Department of Energy & Climate Change

Smart Metering Implementation Programme

Communications Hub Technical Specifications

Version 1.46

Draft document V1.46 28 November 2014

Department of Energy and Climate Change
3 Whitehall Place
London
SW1A 2AW

Telephone: 0300 068 4000
Website: www.gov.uk/decc

For further information on this document, contact:
Smart Metering Implementation Programme
Department of Energy and Climate Change
3 Whitehall Place
London
SW1A 2AW
Telephone: 0300 068 6083
Email: mailto: smartmetering@decc.gsi.gov.uk

The document can be found on DECC's website: www.gov.uk/decc

Published by the Department of Energy and Climate Change.

1 Table of Contents

1 Table of Contents 3
2 Revision History 4
3 Introduction 6
4 Technical Specifications 7
4.1 Overview 7
4.2 Testing and Certification Requirements 7
4.2.1 Conformance with the CHTS 7
4.2.2 Conformance with the Great Britain Companion Specifications 7
4.2.3 Conformance with the Commercial Product Assurance Security Characteristic for GB Smart Metering 7
4.2.4 Interoperability with the Data and Communications Company Systems 7
4.3 Physical Requirements 8
4.4 Functional Requirements 9
4.4.1 Clock 9
4.4.2 Communications 9
4.4.3 Data Storage 12
4.4.4 Buffering 13
4.4.5 Monitoring 13
4.4.6 Security 13
4.4.7 Inter-PAN Connection 16
4.5 Interface Requirements 17
4.5.1 CHF Interface Commands 17
4.5.2 Receipt of Information by the GPF via the HAN Interface 19
4.5.3 Type 1 Device and Type 2 Device Information Provision from the GPF via the HAN Interface 19
4.5.4 GPF Interface Commands 20
4.6 Data Requirements 21
4.6.1 Constant Data 21
4.6.2 Configuration Data 22
4.6.3 Operational Data 22
5 Glossary 24

2 Revision History

Version	Date	Status	Change Summary
1.46	28 November 14	Draft	Draft version to align with GBCS v0.8.1. Changes include removal of Data Restriction Flag, and specification of number of Devices to be supported by GPF / CHF
1.45	29 July 14	Draft	Draft version clarifying Random Number Generator requirements.
1.45	10 July 14	Draft	Draft version incorporating comments on the changes proposed in 1.43 and 1.44.
1.44	03 July 14	Draft	Draft version incorporating comments on the changes proposed in 1.43.
1.43	25 June 14	Draft	Draft version for informal TBDG review incorporating changes proposed in email to TBDG members on 10 June.
1.42	28 May 14	Draft	Draft version incorporating comments on the changes proposed in 1.41.
1.41	30 April 14	Draft	Draft version incorporating changes emerging following GBCS review, previous TBDG review and CPA review.
1.4	23-Dec-13	Draft	Draft version incorporating changes made following internal review and previously suggested revisions.
1.32	13-Sep-13	Draft	Baseline draft
1.31	6-Sep-13	Draft	Incorporating further stakeholder comments
1.30	23-Aug-13	Draft	Incorporating legal review comments, internal work on GBCS and clarifications on security credentials.
1.21	05-Jun-13	Draft	Pre-Wragge review
1.20	16-Apr-13	Draft	For issue with Final ISFT.
1.19	15-Apr-13	Draft	Updates following regulatory review. Includes restructuring of the document, and making more explicit the difference between the Comms Hub functionality and the Gas Proxy.
1.18	27-Mar-13	Draft	Includes comments from internal review
1.17	25-Mar-13	Draft	Includes comments from review with SDAG, CSP bidders and BEAMA

Version	Date	Status	Change Summary
1.16	12-Feb-13	Draft	Draft for issue with ISFT Includes comments from internal review and feedback from BEAMA
1.14	08-Feb-13	Draft	Draft for review
1.12	05-Feb-13	Draft	Draft for review
1.10	09-Jan-13	Draft	Draft for review
0.90	13-Sep-12	Draft	Draft for issue with ISDS Included comments from internal review, added missing content, removed placeholders
0.86e	11-Sep-12	Draft	Added placeholders for content to cover monitoring, historic gas calculations, buffering, network coordination and routing
0.86d	10-Sep-12	Draft	Restructured as per SMETS
0.86	07-Sep-12	Draft	Internal Team Review for ISDS issue
0.81	29-Aug-12	Draft	Updated following SSAG review comments and establishment of new drafting principles
0.8	17-Aug-12	Draft	Updated following issue clarification
0.75	08-Aug-12	Draft	Updated following preliminary review
0.72	02-Aug-12	Draft	Draft for review
0.6	Jul-12	Draft	Draft sent out for external review

3 Introduction

The requirement on the Data and Communications Company (DCC) to provide Communications Hubs that comply with these Communications Hub Technical Specifications (CHTS) arises from Part E of the Smart Meter Communication Licence (granted pursuant to sections 7AB(2) and (4) of the Gas Act 1986 and sections 6(1A) and (1C) of the Electricity Act 1989).

Section 4 of this document describes the minimum physical, functional, interface, data, testing and certification requirements of a Communications Hub that the DCC is required to provide to comply with these Licence and SEC requirements.

This document has been brought into force by the Secretary of State on [ ] for the purposes of the relevant licence conditions. CHTS v1.45 was notified to the European Commission in accordance with the requirements of Article 8 of Directive 98/34/EC of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, p. 37) as amended by Directive 98/48/EC of the European Parliament and of the Council (OJ L 217, 5.8.1998, p. 18). The Government is currently considering if renotification is required due to the changes made in this version (v1.46), compared to v1.45.

The Smart Metering technical and security architecture is based on a suite of agreed, open standards, reflecting the UK Government strategy to facilitate the development of third party innovative solutions for consumer devices.

Mutual recognition: Any requirement for a Communications Hub to comply with the CHTS or any of the technical specifications contained or referred to in this document shall be satisfied by compliance with:

i. a relevant standard or code of practice of a national standards body or equivalent body of any EEA State or Turkey; or

ii. any relevant international standard recognised for use in any EEA State or Turkey; or

iii. any relevant technical regulation with mandatory or de facto mandatory application for marketing or use in any EEA State or Turkey,

in so far as compliance with the standard, code of practice or technical regulation in question enables the equipment to achieve, in an equivalent manner, all of the physical, functional, interface and data capabilities that are achieved by compliance with the requirements of CHTS or any of the technical specifications contained or referred to in this document.

