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

End to End Technical Architecture

Version 3.0

Approved for publication on:

20 June 2019

Contents

1 Document Information

1.1 Amendment History

Version	Date of Issue	Amendment History
0.1	01/07/2012	First draft of Technical Architecture for public consumption
0.2	12/11/2012	Update following SRG review and CESG Trust modelling activities
0.3	19/12/2012	Update following Supplier Stakeholder Architecture workshops
0.4	04/04/2013	Interim update to align with SMETS2+ and to support Final ISFT.
1.0	31/08/2013	Finalised revisions following further stakeholder review and incorporation of outstanding areas of architectural detail.
1.1	14/10/2015	Re-write to reflect change in need from early definition of requirements pre-design to a post design, high level, explanation of the current architecture.
2.0 (draft 0.1)	14/03/2018	Re-formatting of Technical Architecture Document and application of amendments to reflect Release 2.0 content and issued for Industry review
2.0 (draft 0.2)	30/04/2018	Updated version actioning Industry review comments for final internal review
2.0 (draft 0.3)	10/05/2018	Final draft submitted to TABASC for approval
2.0	17/05/2018	Release 2.0 updates to the TAD approved for publication
3.0	20/06/2019	Re-formatting of the End To End Technical Architecture document and inclusion of SMETS1 enrolment.

1.2 Reviewers

This document must be reviewed by the following:

Name	Title/Responsibility	Date	version
Tim Guy	Head of DECC (now BEIS) Delivery	08/10/2015	1.1
Julian Hughes	SMIP Chief Technology Officer	08/10/2015	1.1
SECAS	Smart Energy Code Administrator and Secretariat	14/02/2018	2.0 (draft 0.1)
SEC Parties	Industry review of content changes for Release 2.0	14/03/2018	2.0 (draft 0.1)
TABASC	Technical Architecture and Business Architecture Sub-Committee	10/05/2018	2.0
TABASC	Technical Architecture and Business Architecture Sub-Committee	20/06/2019	3.0

1.3 Approvals

Name	Title/Responsibility	Date	version
Julian Hughes	SMIP Chief Technology Officer	14/10/2015	1.1
TABASC	Technical Architecture and Business Architecture Sub-Committee	17/05/2018	2.0
TABASC	Technical Architecture and Business Architecture Sub-Committee	20/06/2018	3.0

1.4 Document References

The following documents are referenced in this document

Ref #	Title	Date	Version
1	SMIP End to End Technical Architecture first released version	31/08/2013	1006 / Version 1.0
2	Smart Energy Code (SEC)	26/04/2019	6.12
3	Smart Metering Equipment Technical Specifications: Second Version (SMETS2+)	30/09/2016	Version 2.0
		08/11/2018	Version 3.1
		08/11/2018	Version 4.1
		10/06/2019	Version 4.2 (baselined version)
4	Communications Hub Technical Specifications (CHTS)	30/09/2016	Version 1.0
		01/02/2018	Version 1.1
		01/02/2018	Version 1.2 (designated but not in force)
		10/06/2019	Version 1.3 Draft 1 (baselined version)
5	GB Companion Specification (GBCS)	06/11/2017	Version 1.1
		01/02/2018	Version 2.0
		05/06/2018	Version 2.1
		10/06/2019	Version 3.2 Draft 3 (baselined version)
6	DCC User Interface Specification (DUIS)	21/07/2017	Version 1.0
		01/02/2018	Version 2.0 (designated but not in force)
		18/10/2018	Version 3.1 draft 4 (baselined version)
7	Message Mapping Catalogue	08/11/2016	Version 1.0
		01/02/2018	Version 2.0 (designated but not in force)
		10/06/2018	Version 3.1 draft 2 (baselined version)
8	CPA Security Characteristics	02/ 08/2017	Communications Hub; Version 1.3
		18/11/2015	ESME; Version 1.2
		18/11/2015	GSME; Version 1.2
		18/11/2015	HCALCS; Version 1.2
9	End to End Security Architecture	23/05/208	Version 0.3 Includes the associated Release 2.0 changes to the Security Architecture.

Ref #	Title	Date	Version
			It is available to SEC Parties on request
10	Parse & Correlate Requirements	28/10/2013	1.1a
11	ZigBee Smart Energy Profile Specification		ZigBee Smart Energy (ZSE) Profile Specification 1.4 http://zigbee.org/About/GBCSPartner.aspx
12	DLMS / COSEM Green Book (Architecture and Protocols)	07/07/2014	DLMS UA 1000-2 Ed. 8.0 http://www.dlms.com
13	DLMS / COSEM Blue Book (COSEM meter object model)	12/09/2014	DLMS UA 1000-1 Ed. 12.0 http://www.dlms.com
14	ASN.1 Specification	November 2008	http://www.itu.int/rec/T-REC-X.680-X.693-201508-I/en
15	Business Architecture Document	06/11/2017	Version 1.1
		17/05/2018	Version 2.0 (capturing content introduced by Release 2.0)
		17/06/2019	Version 2.1 draft
16	Smart Metering Equipment Technical Specifications (SMETS1)	31/03/2014	Version 1.1
17	SMETS1 Supporting Requirements (S1SR)	17/04/2019	Version 0014 (baselined version)

2 Introduction

2.1 Background

The Government stated in the Smart Metering Prospectus[1] response published in March 2011, that every home in Great Britain should have smart energy meters, giving people far better information about and control over their energy consumption than today. The rollout of smart meters will play an important role in Britain's transition to a low-carbon economy, and help us meet some of the long-term challenges we face in ensuring an affordable, secure and sustainable energy supply.

In order to bring forward the start of rollout and help deliver early benefits, a staged approach to implementation was adopted, under which energy Suppliers have started to install smart meters that meet a minimum set of requirements (SMETS1) followed by the implementation of a central data and communications entity, supporting wide area networks and richer functionality (SMETS2+).

This Technical Architecture describes the target architecture of the SMETS2+ system, SMETS2+ devices, the end-to-end communication and the security aspects.

Prior to the establishing of the SMETS2+ system a large number of SMETS1 devices had been installed. These SMETS1 devices are being enrolled into the SMETS2+ system and will share the supplier interface into the data and communications entity. SMETS1 messages and device properties differ from SMETS2+ and are described in Section 6 dedicated to SMETS1.

2.2 Document Purpose

The GB Smart Metering system is complex and for the uninitiated represents a steep learning curve. For long established experts in GB Smart Metering, more detailed specifications will be of higher value. For new entrants to the programme and decision makers who a need more concise technical view, this document should be their starting point.

This Technical Architecture document provides an entry point into a wider set of technical specifications that describe the requirements for the GB Smart Metering Implementation Programme (SMIP). This document is informative only and should be treated as such. It contains high level descriptions and explanations intended to allow the reader to gain sufficient understanding of the logical architecture of the smart metering end to end system without the need to first digest a larger number of very detailed specifications.

Since the majority of the technical design of SMIP has already been completed, this document is not intended as a design artefact. Rather, it is aimed to be an informative, high level explanation of the overall logical architecture to help contextualise more detailed specifications. It is a logical architecture and so, there is detail that is not covered such as the physical architecture and logical technology model[2]. Many of the models included are in sufficient detail to convey the architecture

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/42742/1475-smart-metering-imp-responseoverview.pdf

[2] which falls to solution providers to develop where appropriate.

but may not include every detailed element as these are contained in the referenced specifications[3]. The scope is the core smart metering system – that is the Smart Metering Equipment, the communications networks and DCC systems that enable access to the system by Service Users.

In all cases, requirements specified in normative documents such as SEC[2], SMETS2+[3], CHTS[4], GBCS[5], DUIS[6], MMC[7], CPA Security Characteristics[8], SMETS1[16] and others take precedence over any statement contained within this document.

Where high level architectural views are supported by more detailed specifications, these are signposted to the relevant specification where possible.

The intended audience includes:

- Enterprise and solution architects;
- Senior managers and decision makers; and
- New entrants to the programme seeking a high level understanding of the technical foundation of the system.

2.3 Technical Architecture Status

The initial version of this document[1] was written before many other documents and specifications that are now in existence and sought to capture design decisions as well as help guide further design and subsequent development of detailed specifications.

In this version, the focus is different, as there is a different need. The end to end architecture is now well developed and this document is now more focussed on describing the architecture and signposting other documents that provide detailed requirements, design and specifications. This and future revisions, will be focused on updating the content to reflect new details, caused by the introduction and implementation of new content and functionality via SEC releases.

2.4 Structure of this Document

This document is divided into the following main sections:

- **Introduction** (this section)

  This section includes background, status of this Technical Architecture document, how the architecture is governed and the principles that underpinned the development of the original GB Smart Metering architecture design.

- **Conceptual Architecture**

  This section provides the highest level conceptual view of the smart metering system to provide the reader with the context in which to read the more detailed sections of this document and its references. This includes the programme vision, objectives, target operating model and a description of each of the four solution domains of the system.

[3] for example, the information model in Section 3.4 includes some key attributes in the entities shown but the reader is referred to SMETS2+[3] for a complete list

- **Logical Architecture**

  This section is the core component of this document and explains the logical architecture of the smart metering system from a number of different perspectives using architectural models which include business, application, integration, information and security. These models with their different perspectives provide high level views which orient the reader to key concepts in the architecture and signpost where more detailed specifications for these areas can be found.

- **Architecture Considerations**

  This section addresses a number of topics that are important to understand and which do not convey themselves intuitively in any of the models described in the logical architecture. It is expected that as this document is further updated, additional topics, for which a brief explanation would be helpful, will be added.

- Enrolment of SMETS1

  SMETS1 meters have been installed in large numbers and utilise a bespoke Head End System (HES) for the remote communication between the Supplier and the metering devices. In order to offer seamless smart metering services to consumers, SMETS1 meters will be added to the GB Smart metering system. This final section explains the main characteristics of the SMETS1 enrolment.

2.5 Governance

The Government announced as part of the SMETS2+ response on 1st July 2013 the modification process for technical specifications[4] as part of the Smart Energy Code (SEC) [2], and that the specifications will transfer to the SEC Panel[5] in due course. The SEC Panel has established a Technical Architecture and Business Architecture Sub-Committee (TABASC)[6] with responsibility for advising the SEC Panel on the end-to-end smart metering system, including:

- assessment of the impact of modifications of technical specifications on the end-to-end system;
- periodic pro-active review and report of the end-to-end system;
- maintenance of an up-to-date view of the end-to-end technical architecture for smart metering;
- consideration of any proposed Data Communications Company (DCC) changes; and
- resolution of any disputes concerning technical specifications.

The SEC Panel is responsible for maintaining, via the SEC Section D - Modifications Process, the base documents, including but not limited to:

- this End to End Technical Architecture;

[4] See SEC[2] Section D for details of the Modification Process
[5] See SEC[2] Section C for details regarding governance of the SEC, SEC Panel and sub-committees
[6] See SEC[2] Section F1 for details of the Technical Architecture and Business Architecture Sub-Committee

- SMETS2+[3];
- CHTS[4];
- GBCS[5];
- DUIS[6];
- MMC[7];
- CPA Security Characteristics[8]; and
- Security Architecture[7][9].

The architecture will be reviewed annually but with the possibility of more regular reviews early in the process to be determined by the SEC Panel.

The SEC Panel will consult the TABASC in considering modification proposals to the technical specifications.

As such the TABASC will:

- have a duty to review and report at appropriate intervals to the SEC Panel upon the effectiveness of the end-to-end system's technical architecture. The TABASC report would include recommendations for any action that it believes is necessary for ensuring that the end-to-end system is as effective as is reasonably possible; and
- be required to maintain an up to date view of the end-to-end technical and security architecture for smart metering and make this available to SEC parties, the SEC Panel and the Authority[8] on request.

2.6 Architecture Framework

Within the Smart Meters Implementation Programme (SMIP), there is a need to articulate a wide range of artefacts describing business through to technical and high level through to very detailed. Responsibility for producing design artefacts is distributed across several parties involved in the SMIP.

In 2011, The Government committed to delivering a Reference Architecture, which, together with the asset and services knowledge base, was intended to enable the sharing and re-use of Information and Communications Technology (ICT) services and solutions and the creation of a common ICT infrastructure. In addition to enabling the sharing and re-use of ICT services and infrastructure the framework reflects industry frameworks such as TOGAF and Zachman in their approach to decomposing and communicating architectures.

Figure 2.6 below shows this reference architecture overlaid with the key sections of this Technical Architecture showing the scope of this document. Additionally, other related documents are shown in the framework according to their content and focus.

[7] via NCSC – see https://www.ncsc.gov.uk/document/security-characteristics-smart-meters
[8] Gas and Electricity Markets Authority as established under section 1 of the Utilities Act 2000

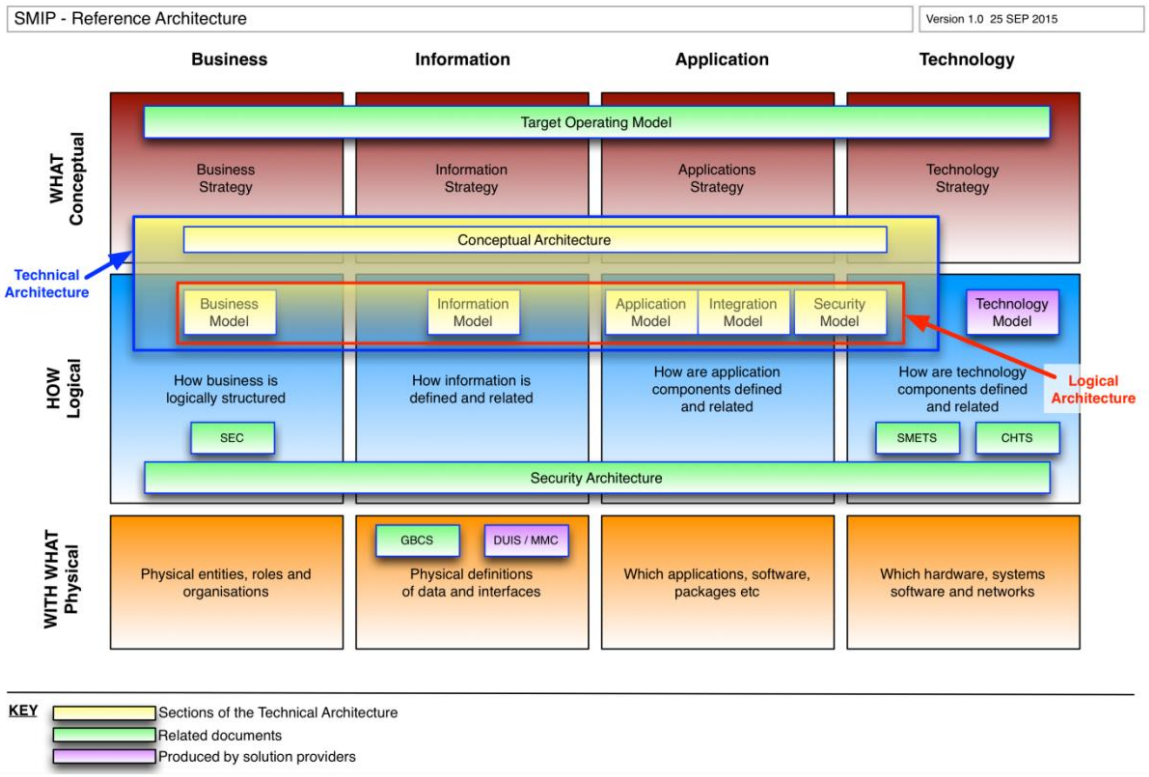

Figure 2.6: SMIP Reference Architecture Framework

In terms of the reference architecture above, this document describes primarily the Logical Architecture for the SMIP. In order to contextualise the models contained in the Logical Architecture, this document begins with a Conceptual Architecture description including an organisational view of the target operating model. The document does not cover the Physical Architecture or Technology Model as these are within the remit of the various solution providers involved in the SMIP.

