke-id | 0x000002 | | 3 | |
| \_\_\_\_date-time | 0x00 | | 1 | |
| \_\_\_\_access-request-body |  | |  | |
| \_\_\_\_access-request-specification |  | |  | |
| \_\_\_\_SEQUENCE OF | 0x01 | | 1 | |
| \_\_\_\_\_\_\_\_Request number 1 |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-request-set | 0x02 | | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_cosem-attribute-descriptor |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_class-id | 0x0001 | | 2 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_instance-id | 0x00005E2C0302 | | 6 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_attribute-id | 0x02 | | 1 | |
| \_\_\_\_access-request-list-of-data |  | |  | |
| \_\_\_\_SEQUENCE OF | 0x01 | | 1 | |
| \_\_\_\_\_\_\_\_Parameter for request number 1 |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_Names |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x09 | | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Length | 0x0C | | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Value | 0x07DF0105FF000000008000FF | | 12 | |
| \_\_\_\_signature-length | 0x00 | | 1 | |
| \_\_\_\_mac-content | 0xD748D3F87C9764E42D681C11 | | 12 | |
|  |  | |  | |
| Response Message Structure |  | |  | |
|  |  | |  | |
| **Name** | **Encoded Content** | | **Encoded Length** | |
| MAC Header (general-ciphering) |  | |  | |
| \_\_\_\_tag | 0xDD | | 1 | |
| \_\_\_\_contents | 0x000000000000 | | 6 | |
| \_\_\_\_ciphered-service |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x40 | | 1 | |
| \_\_\_\_\_\_\_\_security header |  | |  | |
| \_\_\_\_\_\_\_\_security control byte (SC) | 0x11 | | 1 | |
| \_\_\_\_\_\_\_\_invocation counter (IC) | 0x00000000 | | 4 | |
| Grouping Header (general-signing) |  | |  | |
| \_\_\_\_tag | 0xDF | | 1 | |
| \_\_\_\_transaction-id |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x09 | | 1 | |
| \_\_\_\_\_\_\_\_value (CRA FLAG) | 0x02 | | 1 | |
| \_\_\_\_\_\_\_\_value (Originator Counter) | 0x0000000000000002 | | 8 | |
| \_\_\_\_originator-system-title |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | | 1 | |
| \_\_\_\_\_\_\_\_value | 0xFFFFFFFFFFFFFFFE | | 8 | |
| \_\_\_\_recipient-system-title |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x08 | | 1 | |
| \_\_\_\_\_\_\_\_value | 0x123456789ABCDEF0 | | 8 | |
| \_\_\_\_date-time |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x00 | | 1 | |
| \_\_\_\_other-information |  | |  | |
| \_\_\_\_\_\_\_\_Length | 0x02 | | 1 | |
| \_\_\_\_\_\_\_\_Message Code | 0x0022 | | 2 | |
| \_\_\_\_content |  | |  | |
| \_\_\_\_\_\_\_\_length | 0x0C | | 1 | |
| access-response |  | |  | |
| \_\_\_\_tag | 0xDA | | 1 | |
| \_\_\_\_long-invoke-id-and-priority |  | |  | |
| \_\_\_\_\_\_\_\_configuration | 0x20 | | 1 | |
| \_\_\_\_\_\_\_\_invoke-id | 0x000002 | | 3 | |
| \_\_\_\_date-time | 0x00 | | 1 | |
| \_\_\_\_access-request-specification | 0x00 | | 1 | |
| \_\_\_\_access-response-list-of-data |  | |  | |
| \_\_\_\_SEQUENCE OF | 0x01 | | 1 | |
| \_\_\_\_\_\_\_\_Response for request number 1 |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Tag | 0x00 | | 1 | |
| \_\_\_\_access-response-specification |  | |  | |
| \_\_\_\_SEQUENCE OF | 0x01 | | 1 | |
| \_\_\_\_\_\_\_\_Result for request number 1 |  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_access-response-set | 0x02 | | 1 | |
| \_\_\_\_\_\_\_\_\_\_\_\_result | 0x00 | | 1 | |
| \_\_\_\_signature-length | 0x00 | | 1 | |
| \_\_\_\_mac-content | 0xDF27D0FE42DDED6DC5DCF3F6 | | 12 | |

# Use Cases

The Use Cases are contained in the embedded HTML document at Table 19.4. Each Use Case represents one or more interactions with a Device that make up a GBCS Command, Response and / or Alert. This Section 19 provides an overview of the repeatable content within these Use Cases.

## Use Case Title

Each Use Case Title section in Table 19.4 provides common information regarding the Use Cases that follow. Each section and its purpose is outlined in Table 19.1.

|  |  |
| --- | --- |
| **Section** | **Content** |
| Description | A textual summary of the purpose and scope of the Use Cases encompassed by the Use Case Title |
| Use Case | Details the Unique Use Case reference, the Use Case name and the Use Case Message Code (see Section 15) |
| Use Case Cross References | See Section 19.1.1 |
| Use Case Access Permissions | A summary of User Roles that can perform the Use Case. See Section 17 for Remote Party Usage Rights and Section 4.3.2.6 for Trust Anchor Cells applicable. Note that Use Cases from Unknown Remote Parties are performed using the Remote Party Role of Access Control Broker |
| SMETS / CHTS Objects applicable to Use Case | A list of SMETS / CHTS attributes and associated methods that are applicable to the Use Case. This confirms the properties required by SMETS / CHTS for the attribute/method.  This also provides information on the User Gateway Service Request invoked.  This table is sorted alphabetically by the entry in the column ‘name’ concatenated with the entry in the column ‘attribute / method’ |

Table 19.1: SMETS / CHTS content of Use Cases

### Use Case Cross Reference Section

Table 19.4 provides an overview of important information relevant to the Use Case. It has a structured table as summarised in Table 19.1.1.

| **Cross Reference** | **Possible Values** | **Notes** |
| --- | --- | --- |
| Remote Party or HAN message | HAN Only Message / Remote Party Message | Needed to identify which GBCS requirements apply. See Section 6 |
| Message Type | Command and Response / Alert with reference to the message categories in Section 6 | Needed to identify which GBCS requirements apply |
| Capable of future dated invocation? | Yes / No | Needed to identify which GBCS requirements apply. See Section 9.2 |
| Requires protection against replay? | Yes / No | Needed to identify which GBCS requirements apply. See Section 4.3.1.5 |
| SEC User Gateway Services Schedule (Service Request) Reference | [e.g. 6.20 SetDeviceConfiguration(MPxN)] | Traceability to SEC-listed DCC Service Requests |
| Read Or Update | Read, Update | Identifies whether the purpose of the Use Case is ‘Read’ or ‘Update’ |
| Response Recipient different from Command Sender | Yes or Blank | Identifies where a Response is sent to a different Remote Party than the originator of the associated Service Request. |
| Use Case Access Permissions | Supplier (C)  Supplier (NC)  Supplier prepay top up  Network Operator (C)  Network Operator (NC)  Access Control Broker (NC)  WAN Provider (C)  Security (C) | Lists which Remote Party Roles may originate the Command within the Use Case. This separates (C) critical and (NC) non critical  See Section 17 for more details |

Table 19.1.1: Allowable values for SMETS / CHTS Use Case Cross References

### Objects Applicable to Use Case Section

This section in Table 19.4 contains a ‘SMETS Objects applicable to Use Case’ table to provide traceability between SMETS functions and methods and the Use Case.