4 Technical Specifications

4.1 Overview

Section 4 of this document describes the minimum physical, minimum functional, minimum interface, minimum data and minimum testing and certification requirements of a Communications Hub (CH) that the DCC is required to provide to comply with Part E of the Smart Meter Communication Licence and section xxx of the Smart Energy Code (SEC).

This *section 4* includes requirements for:

i. Communications Hub Function (CHF) of a CH; and
ii. Gas Proxy Function (GPF) of a CH.

Where in this Section 4 a requirement is expressed to be a requirement of the CHF or the GPF it shall be construed as a requirement of the CH to be delivered through the CHF or the GPF as the case may be.

4.2 Testing and Certification Requirements

4.2.1 Conformance with the CHTS

A CH shall have been tested to ensure that it meets the requirements described in this *section 4*, and evidence must be available to confirm such testing and conformance.

4.2.2 Conformance with the Great Britain Companion Specifications

A CH shall meet the requirements described in the Great Britain Companion Specifications v0.8.1.

A CH shall have been certified by the ZigBee Alliance as compliant with the ZigBee SEP v1.2 requirements described in the Great Britain Companion Specifications v0.8.1.

4.2.3 Conformance with the Commercial Product Assurance Security Characteristic for GB Smart Metering

A CH shall meet the requirements described in the Commercial Product Assurance Security Characteristic Smart Metering - Communications Hub v1.0.

A CH shall be certified by CESG as compliant with the Commercial Product Assurance Security Characteristic Smart Metering - Communications Hub v1.0.

4.2.4 Interoperability with the Data and Communications Company Systems

A CH shall be interoperable with DCC systems such that the DCC need not make any adjustments to its systems in order to establish Communications Links (as described in this *section 4*) with the CH via its WAN Interface.

4.3 Physical Requirements

A CH shall as a minimum include the following components:

i. a Clock;
ii. a Data Store;
iii. a HAN Interface;
iv. a Random Number Generator;
v. a WAN Interface; and
vi. an Intimate Physical Interface.

A CH shall operate using DC power and be capable of performing the minimum functional, interface and data requirements described in sections *4.4, 4.5* and *4.6* respectively without consuming more than an average of 1 watt of electricity under normal operating conditions.

A CH shall be capable of automatically resuming operation after a power failure in its operating state prior to such failure.

The CH shall:

vii. permanently display the *CHF Identifier*(*4.6.1.1*) on the CH;
viii. permanently display the *GPF Identifier*(*4.6.1.4*) on the CH; and
ix. have a Secure Perimeter.

The HAN Interface of the CH shall be capable of establishing a ZigBee SEP v1.2 Smart Metering Home Area Network which:

x. operates within the 2400 – 2483.5 MHz harmonised frequency band;
xi. supports the routing (as set-out in section *4.4.2.1*) of Commands, Responses, and Alerts to and from Devices;
xii. supports the Communications Links described in section *4.5.2* and *4.5.3*; and
xiii. supports Certificate-based Key Establishment Cryptographic Suite 2 as described in ZigBee SEP v1.2.

On first establishing a ZigBee SEP v1.2 Smart Metering Home Area Network the CH shall be capable of fixing the frequency at which its HAN Interface operates.

The CH shall be designed taking all reasonable steps so as to prevent Unauthorised Physical Access and Unauthorised communications through its Secure Perimeter that could compromise the Confidentiality and/or Data Integrity of:

xiv. Personal Data;
xv. Consumption data used for billing;
xvi. Security Credentials;
xvii. Random Number Generator;
xviii. Cryptographic Algorithms; and
xix. Firmware and data essential for ensuring its Integrity,

stored or executing on the CH.

The CH shall be capable of detecting any attempt at Unauthorised Physical Access through its Secure Perimeter that could compromise such Confidentiality and/or Data Integrity and on such detection shall be capable of:

xx. providing evidence of such an attempt through the use of tamper evident coatings or seals;

and where reasonably practicable:

xxi. generating an entry to that effect in the *CHF Security Log (4.6.3.5)*; and
xxii. generating and sending an Alert to that effect via its WAN Interface.

The CH shall be designed taking all reasonable steps to ensure that its HAN Interface and WAN Interface do not cause detriment to Communications Links formed with Devices connected to its Intimate Physical Interface.

4.4 Functional Requirements

This section describes the minimum functions that a CH shall be capable of performing.

4.4.1 Clock

The Clock forming part of the CH shall be capable of operating so as to be accurate to within 10 seconds of the UTC date and time under normal operating conditions. The CH shall be capable of maintaining the *CHF Date and Time*(*4.6.3.1*) and:

i. marking this to indicate if its Communications Link via the WAN Interface is not available; and
ii. making the *CHF Date and Time*(*4.6.3.1*) available to Devices with which the CHF has established a Communications Link (as set-out in section *4.4.2.1*) via its HAN interface.

4.4.2 Communications

4.4.2.1 Communications Links with the CHF

The CHF shall be capable of establishing and maintaining Communications Links via the HAN interface with a minimum of four ESME, one GSME, one GPF, seven Type 1 Devices (including a minimum of two PPMIDs) and three Type 2 Devices.

The CHF shall be capable of establishing a Communications Link via the HAN Interface with a Device for a minimum of one hour following receipt of that Device's Security Credentials (as set-out in *section 4.5.1.2*).

The CHF shall only be capable of establishing a Communications Link via the HAN Interface with a Device with Security Credentials in the *CHF Device Log(4.6.2.1)* and shall not be capable of establishing a Communications Link via the HAN Interface with any other Devices.

On establishing such a Communications Link with a Device, the CHF shall be capable of recording the UTC date and time of such establishment in the relevant part of the *CHF Communications Store(4.6.3.2)*.

The CHF shall only be capable of establishing and maintaining a Communications Link via the WAN Interface with the Wide Area Network Provider for the premises in which the CH is installed and shall not be capable of establishing a Communications Link via the WAN Interface with any other person.

The CHF shall be capable of ensuring that the security characteristics of all Communications Links it establishes meet the requirements described in *CHF Secure Communications(4.4.6.6)*.

When any Command addressed to the CHF is received by the CHF via any Communications Link, and again when the Command is due to be executed, the CHF shall be capable of:

i. using the Security Credentials the CHF holds, Authenticating to a Trusted Source the Command;
ii. verifying in accordance with *CHF Role-based Access Control(4.4.6.2.3)* that the sender of the Command is Authorised to execute the Command; and
iii. verifying the integrity of the Command.