The Technical Architecture is supported and elaborated by a series of related documents including:

- **Smart Energy Code[2]** which governs the operation of GB smart metering;
- **SMETS2+[3**] – Technical Specifications for Smart Metering Equipment;
- **CHTS[4]** – Technical Specifications for Communications Hub;
- **GBCS[5]** – Great Britain Companion Specification describing detailed integration protocols;
- **DUIS[6]** – DCC User Interface Specification describing the interface between Service Users' systems and the DCC Data Services Provider;
- **MMC[7]** – DCC Message Mapping Catalogue describing the format of outbound messages from the Parse & Correlate software;
- **CPA Security Characteristics[8]** – Commercial Product Assurance (CPA) Security Characteristics documents which describes features, testing and deployment requirements necessary to meet CPA certification requirements;
- **SMIP End to End Security Architecture[9**] – Defines the overall security architecture;

- **BAD[15] – Business Architecture Document –** Defines the End-to-End SEC Business Architecture and associated processes;
- **SMETS1[16] Smart Metering Equipment Technical Specifications** – Defines the properties of SMETS1; and
- **S1SR[17] SMETS1 Supporting Requirements** – Defines the requirements for the communication with SMETS1 devices on the DUIS interface.

Where appropriate, this document signposts the above specifications and provides context and guidance on their use.

2.7 Technical Architecture Principles

The technical architecture principles represent the key underlying drivers that were used in development of the original SMIP architecture. Any change to the principles or deviation from them should be managed with reference to the architecture governance arrangements described in Section 2.5. The principles also provide important context in terms of understanding the architectural models and the decisions that have been made and described in the remainder of this document.

Ref	Principle
Best Practice	
B01	**Requirements Based Design** Where practicable the selection of technology should be driven in response to the needs of the business, rather than having the business change in response to technological challenges. However, where a choice in technology provides an opportunity to improve the business process then this should be used to inform the requirements documentation process. The purpose of this principle is to keep focused on business, not technology needs.
B02	**Requirements traceability** Requirements traceability is concerned with documenting the life of a requirement. Traceability ensures that the origin of each requirement can be traced and ensure that every change made to a requirement, is clearly documented. Requirements come from many different sources, but must be captured and validated into a single repository. This provides a basis for managing and implementing requirement change control with minimal impact. In addition, traceability enables requirement challenges and prioritisation resulting from technological constraints to be discussed and validated with all relevant stakeholders.
B03	**Reuse** Reuse existing and proven solutions where appropriate, for example through the use of security architecture patterns.
B04	**Adherence to legislation** Comply with applicable legislation
B05	**Single points of failure** The existence of single points of failure in architecture can lead to entire system outage and the resulting financial & reputational risks.
B06	**Design simplicity** Complexity introduces risk and exposes the end-to-end architecture to both greater cost of delivery and maintenance. A result of ensuring design simplicity is that technological diversity is controlled minimising the non-trivial cost of

Ref	Principle
	interoperability and connectivity between multiple processing environments. Limiting the number of supported components will simplify maintainability, reduce costs and provide increased flexibility to accommodate technological advancements. Technical administration and service management costs are better controlled when limited resources can focus on a reduced set of technology.
B07	**Separation of concerns** Separation ensures that functions can be optimised independently of other functions, so that failure of one function does not cause other functions to fail, and in general to make it easier to understand, design and manage complex interdependent systems.
B08	**Standards** The end-to-end interoperability required by the programme can be achieved through the use of multiple open standards and translation/transformation services using message brokers where interface boundaries exist, e.g. due to separation of components and their use of differing protocols. Standards help promote interoperability and ensure consistency, thus improving the ability to manage systems, improve user satisfaction and enable an innovative market. Standards also promote the protection of existing IT investments, maximising return on investment and reducing costs. Open standards are important in controlling costs over time and facilitating inter-operability between systems in the exchange of data, ensuring that smart meters enhance choices for individual consumers.
Programme	
P01	**Support foundation and endurance** Although the architecture may evolve over time, any published baseline must ensure that the architecture is equally applicable to both foundation and enduring phases. This will ensure that the architecture is developed with minimal duplication of effort between phases and is backward compatible. This will also maintain consistency in the implementation of the high level operation that defines a Smart Metering installation[9]
P02	**Initiation of interactions** Interactions with devices should only be initiated in response to Service User requests. This provides a basis from which security principles and data privacy rules can be developed and applied.
P03	**Adaptability to change** Systems and services should be designed to allow changes, whether minor or major, to be implemented in a responsive manner, at low cost and low risk and to support test management. This ensures that adaptability for changing requirements does not materially impact the overall business case and an ability to assure changes in advance of any impact to the live service.
Security	
S01	**Layered Security** Provide defence in depth through multi-layered controls within various components and entities.
S02	**Least Privilege** Support the principle of least privilege, whereby each component or entity involved in the end-to-end Smart Metering system should have the minimum privileges required to carry out their defined function.
S03	**Need to Know**

9

Ref	Principle
	Support the concept of 'need to know', whereby each component or entity should only be in receipt of information, or access to information, if it has appropriate authorisation and requires access to that information to conduct its duties. Access to information and systems should be denied by default.
S04	**DCC will not store meter data** The DCC must not store consumption data retrieved from devices. DCC will execute service requests (ad hoc, on demand or scheduled) to retrieve meter reading data and will pass this data directly to the requesting party. The data may be retained in DCC to allow for batching of output or provision of data to multiple parties but will not be stored to allow for any prospective enquiry by other parties. Meter readings are private data which can only be retrieved in accordance with an agreement between a customer and another party (e.g. Supplier). Accordingly DCC is only acting as an agent to retrieve information from Smart Metering Systems on instruction; it is not providing a central repository of meter data for access by authorised parties. Some data relating to meters is stored by the DCC such as identifiers, addresses and manufacturer details but this is not classed a meter data.
Architectural	
A01	**Well defined interfaces** A common end-to-end system data model and message specifications for all component boundaries are required. The use of published open standards can only provide guarantees with respect to syntactic interoperability, i.e. the ability to exchange data. Semantic interoperability is the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results wherever user interaction occurs within the end-to-end system.
A02	**Design simplicity** The number of 'brokered interfaces', as opposed to 'pass through' protocols at component boundaries should where possible be minimised. This is a specific application of the 'ensure design simplicity' principle, but is key in relation to minimising security risk and delivery complexity based on the number of components and commonality of protocols within the stack and across the end-to-end architecture. There are many other factors that also influence the need to consider optimising the design, including: • Security – the greater the number of component and interface boundaries the greater the security risk; • Power consumption – more brokers requires more processing overhead; and • Complexity – more interface boundaries with varying protocols leads to increased complexity for design, build, test and deployment, and so increased cost.
A03	**Interoperability** Interoperability, along with open standards, allows for market participants to innovate and make the best technology decisions without being constrained by proprietary standards and an inflexible architecture. The impact of non-interoperability will result in, at best, an inconsistent consumer experience and, at worst, a restricted/closed market in which switching Supplier becomes near impossible for consumers
A04	**Early data validation** Data validation should be performed as 'high up the chain' as possible

Ref	Principle
	DCC Service User systems should be the prime point of validation of data being transmitted to the smart metering system. DCC perform Access Control and verification that requests are consistent with the request type but do not check the consistency of a request against the device configuration or the content of the message. This ensures that DCC do not need to retain details about the configuration of each device or consumer premises (e.g. mode, register settings, tariff).
A05	**Loose coupling** Operational interdependencies between systems and networks should be minimised. This allows systems the flexibility to be individually optimised.

Table 2.7 Architectural Principles

2.8 Out of Scope

This document focuses on the elements of the end to end architecture relating to the operation of smart metering equipment. Although some references are included, the document does not seek to describe in any detail the systems and solutions that surround this core of the smart metering system (for example home automation, energy Supplier financial and billing systems, smart grids and demand side management).

3 Conceptual Architecture

3.1 Vision

The Government's vision is for every home and smaller businesses in Great Britain to have smart electricity and gas meters. Smart meters give energy Suppliers access to accurate data for billing, removing the need to manually read meters. Domestic customers will be offered an In-Home Display (IHD) enabling them to see what energy they are using and how much it is costing, to put them in control and avoid wasting energy and money.

3.2 Programme Objectives

The objectives for the Programme are to:

1. Provide the technical and regulatory framework for the roll-out of smart meters;
2. Support industry delivery of an on-time, cost-efficient and safe smart metering system;
3. Drive consumer demand for smart meters through increased awareness and support for the Programme;
4. Ensure Programme benefits are maximised for consumers, industry and society through reduced energy use and a more efficient and competitive energy market;
5. Ensure the smart metering system is a platform for wider smart system benefits, by delivering a secure and effective end-to-end technical solution; and
6. Ensure the Programme is delivered in a transparent manner to allow all Suppliers, Networks, Energy Service Companies, and other participants in the supply chain the opportunity to make the most of the Smart Metering delivery.

3.3 Target Operating Model

The organisation based view of the Target Operating Model (TOM) in Figure 3.3 shows a top level view of the parties involved in the Smart Metering Implementation Programme (SMIP).

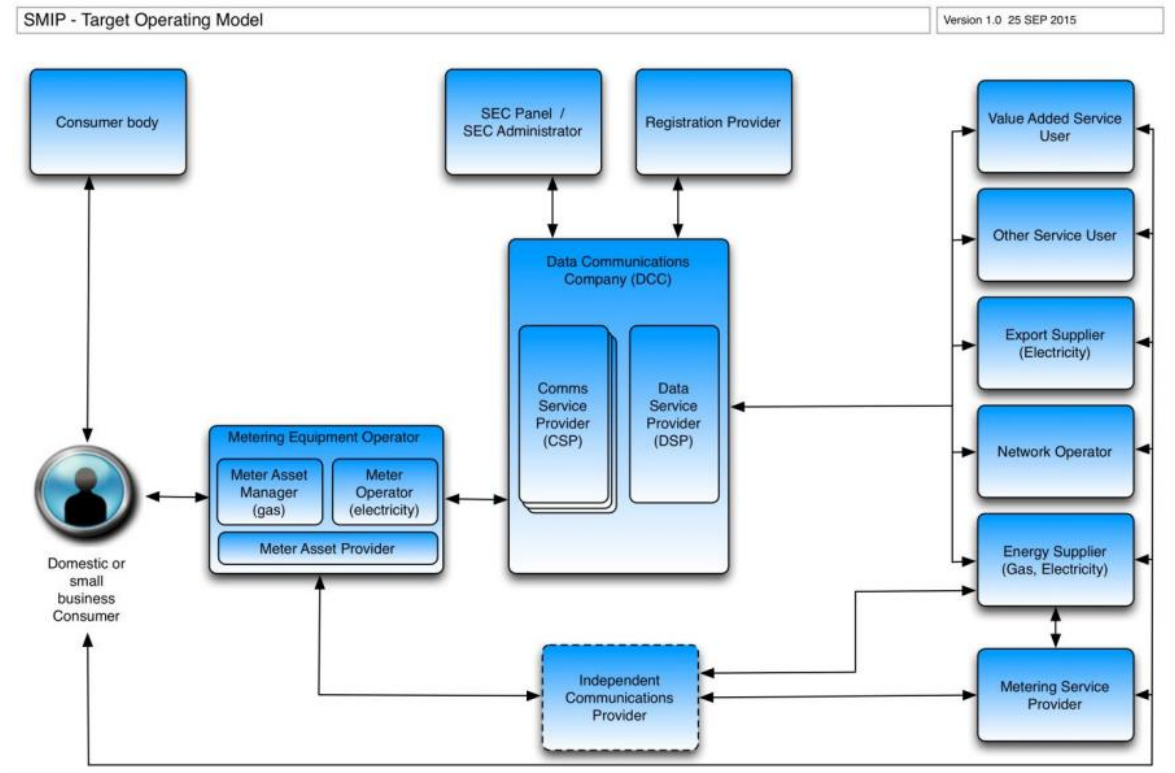

Figure 3.3: Organisation view of the smart metering target operating model

Table 3.3 describes each of the key elements of the operating model.