The table contains the values set out in Table 19.1.2.

|  |  |
| --- | --- |
| **Row Name** | **Meaning** |
| Mapping Table row # | Identifier of the SMETS / CHTS object’s row in the Mapping Table |
| Ref | SMETS/CHTS document location of the Attribute (prefixed by the document) |
| Name | The attribute name as specified in SMETS or CHTS |
| Attribute / Method | The attribute or method being applied to the SMETS/CHTS |
| Notes | Describes the Method being applied to the SMETS/CHTS attribute or method in the Use Case. |
| Sub Category | Specifies whether an attribute or method |
| Data Type | Details of the data type for the attribute as specified in SMETS or CHTS. |

Table 19.1.2: SMETS objects applicable to Use Case

### Pre-conditions

Pre-conditions represent conditions for which Device logic is required to ensure correct operation of commands contained within a message, on the Device. Exception conditions (such as failures) that are managed by the Protocol are not captured as Pre-conditions. Manufacturers of Devices must only enforce Pre-conditions that are stated in the Use Cases. Note that the use of Pre-conditions is minimised in favour of controls being implemented on Service User systems.

## Use Case-specific content

Each Use Case is given a unique reference and a title.

### DLMS COSEM Specific Content

Table 19.2.1 sets out the Use Case specific attributes and methods and the DLMS specific mapping.

Within any DLMS COSEM Payload, cosem-attribute-descriptors and cosem-method-descriptors, and associated fields, shall be ordered based on the contents of columns in the Mapping Table. The sort order, described by columns headings in the Mapping Table, shall be:

* first by Update Sequence;
* then by DLMS: Class;
* then by OBIS Code;
* then by Attribute (A) / Method (M); and
* then by Attribute / Method Number.

The sort order shall be ascending in all cases.

For structures, the sequence of elements within a structure shall be as defined in the Blue Book, where it is defined in the Blue Book, or as per the Mapping Table, where it is not defined in the Blue Book.

For clarity, the SMETS / CHTS table in each Use Case is sorted in this same order.

|  |  |
| --- | --- |
| **Row Name** | **Meaning** |
| Mapping table row # | Identifier of the SMETS / CHTS object’s row in the Mapping Table |
| SMETS / CHTS Ref | The section(s) with SMETS/CHTS that refer to the SMETS / CHTS name |
| SMETS / CHTS Name | The attribute name as specified in SMETS / CHTS |
| Class | Denotes the DLMS Interface Class |
| OBIS Code | defines identification codes for all data in DLMS / COSEM compliant metering equipment |
| Attribute or Method | Denotes whether the row relates to an (A)ttribute or (M)ethod |
| Attribute / Method Number | Forms part of the attribute identity. |
| Attribute / Method Name and Blue Book reference | The name given to the DLMS object |
| DLMS COSEM Data type | The data type assigned to the DLMS object |
| Constant Value | Where this field is present, this is a fixed value for the life of the Device |
| Notes | Additional useful information |

Table 19.2.1: DLMS mapping for Use Case specific attributes / methods

## ZSE specific content

Table 19.4 provides information on the ZSE commands required successfully to complete the Use Case. These must be processed in the order listed in Table 19.3.

Table 19.3 is grouped by ZSE command.

|  |  |
| --- | --- |
| **Row Name** | **Meaning** |
| Mapping table row # | Identifier of the row in the Mapping Table |
| SMETS / CHTS Ref | Identifies the SMETS / CHTS section that describes the attribute. |
| SMETS / CHTS Name | The attribute name as specified in SMETS / CHTS The method being applied to the SMETS / CHTS attribute |
| Data Type | Identifies the ZSE data type for the attribute |
| Range | The allowable value range for the attribute |
| Attribute / Value / Parameter | For ZSE read operations – the attribute or a value returned  For ZSE update operations – the attribute or parameter updated. |
| Cluster :ID | Identifies the ZSE cluster that supports the required functionality |
| Command :ID | Identifies the command and its unique identifier within the ZSE cluster that is used to read or manipulate the attribute for the purpose of the Use Case. Its ZSE identifier is included |
| Response :ID | Where specified, this identifies the Response and its unique identifier to the read or update command |

Table 19.3: ZSE specific content

## Embedded Use Cases

Table 19.4 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 19.4: Use Cases

# 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.



Table 20: Mapping Table

# 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

Command described in SMETS.

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

Asdfasdfasdf

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 Load Control Switch

A switch or other means of controlling a load on the Supply.

Boost Function

ESME functionality described in SMETS.

Business Originator ID

Shall have the meaning defined in Section 4.3.1.1.

Business Target ID

Shall have the meaning defined in Section 4.3.1.1.

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 and shall be undertaken by the Access Control Broker and not Devices.

Ciphered Information

Shall have the meaning defined in Section 8.4.

Ciphertext

An output of the Authenticated Encryption function and 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 which has a minimum resolution of 1 second.

Command

An instruction to perform a function received or sent by 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

Communications Hub

A Device complying with the CHTS.

Communications Hub Function (CHF)

The functionality in the Communications Hub specific to its operation as a bridge between the WAN Interface and the HAN Interface.

Communications Hub Technical Specifications (CHTS)

The document designated by the Secretary of State to describe the minimum capabilities of Communications Hubs installed to satisfy the roll-out licence conditions.

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, supports 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 Private Key for which the Device has 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, Type 1 Device 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 Certification Authority (DCA)

A trusted entity which issues Device Certificates.

Device Log

Data item described in SMETS and CHTS.

Device Specifications

The document set comprising SMETS (including the IHDTS, HCALCSTS and PPMIDTS), and CHTS.

Digital Signature

The information appended to a Message which is created using the sender’s Private Key, 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 sender sent 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 <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>

DLMS COSEM

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

Elliptic Curve DSA (ECDSA)

The Elliptic Curve Digital Signature Algorithm forming part of the NSA Suite B standard (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 encrypted Encrypted data items.

Entity Identifier

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

ESME

Electricity Smart Metering Equipment, as described in the 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. The Alert Code and Event Code are the same for a given Event.

Event Log

Data item described in SMETS and CHTS.

Firmware

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

Force Replace

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

Future Dated Counter

Shall have the meaning defined in Section 4.3.1.5.

Gas Proxy Function (GPF)

The Gas Proxy Function as defined in the Communications Hub Technical Specification.

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.*

GSME

Gas Smart Metering Equipment, as described in the 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)

A Type 1 Device capable of communicating with an ESME.

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.

HCALCS

HAN Connected ALCS.

HCALCSTS

The HAN Connected Auxiliary Load Control Switches (HCALCS) Technical Specification.

Highest Prior Sequence Number

Shall have the meaning defined in Section 13.3.5.3.

Home Area Network Interface (HAN Interface)

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

Immediate Execution Counter

Shall have the meaning defined in Section 4.3.1.5.

IHDTS

The In Home Display Technical Specifications.

IHD

In Home Display.

IHD Source Device

An ESME or GPF.

Immediate Execution counter

Shall have the meaning defined in Section 4.3.1.5.

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.

Instance

Shall be an Instance of one of the Messages detailed in this GBCS.

Inter-PAN

Glossary term 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 the 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 generated 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.

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 Hash Image

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 Prepayment Credit

Shall have the meaning defined in SMETS.

Maximum Vend

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; and
* Originator Counter.

Message Instance

A particular instance of a Message sent to, or received from, a Device, which is atomic in that it cannot be fully processed by the recipient without all parts of the Message being received.

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 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.

Organisation Certificate

Shall have the meaning set out in Section 12.

Originator Counter

Shall have the meaning defined in Section 4.3.1.2.

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 GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

Pending Private Key

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

Personal Data

Any information comprising Personal Data as such term is defined in the Data Protection Act 1998 at the date the GBCS is brought into force.

Pre-Payment Interface Device (PPMID)

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

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 Specification.