On failure of any of *(i)* to *(iii)* above, the CHF shall be capable of generating an entry in the *CHF Security Log (4.6.3.5)* to that effect, discarding the Command without execution and without either generating or sending a Response, and generating and sending an Alert to that effect via the WAN Interface.

Where the Command is not due to be executed immediately, the CHF shall be capable of generating and sending a Response via the WAN Interface to confirm successful receipt.

When executing a Command, the CHF shall be capable of generating and sending a Response via both the WAN Interface and the HAN Interface, which shall either confirm successful execution of the Command or shall detail why it has failed to execute the Command.

The CHF shall only be capable of addressing a Response to the sender of the relevant Command.

The CHF shall be capable of routing Commands, Responses, and Alerts:

iv. from each Device in the *CHF Device Log(4.6.2.1)* to the Devices in the *CHF Device Log(4.6.2.1)* that is the intended recipient;
v. from each Device in the *CHF Device Log(4.6.2.1)* to the WAN Interface; and
vi. from the WAN Interface to the Device in the *CHF Device Log(4.6.2.1)* that is the intended recipient.

The CHF shall be capable of storing the Security Credentials of a minimum of 16 Devices in the *CHF Device Log(4.6.2.1).*

4.4.2.2 **Communications Links with the GPF**

A GPF shall be capable of ensuring that the security characteristics of all Communications Links it establishes meet the requirements described in *GPF Secure Communications(4.4.6.7)*.

When any Command addressed to the GPF is received by the GPF via any Communications Link, and again when the Command is due to be executed, a GPF shall be capable of:

i. using the Security Credentials the GPF holds, Authenticating to a Trusted Source the Command;

ii. verifying in accordance with *GPF Role-based Access Control(4.4.6.2.6)* that the sender of the Command is Authorised to execute the Command; and
iii. verifying the integrity of the Command.

On failure of any of *(i)* to *(iii)* above, the GPF shall be capable of generating an entry in the *GPF Security Log(4.6.3.11)* to that effect, discarding the Command without execution and without either generating or sending a Response, and generating and sending an Alert to that effect via the WAN Interface.

Where the Command is not due to be executed immediately, the GPF shall be capable of generating and sending a Response via the WAN Interface to confirm successful receipt.

When executing the Command the GPF shall be capable of generating and sending a Response via the WAN Interface, which shall either confirm successful execution of the Command or shall detail why it has failed to execute the Command.

The GPF shall only be capable of addressing a Response to the sender of the relevant Command.

4.4.2.2.1 Communications Links with GSME over the HAN Interface

The GPF shall be capable of establishing and maintaining Communications Links via the HAN Interface with GSME.

The GPF shall be capable of receiving the information defined in *Section 4.6.3.9* from GSME.

4.4.2.2.2 Communications Links with Type 1 Devices over the HAN Interface

The GPF shall be capable of establishing and maintaining Communications Links via the HAN Interface with a minimum of one Type 1 Device.

The GPF shall only be capable of establishing a Communications Link with a Type 1 Device with Security Credentials in the *GPF Device Log(4.6.2.3)* and shall not be capable of establishing a Communications Link via the HAN Interface with any other Devices.

The GPF shall be capable of supporting the following types of Communications Links:

i. receiving the Commands (set-out in *Section 4.5.4)* from a Type 1 Device;
ii. generating and sending the Responses (set-out in *Section 4.5.4)* to a Type 1 Device;
iii. generating and sending the information (set-out in *Section 4.6)* to a Type 1 Device; and
iv. sending Alerts to a Type 1 Device, including those it has received from GSME.

4.4.2.2.3 Communications Links with Type 2 Devices over the HAN Interface

The GPF shall be capable of establishing and maintaining Communications Links via the HAN Interface with a minimum of four Type 2 Devices.

The GPF shall only be capable of establishing a Communications Link with a Type 2 Device with Security Credentials in the *GPF Device Log(4.6.2.3)* and shall not be capable of establishing a Communications Link via the HAN Interface with any other Devices.

The GPF shall be capable of supporting the following types of Communications Links:

i. generating and sending information (set-out in *Section 4.6*) to a Type 2 Device; and
ii. sending Alerts to a Type 2 Device, including those it has received from the GSME.

4.4.3 Data Storage

A CH shall be capable of retaining all information held in its Data Store at all times, including on loss of power.

4.4.3.1 GSME data

4.4.3.1.1 Gas Consumption and Energy Consumption data

The GPF shall be capable of using the GSME Cumulative and Historical Value Store and the GSME Cumulative Current Day Value Store (received from GSME as set-out in *section 4.5.2*) to calculate and store to:

i. the *GPF Cumulative and Historical Value Store(4.6.3.6)*:
    a. Energy Consumption on the Day up to the Local Time;
    b. Energy Consumption on each of the eight Days prior to such Day;
    c. Energy Consumption in the Week in which the calculation is performed;
    d. Energy Consumption in each of the five Weeks prior to such Week;
    e. Energy Consumption in the month in which the calculation is performed;
    f. Energy Consumption in the thirteen months prior to such month; and
ii. the *GPF Daily Gas Consumption Log(4.6.3.7)*, the Gas Consumption on each of the 731 Days prior to the current Day.

4.4.3.1.2 Cost of Gas Consumption data

The GPF shall be capable of using the GSME Cumulative and Historical Value Store and the GSME Cumulative Current Day Value Store (received from GSME as set-out in *section 4.5.2*) to calculate and store to the *GPF Cumulative and Historical Value Store(4.6.3.6)* the cost of:

i. Energy Consumption on the Day up to the Local Time;
ii. Energy Consumption on each of the eight Days prior to such Day;
iii. Energy Consumption in the Week in which the calculation is performed;
iv. Energy Consumption in each of the five Weeks prior to such Week;
v. Energy Consumption in the month in which the calculation is performed; and
vi. Energy Consumption in the thirteen months prior to such month.

4.4.3.1.3 Half hour profile data

The GPF shall be capable of using the GSME Profile Data Log, the GSME Cumulative Current Day Value Store, the GSME Conversion Factor and the GSME

Calorific Value (received from GSME as set-out in *section 4.5.2*) to calculate and store to the *GPF Profile Data Log(4.6.3.10)* Gas Consumption in each 30 minute period (commencing at the start of minutes 00 and 30 in each hour) and the UTC date and time at the end of the 30 minute period to which the Gas Consumption relates.