Element	Description
Domestic or Small Business Consumer	Consumer refers to either (1) a domestic gas and /or electricity consumer in Great Britain or (2) a smaller, business gas and /or electricity consumer in Great Britain. The latter is referred to as a 'non domestic' consumer.
Consumer Body	Several independent organisations exist whose remit is to provide advice and support to consumers where an issue cannot be resolved with the energy supplier directly. These include The Ombudsman Service[10] and Citizen's Advice[11].
Metering Equipment Operator	The organisation that is responsible for the metering equipment, including site visits to fix any failures. This is in many cases the energy Supplier but may be subcontracted out to another party.
Meter Asset Manager (gas)	The Meter Asset Manager is the gas industry term given to the organisation that is responsible for installation and maintenance of Metering Equipment.
Meter Operator (electricity)	The Meter Operator the electricity industry term given to the organisation that is responsible for installation and maintenance of Metering Equipment.
Meter Asset Provider	A Meter Asset Provider provides the financing to meet up-front purchase costs of Metering Equipment. They then charge the Energy Supplier an annual amount for the meter, to recover the initial investment cost.
SEC Panel / SEC Administrator	The SEC Administrator manages on behalf of the SEC Panel aspects of the day-to-day governance of the Smart Energy Code, including

[10] http://www.ombudsman-services.org/
[11] http://www.consumerfocus.org.uk/

Element	Description
	administrative tasks such as processing SEC applications from organisations who wish to become part of the smart metering scheme.
Registration Provider	The Registration Provider maintains information regarding which metering equipment is installed in which properties and connected to which supply point to ensure that billing is applied to the correct customer, maintenance engineers are directed to the right equipment and switching between suppliers can be affected.
Data Communications Company (DCC)	The DCC is a new entity that has been created and licensed to provide smart meter communication services. The DCC is responsible for the procurement and contract management of data and communications services (the CSPs and the DSP) to providing remote access to smart metering equipment.
Communications Service Provider (CSP)	The DCC has a set of three[12] sub contracts with Communication Services Providers, who will each provide wide area networking between Smart Metering Equipment and the Data Service Provider central facilities. Each CSP will cover one of three geographic parts of Great Britain
Data Service Provider (DSP)	The DCC has a single sub contract with a Data Services Provider who operates central facilities to control the flow of messages to and from smart metering equipment. Service User organisations communicate via these central DSP facilities.
Independent Communications Provider (transitional)	During transition to the target operating model whereby all electricity and gas meters within the scope if the SMIP are connected to the DCC (SMETS2+ compliant meters), other smart meters (including SMETS1 compliant meters and other smart meters) implemented before the DCC go live will be connected to suppliers through one or more independent communications networks.
Value Added Service User	An organisation using the smart metering infrastructure to provide value added services to the Consumer by remotely accessing equipment on the Consumer's premises.
Other Service User	An organisation, other than an Energy Supplier or Network Operator, which can use the DCC's energy related services. This could be, for example, a third party, authorised by the Consumer to access the Consumer's energy consumption information, so as to provide the Consumer with energy related services, such as advice on energy efficiency, alternative tariffs and changing Energy Supplier.
Export Supplier	An Energy Supplier who contracts with a Consumer to pay the Consumer for the electricity they generate and export, from Microgeneration equipment on their premises.
Network Operator	The term Network Operators refers collectively to electricity distribution and gas transportation companies that are responsible for the gas and electricity networks that deliver energy to consumers' homes / business premises.
Energy Supplier	A company licensed to supply gas and / or electricity to Consumers in Great Britain. The Energy Supplier holds the contract with the consumer and is central to the provision of services, including metering (unless the Consumer opts to get metering from elsewhere).

[12] Note that two of the three contracts have been awarded to one company making for two smart meter wide area network solutions

Element	Description
Metering Service Provider	Where a Consumer has a Metering Equipment Operator different from their Energy Supplier, that provider would normally undertake remote communications, not least meter reading – where companies do this, they are referred to as Metering Service Providers.

Table 3.3: Organisational view of the target operating model

3.4 Conceptual Model

The conceptual architecture (Figure 3.4) provides a view of the major components supporting the end-to-end operational model for the SMIP. It shows the metering equipment, communicated with via the Data Communications Company (DCC) using Communications Service Provider (CSP) wide area networks[13], and the relevant components, domain boundaries and interconnections.

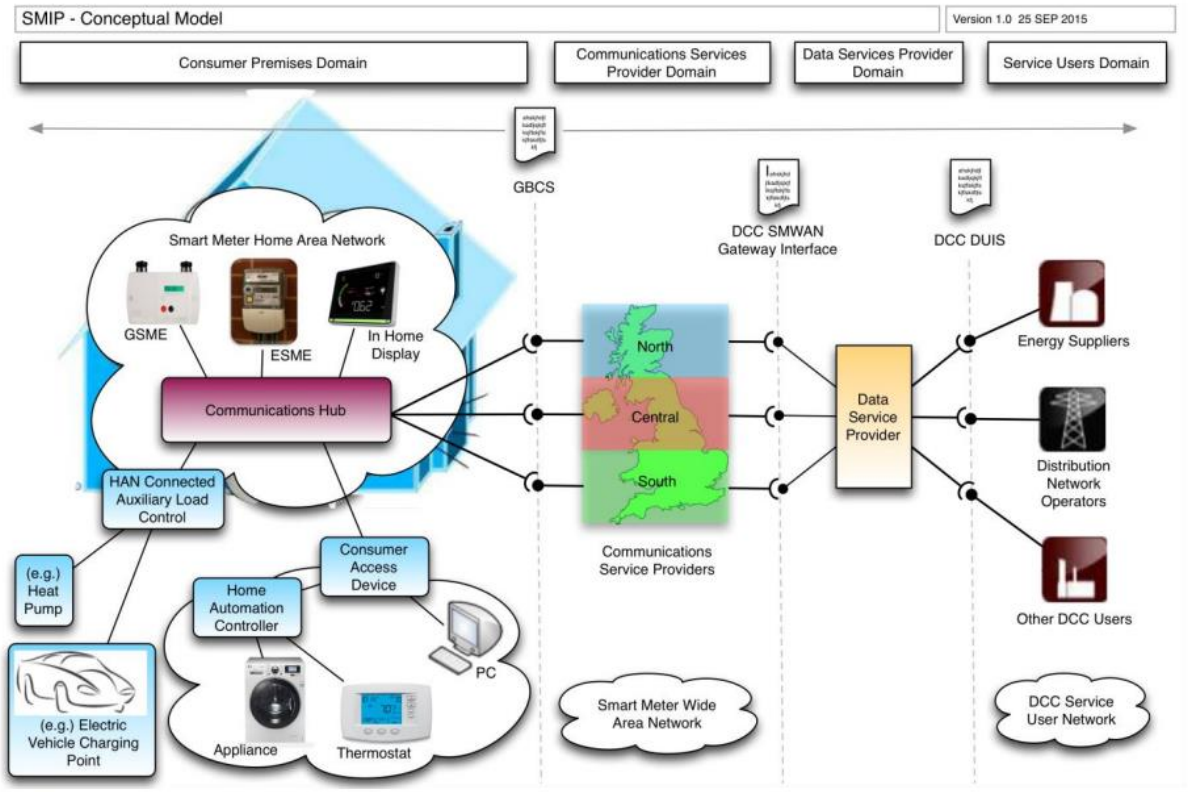

Figure 3.4: Conceptual Model

The Conceptual Architecture is split into four solution domains supporting architecture principle A05 (see Section 2.7). Each domain is explained at a high level in this section.

The key solution domains depicted are:

- Consumer premises domain including the Smart Meter Home Area Network (SMHAN);

[13] This architecture does not address other routes to communicate with metering equipment (e.g. those used for opted out, nondomestic
metering equipment).

- Communications Service Provider (CSP) domain including the Smart Meter Wide Area Network (SMWAN);
- Data Service Provider (DSP) domain; and
- Service Users domain including the DCC user wide area network (DCC User Network).

The following sections explain each of the above domains and their components, networks and interfaces at the conceptual level.

The Consumer premises domain and the Communications Service Provider domain for SMETS1 differ from the conceptual architecture model shown in Figure 3.4; please see Section 6 for details.

3.4.1 Consumer Premises Domain

At the consumer premises, the Smart Meter Home Area Network (SMHAN) links a number of devices together that participate in the smart metering system including electricity and gas meters (ESME & GSME), a Communications Hub (CH), Pre-Payment Metering Interface Devices (PPMID) and an In Home Display (IHD). A Consumer Access Device (CAD) may optionally link other consumer devices including computers, home automation and electrical appliances into the smart meter system. The components in this domain enable much more than traditional energy metering through connectivity between the consumer premises devices and the wider, end-to-end smart meter system. The key capabilities provided are:

- measurement of electricity and gas consumption and the ability to enable / disable supply to the premises;
- measurement of electricity export from the premises (microgeneration);
- transfer of data to and from Smart Metering Equipment (SME) in the home to Service Users such as energy Suppliers and Distribution Network Operators (DNO);
- presentation of consumption and related data to the consumer;
- addition of pre-payment credit to meters and management of consumer debt; and
- control of auxiliary electrical loads.

The SMHAN is linked to the Smart Meter Wide Area Network (SMWAN) through the Communications Hub which provides a secure short range wireless network within the consumer premises. The SMHAN and SMWAN networks are implemented using different network technologies individually suited to each environment. Through a Consumer Access Device (CAD), other consumer home area networks can be connected to the SMHAN for the provision of consumption data to consumer devices[14].

The components within this domain are described in Section 4.2.1 but in summary they are:

- Electricity Smart Meter Equipment (ESME);
- Gas Smart Meter Equipment (GSME);

[14] The consumer home area network is outside of the scope of the SMIP Technical Architecture

- In Home Display (IHD);
- Pre-Payment Metering Interface Device (PPMID);
- Communications Hub (CH);
- HAN Connected Auxiliary Load Control Switch (HCALCS) or directly connected Auxiliary Load Control Switch (ALCS);
- Hand held terminal (HHT) used for maintenance; and
- Consumer Access Device (CAD).

The components for the consumer domain in SMETS1 are slightly different; please see please see Section 6 for details.

As the network of Smart Metering Equipment (SME) will include some 30 million households and more than 100 million devices by rollout completion, it is necessary to provide a robust infrastructure to securely manage and route requests and responses between Service Users and SME rather than allow direct access to these devices. In order to achieve this, two intermediate domains and associated system components sit between the service user domain and the SME contained within the consumer premises domain. These are described in the next two sections.

3.4.2 Communications Service Provider Domain

SME in the consumer premises is connected via one of three[15] possible wide area networks operated by the Communications Service Providers (CSPs) covering the north, central and south geographies respectively. The wide area networks converge at the Access Control Broker (ACB) within the Data Service Provider (DSP) domain which then provides connectivity via a set of defined services to authorised Service Users. The services provided by the DSP interact with the SME within the consumer premises domain.

Each CSP's SMWAN implementation may use different communication technology such as Long Range Radio, GSM or other technologies. Each CSP provides connectivity from the DSP to all the Communications Hubs that are part of the smart meter installations for which it is responsible[16]. The CSPs provide features to manage performance, reliability and availability through traffic optimisation and management specific to their individual infrastructure.

The CSPs manage, route and deliver all messages from the DSP to designated Communications Hubs that form the entry point to associated gas / electricity Smart Metering Equipment and other devices within consumer premises. Communications Hubs route alerts and responses from Smart Metering equipment to the CSP for onward delivery to the DSP.

For SMETS1 equivalent of the Communications Service Provider Domain please see Section 6.

[15] Note that two of the three CSP contracts have been awarded to one solution provider making for two distinct wide area networks although this need not be the case from an architecture perspective, nor in future re-procurement by DCC.
[16] The CSPs are also responsible for the Communications Hub itself.

3.4.3 Data Service Provider Domain

The purpose of the Data Service Provider domain is to provide a single secure interface through which service requests from Service Users can be routed via the correct CSP's SMWAN to the correct Communications Hub within the consumer premises. The architecture separates the scheduling and routing of service requests (DSP) from aspects of wide area network transport (CSP) allowing flexibility in the implementation and future change.

The DSP takes service requests from DCC Service Users, then validates and translates these into commands that can be understood by the Smart Metering Equipment connected to the SMHAN ('HAN Ready' commands). The DSP also provides responses back to originating Service Users, as well as routing Alerts from consumer premises equipment to Service Users.

The Data Service Provider domain also provides the following capabilities:

- the management of scheduled transactions;
- an interface for the registration and management of Smart Metering Equipment in a smart metering inventory;
- access control for DCC Service Users in addition to smart meters own access controls;
- an anomaly detection and intruder prevention service for all traffic transiting through it (e.g. to detect potentially aberrant patterns of behaviour by DCC Service Users that may suggest operational compromise or mis-function);
- manages the tracking of SME service incidents; and
- storage of Security Credentials for entities involved in smart metering.

Service Users' and Service User systems gain connectivity to the DSP domain through the DSP Service User Network which provides a separate infrastructure for the transportation of service requests from Service Users to the DSP.

The components within this domain are fully described in Section 4.2 but in summary they are:

- The Access Control Broker (ACB);
- The Transitional Change of Supplier (TCoS) service;
- The Transform service; and
- The Smart Meter Registration service.

The Data Service Provider Domain connectivity also applies to SMETS1 metering devices with the exception of 'HAN Ready' commands not being created for SMETS1 communications. Please see Section 6 for further details.

3.4.4 Service User Domain

The Service Users domain contains the different organisational entities and their business systems that use the services of the DSP to interoperate with the smart metering capability provided in the consumer premises domain. Service Users include:

- Energy Suppliers (Gas / Electricity);
- Distribution Network Operators;
- Export Supplier (Electricity); and
- other value added service providers.

Within the service user domain there is a component called Parse & Correlate which is provided by the DCC and may be incorporated into Service Users' business systems. Further explanation of this component can be found in Section 4.2.4.2. The Parse & Correlate function is not used for SMETS1 communications.

3.4.5 Key Interfaces between Domains

Within the SMETS2+ end-to-end architecture are a number of key interface specifications that define the format of requests and messages that flow between different domains, parties, systems and equipment. The following interfaces are key at the level of this conceptual architecture view:

- the interface to SME and the end to end operation of the system which applies to the DSP and Service Users is defined by the GBCS[2];
- the interface between the CSPs and the DSP is an internal to DCC interface specification and is not public; and
- the interface between the DSP and the Service Users is defined by the DCC User Interface Specification (DUIS) [6] and Message Mapping Catalogue[17] (MMC) [7].

Note that at this conceptual level we do not distinguish whether an interface specification describes physical, network, application or other aspects of the system, only that they are relevant. Further details can be found in Sections 4.2 (Application Model) and 4.3 (Integration Model). These interfaces are built on top of other open interface standards and more detail on this can be found in Section 4.3.1 of this document.

Note that GBCS[2] does not apply for SMETS1 communications; please see Section 6 for further details.

[17] This interface is provided by DCC but the software is physically deployed in the Service Users domain.

4 Logical Architecture

Building on the conceptual architecture described in Section 2, the logical architecture elaborates the design to a further level of detail, showing logically how the system is required to work but importantly not detailing the actual physical implementation, e.g. the specific hardware used or the software applications. This provides an implementation agnostic view with flexibility for different system providers to meet the logical requirements of the system in different ways, maximising innovation, increasing value for money and flexibility for future change. Please refer to Section 6 for additional information about SMETS1.

The logical architecture is described in the following sequence to help the reader by building a picture starting with higher level concepts (business, application) before elaborating further (integration, information and security).

- **the business model** – this explains the system from a business perspective including the functions that the system can perform and certain business processes that the system must support;
- **the application model** – this explains the logical components of the architecture, and their capabilities, which support the business functions. This view is essential to understanding other more detailed aspects of the system;
- **the integration model** – this explains how certain components communicate with each other where there is a boundary between components or where certain aspects of the communication need to be standardised across the system. Some interfaces are internal to DCC however and therefore not covered in this logical architecture;
- **the information model** – this explains at a high level the key data items, relationships, and where these data items reside with respect to the system components; and
- **the security model** – The security architecture is fully described in the Security Architecture [9] but is presented at a high level in this logical architecture to help the reader's understanding, and because some of the security concepts are important to, and are addressed, at the logical architecture level.