Polyphase Electricity Metering Equipment

Electricity metering equipment 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

Data item described in SMETS.

Prepayment Token Decimal (PPTD)

Shall have the meaning defined in Section 14.1.

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.

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 Pairs

Two mathematically related numbers that are used in Cryptographic Algorithms.

Recovery

In the context 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 the Premises and is able to either send Messages to or receive Messages from a Device within the Premises, 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

A class of Remote Party in relation to which one or more Devices is capable of storing Security Credentials.

Remote Party Role Code

An 8 bit unsigned integer which uniquely identifies a Remote Party Role. The value for each Remote Party Role shall be as defined in Section 4.3.2.4.

Replay Attack

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

Response

Sent on, or received from the User Interface or HAN Interface or any other interface containing information in response to a Command.

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

Secure Perimeter

A physical border surrounding ESME, GSME or the PPMID.

Security Credentials

Information used to identify and / or Authenticate a Device, Party or system.

Security Credential Document

A Security Credential Document shall be defined as either a:

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

Security Log

Data item described in SMETS and CHTS.

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.

SHA-256

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

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)

The document designated by the Secretary of State to describe the minimum capabilities of equipment installed to satisfy the roll-out licence conditions.

Smart Metering Home Area Network (SMHAN)

The network enabling communications between the Devices recorded within a Communications Hubs’ Device Log (as defined in CHTS).SMD Signature

A Digital Signature generated by a Device.

Supplementary Originator Counter

Shall have the meaning defined in Section 23.

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.

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.

Tamper Event

The detection of Unauthorised Physical Access or any other occurrence that has the potential to put Supply at risk and/or compromise the Integrity of a Device.

Tariff

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

Tariff Block Counter Matrix

Data item described in SMETS.

TOU

Time of Use.

Transactional Atomicity

The type and order of the constituent parts of a Command.

Transitional Change of Supplier

In the context a specific Device, the Known Remote Party whose Security Credentials are stored in relation to the Transitional Change of Supplier role.

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 (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.

Trusted Source

A source whose identity is confidently and reliably validated.

Twin Element Electricity Metering Equipment

Electricity metering equipment containing two measuring elements.

Type 1 Device

A Device, other than GSME, ESME, Communications Hub, Communications Hub Function or Gas Proxy Function, that stores and uses the Security Credentials of other Devices for the purposes of communicating with them via its HAN Interface.

Type 2 Device

A Device that does not store or use the Security Credentials of other Devices for the purposes of communicating with them via its HAN Interface.

Unauthorised

Not Authorised.

Unauthorised Physical Access

Unauthorised access to the internal components of any Device within GSME or ESME through its Secure Perimeter.

Unique Transaction Reference Number (UTRN)

A 20 decimal digit number that is used to convey a Pre-Payment Top-Up Remote Party Command to an ESME / GSME.

Unknown Remote Party (URP)

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

Upgrade Image

Shall have the meaning defined in Section 11.2.2.

Use Case

The structure, format and processing of a Message.

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 SE (ZSE)

The ZigBee Smart Energy Profile Specification as defined in the ‘Documentation Alignment’ section of this GBCS.

ZigBee Cluster Library (ZCL)

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

# Annex 1 – Additional DLMS Class

The class described below shall be supported by ESME. Extended Data (class\_id: 9000 version: 0)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute(s)** | | | | **Data type** | **Min.** | **Max.** | **Def.** |
| 1. | logical\_name | | (static) | octet-string[6] |  |  |  |
| 2. | value\_active | | (dyn.) | *CHOICE* |  |  |  |
| 3. | scaler\_unit\_active | | (dyn.) | scal\_unit\_type |  |  |  |
| 4. | value\_passive | | (static) | *CHOICE* |  |  |  |
| 5. | scaler\_unit\_passive | | (static) | scal\_unit\_type |  |  |  |
| 6. | activate\_passive\_value\_time | | (static) | octet-string |  |  |  |
| **Methods(s)** | | | | **Data type** |  | | |
| 1. | | reset(data) | | integer |  | | |
| 2. | | activate\_passive\_value(data) | | integer |  | | |

## Attribute description

|  |  |  |  |
| --- | --- | --- | --- |
| **logical\_name** | Identifies the ‘Data’ object instance | | |
| **value\_active** | Contains the data.  *CHOICE*  {  -- simple data types  null-data [0],  Boolean [3],  bit-string [4],  double-long [5],  double-long-unsigned [6],  octet-string [9],  visible-string [10],  UTF8-string [12],  Bcd [13],  integer [15],  long [16],  unsigned [17],  long-unsigned [18],  long64 [20],  long64-unsigned [21],  enum [22],  float32 [23],  float64 [24],  date-time [25],  date [26],  time [27],  -- complex data types  array [1],  structure [2],  compact-array [19]  } | The data type depends on the instantiation defined by the ‘logical name’. It has to be chosen so, that together with the logical name, an unambiguous interpretation is possible. | |
| **scaler\_unit\_active** | Provides information on the unit and the scalar for the value.  scal\_unit\_type: structure  {  scalar,  unit  }  scalar: integer  This is the exponent (to the base of 10) of the multiplication factor  unit: enum  Enumeration defining the physical unit; for more information check the Blue Book | | |
| **value\_passive** | Contains the data.  *CHOICE*  {  -- simple data types  null-data [0],  Boolean [3],  bit-string [4],  double-long [5],  double-long-unsigned [6],  octet-string [9],  visible-string [10],  UTF8-string [12],  Bcd [13],  integer [15],  long [16],  unsigned [17],  long-unsigned [18],  long64 [20],  long64-unsigned [21],  enum [22],  float32 [23],  float64 [24],  date-time [25],  date [26],  time [27],  -- complex data types  array [1],  structure [2],  compact-array [19]  }  The data type depends on the instantiation defined by the ‘logical name’. It has to be chosen so, that together with the logical name, an unambiguous interpretation is possible. | |  |
| **scaler\_unit\_passive** | Provides information on the unit and the scalar for the value.  scal\_unit\_type: structure  {  scalar,  unit  }  scalar: integer  This is the exponent (to the base of 10) of the multiplication factor  unit: enum  Enumeration defining the physical unit; for more information check the Blue Book | | |
| **activate\_passive\_value\_time** | Defines the time when the object itself calls the specific method activate\_passive\_value. A definition with ‘not specified’ notation in all fields of the attribute will deactivate this automatic activation. Partial ‘not specified’ notation in just some fields of date and time is not allowed.  octet-string, formatted as set in 4.1.6.1 for date\_time of the Blue DLMS Book | | |

## Method description

|  |  |
| --- | --- |
| **reset** | This method forces a reset of the object. By invoking this method, the value is set to the default value. The default value is an instance specific constant.  data ::= integer(0) |
| **activate\_passive\_value** | This method copies all attributes called …\_passive to the corresponding attributes called …\_active.  data ::= integer(0) |