4.4.4 Buffering

A CHF shall be capable of Buffering all Commands intended for GSME with Security Credentials recorded in the *CHF Device Log(4.6.2.1)*.

A CHF shall be capable of prioritising the forwarding of any GSME Add Credit Commands and GSME Activate Emergency Credit Commands.

A CHF shall be capable of Buffering a Command to receive Firmware intended for ESME.

A CHF shall be capable of Buffering Commands, Responses and Alerts to be sent via the WAN interface.

Under normal operating conditions, a CHF shall be capable of Buffering at all times:

i. *CHF Device Log*(*4.6.2.1*) Alerts;
ii. Device Commissioning Alerts;
iii. Responses to Critical Commands; and
iv. other Critical Alerts.

4.4.5 Monitoring

A CH shall be capable of recording the UTC date and time at which the power supply to the CH is interrupted and the UTC date and time at which the power supply to the CH is restored and generating entries to that effect in the *CHF Event Log(4.6.3.3)*.

4.4.6 Security

4.4.6.1 General

A CH shall be designed taking all reasonable steps so as to ensure that any failure or compromise of its integrity shall not compromise the Security Credentials or Personal Data stored on it or compromise the integrity of any other Device to which it is connected by means of a Communications Link.

The CH shall be capable of verifying its Firmware at power-on and prior to activation of the Firmware, to verify that the Firmware, at that time, is in the form originally received. On failure of verification the CH shall be capable of:

i. generating an entry to that effect in the *CHF Security Log (4.6.3.5)*; and
ii. generating and sending an Alert to that effect via the WAN Interface.

A CHF shall be capable of logging in the *CHF Security Log (4.6.3.5)* the occurrence and type of any Sensitive Event.

A GPF shall be capable of logging in the *GPF Security Log(4.6.3.11)* the occurrence and type of any Sensitive Event.

A CHF shall be capable of securely disabling Critical Commands other than those Commands set-out in *Section 4.5.1* that are Critical Commands.

A GPF shall be capable of securely disabling Critical Commands other than those Commands set-out in *Section 4.5.4* that are Critical Commands.

4.4.6.2 Security Credentials

4.4.6.2.1 CHF Private Keys

A CHF shall be capable of generating Public-Private Key Pairs to support the Cryptographic Algorithms set-out in *Section 4.4.6.3*.

The CHF shall be capable of securely storing such Private Keys and shall be capable of formatting and sending via each of the HAN Interface and the WAN Interface a Certificate Signing Request containing the corresponding Public Key and the *CHF Identifier* (*4.6.1.1*).

The CHF shall be capable of securely storing Key Agreement values.

4.4.6.2.2 CHF Public Key Certificates

A CHF shall be capable of securely storing Security Credentials from Certificates including for use in the Cryptographic Algorithms as set-out in *Section 4.4.6.3*.

During the replacement of any *CHF Security Credentials(4.6.2.2)*(as set-out in *Section 4.5.1.10*), the CHF shall be capable of ensuring that the *CHF Security Credentials(4.6.2.2)* being replaced remain usable until the successful completion of the replacement.

4.4.6.2.3 CHF Role-based Access Control

The CHF shall be capable of restricting Authorisation to execute Commands and of issuing Alerts according to Role permissions.

4.4.6.2.4 GPF Private Keys

A GPF shall be capable of generating Public-Private Key Pairs to support the Cryptographic Algorithms set-out in *Section 4.4.6.4*.

The GPF shall be capable of securely storing such Private Keys and shall be capable of formatting and sending via the WAN Interface a Certificate Signing Request containing the corresponding Public Key and the *GPF Identifier* (*4.6.1.4*).

The GPF shall be capable of securely storing Key Agreement values.

4.4.6.2.5 GPF Public Key Certificates

A GPF shall be capable of securely storing Security Credentials from Certificates including for use in the Cryptographic Algorithms as set-out in *Section 4.4.6.4*.

During the replacement of any *GPF Security Credentials(4.6.2.4)* (as set-out in *Section 4.5.4.8*) the GPF shall be capable of ensuring that the *GPF Security Credentials(4.6.2.4)* being replaced remain usable until the successful completion of the replacement.

4.4.6.2.6 GPF Role-based Access Control

The GPF shall be capable of restricting Authorisation to execute Commands and of issuing Alerts according to Role permissions.

4.4.6.3 CHF Cryptographic Algorithms

The CHF shall be capable of supporting the following Cryptographic Algorithms:

i. Elliptic Curve DSA;
ii. Elliptic Curve DH; and
iii. SHA-256.

In executing and creating any Command, Response or Alert, the CHF shall be capable of applying Cryptographic Algorithms (alone or in combination) for:

iv. Digital Signing;
v. Digital Signature verification;
vi. Hashing;
vii. Message Authentication; and
viii. Encryption and Decryption.

4.4.6.4 GPF Cryptographic Algorithms

The GPF shall be capable of supporting the following Cryptographic Algorithms:

i. Elliptic Curve DSA;
ii. Elliptic Curve DH; and
iii. SHA-256.

In executing and creating any Command, Response or Alert, the GPF shall be capable of applying Cryptographic Algorithms (alone or in combination) for:

iv. Digital Signing;
v. Digital Signature verification;
vi. Hashing;
vii. Message Authentication; and
viii. Encryption and Decryption.

4.4.6.5 CH Firmware

The CH shall only be capable of activating its Firmware on receipt of an Activate CH Firmware Command (as set-out in *Section 4.5.1.1)*.

4.4.6.6 CHF Secure Communications

The CHF shall be capable of preventing and detecting, on all of its interfaces, Unauthorised access that could compromise the Confidentiality and/or Data Integrity of:

i. Personal Data whilst being transferred via an interface;
ii. Consumption data used for billing whilst being transferred via an interface;
iii. Security Credentials whilst being transferred via an interface; and
iv. Firmware and data essential for ensuring its Integrity whilst being transferred via an interface,

and any Command that could compromise the Confidentiality and/or Data Integrity of:

v. Personal Data;
vi. Consumption data used for billing;
vii. Security Credentials; and
viii. Firmware and data essential for ensuring its Integrity,

stored or executing on the CHF, and on such detection shall be capable of:

ix. generating an entry to that effect in the *CHF Security Log (4.6.3.5)*; and
x. generating and sending an Alert to that effect via the WAN Interface.

The CHF shall be capable of employing techniques to protect against Replay Attacks relating to Commands received.