The above architecture models represent the most useful views of the logical architecture to help describe the system. Intuitively, the business and information models relate to their respective SMIP Reference Architecture columns (see Section 2.6). The application, integration and security models relate to the application architecture column.

4.1 Business Model

The business model describes how the business is decomposed into a number of functional areas and business functions. The Business Model further describes a number of end to end interactions that relate to those functions. However, since different parties making use of the smart metering system will implement their own business processes, there is no harmonised view and therefore business processes are not described in this document. For further information please refer to the BAD[15].

4.1.1 Key Organisations and people

The key organisations and people referenced in the various parts of this document are as follows (definitions of each can be found in the Glossary):

- Consumers;
- Data Communications Company (DCC);
- Communications Service Providers (CSP);
- Data Services Provider (DSP);
- Energy Suppliers;
- Distribution Network Operators (DNO);
- DCC Service Users; and
- SEC Panel.

4.1.2 Example of Key Business Process

The following represent some examples of key business processes that make use of smart metering capabilities. This is a non-exclusive list provided for context only and the reader is referred to the business process designs of specific parties involved in the overall smart metering system where appropriate.

- Install & Commission;
- Diarised Billing Read;
- Update Tariff;
- Ad Hoc Third Party Read;
- Equipment tamper Alert;
- Over Voltage Alert;
- Customer Identification Number (CIN);
- Change of security credentials; and
- Firmware update.

4.1.3 Key Business Processes

Figure 4.1.3 shows the key logical business functions relating to Smart Metering Equipment categorised under the following headings:

- **Consumer functions** – these are the key functions that Consumers can undertake with the Smart Metering Equipment (SME);
- **Smart metering functions** – These are the key functions implemented by the Smart Metering Equipment itself;

- **Service User functions** – Service Users are those end users who interact with the Smart Metering system via the DCC User Interface (See DUIS[6] for a description of this interface);
- **Security functions** – These functions exist across the end-to-end-architecture but are grouped and identified distinctly according to common approaches to architecture definition; and
- **Business support functions** – These functions are those that are required to operate the Smart Metering system but which are not elaborated in this Technical Architecture as they are not as closely related to the operation of Smart Metering Equipment.

Although actors such as consumers and Service Users do have other business functions available to them as part of the wider smart metering system (some are shown in Figure 4.1.3, e.g. B01-Service User Systems), this section focuses primarily on those business functions that relate directly to the operation of the Smart Metering Equipment.

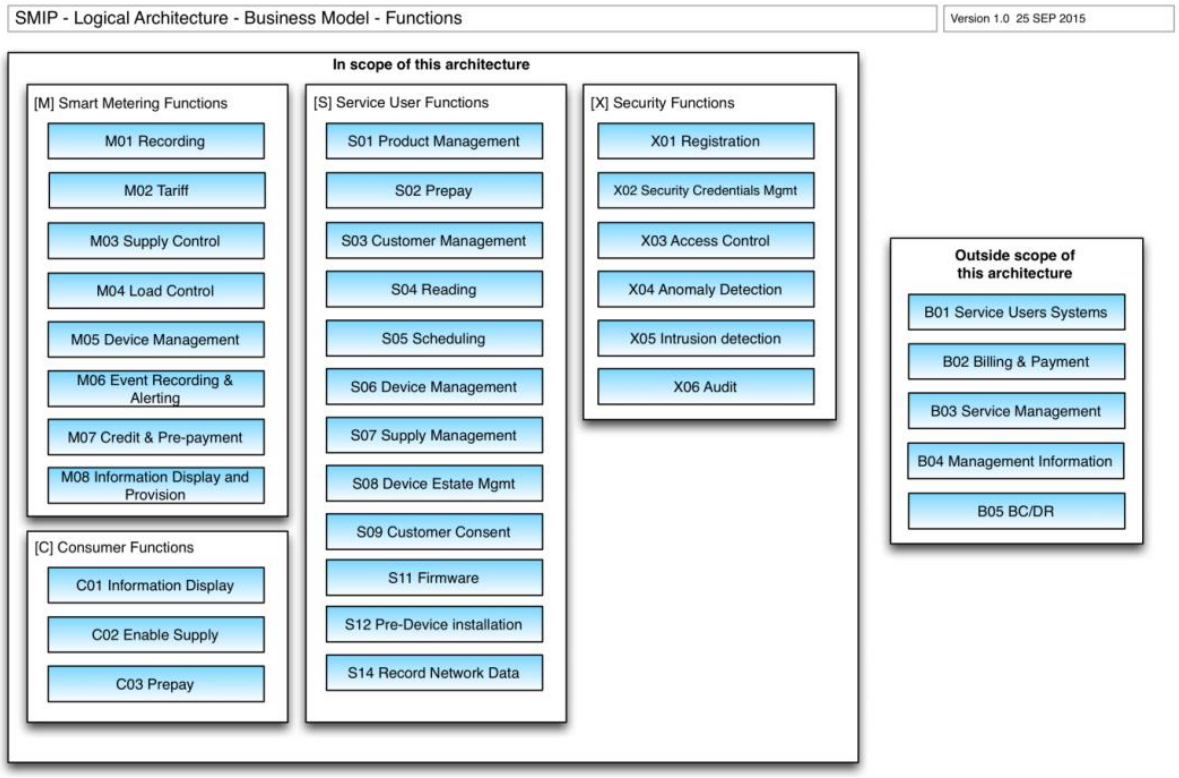

Figure 4.1.3: Business Function View

Table 4.1.3 lists the business functions in Figure 4.1.3 and decomposes them into their constituent business sub-functions for SMETS2+; the majority of these functions is also supported in SMETS1 and these functions are listed in Table 6.6. A further level of decomposition exists where it is sensible to implement multiple discrete sub-functions, service requests or interface interactions which are not shown here. These can be found in SMETS2+[3], CHTS[4], DUIS[6], MMC[7] and GBCS[5].

Ref	Name	Description
Consumer Functions		
C01	Information Display	The Consumer is able to read messages from the device displays originated by the Supplier as well as pricing and consumption data generated within the Smart Metering Equipment (SME).

Ref	Name	Description
C02	Enable Supply	The Consumer is able to enable the energy supply to the premises manually
C03	Pre-pay	The Consumer is able to add pre-pay credit and activate emergency credit to the SME.
Smart Metering Functions		
M01	Recording	The SME is able to record energy consumption and billing data in relation to time of use and block pricing tariffs. See SMETS2+[3] Sections 4.4.8 & 4.4.9, 5.5.8 & 5.5.9 and 5.11.3 & 5.11.4.
M02	Tariff	The SME is able to apply Time of Use (TOU) and Block pricing tariffs and switch between tariffs according to entries in the Tariff and measured consumption.
M03	Supply Control	The SME is able to Arm and Lock energy supply through remotely initiated commands and additionally according to defined rules when operating in pre-payment mode. See SMETS2+[3] Sections 4.4.7, 5.5.7, 5.11.2 and 7.4.
M04	Load Control	The SME is able to close and open Auxiliary Load Control Switches that are connected to the Home Area Network through remotely initiated commands. See SMETS2+[3] Section 6 Part D (for ALCS) and Section 9 (for HCALCS) for detailed requirements relating to Auxiliary Load Control.
M05	Device Management	The SME consists of several discrete devices which are interconnected in the Home Area Network. The end-to-end solution provides a secure process for registering devices onto the network and allowing devices to communicate with each other. See Section 4.3.4 for more information on device joining. In addition, it is possible to update the Firmware on certain devices in a secure way. See GBCS[5] Section 11 for detailed requirements relating to firmware.
M06	Event Recording & Alerting	The SME is able to record various events that occur during its operation in logs that are held on each device as well as sending Alerts for certain events across the SMHAN and SMWAN to authorised remote parties. See GBCS [5] Section 16.2 for a full table of Events and Alerts.
M07	Credit & Pre-payment	The SME is able to operate in both credit and pre-payment modes and maintain the current meter balance. When in pre-payment mode, the SME is able to accept prepayment credits from the Consumer. See SMETS2+[3] Sections 4.4.7, 5.5.7, 5.11.2 and 7.4.
M08	Information Display and Provision	The SME is able to display information to the Consumer including energy consumption and messages from the energy Supplier on the meters and In Home Display.
Service User Functions		
S01	Product Management	Functions in this category allow a DCC Service User to manage the mode of operation, price or tariff at a specified meter and for the meter to update its configuration to that effect. This service may be initiated by a variety of events, such as: • Change of Tenancy (CoT) • Change of Supplier (CoS) • New product offerings • Customer initiated

Ref	Name	Description
		• Supplier price changes Sub functions (see DUIS[6] for more detail) • Update Import Tariff • Update Price • Update Meter Balance • Update Payment Mode • Reset Tariff Block Counter Matrix
S02	Prepay	Functions in this category enable a DCC Service User to manage their prepayment metering estate such that credit can be purchased, prepayment specific configurations can be amended, and debt can be managed. In managing their Prepayment metering estate, DCC Service Users may experience the following business events that initiate use of a Prepay service request: • following a business event (such as CoT or CoS) a DCC Service User wishes to amend one or more of Prepayment configuration (e.g. non-disconnection calendar), and / or debt register values; • a customer makes a prepayment credit purchase resulting in a request to send a prepayment top up to the device to apply the credit purchase to the device registers; or Sub functions (see DUIS[6] for more detail) • Update Prepay Configuration • Top Up Device • Update Debt • Activate Emergency Credit
S03	Customer Management	Functions in this category enable DCC Service Users to manage customer facing elements of a device at a specified meter. Sub functions (see DUIS[6] for more detail) • Display Message to Customer • Restrict Access To Data For Change Of Tenancy • Clear Event Log • Update Supplier Name • Disable Privacy PIN
S04	Reading	Functions in this category enable a DCC Service User to retrieve an entry from various logs, counters, profile and configuration data on a specified device, or read the import or export register values at a point in time, of a specific device so that the DCC Service User can obtain Electricity or Gas Smart Metering Equipment consumption and usage details. Sub functions (see DUIS[6] for more detail)

Ref	Name	Description
		• Read Instantaneous Import / Export Registers • Read Instantaneous Prepayment Values • Retrieve Billing Data Log • Retrieve Import / Export Daily Read Log • Read Import / Export Profile Data • Read Network Data • Read Tariff • Read Maximum Demand Import / Export Registers • Read Prepayment Configuration • Read Prepayment Daily Read Log • Read Load Limit Data • Read Active Power Import • Retrieve Daily Consumption Log • Read Meter Balance
S05	Scheduling	Functions in this category enable a DCC Service User to request that the DCC creates, maintains and operates a schedule of regular and repeating actions for a specified device. Billing data retrieval schedules are not part of this service. Sub-functions (see DUIS[6] for more detail) • Create Schedule • Read Schedule • Delete Schedule
S06	Device Management	Functions in this category allow a DCC Service User to manage the products/operating settings associated with a specific device. Sub-functions (see DUIS[6] for more detail) • Read Device Configuration (e.g. Voltage, Randomisation, Billing Calendar, Payment Mode, Event and Alert Behaviours, etc) • Update Device Configuration (e.g. Voltage, Load Limiting, Billing Calendar, Gas Flow, etc) • Set Device Configuration (Import / Export MPxN) • Synchronise Clock • Read Event or Security Logs • Issue or Update Security Credentials • Reset Maximum Demand Registers / Configurable Time Period • Request Handover Of DCC Controlled Device • Configure Alert Behaviour • Read Device Log

Ref	Name	Description
		• Retrieve Device Security Credentials • Update Security Credentials (Change of Supplier) • Set Electricity Supply Tamper State • Set CHF Sub GHz Configuration (DBCH only)
S07	Supply Management	Functions in this category enable an authorised DCC Service User to remotely manage the energy at a consumer premises without the need for local interaction. These functions may affect supply switching of auxiliary (e.g. heating) electrical circuits. Sub-functions (see DUIS[6] for more detail) • Enable Supply (Electricity only) • Disable Supply • Arm Supply • Read Supply Status • Activate / Deactivate / Reset Auxiliary Load • Read Auxiliary Load Switch Data • Add / Remove Auxiliary Load To Boost Button • Read Boost Button Details • Set Randomised Offset Limit
S08	Device Estate Management	Functions in this category allow a DCC Service User to manage a device within the DCC estate such as commissioning, decommissioning, joining and un-joining devices moved in or out of the DCC estate or to confirm information held within the DCC for a specific device. Sub-functions (see DUIS[6] for more detail) • Commission / Decommission Device • Read / Update Inventory • Service Opt In / Out • Join / Unjoin Service • Read Device Log • Update / Restore Device Log(s) • Return Local Command Response (HHT) • Communications Hub Status Updates
S09	Customer Consent	Functions in this category enable a DCC Service User to generate and send a Customer Identification Number (CIN) to a specified Smart Meter and return the generated CIN to the sender of the Service Request. The customer can read the CIN from the device to the DCC Service User as evidence that they are the relevant householder and can give consent for the DCC Service User to access their consumption data. Sub-functions (see DUIS[6] for more detail)

Ref	Name	Description
		• Request Customer Identification Number
S10	This row is intentionally blank	
S11	Firmware	Functions in the category enable a DCC Service User to upgrade the firmware on a ESME or GSME, e.g. following a firmware fix (or up-to-date version) being released by the meter manufacturer. Sub-functions (see DUIS[6] for more detail) • Update Firmware • Read Firmware Version • Activate Firmware
S12	Pre-Device Installation	Functions in the category enable a DCC Service User to obtain or provide details to support the installation of Smart Metering Devices such as checking coverage information to support a prospective installation or provide device details to the Smart Metering Inventory to start the Smart Metering installation and commission process. Sub-functions (see DUIS[6] for more detail) • Request WAN Matrix • Device Pre-notification
S13	This row is intentionally blank	
S14	Record Network Data	Functions in this category enable a DCC Service User to initiate the recording of gas consumption data at 6 minute intervals over a 4 hour period, in the Gas Smart Metering Equipment Network Data Log. This enables the Distribution Network Operator to understand gas distribution network issues Sub-functions (see DUIS[6] for more detail) • Record Network Data (Gas)
Security Functions		
X01	Registration	Functions in this category refer to the requirement to register devices, organisations and Service Users before they can be allowed to perform business operations on the Smart Meter system. Registration data is used in the system to identify Supplier to SME relationships as well as the specific wide area network that connects the SME to the DSP.
X02	Security Credentials Management	Functions in this category relate to the issue, update and removal of security credentials for devices, organisations and end users.
X03	Access Control	Access Control is implemented within individual devices and within the ACB to ensure only defined operations can be executed by defined organisations and roles.
X04	Anomaly Detection	Anomaly detection and prevention is a service of the DSP which detects and alerts for potentially aberrant patterns of behaviour by DCC Users that may suggest operational compromise or malfunction.
X05	Intrusion Detection	Prevention of unauthorised access to networks.
X06	Audit	Audit capability requirements are detailed in SEC[2]
Business Support Functions – outside the scope of the architecture		
B01	Service Users Systems	These are the systems that exist within the Service Users domain which provide functions such as customer relationship management

Ref	Name	Description
B02	Billing and Payment	Billing & Payment functionality is a key element of the solution but is not a core element of the Smart Metering functionality. It is not described in this or referenced documents and is the concern of individual commercial parties to the Smart Metering system.
B03	Service Management	Service Management (including incident, problem and change management) is a key element of the solution and is referenced in some detail in SEC[2]. There is no further discussion within this Technical Architecture as this capability is defined by each commercial party to the Smart Metering system.
B04	Management Information	Management Information functionality is a key element of the solution but is not a core element of the Smart Metering functionality. Other than describing the data requirements of SME in this Technical Architecture and referenced specifications such as SMETS2+[3] and CHTS[4], the means of gathering, storing, processing and presenting Management Information is not discussed further
B05	Business Continuity and Disaster Recovery	Business Continuity & Disaster Recovery is a key element of the service provided and requirements for this are defined in SEC[2]. There is no further discussion within this Technical Architecture.