# 

# Annex 2 - Counters and their use in transaction identification and Protection Against Replay protection - informative

Table 23 provides a summary of the Counters used in GB Smart Metering and outlines the purpose each serves in providing transaction identity, traceability and Protection Against Replay protection. These are fully detailed in Section 4.3.1 and Section 14 and are provided here as a review aid only.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Description** | **Purpose** | **Impact on Device** |
| [Remote Party] Originator Counter | The KRP or the ACB’s Originator Counter.  Originator Counters are always strictly numerically greater than any previous Originator Counter from that Message originator to the targeted Device.  Originator Counters shall not use the UTRN reserved range unless as part of a Prepayment Top Up Command. Remote Parties may choose to increment a UTRN Originator Counter separately from other Originator Counters. | The Originator Counter provides a unique Message identity (in combination with CRA Flag, sender id and recipient id).  The Originator Counter is also used as an input value for symmetric Key Derivation Functions.  The Originator Counter is used for Protection Against Replay protection. | The highest accepted value is stored as the Immediate Execution Counter, Future Dating Counter or in the UTRN Counter cache as appropriate. |
| [Device] Originator Counter | A Device’s Originator Counter  This must be strictly numerically greater than any previous Originator Counter from that Device. | The Originator Counter provides a unique Message Identity (in combination with CRA Flag, sender id and recipient id)  The Originator Counter is also used as an input value for symmetric Key Derivation Functions. | The Device shall ensure that the value it generates (e.g. for Alerts) is strictly numerically greater than any previous Originator Counter value or Supplementary Originator Counter value it has placed in any previous Message it has generated. |
| Supplementary Remote Party Counter | The Originator Counter (or reference) of an Unknown Remote Party requesting the service from the ACB. | The Supplementary Remote Party Counter supports Message identification of Responses by the URP as the originator of the service request associated to the Command. | The Supplementary Remote Party Counter is incorporated into the corresponding Response by the Device.  The Response also contains the Originator Counter of the ACB |
| Supplementary Originator Counter | The Supplementary Originator Counter is a Device generated number which is strictly numerically greater than any previous Supplementary Originator Counter or Originator Counter placed in previous Messages by the Device). This is used in response to Commands as specified in Section 4.3.1.4 (URP accessible Commands where the response contains sensitive values). | The Supplementary Originator Counter is used in a Response to a Command from an URP for the generation of symmetric keys for use in MAC creation and Encryption of sensitive values. | The Device shall ensure that the value it generates (e.g. for Alerts) is strictly numerically greater than any previous Originator Counter or Supplementary Originator Counter values it has used in any previous Message.  The Supplementary Originator Counter may be the same as Originator Counter in any given Message but this is an implementation decision). |
| Immediate Execution Counter | The Immediate Execution Counter is the last accepted Originator Counter value for commands requiring Protection Against Replay and which cannot be future dated. It is stored by the Device for each Remote Party/Command combination.  Note that only the Supplier (or for CHF the WAN Provider) can send Commands that require Protection Against Replay with the exception of the Update Security Credentials Command which can be sent by multiple roles. | The Immediate Execution Counter is used to support Protection Against Replay of Commands for immediate execution.  Where Commands are protected from Protection Against Replay then Devices will reject Commands where the Originator Counter in the Command not greater than the existing value of the Immediate Execution Counter stored on the Device. | Each Device will store an Immediate Execution Counter value for each KRP/Command- type combination. |
| Future Dated Counter | The Future Dated Counter is the last accepted Originator Counter value for commands requiring Protection Against Replay and for which invocation is future dated. It is stored by the Device for each Remote Party/Command combination.  Note that only the Supplier (or for CHF the WAN Provider) can send Commands that require Protection Against Replay for future dateable Commands. | The Future Dated Counter is used to support Protection Against Replay of future dated Commands. This is separated from the Immediate Execution Counter to accommodate latency.  Where Commands are protected from Protection Against Replay and are future dated then the Device will reject Commands where the Originator Counter in the Command is not greater than the existing value of the Future Dated Counter on the Device. | Each Device will store an Originator Counter value for each KRP/Command –type combination. |
| UTRN Counter | The UTRN Counter is detailed separately in Section 14 but a summary is included here for completeness.  The UTRN Counter must be strictly greater by one than the highest previous UTRN Counter issued for the target Device by the KRP  The UTRN Counter comprises the 32 most significant bits of the Originator Counter (this is a reserved range of Originator Counters where the least significant 32 bits are set to 0) which is included in a Pre-payment Top-Up Command (whether entered locally or received over the WAN).  The Device checks:   * that the UTRN Counter contained within a UTRN is greater than the lowest value in the UTRN Counter cache held on the Device. This ensures that a limited number of UTRNs can be executed out of sequence); and * that the UTRN Counter is not equal to any value currently held in the UTRN Counter cache, i.e. that the Pre-payment Command has not be accepted before. | The UTRN Counter provides a specific Protection Against Replay mechanism for pre-pay  Where the Command is received over the WAN, the Originator Counter (and therefore the UTRN Counter) is as contained in the WAN Prepayment Top Up Command.  If the UTRN Counter contained within a prepayment Command (whether entered locally or received over the WAN) is already in the UTRN Counter Cache or is less than the lowest value in the UTRN Counter Cache on the Device, then Devices will reject the UTRN. | Each ESME and GSME must maintain a UTRN Counter Cache as an array of the last 100 UTRN Counter entries. Where the array is full, the numerically lowest value in the array is overwritten. |
| PTUT Truncated Originator Counter | The PTUT Truncated Originator Counter is detailed separately in Section 14 but a summary is included here for completeness.  This is the UTRN Counter as carried in the locally entered 20 digit UTRN. It is the 10 least significant bits of the UTRN Counter, which is itself the 32 most significant bits of the Originator Counter for the Command.  The PTUT truncated counter is not processed in WAN received top-up commands. | The PTUT Truncated Originator provides a means for a Device to derive the Originator Counter (and therefore the UTRN Counter) for the Prepayment Top Up Command when it is entered locally (as a numeric 20 digit code).  In order to determine the UTRN Counter, the Device uses the algorithm defined in Section 14.6. | There is no additional impact to the Device as the same UTRN Counter cache is used as for the UTRN Counter. |
| Remote Party Floor Sequence Numbers | 64-bit values carried in Update Security Credentials Command, in:   * newRemotePartyFloorSeqNumber attribute; * otherRemotePartyFloorSeqNumber sequence; * newRemotePartySpecialistFloorSeqNumber attribute; and * otherRemotePartySpecialistFloorSeqNumber sequence;   The values are used to set Counters associated with the credential being updated to new values. Processing is as detailed in Section 13.3.5.10. | Remote Party Floor Sequence Numbers are of two types:   * Remote Party Sequence Numbers. Values used to set Future Dated and Immediate Execution Counters on a change of a Remote Party’s digital signing credential with which the counter is associated; and * Remote Party Specialist Sequence Numbers. Value is used to populate UTRN Counter cache following its clearance on change of the Supplier Key Agreement Prepayment credential.   Both types have a ‘new’ and ‘other’ variant. ‘new’ is used when the authorising remote party is changing its own credentials (e.g. supplier changing its own digital signing credential).  ‘other’ is used when the authorising remote party is changing the credentials of another remote party (e.g. TCoS changing supplier’s credentials).  Where – and only where - the Update Credentials Command changes the supplier entity ID (or indicates change of supplier), Counters are always reset – either to the Remote Party Sequence number indicated or to zero where the attribute is absent . Otherwise, Counters are only reset where the Remote Party Sequence Number is present. |  |
| Encryption Originator Counter | The Counter value used for the purposes of encryption (see Section 8.3) for Responses and Alerts sent from the Device. | This is either the Supplementary Originator Counter in the case that this is to be included in the message (e.g. for an Unknown Remote Party) or the [Device] Originator Counter in all other instances. | The Device re-uses either the Supplementary Originator Counter or [Device] Originator Counter. |

Table 23: Counters and their use in transaction identification and Protection Against Replay protection

# Annex 3 – ASN.1 modules - informative

This Annex collates all ASN.1 used in this GBCS. Please note that this is a duplicate; the authoritative content remains as documented in the appropriate section.