The CHF shall not be capable of executing a Command to modify or delete entries from the *CHF Security Log (4.6.3.5)* or the *GPF Security Log(4.6.3.11)*.

4.4.6.7 GPF Secure Communications

The GPF shall be capable of preventing and detecting, on all of its interfaces, Unauthorised access that could compromise the Confidentiality and/or Data Integrity of:

i. Personal Data whilst being transferred via an interface;
ii. Gas Consumption data used for billing whilst being transferred via an interface;
iii. Security Credentials whilst being transferred via an interface; and
iv. Firmware and data essential for ensuring its Integrity whilst being transferred via an interface,

and any Command that could compromise the Confidentiality and/or Data Integrity of:

v. Personal Data;
vi. Gas Consumption data used for billing;
vii. Security Credentials; and
viii. Firmware and data essential for ensuring its Integrity,

stored or executing on the GPF, and on such detection shall be capable of:

ix. generating an entry to that effect in the *GPF Security Log(4.6.3.11)*; and
x. generating and sending an Alert to that effect via the WAN Interface.

The GPF shall be capable of employing techniques to protect against Replay Attacks relating to Commands received.

The GPF shall not be capable of executing a Command to modify or delete entries from the *GPF Security Log(4.6.3.11)*.

4.4.7 Inter-PAN Connection

The CH shall be capable of permitting devices to establish an Inter-PAN Connection for a period of one hour at CH power-on. Where such a connection has been established, the CH shall be capable of sending:

i. Responses and Alerts it has generated; and
ii. Responses and Alerts it has received from other Devices,

to the Inter-PAN connected device.

4.5 Interface Requirements

This section describes the minimum required interactions that a CH shall be capable of undertaking via the HAN Interface and the WAN Interface.

4.5.1 CHF Interface Commands

The CHF shall be capable of executing the Commands set-out in this *Section* (*4.5.1*). The CHF shall be capable of logging all Commands received and Outcomes in the *CHF Event Log(4.6.3.3)*.

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

The CHF shall be capable of cancelling a future dated Command. A future dated Command shall be capable of being cancelled by an Authorised party, subject to CHF Role-based Access Control (as set-out in section *4.4.6.2.3)*. The CHF shall be capable of generating and sending a Response acknowledging that a future dated Command has been successfully cancelled.

4.5.1.1 **Activate CH Firmware**

A Command to activate Firmware.

In executing the Command the CH shall be capable of installing new CH Firmware using a mechanism that is robust against failure and loss of data.

The new Firmware shall include version information. Where new Firmware is successfully installed, the CH shall be capable of recording the version information of that new Firmware in *CH Firmware Version(4.6.3.4).*

4.5.1.2 **Add CHF Device Security Credentials**

A Command to add Security Credentials for a Type 1 Device, Type 2 Device, ESME, GSME or a GPF to the *CHF Device Log(4.6.2.1).*

In executing the Command, the CHF shall be capable of:

i. verifying the Security Credentials;
ii. generating and sending an Alert to this effect, including details of the revised *CHF Device Log(4.6.2.1)*, via the WAN Interface; and
iii. recording the Command and Outcome to the *CHF Security Log (4.6.3.5).*

4.5.1.3 **Clear CHF Event Log**

A Command to clear all entries from the *CHF Event Log(4.6.3.3)*.

The CHF shall be capable of logging that the Command has been executed in the *CHF Security Log (4.6.3.5)*.

4.5.1.4 **Issue CHF Security Credentials**

A Command to generate a Public–Private Key Pair and issue a corresponding Certificate Signing Request.

4.5.1.5 Read CHF Configuration Data

A Command to read the value of one or more of the CHF configuration data items set-out in *Section 4.6.2*.

In executing the Command, the CHF shall be capable of sending such value(s) in a Response.

4.5.1.6 Read CHF Constant Data

A Command to read the value of one or more of the constant data items set-out in *Section 4.6.1*.

In executing the Command, the CHF shall be capable of sending such value(s) in a Response.

4.5.1.7 Read CHF Operational Data

A Command to read the value of one or more of the operational data items set-out in *Section 4.6.3*.

In executing the Command, the CHF shall be capable of sending such value(s) in a Response.

4.5.1.8 Receive CH Firmware

A Command to receive CH Firmware.

In executing the Command the CH shall be capable of:

i. only accepting new Firmware from an Authorised and Authenticated source; and
ii. verifying the Authenticity and integrity of new Firmware before installation.

4.5.1.9 Remove CHF Device Security Credentials

A Command to remove Security Credentials for a Device from the *CHF Device Log(4.6.2.1)*.

In executing the Command the CHF shall be capable of:

i. generating and sending an Alert to this effect, including details of the revised *CHF Device Log(4.6.2.1)*, via the WAN interface; and
ii. recording the Command and Outcome to the *CHF Security Log (4.6.3.5).*

4.5.1.10 Replace CHF Security Credentials

A Command to replace *CHF Security Credentials(4.6.2.2)* held within the CHF.

In executing the Command the CHF shall be capable of:

i. maintaining the Command's Transactional Atomicity; and
ii. recording the Command and Outcome to the *CHF Security Log (4.6.3.5)*

4.5.1.11 Restore CHF Device Log

A Command to restore the details in the *CHF Device Log(4.6.2.1).*

In executing the Command, the CHF shall be capable of recording the Command and Outcome to the *CHF Security Log (4.6.3.5)*

4.5.2 Receipt of Information by the GPF via the HAN Interface

A GPF shall be capable, immediately upon establishment of a Communications Link with GSME of receiving GSME Constant Data, GSME Configuration Data, GSME Operational Data (and with the exception of the GSME Cumulative and Historical Value Store and the GSME Profile Data Log) receiving updates of any changes in that data).

Where changes have been made to the GSME Billing Data Log in accordance with the timetable set-out in the GSME Billing Calendar, the GPF shall be capable of generating and sending an Alert containing the most recent entries of the GSME Tariff TOU Register Matrix, the GSME Tariff Block Counter Matrix and the GSME Consumption Register in the GSME Billing Data Log.