Table 4.1.3: Business functions relating to Smart Metering Equipment

4.1.4 Business Interactions

This section provides a more dynamic view by describing the business interactions between entities (for example the Consumer and Service Users or 'Remote Parties') and the Smart Metering Equipment for SMETS2+; please see Section 6 for information on SMETS1. Figure 4.1.4 shows how the business interactions flow between these entities and Table 4.1.4 describes the possible business interactions relating to each flow. All interactions are subject to Role Based Access Control (RBAC) – see GBCS[5] Section 20 Mapping Table for definitions of access control mapping against every Remote Party – device interaction (Use Case) defined in the system.

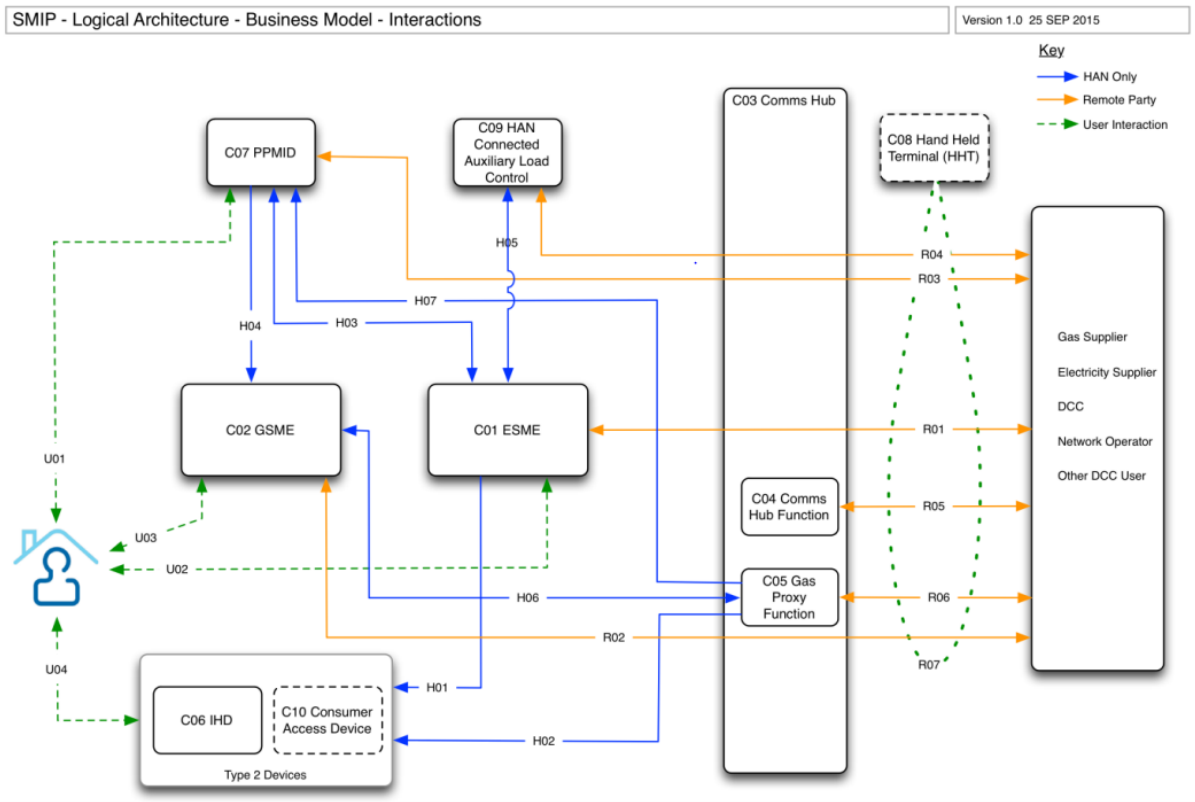

Figure 4.1.4: Business Interactions

In Table 4.1.4 below, business interactions, which are realised through message 'Use Cases' in GBCS[5], are listed against each of the flows in Figure 4.1.4[18]. These are grouped according to the devices that the interactions affect with some interactions being valid for multiple devices (e.g. ESME and GSME) and others being specific to a device (e.g. just GSME) This is an indicative, non-exhaustive list; for a complete list of message flows, see the 'Use Case' tab in the embedded spreadsheet "Table 20 GBCS 0.8.1 SMETS2+ Requirements Mapping Table" in GBCS[5] Section 20. This spreadsheet details each message use case along with the permitted sending roles and valid target devices. The language in the table below reflects that used in the GBCS for ease of cross reference.

Flow	Refs	Example Interactions
Consumer to PPMID user operations	U01	This flow involves the consumer interacting with the PPMID to undertake such functions as adding credit and activating emergency credit.
Consumer to ESME and GSME user operations	U02 and U03	This flow represents the interaction the consumer may have with the ESME and GSME directly including reading, initiating the boost button where fitted, adding credit or activating emergency credit where this function is present.
Consumer to Type 2 Device user operations	U04	The Consumer interacts with Type 2 devices such as an IHD or CAD.
ESME / GPF to Type 2 devices and PPMID information display	H01, H02, H03 & H07	This flow allows the ESME and GPF to send certain data items in a one way flow for display

[18] Prefixed 'U' for User (consumer), 'H' for HAN, 'R' for Remote Party interactions

Flow	Refs	Example Interactions
		on Type 2 Devices (such as In Home Displays and Consumer Access Devices) and PPMID.
PPMID to ESME top-up	H03	This flow involves HAN only interactions between the PPMID and the ESME. The PPMID sends an SMHAN only message to the ESME as a ZigBee Smart Energy (ZSE) Consumer Top-up command (see ZigBee Smart Energy Profile[11]). The ESME also provides information for display on the PPMID. Note: these interactions are not listed in Table 20 of the GBCS[5] since they utilise native ZSE commands – see GBCS[5] Section 14.7. • Activate Emergency Credit • Add Credit • Enable Supply
PPMID – GSME top-up	H04	This SMHAN only flow involves interactions between the PPMID and the GSME. In this flow the PPMID sends a message to the GSME as a GBCS specific (GBZ) Consumer Top-up command. As the GSME could be in a low power state at the time these interactions occur, the communication flow goes via the Communications Hub which buffers commands until the GSME wakes up and retrieves them. See CHTS[4] Section 4.4.4 and GBCS[5] Section 14.7 and Table 20. • Activate Emergency Credit • Add Credit Note that GSME cannot be remotely enabled for safety reasons so unlike ESME, the Consumer must press a button on the GSME to enable the flow of gas.
ESME to HCALCS	H05	Auxiliary Load Control Switches (ALCS), which may be directly connected to the ESME or SMHAN connected, are controlled by the ESME in response to Remote Party Commands or a scheduled event in the ESME calendar. Where the ALCS is SMHAN Connected (HCALCS) the ESME sends ZigBee Smart Energy (ZSE) commands to the HCALCS over the SMHAN. These are detailed in GBCS[5] Section 18.1.1.
Gas Proxy Function to GSME	H06	The Gas Proxy Function acts as a mirror for certain GSME data so that this data can be read in real-time even if the GSME is in a low power state. H06 represents the transfer of GSME data to the GPF and also the flow of commands to the GSME that have been buffered by the Communications Hub. See Section 4.3.5for a

Flow	Refs	Example Interactions
		fuller explanation of GSME mirroring and Tapping Off Commands.
The following rows group interactions together where they are the same for multiple devices and then show the exceptions that are targeted at a specific device – this is to aid readability since a large number of interactions are common to ESME and GSME.		
Remote Party to ESME and GSME	R01 & R02	A number of interactions are common to both the ESME and the GSME including for example: • Set Tariff and Price • Set Payment mode • Apply Pre-prepayment Top-up • Manage Debt • Update Prepayment Configuration • Activate Emergency Credit • Send Message • Disable Privacy PIN Protection • Write Supplier Contact Details • Set Alert Behaviours • Set Billing Calendar • Set MPxN Value • Remotely Open Load Switch / Close Valve • Arm Supply • Send Customer Identification Number (CIN) • Read Configuration Data Device Information (Smart Meter identity and type, including supply tamper / depletion state)
Remote Party to ESME only	R01	These interactions are targeted at the ESME only: • Set Tariff & Price on Secondary Element • Reset Tariff Block Counter Matrix • Read Energy Registers • Read Maximum Demand Registers • Read Electricity Daily Read Log (export only) • Read Electricity Half Hour Profile Data (export only) • Read Voltage Operational Data

Flow	Refs	Example Interactions
		• Read Configuration Data • Read Load Limit Data • Set Voltage Configuration • Read ESME Power Event Log • Read ALCS Event Log • Set Maximum Demand Configurable Time Period • Update Randomised Offset Limit • Set Export MPAN Value • Remotely Close the Load Switch • Set HCALCS or ALCS Labels • Set or Reset HCALCS or ALCS State • Reset ESME Maximum Demand Registers • Read HCALCS or ALCS State • Read Boost Button Data • Set ALCS and Boost Button Association • Set Supply Tamper State • Read Tariff Data second element • Read operational data (3 phase) • Set HCALCS or ALCS configuration (excluding labels) • Clear ALCS Event Log • Set Price on secondary element • Adjust Meter Balance • Reset Meter Balance • Set Alert Behaviours • Set Instantaneous Power Threshold
Remote Party to GSME only	R02	• Reset / Adjust Meter Balance (Payment Mode / Credit Mode) • Start Network Data Log • Read Network Data Log • Read Gas Configuration Data • Set CV and Conversion Factor Values • Set Uncontrolled Gas Flow Rate / Supply Tamper State

Flow	Refs	Example Interactions
		• Set Clock
Remote Party to ESME and GPF	R01 & R06	These interactions target the ESME and the GPF. The GPF target is an alternative to the GSME itself making use of its mirror of GSME data to enable a real-time interaction where the GSME might otherwise be in a low power mode and unable to communicate. • Set Change of Tenancy • Read Energy Registers (ESME) / Gas Consumption (GSME) (TOU) • Read Prepayment Registers • Read Billing Data Log • Read Daily Read Log • Read Tariff Data • Read Half Hour Profile Data • Read Configuration Data (Billing Calendar, Device Identity, Payment Mode, Pre-payment) • Read MPxN Value • Read Status of Load Switch / Valve • Read Daily Consumption Log • Read Meter Balance
Remote Party to GPF only	R06	• Restore GPF Device Log
Remote Party to PPMID	R03	• PPMID Commission Request (Supplier only) • Remove Device Security Credentials (Supplier only) • Update Security Credentials
Remote Party to HCALCS	R04	• HCALCS Commission Request (Supplier only) • Remove Device Security Credentials (Supplier only) • Update Security Credentials *Note that remote party commands to change the state of the HCALCS are targeted at the ESME rather than the HCALCS directly*
Remote Party to Communications Hub Function	R05	• Add Device to CHF Device Log (whitelist) • Remove Device from CHF Device Log (whitelist)

Flow	Refs	Example Interactions
		• Restore CHF Device Log • Read CHF Device Log / Check SMHAN Communications • Read CHF Event Log • Read CHF Security Log • Read CHF Configuration Data Device information (CH identify and type) • Read CHF Sub-GHz Channel (DBCH only) • Read CHF Sub GHz Channel Log (DBCH only) • Read CHF Sub GHz Configuration (DBCH only) • Set CHF Sub GHz Configuration (DBCH only) • Request CHF Sub GHz Channel Scan (DBCH only)
Hand Held Terminal (HHT) to Communications Hub	R07	• The HHT establishes a temporary connection to the Communications Hub for installation and maintenance and essentially acts as a proxy to the Service Users for all the Remote Party flows (R01 to R06). *This is indicated in Figure 4.1.4 with the green dotted lasso.*
Remote Party to ESME, GSME & CH	R01, R02, R05	• Read Firmware Version • Distribute Firmware • Activate Firmware
Remote Party to ESME, GSME, CH, GPF, PPMID & HCALCS	R01 – R06	• Provide Security Credentials Details • Issue / Update Security Credentials • Provide Device Certificates from Device • Update Device Certificates on Device • Clear Event Log
Remote Party to SMHAN devices	Several remote party flows – See Section 4.3.4	• Read Device join details • Join Device • Unjoin Device
Alerts from ESME to Remote Party	R01	• Active Power Import above Load Limit Threshold • Average RMS Voltage above Over Voltage Threshold

Flow	Refs	Example Interactions
		• Average RMS Voltage below Under Voltage Threshold • RMS above Extreme Over Voltage Threshold • RMS below Extreme Under Voltage Threshold • RMS above Voltage Swell Threshold • RMS below Voltage Sag Threshold • Supply Enabled • Power Loss / Supply Outage • Supply Outage Restored • Supply Armed • Supply Outage on Phase N • Supply Outage on Phase N Restored • Smart Meter Operational Integrity • Supply Disabled • Disablement of Supply Suspended
Alerts issued by the GSME to Remote Party	R02	• Unauthorised Physical Access • Trusted Source Authentication Failure • Not intended recipient of Command • Source Does not have Permission for Command • Low Battery Capacity • Emergency Credit Available • Credit Below Low Credit Threshold (prepayment mode) • Credit Below Disablement Threshold (prepayment mode) • Disablement of Supply Suspended • Unauthorised Communication Access attempted • Power Loss • Valve Armed • Smart Meter Operational Integrity • Supply Disabled
Alerts from the Gas Proxy Function	R06	• Trusted Source Authentication Failure

Flow	Refs	Example Interactions
		• Not intended recipient of Command • Source Does not have Permission for Command • GSME Billing Data Log Updated • Backup GPF Device Log
Alerts from SMHAN Devices to Remote Party	See Section 4.3.4	• Device join / unjoin alerts
Alerts from CHF to Remote Party	R05	• Device Addition To / Removal from HAN Whitelist • Limited Duty Cycle Action Taken Sub GHz; • Sub GHz Channel Changed; • Sub GHz Channel Scan Request Assessment Outcome; • Sub GHz Configuration; • Message Discarded Due to Duty Cycle Management; • No More Sub GHz Device Capacity. • Failure to Deliver Remote Party Message to ESME.