SetTime DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the period within which the Communications Hub’s time must lie

-- if this Command is successfully to set time

validityIntervalStart GeneralizedTime,

validityIntervalEnd GeneralizedTime

}

ResponsePayload ::= SEQUENCE

{

-- Specify the Device’s now current time

deviceTime GeneralizedTime,

-- Specify the Device’s now current Time Status

deviceTimeStatus DeviceTimeStatus

}

DeviceTimeStatus ::= INTEGER

{

reliable (0),

invalid (1),

unreliable (2)

}

END

ActivateFirmware DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the hash of the Manufacturer Image to be activated

manufacturerImageHash OCTET STRING,

-- the Originator Counter as in the Grouping Header of the Command

originatorCounter INTEGER (0..9223372036854775807),

-- the date-time at which the Command is to execute, if future dated

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

}

AlertPayload ::= SEQUENCE

{

-- specify the Alert Code

alertCode INTEGER(0..4294967295),

-- specify the date-time of execution

executionDateTime GeneralizedTime,

-- the Originator Counter as in the Grouping Header of the corresponding Command

originatorCounter INTEGER (0..9223372036854775807),

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

executionOutcome ExecutionOutcome

}

ExecutionOutcome ::= SEQUENCE

{

-- Specify whether the activation was successful or not

activateImageResponseCode ActivateImageResponseCode,

-- Specify the Device’s now current firmware version

firmwareVersion OCTET STRING

}

ActivateImageResponseCode::= INTEGER

{

success (0),

noImageHeld (1),

hashMismatch (2),

activationFailure (3)

}

END

ProvideSecurityCredentialDetails DEFINITIONS ::= BEGIN

Command ::= SEQUENCE

{

-- Identify which of the Public Keys on the Device is to be used in verifying the Signature or MAC

-- (so defining the nature of the verification by way of the KeyUsage parameter held on the

-- Device for the Public Key so identified).

authorisingRemotePartyTACellIdentifier TrustAnchorCellIdentifier,

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

remotePartyRolesCredentialsRequired SEQUENCE OF RemotePartyRole

}

Response ::= SEQUENCE OF RemotePartyDetails

RemotePartyDetails ::= SEQUENCE

{

-- Which Remote Party do these details relate to?

remotePartyRole RemotePartyRole,

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

statusCode StatusCode,

-- What is the current Update Security Credentials Protection Against Replay number on the Device for this role, where there is such a number for this role?

currentSeqNumber SeqNumber OPTIONAL,

-- What are the details held on the Device for each of the Cells related to this role? The list shall have between one and

-- three entries (e.g. there will be one if role is transitional change of supplier; there may be three if role is supplier)

trustAnchorCellsDetails SEQUENCE OF TrustAnchorCellContents OPTIONAL

}

SeqNumber ::= INTEGER (0..9223372036854775807)

TrustAnchorCellContents ::= SEQUENCE

{

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. This will be absent except where used to refer to the Supplier Key Agreement Key.

-- This Key is used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions.

trustAnchorCellUsage CellUsage DEFAULT management,

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

existingSubjectUniqueID OCTET STRING,

-- The APKI requirements mean that KeyIdentifier attributes will all be 8 byte SHA-1 Hashes.

-- existingSubjectKeyIdentifier shall be set accordingly based on the contents of the Trust Anchor Cell

existingSubjectKeyIdentifier OCTET STRING

}

TrustAnchorCellIdentifier ::= SEQUENCE

{

-- Which Remote Party Role does this Cell relate to?

trustAnchorCellRemotePartyRole RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. This may be absent except where use to refer to the Supplier Key

-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up transactions

trustAnchorCellUsage CellUsage DEFAULT management

}

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

RemotePartyRole ::= INTEGER

{

-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake

-- processing. Note that most Devices will only support processing in relation to a subset of these.

root (0),

recovery (1),

supplier (2),

networkOperator (3),

accessControlBroker (4),

transitionalCoS (5),

wanProvider (6),

issuingAuthority (7), -- Devices will receive such Certificates but they do not

-- need to store them over an extended period

-- The ‘other’ RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from

-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid

-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is bought in to operation

other (127)

}

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

KeyUsage ::= BIT STRING

{

-- Define valid uses of Public Keys.

digitalSignature (0),

contentCommitment (1), -- not valid for GBCS compliant transactions

keyEncipherment (2), -- not valid for GBCS compliant transactions

dataEncipherment (3),

keyAgreement (4),

keyCertSign (5),

cRLSign (6),

encipherOnly (7),

decipherOnly (8) -- not valid for GBCS compliant transactions

}

-- The GBCS only allows for a constrained set of Trust Anchor Cell operations and so the list of possible outcomes

-- is more limited than in IETF RFC 5934. The list below is that more constrained subset

StatusCode ::= ENUMERATED {

success (0),

-- trustAnchorNotFound indicates that details of a trust anchor were requested, but the referenced trust anchor

-- is not represented on the Device

trustAnchorNotFound (25),

other (127)}

END

UpdateSecurityCredentials DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- Provide details to allow the Device to identify the Remote Party Role authorising

-- this Command, check whether the rest of the payload is allowable, prevent replay attacks

-- and allow counters / counter caches on the Device to be reset, if the Command changes the Remote Party

-- in control.

-- The Remote Party authorising the Command is that party which generated the KRP Signature (or the Access Control Broker

-- if there is no KRP Signature)

authorisingRemotePartyControl AuthorisingRemotePartyControl,

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

replacements SEQUENCE OF TrustAnchorReplacement,

-- Provide the certificates needed to undertake Certification Path Validation of the new

-- end entity certificate against the root public key held on the Device. The number of these may be less

-- than the number of replacement certificates (e.g. a supplier may replace all of its certificates but

-- may only need to supply one Certification Authority Certificate to link them all back to the root public

-- key as currently stored on the Device.

certificationPathCertificates SEQUENCE OF Certificate,

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

executionDateTime GeneralizedTime OPTIONAL

}

ResponsePayload ::= SEQUENCE

{

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

commandAccepted NULL,

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

executionOutcome ExecutionOutcome OPTIONAL

}

AlertPayload ::= SEQUENCE

{

-- specify the Alert Code

alertCode INTEGER(0..4294967295),

-- specify the date-time of execution

executionDateTime GeneralizedTime,

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

executionOutcome ExecutionOutcome

}

ExecutionOutcome ::= SEQUENCE

{

-- Provide details of the corresponding Command that may not be in the standard GBCS message header. Specifically the

-- mode in which the Command was invoked, the Originator Counter in the original Command and the resulting changes to any

-- replay counters held on the Device

authorisingRemotePartySeqNumber SeqNumber,

credentialsReplacementMode CredentialsReplacementMode,

remotePartySeqNumberChanges SEQUENCE OF RemotePartySeqNumberChange,

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

replacementOutcomes SEQUENCE OF ReplacementOutcome

}

AuthorisingRemotePartyControl ::= SEQUENCE

{

-- Specify the replacement mode so that the Device can check that the Remote Party Role is allowed to

-- authorise this type of replacement and that all replacements in the payload are allowed within this

-- replacement mode

credentialsReplacementMode CredentialsReplacementMode,

-- Only if credentialsReplacementMode = anyByContingency, provide the symmetric key to decrypt

-- the Contingency Public Key in the (root, digitalSignature, management) Trust Anchor Cell

plaintextSymmetricKey [0] IMPLICIT OCTET STRING OPTIONAL,

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

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

-- Identify which of the Public Keys on the Device is to be used in checking KRP Signature

-- ‘authorisingRemotePartyTACellIdentifier’ can only be omitted when

-- the access control broker is updating its own credentials. 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 newTrustAnchorFloorSeqNumber must be included

-- and will be the value used to prevent replay of Update Security Credentials Commands for the

-- new controlling Remote Party.

newRemotePartyFloorSeqNumber [4] IMPLICIT SeqNumber OPTIONAL,

-- Some Commands on the Device may use a different Originator Counter sequence for Protection Against Replay. At this

-- version of the GBCS, the only example is the Prepayment Top Up Command on ESME and GSME. The

-- SpecialistSeqNumber structure allows such Counters to also be reset on change of control.

newRemotePartySpecialistFloorSeqNumber [5] IMPLICIT SEQUENCE OF SpecialistSeqNumber OPTIONAL,

-- In some cases, one party acting in one Remote Party Role may be replacing certificates for a different Remote Party Role.