4.5.3 Type 1 Device and Type 2 Device Information Provision from the GPF via the HAN Interface

The GPF shall be capable, immediately upon establishment of a Communications Link with a Type 1 Device (as set-out in *Section 4.4.2.2.2*) and a Type 2 Device (as set-out in *Section 4.4.2.2.3*), of providing the data annotated [INFO] set-out in *Section 4.6* and in addition the following data from the *GPF GSME Proxy Log*(*4.6.3.9*) to the Type 1 Device or the Type 2 Device as applicable (with timely updates of any changes to all such data):

i. Accumulated Debt Register;
ii. Active Tariff Price;
iii. Calorific Value;
iv. Consumption Register;
v. Contact Details;
vi. Conversion Factor;
vii. Currency Units;
viii. Customer Identification Number;
ix. Debt Recovery per Payment;
x. Debt Recovery Rates [1 … 2];
xi. Debt Recovery Rate Cap;
xii. Disablement Threshold;
xiii. Emergency Credit Balance;
xiv. Emergency Credit Limit;
xv. Emergency Credit Threshold;
xvi. Low Credit Threshold;
xvii. Meter Balance;
xviii. Meter Point Reference Number (MPRN);
xix. Non-Disablement Calendar;
xx. Payment Debt Register;
xxi. Payment Mode;
xxii. Profile Data Log;
xxiii. Standing Charge;
xxiv. Supplier Message;
xxv. Supply State;
xxvi. Tariff Block Counter Matrix;
xxvii. Tariff Block Price Matrix;
xxviii. Tariff Switching Table;

xxix. Tariff Threshold Matrix;
xxx. Tariff TOU Price Matrix;
xxxi. Tariff TOU Register Matrix; and
xxxii. Time Debt Registers [1 … 2].

4.5.4 GPF Interface Commands

The GPF shall be capable of executing the Commands set-out in this *Section (4.5.4)*. The GPF shall be capable of logging all Commands received and Outcomes in the *GPF Event Log(4.6.3.8)*.

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

The GPF shall be capable of cancelling a future dated Command. A future dated Command shall be capable of being cancelled by an Authorised party, subject to GPF Role-based Access Control (as set-out in section *4.4.6.2.6)*. The GPF shall be capable of generating and sending a Response acknowledging that a future-dated Command has been successfully cancelled.

4.5.4.1 **Add GPF Device Security Credentials**

A Command to add Security Credentials for a Type 1 Device, Type 2 Device or GSME to the *GPF Device Log(4.6.2.3)*.

In executing the Command, the GPF shall be capable of:

i. verifying the Security Credentials;
ii. generating and sending an Alert to this effect, including details of the revised *GPF Device Log(4.6.2.3)*, via the WAN Interface; and
iii. recording the Command and Outcome to the *GPF Security Log(4.6.3.11)*.

4.5.4.2 **Clear GPF Event Log**

A Command to clear all entries from the *GPF Event Log(4.6.3.8)*.

The GPF shall be capable of logging that the Command has been executed in the *GPF Security Log(4.6.3.11)*.

4.5.4.3 **Issue GPF Security Credentials**

A Command to generate a Public-Private Key Pair and issue a corresponding Certificate Signing Request.

4.5.4.4 **Read GPF Configuration Data**

A Command to read the value of one or more of the GPF configuration data items set-out in *Section 4.6.2*.

In executing the Command, the GPF shall be capable of sending such value(s) in a Response.

4.5.4.5 **Read GPF Constant Data**

A Command to read the value of one or more of the GPF constant data items set-out in *Section 4.6.1*.

In executing the Command, the GPF shall be capable of sending such value(s) in a Response.

4.5.4.6 Read GPF Operational Data

A Command to read the value of one or more of the GPF operational data items set-out in *Section 4.6.3*.

In executing the Command, the GPF shall be capable of sending such value(s) in a Response.

4.5.4.7 Remove GPF Device Security Credentials

A Command to remove Security Credentials for a Device from the *GPF Device Log(4.6.2.3).*

Where the Device removed is GSME, the GPF shall be capable of permanently deleting all the data stored in the *GPF Cumulative and Historical Value Store(4.6.3.6)*, *GPF Daily Gas Consumption Log(4.6.3.7)*, *GPF Profile Data Log(4.6.3.10)* and *GPF GSME Proxy Log(4.6.3.9)*.

In executing the Command the GPF shall be capable of:

i. generating and sending an Alert to this effect, including details of the revised *GPF Device Log(4.6.2.3)*, via the WAN Interface; and
ii. recording the Command and Outcome to the *GPF Security Log(4.6.3.11)*.

4.5.4.8 Replace GPF Security Credentials

A Command to replace *GPF Security Credentials(4.6.2.4)* held within the GPF.

In executing the Command the GPF shall be capable of:

i. maintaining the Command's Transactional Atomicity; and
ii. recording the Command and Outcome to the *GPF Security Log(4.6.3.11)*.

4.5.4.9 Restore GPF Device Log

A Command to restore the details in the *GPF Device Log(4.6.2.3).*

In executing the Command, the GPF shall be capable of recording the Command and Outcome to the *GPF Security Log(4.6.3.11)*.

4.5.4.10 Restrict GPF Data

A Command to restrict provision to Type 1 Devices and Type 2 Devices of all items of Personal Data stored in the GPF which have a UTC date and time stamp prior to the date and time stamp specified in the Restrict GPF Data Command.

4.6 Data Requirements

This section describes the minimum information which the CH shall be capable of holding in its Data Store.

4.6.1 Constant Data

Describes data that remains constant and unchangeable at all times.

4.6.1.1 CHF Identifier
A globally unique identifier used to identify the CHF based on the EUI-64 Institute of Electrical and Electronics Engineers (IEEE) standard.

4.6.1.2 CH Manufacturer Identifier
An identifier used to identify the manufacturer of the CH.

4.6.1.3 Model Type
An identifier used to identify the model of the CH.

4.6.1.4 GPF Identifier
A globally unique identifier used to identify the GPF based on the EUI-64 Institute of Electrical and Electronics Engineers (IEEE) standard.

4.6.2 Configuration Data
Describes data that configures the operation of various functions of the CH.

4.6.2.1 CHF Device Log
The Security Credentials for each of the Type 1 Devices, Type 2 Devices, GSME, ESME and GPF with which the CHF can establish Communications Links.

4.6.2.2 CHF Security Credentials
The Security Credentials for the CHF and parties Authorised to establish Communications Links with it.

4.6.2.3 GPF Device Log
The Security Credentials for each of the Type 1 Devices and Type 2 Devices with which the GPF can establish Communications Links.

4.6.2.4 GPF Security Credentials
The Security Credentials for the GPF and parties Authorised to establish Communications Links with it.