Table 4.1.4: Business Interactions

4.2 Application Model

Figure 4.2 below describes the capabilities, collaborations[19] and data storage for key application components (e.g. devices, networks, application software) for the four solution domains introduced in Section 3 for SMETS2+. Please see Section 6 for information about devices and functions for SMETS1 .

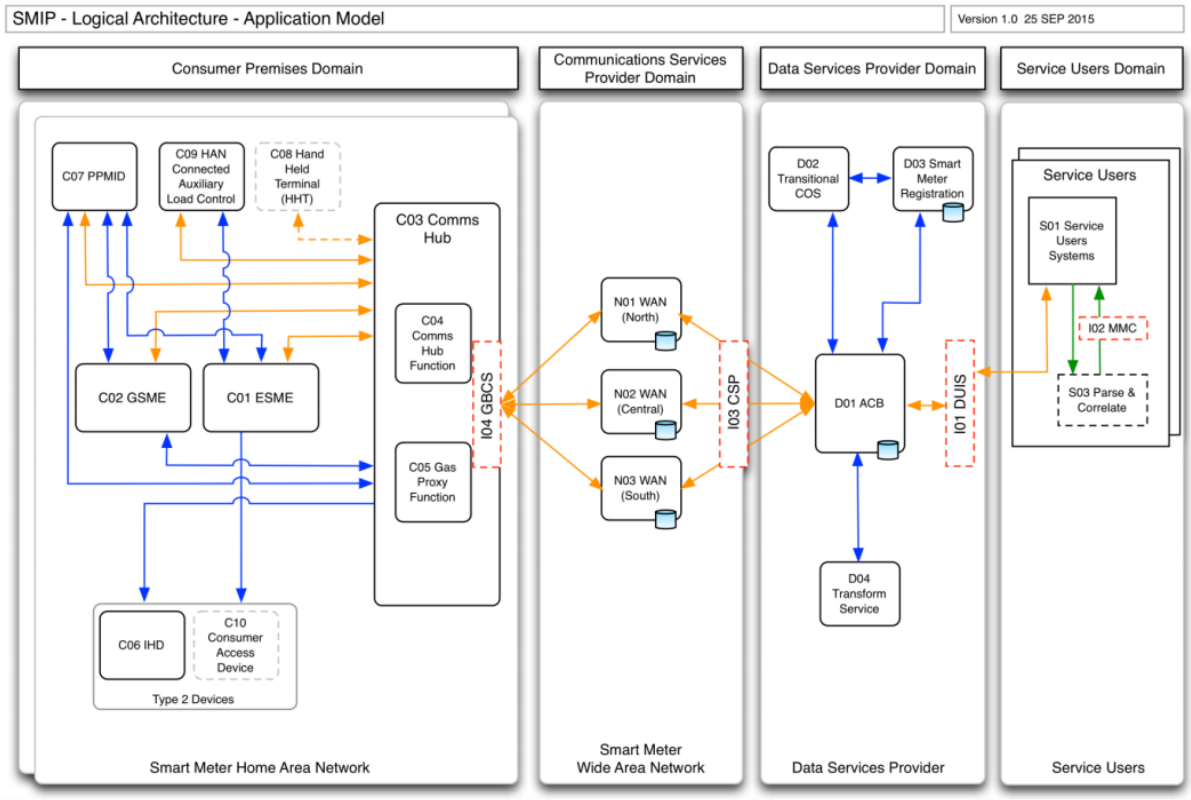

Figure 4.2: Application Model[20]

The application model covers the components domain by domain as follows:

- Consumer premises domain;
- Communications Service Provider domain;
- Data Service Provider domain; and
- Service Users domain.

4.2.1 Application Model

Within the consumer premises domain there are a number of devices interconnected by the Smart Meter Home Area Network (SMHAN). It should be noted that the SMHAN may operate within the 2.4Ghz frequency range only or both the 2.4GHz and Sub-GHz frequency ranges simultaneously. This

[19] At a high level how components relate to each other. See Business Interactions in Section 4.1.4 and Integration Model in Section 4.3 for a more granular view of collaboration from a business and technical perspective.
[20] Note that two of the three CSP contracts have been awarded to one solution provider making for two distinct wide area networks although this need not be the case from an architecture perspective, nor in future re-procurement by DCC.

functionality is dependent on the type of Communications Hub employed within the SMHAN, either Single Band or Dual Band respectively. The Communications Hub is the only device within in the SMHAN capable of support both frequency ranges simultaneously, all other devices are required to support either one or the other.

There are four categories of devices in this domain:

- ESME, GSME, Communications Hub and Gas Proxy Function;
- HHT;
- Type 1 Devices (examples include PPMID & HCALCS); and
- Type 2 Devices (examples include IHDs & CADs).

The first three categories of device require end-to-end interactions, i.e. between device and Service Users in the form of application layer messaging while the last category (Type 2 devices) require only local SMHAN interactions.

See Section 4.3.4 which explains in more detail how these different devices are able to join the SMETS2+ Home Area Network; please see Section 6 for SMETS1 related information, including devices.

4.2.1.1 Electricity Smart Metering Equipment (ESME)

The ESME is a metering device installed in the consumer premises which provides electricity metering functionality as well as additional 'smart metering' capabilities through its connectivity into the wider smart metering end-to-end system. The ESME is required to support SMHAN communications within the 2.4GHz frequency range only.

Reference	C01 ESME
Capabilities	• measuring and registering electricity consumption and support advance tariffing and payment systems; • supporting metering of import and export values, and variant meters – polyphase & twin element meters; • support remote disablement and enablement of supply and control of SMHAN connected and integral Auxiliary Load Control Switches; • receipt and scheduling of commands; • connectivity to the SMHAN, joining to other devices and communication with Remote Parties; • supports the end-to-end security model through verification of digital signatures and message authentication codes and Access Controls; and • support event reporting, firmware and security credential updates.

Reference	C01 ESME
Collaborators	• the ESME sends data and receives data and commands over the SMHAN; and • the ESME provides consumption and pricing data to Type 2 Devices where configured to do so.
Data Stores	• The ESME includes the capability to store constant, internal, configuration and operational data. For data requirements, see SMETS2+[3] Section 5.7 for single element meters, Section 5.13 for twin element meters and 5.19 for polyphase meters.

Table 4.2.1.1: ESME component description

4.2.1.2 Gas Smart Metering Equipment (GSME)

The GSME is a metering device installed in the consumer premises which provides gas metering functionality as well as additional 'smart metering' capabilities through its connectivity into the wider smart metering end-to-end system. The GSME is a 'sleepy device' which is powered only by its own battery which must last many years. As such, it spends much of its time in a low power state, 'waking up' occasionally to process commands or exchange data. To allow data held on the GSME to be accessed while the GSME is 'asleep', certain data is replicated between the GSME and the Gas Proxy Function (GPF) (see Section4.2.1.4) which resides on the Communications Hub (CH) (see Section 4.2.1.3) using a combination of ZSE[21] mirroring and a process called the 'Tapping Off Mechanism' (see Section 4.3.5 for an explanation of this). The Communications Hub will store remote party commands destined for the GSME until such time that the GSME awakes from its low power state to process them.

The GSME is required to support SMHAN communications within either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C02 GSME
Capabilities	• measuring and registering gas consumption and support advance tariffing and payment systems; • support remote disablement of supply; • receipt and scheduling of commands; • connectivity to the SMHAN, joining to other devices and communication with Remote Parties; • supports the end-to-end security model through verification of digital signatures and message authentication codes and Access Controls; and • support event reporting, firmware and security credential updates.
Collaborators	• a GSME requests connectivity to the SMHAN via the Communications Hub; and • the GSME sends data and receives data and commands over the SMHAN.

[21] ZigBee Smart Energy – one of the protocols used to communicate with devices in the smart metering system.

Reference	C02 GSME
Data Stores	• The GSME includes the capability to store constant, configuration and operational data. For data requirements, see SMETS2+[3] Section 4.6.

Table 4.2.1.2: GSME component description

4.2.1.3 Communications Hub

The Communications Hub is a pivotal piece of equipment within the end-to-end smart metering system, providing the routing capability between the wide area network (SMWAN) and the home area network (SMHAN) which connects all devices which comprise the smart metering system within the consumer premises. The Communications Hub is provided by the respective Communication Service Provider. In addition to providing this interface, the Communications Hub also hosts the Gas Proxy Function which is needed to hold a copy of most data that is held on the 'sleepy' GSME device.

The Communications Hub is required to support SMHAN communications using the 2.4GHz (Single Band) or both 2.4GHz and Sub-GHz frequency ranges simultaneously (Dual Band).

Reference	C03 Communications Hub / C04 Comms Hub Function (CHF)
Capabilities	• provides the interface boundary for communications between the DCC Communications Service Provider SMWAN and the SMHAN; • a queue to buffer commands for later delivery; • provision of a ZigBee Trust Centre; • Network coordinator for the SMHAN, either Single Band or Dual Band. • support firmware downloading for the Communications Hub; • support firmware downloading for the Gas Proxy Function (GPF); • SMHAN firmware data store for GSME and ESME; • support security credential updates; • buffering commands from SME (including in the event of the SMWAN being unavailable) and remote parties; and • provision of support for power outage detection and reporting.
Collaborators	• Smart Metering equipment and Consumer Access Devices request connectivity to the SMHAN via the Communications Hub; • the CSP will deliver commands from the DSP to the Communications Hub for onward transmission to designated SME; and • SME will send alert and service request responses to the Communications Hub for onward transmission via the CSP.
Data Stores	• The CH includes the capability to store constant, configuration and operational data. For data requirements, see CHTS[4] Section 4.6.

Table 4.2.1.3: Communications Hub and CHF component description

4.2.1.4 Gas Proxy Function (GPF)

The GPF is a logical device that is hosted on the Communications Hub (see Section 4.2.1.3). Its purpose is to hold a copy of most data that is held on the GSME which is a 'sleepy device' designed to spend much of its time in a low power state waking every 30 minutes to synchronise with the GPF. This data is then subsequently available in real time from the GPF to other devices and Service Users.

Reference	C05 Gas Proxy Function
Capabilities	• a separate logical device within the Communications Hub that provides a partial proxy across the SMHAN and SMWAN interface for the GSME to reduce the processing requirements that would otherwise impact the battery life of the GSME; • the GPF enables real time access to some of the GSME data and related reading functionality in the absence of the GSME itself, which operates on an intermittent basis.
Collaborators	• The GPF receives remote party commands through the Communications Hub Function (CHF); • GSME will periodically provide all data to the Communications Hub for storage and use within the Gas Proxy functionality; • The GPF provides some data held by the GSME; and • The GPF provides data to the IHD, PPMID, GSME and CAD.
Data Stores	• The GPF includes the capability to store replicated operational data from the GSME. See • CHTS[4] Section 4.4.3 for details.

Table 4.2.1.4: Gas Proxy Function component description

4.2.1.5 In Home Display (IHD)

The IHD is an electronic display device forming part of, or linked to, Smart Metering Equipment, which provides information related to a consumer's energy consumption and price data. The IHD does not allow the end user to issue commands to Smart Metering Equipment although it may perform some basic commands associated with joining the SMHAN and requesting specific data sets in association with an event that occurs on its user interface.

The IHD is required to support SMHAN communications using either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C06 IHD
Capabilities	• A device that displays consumption data and price information to the consumer but at a logical level does not issue any commands against SME.
Collaborators	• an IHD will request connectivity to the SMHAN via the Communications Hub; and • a consumer interacts with an IHD to gain access to consumption related information.
Data Stores	• the IHD has a data store to allow navigation and display of data read from other devices; and • does not have a device log but does have a device identifier. See SMETS2+[3] Section 6.6 for details.

Table 4.2.1.5: In Home Display component description

4.2.1.6 Pre-payment Metering Interface Device (PPMID)

The PPMID is a device to facilitate the use of prepayment services by consumers whose meters are typically in locations which are difficult to access. A PPMID is classified as a Type 1 Device, due to its interaction with metering equipment in 'Add Credit', 'Activation of Emergency Credit' and, for electricity only, 'Enabling of Supply'.

The PPMID is required to support SMHAN communications using either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C07 PPMID
Capabilities	• Provides the Consumer with the ability to Add Credit, Activate Emergency Credit, and for electricity, Enable the Supply; and • Provide IHD like display of information from connected devices See SMETS2+[3] Section 7.4.4.
Collaborators	• a PPMID will request connectivity to the SMHAN via the Communications Hub; • a PPMID may receive consumption and/or pricing data from smart meters; and • a PPMID will send 'Add Credit', 'Activate Emergency Credit' & 'Enable Supply' (Electricity Only);
Data Stores	• The PPMID has a data store to support its information display requirements, security credentials and device log. See SMETS2+[3] Section 7.6 for details.

Table 4.2.1.6: PPMID component description

4.2.1.7 Hand Held Terminal (HHT)

The HHT is ancillary equipment that may be used by energy Supplier staff (field engineers) to support installation and maintenance of SME. An HHT allows for delivery of Remote Party Messages to and from the SMHAN and the receipt of responses. 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. See GBCS[5] Section 10.5 for interface requirements but note that the specification of functional requirements beyond this is out of scope of this document or the referenced documents.

The HHT may support SMHAN communications using either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C08 HHT
Capabilities	• is capable of caching remote party messages, to which the appropriate message protection has already been applied; • is capable of sending cached remote party messages via the Communications Hub to specific devices on the SMHAN; and • is capable of receiving remote party message via the Communications Hub from devices on the SMHAN.
Collaborators	• The HHT establishes a connection with the Communications Hub to deliver cached remote party commands and receives responses. • The Communications Hub then relays the commands between other devices on the SMHAN.
Data Stores	• The HHT stores remote party messages to which appropriate message protections have • been applied by the Service User.

Table 4.2.1.7: HHT component description

4.2.1.8 HAN Connected Auxiliary Load Control Switch (ALCS / HCALCS)

The ALCS / HCALCS is a control switch for the provision of energy to functions other than the main supply, e.g. to switch on heating loads or to control an electric vehicle charging circuit. This device may be part of the ESME in which case it is an ALCS and is not connected to the SMHAN or, it may be a separate device in which case it is connected via the SMHAN. In both cases the ALCS and HCALCS are controlled by the ESME which responds to remote party commands for auxiliary load control.

The HCALCS is required to support SMHAN communications using either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C09 HAN Connected Auxiliary Load Control
Capabilities	• Is capable of switching auxiliary loads after receiving a command from the ESME.