-- In some cases, sequence 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..9223372036854775807)

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 subjectUniqueID 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 subjectUniqueID in the subject field of the certificate in this TrustAnchorReplacement

replacingSubjectUniqueID OCTET STRING,

-- The subjectKeyIdentifier in the certificate in this TrustAnchorReplacement

replacingSubjectKeyIdentifier OCTET STRING

}

TrustAnchorCellIdentifier ::= SEQUENCE

{

-- Which Remote Party Role does this Cell relate to?

trustAnchorCellRemotePartyRole RemotePartyRole,

-- To what cryptographic use can the Public Key in this Cell be put? Some Remote Party Roles

-- (e.g. supplier) can have more than one Public Key on a Device and each one would only have

-- a single cryptographic use.

trustAnchorCellKeyUsage KeyUsage,

-- trustAnchorCellUsage is to allow for multiple Public Keys of the same keyUsage for the same Remote

-- Party Role. It will be absent except where used to refer to the Supplier Key

-- Agreement Key used solely in relation to validating Supplier generated MACs on Prepayment Top Up

-- transactions

trustAnchorCellUsage CellUsage DEFAULT management

}

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

RemotePartyRole ::= INTEGER

{

-- Define the full set of Remote Party Roles in relation to which a Device may need to undertake

-- processing. Note that most Devices will only support a subset of these.

root (0),

recovery (1),

supplier (2),

networkOperator (3),

accessControlBroker (4),

transitionalCoS (5),

wanProvider (6),

issuingAuthority (7), -- Devices will receive such Certificates but they do not need to store

-- them over an extended period

-- The ‘other’ RemotePartyRole is for a party whose role does not allow it to invoke any Device function apart from

-- UpdateSecurityCredentials. This is to allow for Device functionality to be locked out of usage until a valid

-- Remote Party can be identified e.g. where roles cannot be fixed until a Device is brought in to operation

other (127)

}

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

KeyUsage ::= BIT STRING

{

-- Define valid uses of Public Keys held by Devices in their Trust Anchor Cells.

digitalSignature (0),

contentCommitment (1), -- not valid for GBCS compliant transactions

keyEncipherment (2), -- not valid for GBCS compliant transactions

dataEncipherment (3), -- not valid for GBCS compliant transactions

keyAgreement (4),

keyCertSign (5),

cRLSign (6),

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

CredentialsReplacementMode ::= INTEGER

{

-- Define the valid combinations as to which Remote Party Roles can replace which kinds of Trust Anchors.

-- Normal operational replacement modes

rootBySupplier (0),

rootByWanProvider (1),

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),

-- contingencyPublicKeyDecrypt indicates that the update could not be processed because an error occurred while

-- decrypting the contingency public key.

contingencyPublicKeyDecrypt (22),

-- trustAnchorNotFound indicates that a change to a trust anchor was requested, but the referenced trust anchor

-- is not represented in the Trust Anchor Cell.

trustAnchorNotFound (25),

-- 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

IssueSecurityCredentials DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the keyUsage to which the generated key-pair will be put, if subsequently authorised

keyUsage KeyUsage

}

ResponsePayload ::= CHOICE

{

-- if the Command was successful, provide the generated Certification Request. CertificationRequest shall

-- be as defined in ASN.1 by IETF RFC 5912. For reference, it is in the section headed ‘ASN.1 Module for RFC 2986’

certificationRequest CertificationRequest,

-- if the Command was unsuccessful, detail the failure

issueCredentialsResponseCode IssueCredentialsResponseCode

}

-- KeyUsage is only repeated here for ease of reference. It is defined in IETF 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), -- not valid for this Use Case

cRLSign (6), -- not valid for this Use Case

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

IssueCredentialsResponseCode::= INTEGER

{

invalidKeyUsage (1),

keyPairGenerationFailed (2),

cRProductionFailed (3)

}

END

UpdateDeviceCertificateonDevice DEFINITIONS ::= BEGIN

CommandPayload ::= Certificate

-- provide the certificate which the Device is to store

-- the ASN.1 specification of certificate shall be as defined in IETF RFC 5912 for IETF RFC 5280

ResponsePayload ::= UpdateDeviceCertResponseCode

-- if the Command was unsuccessful, detail the failure; otherwise respond with success

UpdateDeviceCertResponseCode::= INTEGER

{

success (0),

invalidCertificate (1),

wrongDeviceIdentity (2),

invalidKeyUsage (3),

noCorrespondingKeyPairGenerated (4),

wrongPublicKey (5),

certificateStorageFailed (6),

privateKeyChangeFailed (7)

}

END

ProvideDeviceCertificateFromDevice DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify the KeyUsage of the Certificate to be returned

keyUsage KeyUsage

}

ResponsePayload ::= CHOICE

{

-- if the Command was successful, provide the certificate

certificate Certificate,

-- if the Command was unsuccessful, detail the failure

provideDeviceCertResponseCode ProvideDeviceCertResponseCode

}

-- KeyUsage is only repeated here for ease of reference. 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), -- not valid for this Use Case

cRLSign (6), -- not valid for this Use Case

encipherOnly (7), -- not valid for GBCS compliant transactions

decipherOnly (8) -- not valid for GBCS compliant transactions

}

ProvideDeviceCertResponseCode::= INTEGER

{

invalidKeyUsage (1),

noCertificateHeld (2),

certificateRetrievalFailure (3)

}

END

JoinDevice DEFINITIONS ::= BEGIN

CommandPayload ::= SEQUENCE

{

-- specify which type of joining is being authorised and,

-- for Method A Joins, the role the Device is to play

joinMethodAndRole JoinMethodAndRole,

-- specify the Entity Identifier of the Device which is to be Joined with

otherDeviceEntityIdentifier OCTET STRING,

-- specify the DeviceType of that other Device

otherDeviceType DeviceType,

-- provide the other Device’s Key Agreement certificate, if and only if this

-- is a join between a gSME and a type1PrepaymentInterfaceDevice.

-- Certificate shall be as defined in IETF RFC 5912

otherDeviceCertificate Certificate OPTIONAL

}

-- detail whether the Command successful executed or, if it didn’t,

-- what the failure reason was

ResponsePayload ::= JoinResponseCode

JoinMethodAndRole ::= INTEGER

{

-- methodB is to be used where the other Device is a Type 2 Device or GPF.

-- methodC is used where the Devices involved are a GSME and a PPMID.

-- methodA is used otherwise.