4.6.3 Operational Data
Describes data used by the functions of the CHF and GPF for output of information.

4.6.3.1 CHF Date and Time
The Clock's date and time (in UTC and Local Time).

4.6.3.2 CHF Communications Store
A store holding, for each Device in the *CHF Device Log(4.6.2.1),* the UTC date and time of the last Communications Link established with the CHF.

4.6.3.3 CHF Event Log
A log capable of storing one hundred UTC date and time stamped entries of non-security related information for diagnosis and auditing, arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

4.6.3.4 CH Firmware Version
The active version of Firmware of the CHF and the GPF.

4.6.3.5 CHF Security Log

A log capable of storing one hundred UTC date and time stamped entries of security related information for diagnosis and auditing, arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

4.6.3.6 GPF Cumulative and Historical Value Store [INFO]

A store capable of holding the following values:

i. 9 Days of Energy Consumption comprising the current Day and the prior 8 Days, in kWh and Currency Units;
ii. 6 Weeks of Energy Consumption comprising the current Week and the prior 5 Weeks, in kWh and Currency Units; and
iii. 14 months of Energy Consumption comprising the current month and the prior 13 months, in kWh and Currency Units.

4.6.3.7 GPF Daily Gas Consumption Log [INFO]

A log capable of storing 731 date stamped entries of Gas Consumption arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

4.6.3.8 GPF Event Log

A log capable of storing one hundred UTC date and time stamped entries of non-security related information for diagnosis and auditing, arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

4.6.3.9 GPF GSME Proxy Log

A log capable of storing UTC date and time stamped entries of the GSME Constant Data, GSME Configuration Data and GSME Operational Data except for the following SMETS items:

i. Alerts Configuration Settings
ii. Device Log
iii. GSME Security Credentials
iv. GSME Identifier
v. Public Key Security Credentials Store
vi. Supply Depletion State
vii. Supply Tamper State
viii. Uncontrolled Gas Flow Rate
ix. Network Data Log.

4.6.3.10 GPF Profile Data Log [INFO]

A log capable of storing a minimum of 13 months of UTC date and time stamped half hourly Gas Consumption data arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

4.6.3.11 GPF Security Log

A log capable of storing one hundred UTC date and time stamped entries of security related information for diagnosis and auditing, arranged as a circular buffer such that when full, further writes shall cause the oldest entry to be overwritten.

5 Glossary

5.1.1.1 **Accumulated Debt Register**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.2 **Active Tariff Price**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.3 **Alert**
A message generated by a Device including in response to a problem or the risk of a potential problem.

5.1.1.4 **Authentication**
The method used to confirm the identity of entities or Devices wishing to communicate and “Authenticated” and “Authenticity” shall be construed accordingly.

5.1.1.5 **Authorisation**
The process of granting access to a resource and “Authorised” shall be construed accordingly.

5.1.1.6 **Block Pricing**
A pricing scheme used in conjunction with Time-of-use Pricing where Price varies based on Consumption over a given time period.

5.1.1.7 **Buffer**
An area of the CH capable of storing information for Buffering.

5.1.1.8 **Buffering**
Temporary storage of information pending it being forwarded via the HAN Interface.

5.1.1.9 **Calorific Value**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

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

5.1.1.11 **Certificate Signing Request**
A message requesting the issue of a Certificate by a Certification Authority.

5.1.1.12 **Certification Authority (CA)**
A trusted entity which issues Certificates.

5.1.1.13 **CESG**
The UK Government's national technical authority for information assurance.

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

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

5.1.1.16 **Commercial Product Assurance Security Characteristic for GB Smart Metering**
The document forming part of the Smart Energy Code describing the requirements for evaluation and certification of Communications Hubs under CESG's Commercial Product Assurance scheme.

5.1.1.17 **Communications Hub Function (CHF)**
The functionality in the CH specific to its operation as a bridge between the WAN Interface and HAN interface.

5.1.1.18 **Communications Link**
The exchange of Commands, Responses, Alerts and other information between a system or Device and another system or Device which is independent of the transport mechanism used.

5.1.1.19 **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.

5.1.1.20 **Consumer**
A person who lawfully resides at the premises that is being Supplied.

5.1.1.21 **Consumption**
Gas Consumption or Electricity Consumption information.

5.1.1.22 **Consumption Register**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.23 **Contact Details**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.24 **Conversion Factor**
The value held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.25 **Critical Command**
Those Commands which relate to supply being affected, financial fraud or the compromise of the security of Devices in Consumer Premises.

5.1.1.26 **Cryptographic Algorithm**
An algorithm for performing one or more cryptographic functions which may include: Encryption, Decryption, Digital Signing or Hashing of information, data, or messages; or exchange of Security Credentials.

5.1.1.27 **Currency Units**
The units of monetary value in major and minor units.

5.1.1.28 **Customer Identification Number**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.29 **Data and Communications Company**
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.

5.1.1.30 **Data Integrity**
The state of data where there is assurance that it has not been altered by Unauthorised parties.

5.1.1.31 **Data Store**
An area of the CH capable of storing information for future retrieval.

5.1.1.32 **Day**
The period commencing 00:00:00 Local Time and ending at the next 00:00:00.

5.1.1.33 **Decryption**
The process of converting Encrypted information by an Authorised party to recover the original information and like terms shall be construed accordingly.

5.1.1.34 **Debt Recovery per Payment**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.35 **Debt Recovery Rates [1 … 2]**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.36 **Debt Recovery Rate Cap**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.37 **Debt to Clear**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.38 **Device**
GSME, ESME, a GPF, a CHF, a Type 1 Device or a Type 2 Device.

5.1.1.39 **Device Commissioning Alert**
An Alert sent by a Device as part of the process of bringing that Device into operation.

5.1.1.40 **Digital Signature**
The information appended to a message which is created using the sender's Private Key, can be verified using the 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 is as sent by the sender and that the sender sent the message.

5.1.1.41 **Digital Signing**
The creation of a Digital Signature.

5.1.1.42 **Disablement Threshold**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.43 **Electricity Consumption**
As described at section 5 in the Smart Metering Equipment Technical Specifications.

5.1.1.44 **Elliptic Curve DSA**
The Elliptic Curve Digital Signature Algorithm forming part of the NSA Suite B standard (see *http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml*).

5.1.1.45 **Elliptic Curve DH**
The Elliptic Curve Diffie–Hellman Algorithm forming part of the NSA Suite B standard (see *http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml*).