Reference	C09 HAN Connected Auxiliary Load Control
Collaborators	• An Auxiliary Load Control Switch may be installed in an ESME (ALCS) or may be connected to the SMHAN (HCALCS). • he HCALCS establishes a connection to the Communications Hub and the ESME; and • The HCALCS receives commands and sends commands to one and only one ESME.
Data Stores	• The HCALCS stores constant and configuration data described in SMETS2+[3] Section 8.6.

Table 4.2.1.8: ALCS / HCALCS component description

4.2.1.9 Consumer Access Device

A Consumer Access Device (CAD) is a device that provides consumers with access to consumption and pricing data over the SMHAN. The intention is that the market will design devices that use the data to enable more intelligent use of energy including the ability for remote communication/control of consumer devices that support demand side management for example, a central heating thermostat or electric vehicle charging station.

The CAD is required to support SMHAN communications using either the 2.4GHz or Sub-GHz frequency ranges.

Reference	C10 Consumer Access Device (CAD)
Capabilities	• Is capable of reading certain consumption and data provided by ESME and the Gas Proxy Function;
Collaborators	• the Consumer Access Device will receive consumption and/or pricing data from either the ESME or Gas Proxy Function where the devices have been 'joined'.
Data Stores	• The CAD may have a data store but specification is outside the scope of this document or any of the referenced documents.

Table 4.2.1.9: Consumer Access Device (CAD) component specification

4.2.1.10 Smart Meter Home Area Network (SMHAN)

The SMHAN is a local area network that interconnects the smart metering equipment within the consumer premises. The SMHAN also provides separation from SMWAN communication infrastructure allowing greater flexibility and choice of technology specific to meeting the challenges posed within different geographies or properties.

4.2.2 Communication Service Provider Domain

4.2.2.1 Smart Meter Wide Area Network (SMWAN)

The SMETS2+ SMWAN is comprised of three[22] individual Communications Service Provider (CSP) provisioned wide area networks. Commands, responses and alerts are routed to and from SME via a network addressed Communications Hub using standard network layer mechanisms over shared or insecure physical media. The DSP Access Control Broker (ACB) selects the appropriate CSP WAN according to the registration data held for each Device. For SMETS1 please see Section 6.

Reference	N01, N02 & N03 WAN
Capabilities	• Transport of Commands, Responses and Alerts to and from SME via the Communications Hub
Collaborators	• The DCC Access Control Broker (ACB); and • The Communications Hub Function (CHF).
Data Stores	• The CSP WAN infrastructure stores network addressing and routing information appropriate to its specific implementation.

Table 4.2.2.1: Smart Meter Wide Area Network (SMWAN) component description

4.2.3 Data Service Provider Domain

4.2.3.1 Access Control Broker (ACB)

The Access Control Broker provides a single interface for Service Users to access the smart metering system in a secure way. It provides message handling capabilities such as orchestration and sequencing, queuing and retry processing. It also applies access control to requests and uses anomaly detection mechanisms to identify potentially spurious transaction patterns. The ACB also provides scheduling services for the future delivery of commands to the SME. The ACB applies Message Authentication Codes (MACs) to all[23] commands destined for SME in order to assure authenticity and integrity of messages. The communications between Service Users and the data and communications entity applies also to SMETS1, the communication between the data and communications entity and the SME is routed via the HES; see Section 6 for details.

The DSP is responsible for providing a rules-based pattern matching service to inspect all service requests. Where abnormal request patterns are found, e.g. Critical Command thresholds are exceeded, to place these service requests into a holding queue for analysis and validation before release. This provides an additional layer of security to minimise risks from events such as compromise of energy Supplier back end systems or denial of service attacks.

Reference	D02 Transitional Change of Supplier (CoS) service
Capabilities	• Message routing, orchestration and sequencing; • Message queuing and retry processing;

[22] Note that two of the three CSP contracts have been awarded to one solution provider making for two distinct wide area networks although this need not be the case from an architecture perspective, nor in future re-procurement by DCC.
[23] Except Retrieve Credentials

Reference	D02 Transitional Change of Supplier (CoS) service
	• Access control; • Anomaly detection; and • Command scheduling.
Collaborators	• DCC Service Users; • The Communication Service Providers; • The Transition Change of Supplier (CoS) service; • The Transform service; and • Smart Meter Registration (inventory).
Data Stores	• Smart metering data (for example pricing and consumption data) is not stored in the ACB. • Registration data is accessible to the ACB and also the Transitional Change of Supplier function.

Table 4.2.3.1: Access Control Broker (ACB) component description

4.2.3.2 Smart Meter Registration Data

A set of registration data used to record various details about meter points and corresponding responsibilities.

Reference	D03 Smart Meter Registration Data service
Capabilities	• Holds registration details for all GB Smart Meters
Collaborators	• Transitional Change of Supplier service; and • Access Control Broker
Data Stores	• The Smart Meter Registration Data stores information on devices, organisations and users that are part of the Smart Metering system.

Table 4.2.3.2: Smart Meter Registration Data component description

4.2.3.3 Transform Service

The DSP is responsible for the transformation of all DCC Service User Service Requests received in the format defined by the DCC User Interface Specification (see DUIS[6]) into 'HAN Ready' commands formatted in accordance with the GBCS[5]; this transformation applies only to SMETS2+. The DSP uses an inventory to determine, prior to transform, the correct data protocol / format for each service request received for a smart metering system target device, to ensure that all outgoing commands to the smart metering system are in the correct data format.

Where specified, the DSP will also send a copy of the 'HAN ready' commands with associated DSP Message Authentication Code (MAC) back to the DCC Service User should they wish to load this on to a Hand Held Terminal (HHT).

Reference	D04 Transform service
Capabilities	• For all Critical Commands, the DSP will return 'HAN Ready' commands back to the requesting DCC Service User, via the DCC User Gateway, for parsing, correlation and digital signing. • For Non-Critical Commands, upon successful transformation of the service request, the DSP will route the formatted message to the appropriate CSP without the need to return the formatted message to the DCC Service User for signing.
Collaborators	• Access Control Broker; and • Service Users
Data Stores	• There are no data stores in this component relevant to the end to end architecture.

Table 4.2.3.3: Transform service component description

4.2.4 Service User Domain

Within the Service User domain the components of the end-to-end architecture consist of systems that exist within each of the Service User organisations.

4.2.4.1 DCC Service Users / systems

Reference	S01 / S02 Service Users Systems
Capabilities	• Provide capabilities required by the Service User organisations; and • Capability for digitally signing critical messages before sending to SME.
Collaborators	• Integrate with DCC via the DUIS and MMC
Data Stores	• Data specific to the Service User organisations and the operation of the Smart Metering system

Table 4.2.4.1: Service Users Systems / systems component description

4.2.4.2 Parse & Correlate

Parse & Correlate functionality is implemented within the Service User domain as part of the solution to implement the required end to end trust model. This requires Service Users to digitally sign critical messages for non-repudiation purposes while separating the need for Service Users' systems to understand the encoded format of smart meter messages. The DCC encodes critical messages resulting from a service request through the DCC User Interface and provides the encoded message back to the Service User for signing. The Parse and Correlate component is used by the Service User to ensure the encoded message is semantically equivalent to the service request they submitted before they digitally sign the encoded messages and send that to the meter via another DCC User Interface service request. The Message Mapping Catalogue[7] is the interface specification that defines the format of messages that are returned from Parse & Correlate software[24] Parse & Correlate is also used to parse encoded Alerts and Responses. See Parse & Correlate Requirements[10] and Section 4.3 in this document for further detail on this component. Parse & Correlate applies to SMETS2+ only.

Reference	S03 Parse and Correlate
Capabilities	• Decoding of GBCS HAN ready messages and extraction of data items
Collaborators	• Service Users' systems make calls to Parse and Correlate after receiving GBCS HAN Ready commands from the DCC.
Data Stores	• There are no data stores in this component relevant to the end to end architecture.

Table 4.2.4.2: Parse and Correlate component description

[24] When the 'parse' functionality is used to return the abstracted form of the underlying GBCS format message

4.2.5 Key logical interfaces

A number of key interfaces are defined which allow Smart Metering Equipment manufacturers, Communication Service Providers the Data Service Provider and Service Users to interoperate securely and reliably to a defined standard. These interfaces are more fully described in Section 4.3 and by specific Interface Specifications listed below:

- I01 DUIS - DCC User Interface Specification DUIS[6];
- I02 MMC - DCC Message Mapping Catalogue[7];
- I03 CSP - DCC SMWAN Gateway Interface; and
- I04 GBCS - Great Britain Companion Specification (GBCS) [5].

These Interface Specifications build on other industry specifications and associated standards and the Integration Model in Section 3.3 provides more detail on this. Please note that GBCS[5] is not used for SMETS1, Section 4.2.5.1 Parse & Correlate and Section 4.2.5.4 Great Britain Companion Specification (GBCS) do not apply to SMETS1.

4.2.5.1 Parse & Correlate

The DUIS provides a business level service interface to the DSP for Service Users exposed as a set of web services and supporting the business functionality for Service Users introduced in Section 4.1.3. The DUIS interface provides an abstraction of the underlying encoded interactions with devices which are described by the GBCS[5] as well as some device services. In addition to allowing Service Users to send commands to, and receive responses and alerts from devices, the interface also allows messages to be encoded in the GBCS transmission format required by devices and returned to the Service User for loading onto an HHT. This is to support the end to end trust model which requires the Service User to digitally sign critical messages which in itself requires access to the underlying format of the message. The DUIS is developed and issued by the DCC and is supported by an XML schema formalising the DUIS interface.

4.2.5.2 DCC Message Mapping Catalogue (MMC)

The Message Mapping Catalogue[7] is the interface specification that defines the format of messages that are returned from Parse & Correlate[25] software. Parse & Correlate transforms the underlying GBCS device format of messages into the format described by the MMC.

4.2.5.3 DCC SMWAN Gateway Interface

This interface specification is internal to DCC and is a single set of published services provided by the CSP to the DSP for the transportation of 'HAN Ready' commands to the designated SME. It also provides a defined interface for responses and alerts sent from SME for distribution to requesting/subscribed DCC Service Users.

[25] See Section 4.2.4.2 for a description of Parse & Correlate functionality

4.2.5.4 Great Britain Companion Specification (GBCS)

The GBCS[5] defines the physical implementation standards for the chosen protocols as applicable to the SMIP for Great Britain for end to end and SMHAN only messages. The GBCS is, essentially, the interface to the SME, although its applicability extends across the end to end system with elements of the specification being relevant within the SMHAN, to the DSP and to Service Users.

4.3 Integration Model

This section describes the key interfaces in the SMETS2+ end-to-end system and important concepts and decisions that have been made in the integration design. It therefore provides important contextual information that can be used to navigate and interpret the more detailed specification in GBCS[5]. A number of key interfaces were introduced in the application model in Section 4.2.5 and this integration model provides further context and detail on how those interfaces are implemented. Please refer to Section 6 for information about SMETS1 integration.

Essentially there are two categories of communication for smart metering devices which use different combinations of communication protocols. Firstly there are Remote Party Messages which flow between Service Users and Devices; and secondly 'HAN only' messages which flow between Devices on the SMHAN. This section illustrates what protocols are used for each category of communication and how device to device flows are established, in particular:

- Application of protocol standards in the GB smart metering system;
- Protocols supporting Remote Party Messages;
- Protocol layering;
- SMHAN connected devices and joining; and
- GSME mirroring and tapping off mechanism.

4.3.1 Application of Protocol Standards

In any system, communications protocols specify how different components in the system communicate with each other. Where possible, existing standards should be used which offer a high degree of interoperability and which are supported by key stakeholders within the domain that the standards relate to. However, there are competing standards, and as part of the architectural design of any system, the most appropriate standards at the time must be selected.

The scope of the SMETS2+ GB smart metering system covers both electricity and gas metering which within the energy industry have aligned to two different application layer protocols; for SMETS1 please refer to Section 6. Additionally, different network layer protocols are required to operate in the SMHAN and the SMWAN. The following summarises the main protocol decisions:

- The ESME and the GSME mostly use different communications protocols for Remote Party Messages. The ESME mostly uses DLMS/COSEM [12] [13] and the GSME uses a structure containing ZigBee ZCL/ZSE [11]. As such each of these protocols must be supported on their respective devices and both are encapsulated in messages generated by the DCC to the respective devices.
- Neither DLMS/COSEM nor ZigBee Smart Energy (ZSE) provide all the capabilities required of the GB smart metering system, particularly relating to security, so some messages are encoded using the ASN.1 standard (with DER encoding)[14].
- The GBCS[5] defines a set of structures which carry ZCL / ZSE commands and these are referred to as the GBZ protocol.

- Different network layer protocols are used in the SMHAN and the SMWAN in order that each is fit for purpose in its respective network type.
- Different wide area network protocols are used by each of the regional Communication Service Providers (e.g. Long Range Radio, GSM, 3G and 4G) and others are possible.

4.3.2 Protocol Mapping between Components

From the business interactions shown earlier in Figure 4.1.4, we can see there are a number of end-to-end interactions (or Remote Party Messages) over the SMWAN and some interactions between devices on the SMHAN (or HAN only messages). Figure 4.3.2 below shows the underlying protocols and interconnections between the components through which these end to end business interactions are realised in the SMETS2+ system; please refer to Section 6 for SMETS1. Lower layer protocols (e.g. network) are shown with thicker arrows and the higher layer protocols (e.g. application) are shown with narrower arrows.