-- methodAInitiator is used where the Device this Command is targeted at

-- should initiate the Key Agreement process

-- methodAResponder is used where the Device this Command is targeted at

-- should respond in the Key Agreement process, but shall not initiate it

methodAInitiator (0),

methodAResponder (1),

methodB (2),

methodC (3)

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

JoinResponseCode::= INTEGER

{

success (0),

invalidMessageCodeForJoinMethodAndRole (1),

invalidJoinMethodAndRole (2),

incompatibleWithExistingEntry (3),

deviceLogFull (4),

writeFailure (5),

keyAgreementNoResources (6),

keyAgreementUnknownIssuer (7),

keyAgreementUnsupportedSuite (8),

keyAgreementBadMessage (9),

keyAgreementBadKeyConfirm (10),

invalidOrMissingCertificate (11)

}

END

UnjoinDevice DEFINITIONS ::= BEGIN

CommandPayload ::= OtherDeviceEntityIdentifier

-- specify the Entity Identifier of the Device for which authorisation

-- is to be removed

OtherDeviceEntityIdentifier ::= OCTET STRING

ResponsePayload ::= UnjoinResponseCode

-- detail whether the Command successful executed or, if it didn’t,

-- what the failure reason was

UnjoinResponseCode::= INTEGER

{

success (0),

otherDeviceNotInDeviceLog (1),

otherFailure (2)

}

END

ReadDeviceLog DEFINITIONS ::= BEGIN

CommandPayload ::= NULL

ResponsePayload ::= SEQUENCE

{

-- detail whether the Command successful

readLogResponseCode ReadLogResponseCode,

-- if it was, return the Log Entries

deviceLogEntries SEQUENCE OF DeviceLogEntry OPTIONAL

}

DeviceLogEntry ::= SEQUENCE

{

deviceIndentifier OCTET STRING,

deviceType DeviceType

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

ReadLogResponseCode::= INTEGER

{

success (0),

readFailure (1)

}

END

GPFDeviceLog DEFINITIONS ::= BEGIN

BackupAlertPayload ::= SEQUENCE

{

-- specify the Alert Code

alertCode INTEGER(0..4294967295),

-- specify the date-time of the backup

backupDateTime GeneralizedTime,

-- detail the entries in the Device Log now that the change has been made

deviceLogEntries SEQUENCE OF DeviceLogEntry

}

RestoreCommandPayload ::= SEQUENCE

{

-- list the Device Log entries that are to be added

deviceLogEntries SEQUENCE OF DeviceLogEntry

}

DeviceLogEntry ::= SEQUENCE

{

-- specify the Entity Identifier of the Device

deviceEntityIdentifier OCTET STRING,

-- specify the DeviceType of that Device

deviceType DeviceType

}

RestoreResponsePayload ::= SEQUENCE

{

-- for each DeviceLog Entry, detail whether the Command successfully executed or, if it didn’t, what the failure reason was

restoreOutcomes SEQUENCE OF RestoreOutcome

}

RestoreOutcome ::= SEQUENCE

{

deviceLogEntry DeviceLogEntry,

joinResponseCode JoinResponseCode

}

DeviceType ::= INTEGER

{

gSME (0),

eSME (1),

communicationsHubCommunicationsHubFunction (2),

communicationsHubGasProxyFunction (3),

type1HANConnectedAuxiliaryLoadControlSwitch (4),

type1PrepaymentInterfaceDevice (5),

type2 (6)

}

JoinResponseCode::= INTEGER

{

success (0),

invalidMessageCodeForJoinMethodAndRole (1),

invalidJoinMethodAndRole (2),

incompatibleWithExistingEntry (3),

deviceLogFull (4),

writeFailure (5),

keyAgreementNoResources (6),

keyAgreementUnknownIssuer (7),

keyAgreementUnsupportedSuite (8),

keyAgreementBadMessage (9),

keyAgreementBadKeyConfirm (10),

invalidOrMissingCertificate (11)

}

END

# Annex 4 - Use of ZigBee in GBCS - informative

## Purpose

This annex briefly summarises where the GBCS:

* requires the use of ZigBee, specifically where it uses parts of the ZigBee specification, or takes an approach which aligns to the ZigBee specification; and
* does not allow the use of ZigBee / requires its use to be modified, specifically where it:
  + - * mandates a solution that is not ZigBee derived but where there is ZigBee equivalent in the specification;
      * specifies an approach that is derived from ZigBee but the approach is not part of the ZigBee specification; and
      * specifies an approach that uses parts of the ZigBee but varies from it on specific points.

The document is based on the content of ZigBee referenced in the GBCS.

## GBCS requirements to use ZigBee

For all Smart Metering Equipment, the GBCS requires the implementation of functionality equivalent to a subset of the ZigBee standard, including all mandatory components required to achieve ZigBee certification.

GBCS and the ZigBee standard specify all items that need to be certified. GBCS does not require ZSE certification for non-standard ZSE features in Smart Metering Equipment.

## GBCS requirements not to use ZigBee / vary from it

For GSME and PPMID, the GBCS requires functionality equivalent to ZigBee clusters, but transports GBZ payloads using ZigBee tunneling.

GBCS does not require ZSE certification for non-ZSE features in GBCS. End-to-end Messages sent with ZigBee (ZSE / ZCL) commands are referred to as GBZ.

# Annex 5 - Use of DLMS COSEM in GBCS - informative

## Purpose

This document briefly summarises where the GBCS:

* requires the use of DLMS COSEM: specifically where it uses parts of the DLMS COSEM specification, or takes an approach which aligns to the DLMS COSEM specification; and
* does not allow the use of DLMS COSEM / requires its use to be modified: specifically where it:
  + - * Mandates a solution that is not DLMS COSEM derived but where there are DLMS COSEM equivalent in the specification;
      * Specifies an approach that is derived from DLMS COSEM but the approach is not part of the DLMS COSEM specification; or
      * Specifies an approach that uses parts of the DLMS COSEM but varies from it on specific points.

The document is based on the expected contents of the Blue and Green Book versions scheduled to be published in June / July 2014.

## GBCS requirements to use DLMS COSEM

For ESME and CHF, the GBCS requires the implementation of functionality equivalent to a subset of the Blue Book Classes. It does not require functionality equivalent to other Blue Book classes.

For all Devices, GBCS requires a set of cryptographic primitives that align to DLMS Security Suite 1, and so all Devices will need functionality which is in line with the cryptography related parts of the Green Book (for both GBCS and DLMS COSEM, these requirements are NSA Suite B derived).

GBCS requires that all Devices use X.509 Certificates and Certification Requests with a number of optional elements being used / barred. These requirements align with the Green Book requirements (which are X.509 derived).

For ESME and CHF, the GBCS requires functionality equivalent to Green Book access and data notification services.

For all Devices, the GBCS requires functionality equivalent to the Green Book’s general ciphering and general signing services.

For all Devices, the GBCS requires functionality equivalent to the Green Book’s authenticated encryption and decryption.

For all Devices, the GBCS requires corresponding alignment with DLMS COSEM’s ASN.1 schema and its A-XDR encoding.

## GBCS requirements not to use DLMS COSEM / vary from it

### Mandates a solution that is not DLMS COSEM derived but where there are DLMS COSEM equivalent in the specification

For Devices other than ESME and CHF, the GBCS requires functionality equivalent to DLMS COSEM classes but does not use DLMS COSEM classes (rather ZSE / ASN.1 is used).

For Devices other than ESME and CHF, the GBCS requires support for equivalents of the Green Book’s access and data notification services, but uses ZSE or ASN.1 specific structures.

For all Devices, the GBCS requires that the management of X.509 certificates and Device’s key pairs is undertaken using ASN.1 messages derived from the IETF’s TAMP RFCs.

Over the HAN, the GBCS mandates, for all Devices, the use of ZSE for the communication layers below the DLMS/COSEM Application Layer and so does not allow the use of the equivalent Green Book communication profiles. (WAN transport is outside GBCS scope).

For ESME and GSME, distribution of firmware is through the ZSE OTA mechanism.

### Specifies an approach that is derived from DLMS COSEM but the approach is not part of the specification

GBCS specifies the use of a Class 9000 object. This is not in the Blue Book

Although not yet incorporated, the proposals to use the DLMS Blocking Service would see DLMS type structures being used in a way not specified in the DLMS COSEM specification.