5.1.1.46 **Emergency Credit Balance**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.47 **Emergency Credit Limit**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.48 **Emergency Credit Threshold**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.49 **Encryption**
The process of converting information in order to make it unintelligible other than to Authorised parties and like terms shall be construed accordingly.

5.1.1.50 **Energy Consumption**
The amount of gas in kWh supplied to the Premises.

5.1.1.51 **ESME**
Electricity Smart Metering Equipment as described in the SMETS.

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

5.1.1.53 **Gas Consumption**
The volume of gas in cubic metres (m^3) supplied to the Premises and “Consumed” shall be construed accordingly.

5.1.1.54 **Gas Proxy Function (GPF)**
The functionality in the CH specific to its operation as a store of GSME data and associated data.

5.1.1.55 **Great Britain Companion Specification**
The document forming part of the Smart Energy Code describing the nature of Communications Links that the CH must be capable of forming via the HAN Interface and the WAN Interface.

5.1.1.56 **GSME**
Gas Smart Metering Equipment as described in the SMETS.

5.1.1.57 **GSME Activate Emergency Credit Command**
A Command to activate Emergency Credit as described at section 4 in the Smart Metering Equipment Technical Specifications

5.1.1.58 **GSME Add Credit Command**
A Command to accept credit to be applied to GSME as described at section 4 in the Smart Metering Equipment Technical Specifications

5.1.1.59 **GSME Billing Data Log**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.60 **GSME Calorific Value**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.61 **GSME Configuration Data**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.62 **GSME Consumption Register**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications

5.1.1.63 **GSME Constant Data**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.64 **GSME Conversion Factor**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.65 **GSME Cumulative and Historical Value Store**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.66 **GSME Cumulative Current Day Value Store**
The data held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.67 **GSME Operational Data**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.68 **GSME Profile Data Log**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.69 **GSME Tariff Block Counter Matrix**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications

5.1.1.70 **GSME Tariff TOU Register Matrix**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications

5.1.1.71 **Hashing**
A repeatable process to create a fixed size and condensed representation of a message of any arbitrary data. Hash and like terms shall be construed accordingly.

5.1.1.72 **Home Area Network Interface (HAN Interface)**
A component of the CH that is capable of sending and receiving information to and from other Devices.

5.1.1.73 **Inter-PAN**
A lower-layer communications mechanism.

5.1.1.74 **Intimate Physical Interface**
A standardised interface defined by the Data and Communications Company, which includes provision for the DC power supply to the CH.

5.1.1.75 **Key**
Data used to determine the output of a cryptographic operation.

5.1.1.76 **Key Agreement**
A means to calculate a shared Key between two parties.

5.1.1.77 **Local Time**
The UTC date and time adjusted for British Summer Time.

5.1.1.78 **Low Credit Threshold**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.79 **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.

5.1.1.80 **Meter Balance**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.81 **Meter Point Reference Number (MPRN)**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.82 **Non-Disablement Calendar**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

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

5.1.1.84 **Payment Debt Register**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.85 **Payment Mode**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.86 **Personal Data**
Any information comprising Personal Data as such term is defined in the Data Protection Act 1998 at the date the CHTS is brought into force.

5.1.1.87 **Premises**
The premises which is Supplied.

5.1.1.88 **Price**
The value held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

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

5.1.1.90 **Profile Data Log**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

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

5.1.1.92 **Public-Private Key Pair**
Two mathematically related numbers that are used in Cryptographic Algorithms.

5.1.1.93 **Random Number Generator**
A component used to generate a sequence of numbers or symbols that lack any predictable pattern.

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

5.1.1.95 **Response**
Sent on, or received from the User Interface or HAN Interface or any other interface containing information in response to a Command.

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

5.1.1.97 **Secure Perimeter**
A physical border surrounding the CH.

5.1.1.98 **Security Credentials**
Information used to identify and/or Authenticate a Device, party or system.

5.1.1.99 **Sensitive Event**
Each of the following events:

i. a failed Authentication or Authorisation; and

ii. a change in the executing Firmware version.

5.1.1.100 **SHA-256**
The Hashing algorithm of that name approved by the NIST (see *http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html*).

5.1.1.101 **Smart Metering Equipment Technical Specifications (SMETS)**
The document brought into force by the Secretary of State to describe the minimum capabilities of equipment installed to satisfy the roll-out licence conditions.

5.1.1.102 **Smart Metering Home Area Network**
A communications network allowing the exchange of information between Devices.

5.1.1.103 **Software**
The software programmes and/or data structures that control the GPF.

5.1.1.104 **Standing Charge**
The value held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.105 **Supplier Message**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.106 **Supply**
The supply of gas to Premises for GSME and “Supplied” shall be construed accordingly.

5.1.1.107 **Supply State**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.108 **Tariff Block Counter Matrix**
The matrix held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.109 **Tariff Switching Table**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.110 **Tariff Threshold Matrix**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.111 **Tariff TOU Price Matrix**
The matrix held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.112 **Tariff TOU Register Matrix**
The matrix held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.113 **Time Debt Registers [1 … 2]**
The information held on GSME as described at section 4 in the Smart Metering Equipment Technical Specifications.

5.1.1.114 **Transactional Atomicity**
The type and order of the constituent parts of a Command.

5.1.1.115 **Trusted Source**
A source whose identity is confidentially and reliably validated.

5.1.1.116 **Type 1 Device**
A Device, other than GSME, ESME, 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.

5.1.1.117 **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.

5.1.1.118 **Unauthorised**
Not Authorised.

5.1.1.119 **Unauthorised Physical Access**
Unauthorised access to the internal components of the CH through its Secure Perimeter.

5.1.1.120 **UTC**
Coordinated Universal Time.

5.1.1.121 **Wide Area Network (WAN) Interface**
A component of CH that is capable of sending and receiving information via the Wide Area Network Provider.

5.1.1.122 **Wide Area Network Provider**
The organisation providing communications over the WAN Interface.

5.1.1.123 **Week**
The seven day period commencing 00:00:00 Monday Local Time and ending at 00:00:00 on the immediately following Monday.

5.1.1.124 **ZigBee Smart Energy Profile (SEP) Version 1.2**
The ZigBee Smart Energy (ZSE) Profile Specification 1.2a v0.9 (reference 14-0256 Rev 04: *http://zigbee.org/About/GBCSPartner.aspx*).

Department of Energy & Climate Change
3 Whitehall Place
London SW1A 2AW
www.gov.uk/decc

URN 14D/438