Pairwise key agreement between GSME and PPMID uses a structure similar to DLMS COSEM’s message structure, but that is not part of the DLMS COSEM specification.

### Specifies an approach that uses parts of the DLMS COSEM but varies from it on specific points

For all bar Type 2 Devices, the DLMS general-signing structure is used in all remote party messages but the signature field is not populated in messages that do not require a signature (i.e. those that are not critical).

For all bar Type 2 Devices, the GBCS uses the general-ciphering structure for remote party Messages that require a MAC. The GBCS leaves most values empty in the header part of the structure (these value are either in the general-signing structure or are already known to the meter). Correspondingly, the values used in the OtherInput field of the KDF at Section 9.2.3.4.6.5 of the Green Book are those taken from the general-signing structure, rather than the corresponding fields in the general-ciphering structure.

For ESME and GSME, the GBCS specifies particular, additional interpretation of parameters within the DLMS COSEM Class 8 object (Clock).

# Annex 6 - Deducing the UTRN Counter from the Truncated UTRN Counter – informative

This annex provides a worked example of the calculation described in Section 14.6.3.1.5. The calculation uses the 10-bit Truncated UTRN Counter received with the prepay 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 [[37]](#footnote-37))  x = 812 - 512 | 100101100 | 300 |
| 6 | Calculate p + 29 (Call this variable, *y*)  y = 812 + 512 | 10100101100 | 1324 |
| 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   300 < 812 < 1324, 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

Crown copyright 2014

Department of Energy & Climate Change

3 Whitehall Place

London SW1A 2AW

www.gov.uk/decc

1. This document also includes the HAN Connected Auxiliary Load Control Switches (HCALCS) Technical Specification, the Prepayment Interface Device (PPMID) Technical Specification (PPMIDTS), and the In Home Display (IHD) Technical Specification (IHDTS) [↑](#footnote-ref-1)
2. <http://www.itu.int/rec/T-REC-X.680-X.693-200811-I/en> [↑](#footnote-ref-2)
3. <http://tools.ietf.org/html/rfc5912> [↑](#footnote-ref-3)
4. IEC 61334-6 [↑](#footnote-ref-4)
5. <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf> [↑](#footnote-ref-5)
6. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf> [↑](#footnote-ref-6)
7. Supplier and Network Operator credentials on the Communications Hub (Gas Proxy) relate to the supply of gas only. These Trust Anchor Cells on a Communications Hub are still required and valid where there is no GSME connected to the SMHAN, but the stores should be populated with Access Control Broker certificates (so ensuring the Gas Proxy functionality, apart from Update Security Credentials, is inoperable) [↑](#footnote-ref-7)
8. <http://datatracker.ietf.org/doc/rfc5280/> [↑](#footnote-ref-8)
9. <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf> [↑](#footnote-ref-9)
10. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> [↑](#footnote-ref-10)
11. <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf> [↑](#footnote-ref-11)
12. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf> [↑](#footnote-ref-12)
13. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf> [↑](#footnote-ref-13)
14. See Mapping Table for identification of Variant Messages [↑](#footnote-ref-14)
15. <http://tools.ietf.org/html/rfc1700> [↑](#footnote-ref-15)
16. See Green Book. [↑](#footnote-ref-16)
17. Terms defined within this section are only used within this section, and therefore not included in the Glossary (Section 21). [↑](#footnote-ref-17)
18. See Section 6.10.3 of ZigBee Document 09-5264-19 [↑](#footnote-ref-18)
19. As defined in Section 6.10 of ZigBee Document 09-5264-19 [↑](#footnote-ref-19)
20. As defined in Sections 6.10.10 and 6.8.4 of ZigBee Document 09-5264-19 [↑](#footnote-ref-20)
21. ZigBee Document 095264 [↑](#footnote-ref-21)
22. <http://tools.ietf.org/html/rfc5759> [↑](#footnote-ref-22)
23. <http://tools.ietf.org/html/rfc5480> [↑](#footnote-ref-23)
24. The Contingency Key is a second public key held in the Root Certificate (and protected with an encryption key). Its sole purpose is to allow the validation of a specific command that allows direct replacement of the Root Trust Anchor. The command (an Apex Trust Anchor Update message) is signed with a private key (used once only, and only to sign this message) that only the second public key (known as the Contingency Key) can verify and therefore authorise action of. [↑](#footnote-ref-24)
25. Housley, R., Ashmore, S., and C. Wallace, ‘Trust Anchor Management Protocol (TAMP)’, RFC 5934, August 2010. <https://tools.ietf.org/html/rfc5934> [↑](#footnote-ref-25)
26. <http://tools.ietf.org/html/rfc4108> [↑](#footnote-ref-26)
27. <https://www.itu.int/rec/T-REC-X.690/en> [↑](#footnote-ref-27)
28. <https://www.itu.int/rec/T-REC-X.680/en> [↑](#footnote-ref-28)
29. <https://tools.ietf.org/html/rfc2986> [↑](#footnote-ref-29)
30. <https://tools.ietf.org/html/rfc5967> [↑](#footnote-ref-30)
31. This is unrelated to the ZSE meaning of ‘joining’ [↑](#footnote-ref-31)
32. The shared secret between the Communications Hub and the Type 2 Device / GSME established when the Device joined the HAN shall be used by the GPF to authenticate with the Device. [↑](#footnote-ref-32)
33. To avoid duplication of specification, the Use Cases here are grouped together, and the standard Use Case cross reference table is not used. [↑](#footnote-ref-33)
34. As defined in the ZSE specification [↑](#footnote-ref-34)
35. This derivation places a practical limit on the maximum increment between issued sequentially UTRN Counters. An increment of greater than (29 -1) between a UTRN Counter and the next one issued will cause this derivation to be inaccurate [↑](#footnote-ref-35)
36. See: (1) Verhoeff, J. (1969). *Error Detecting Decimal Codes (Tract 29)*. The Mathematical Centre, Amsterdam. [doi](http://en.wikipedia.org/wiki/Digital_object_identifier):[10.1002/zamm.19710510323](http://dx.doi.org/10.1002%2Fzamm.19710510323)., (2) Kirtland, Joseph (2001). [*Identification Numbers and Check Digit Schemes*](http://books.google.com/books?id=npTxORxmLosC&pg=PA121&lpg=PA121&dq=verhoeff+check+digit&source=bl&ots=ovegXzJqwI&sig=YA10aVVcv7Uw-hRGuxX6LO7ai04&hl=en&ei=ONpXTqi_EcfSiAKtotWSCQ&sa=X&oi=book_result&ct=result&resnum=6&ved=0CDYQ6AEwBTgU#v=onepage&q=verhoeff%20check%20digit&f=false). Mathematical Association of America. p. 153. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-88385-720-0](http://en.wikipedia.org/wiki/Special:BookSources/0-88385-720-0). Retrieved August 26, 2011. (3) Salomon, David (2005). [*Coding for Data and Computer Communications*](http://books.google.com/books?id=A88kvYwIVu0C&pg=PA57&lpg=PA57&dq=verhoeff+check+digit&source=bl&ots=yEqVwTaslG&sig=t4whVVHrJUJ7x8eWgIsarvD3hh8&hl=en&ei=WNpXTsXdHLPSiAKm_LimCQ&sa=X&oi=book_result&ct=result&resnum=7&ved=0CDwQ6AEwBjge#v=onepage&q=verhoeff%20check%20digit&f=false). Springer. p. 56. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-387-21245-0](http://en.wikipedia.org/wiki/Special:BookSources/0-387-21245-0). Retrieved August 26, 2011 [↑](#footnote-ref-36)
37. 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-37)