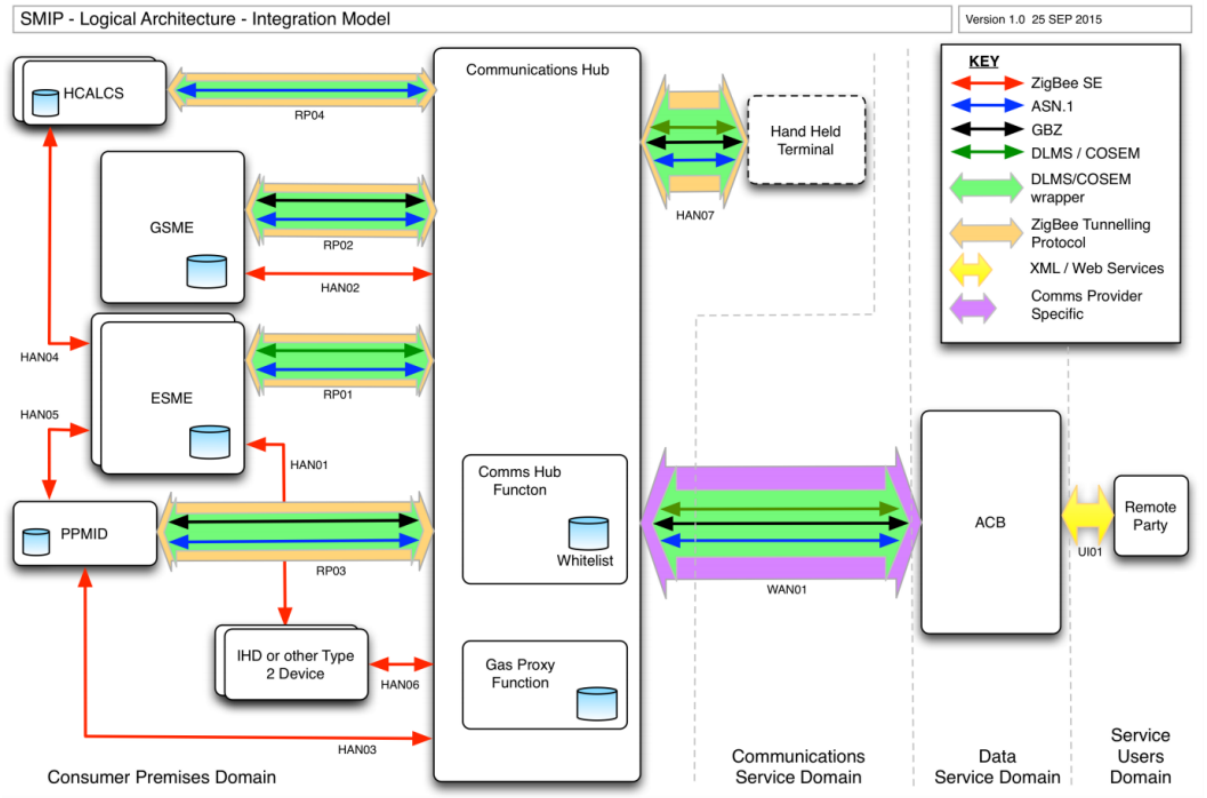

Figure 4.3.2: Integration Model

Flow	Description
Remote Party Flows	
RP01	The Communications Hub and the ESME communicate through a ZigBee tunnel. Remote party messages are encoded in DLMS/COSEM for most meter functions and ASN.1 for security functions, both being carried in a DLMS/COSEM wrapper.
RP02	The Communications Hub and the GSME communicate through a ZigBee tunnel. Remote party messages are encoded in ZigBee GBZ for most meter functions and ASN.1 for security functions, both being carried in a DLMS/COSEM wrapper.

Flow	Description
RP03	The Communications Hub and the PPMID communicate through a ZigBee tunnel. Remote party messages are encoded in ZigBee GBZ for pre-payment functions and ASN.1 for security functions, both being carried in a DLMS/COSEM wrapper. In addition, Prepayment messages between the PPMID and the GSME flow via the Communications Hub since the PPMID cannot communicate directly with the GSME using native ZigBee Smart Energy (ZSE) as is possible with the ESME. See 3.3.2.1 below regarding differences between ESME and GSME communication with PPMID.
RP04	The Communications Hub and the HCALCS communicate through a ZigBee tunnel. Remote party messages are encoded in ASN.1 carried in a DLMS/COSEM wrapper. However, note this is in contrast with the ESME which communicates with the HCALCS using native ZigBee Smart Energy (ZSE) (see HAN04 below).
SMHAN Only Flows	
HAN01	Type 2 devices such as In Home Displays or Consumer Access Devices may retrieve data from the ESME for display using native ZSE commands
HAN02	The GSME mirrors data to the Gas Proxy Function using native ZSE so that this data is available in real-time to other devices and Service Users while the GSME is in a low power state.
HAN03	The PPMID and the Gas proxy Function communicate using native ZSE for the purpose of displaying certain information on the PPMID that is held in the GPF.
HAN04	The ESME and the HCALCS communicate using native ZSE. Remote party commands to the ESME result in the ESME controlling the ALCS / HCALCS using this flow. Note that the HCALCS can also receive remote party commands directly (see RP04) but these are for interactions other than switching the state of the load control switch.
HAN05	The ESME and PPMID communicate using Native ZSE. See 4.3.2.1 below regarding differences between ESME and GSME communication with PPMID.
HAN06	Type 2 devices such as In Home Displays or Consumer Access Devices may retrieve data from the Gas Proxy Function for display using native ZSE commands.
HAN07	The Hand Held Terminal is used by maintenance engineers to issue pre-authorised Remote Party Commands and receive responses directly with the Communications Hub using a temporary ZigBee tunnel connection.
SMWAN Flows	
WAN01	This flow is between the ACB and the Communications Hub and uses a network protocol specific to the respective WAN CSP to carry 'HAN Ready Commands' which are encoded in GBZ, DLMS/COSEM and ASN.1 and wrapped in DLMS/COSEM wrapper
DCC Network Flows	
U01	This interface is defined by the DCC and is based on XML and Web Services. The DUIS and MMC define the interface

Table 4.3.2: Integration Model flows

4.3.2.1 PPMID connectivity

There are two different methods of communication for the PPMID for each of the ESME and the GSME which use different approaches for cryptographic key establishment. As such PPMID communicates via the CH with GSME using GBZ commands in a DLMS/COSEM wrapper over a ZigBee tunnel while the PPMID to ESME interface is implemented using the ZSE protocol. The PPMID function is defined for SMETS2+; please refer to Section 6 for information about SMETS1.

4.3.3 Protocol Layer View

4.3.3.1 Remote Party Messages

Figure 4.3.3 below shows how the different protocols are used in the SMETS2+ system for Remote Party communications to integrate:

- the Communications Hub with the device;
- the Communications Hub with the Access Control Broker (ACB); and
- Remote Party with the ACB.

At the transport layer at the bottom of the protocol stacks shown, different protocols are used within the SMHAN, the SMWAN and the DCC user network.

One layer up shows the DLMS wrapper operating end-to-end between the Remote Party and the Device.

At the application layer, because different protocols are used depending on the device being addressed and the particular message being sent[26], the end-to-end interaction may use either DLMS / COSEM, ZigBee GBZ or ASN.1 application layer protocols[27].

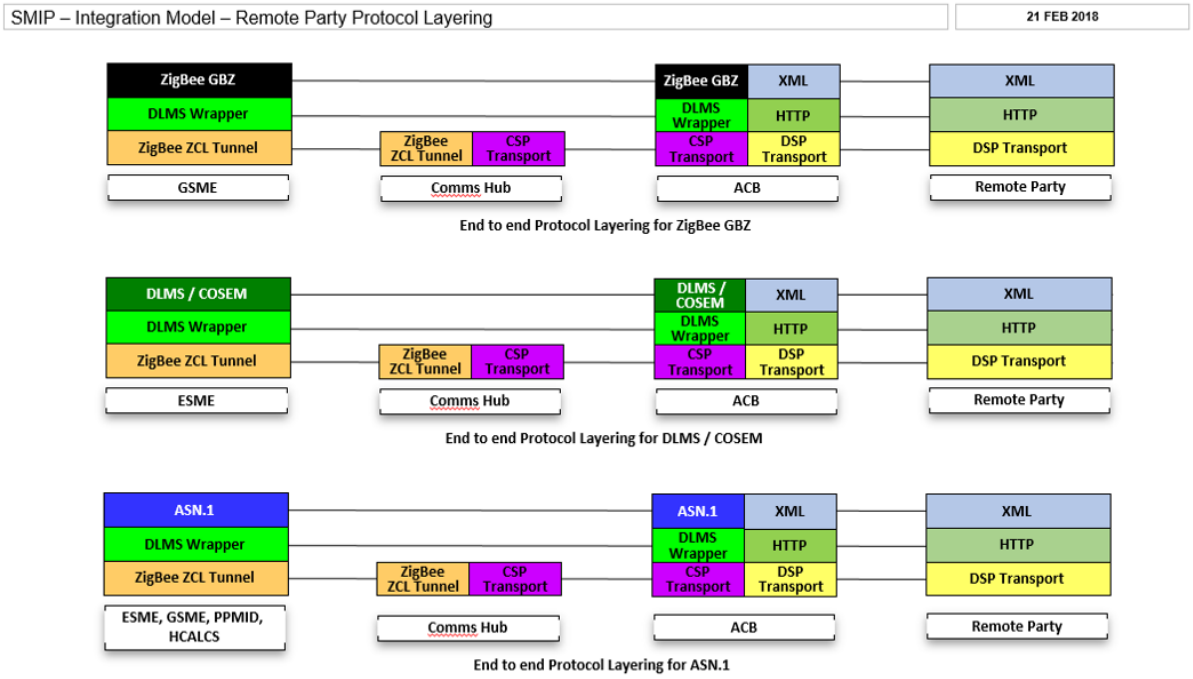

Figure 4.3.3: Protocol layers for remote party messages

[26] For example, some security configuration related messages use ASN.1 rather than DLMS/COSEM or ZigBee GBZ

[27] Strictly speaking ASN.1 is a presentation layer protocol but we roll up for ease of understanding this architecture

4.3.3.2 HAN Only Messages

In addition to the above end to end remote party messages, there are also device to device 'HAN only' messages in SMETS2+. These operate on a native ZigBee protocol stack and do not involve the same set of protocols in the above diagram which are used for remote party messages.

4.3.4 SMHAN connected devices and joining

In order for devices on the SMETS2+ SMHAN to communicate with each other the devices must have been added to the white-list which is the device log on the Communications Hub (CHF). This effectively provides a network level access control to stop unknown devices participating in SMHAN communications. Additionally, as shown in Figure 4.3.4 below, devices in the SMHAN are only permitted to communicate with each other in certain combinations which are defined in the GBCS (see GBCS[5] Section 13.7.1.2). Establishing this connection between devices on the SMHAN is called joining. For SMETS1 please see Section 6.

Figure 4.3.4 below illustrates the types of join that can be established between different device types and the resulting flow of information. The narrative below explains how each device is joined.

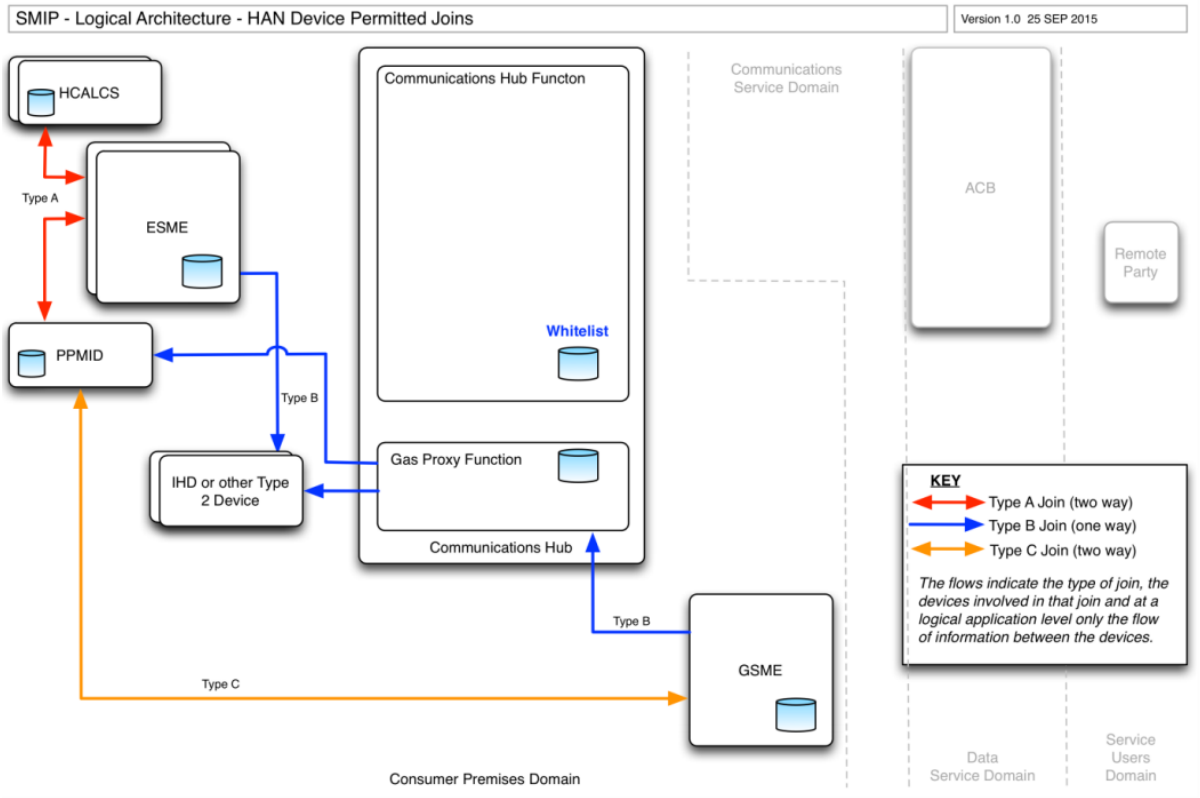

Figure 4.3.4: SMHAN device permitted joins

There are three mechanisms for joining and these are used by different devices:

- **Type A join** – in this type of join which involves an ESME and either a PPMID or HCALCS; both devices are sent remote party commands. Firstly the PPMID or HCALCS is sent details of the specific ESME that it will join with and these details are added to the device log. Secondly a remote party message instructs the ESME to join the other device which it then

instigates over the SMHAN with both devices communicating with each other for key establishment. The subsequent flow of information and commands between the devices is two way.

- **Type B join** – For a type B join, a remote party command is sent to only one device (ESME, GSME or GPF) which adds the target device to its own device log and then instigates the join over the SMHAN to the other device. In the case of the ESME, it will then communicate with the target device for key establishment. The resulting flow of information between the devices is one way (but may be pulled or pushed).
- **Type C join** – In this case, a remote party command is sent to both devices (GSME and PPMID) but unlike a Type A join, the commands include a Key Agreement Certificate from which the two devices will calculate a shared secret individually as opposed to exchanging messages over the SMHAN to establish a shared secret. Subsequent flow of information and commands is two way between the devices.

4.3.5 GSME Mirroring and Tapping Off Mechanism

This section applies to SMETS2+, for information about SMETS1 please refer to Section 6.

Because the GSME is a sleepy device, mechanisms are required to ensure that:

- data contained in the GSME is available in real time to other devices such as the In Home Display (IHD);
- Remote Party Commands can be buffered by the Communications Hub until such time that the GSME wakes up and can retrieve and process them; and
- any commands that change the data in the GSME also change the same data in the Gas Proxy Function copy provided the commands were accepted and executed successfully by the GSME.

The ZigBee protocol provides some features to mirror certain defined data (clusters) between the GSME and the Gas Proxy Function (GPF) but it cannot do this for all the data required to be mirrored by the GPF so two further mechanisms are required, the complete set being:

- **Native ZSE cluster mirroring** – e.g. for Metering and Pre-payment clusters;
- **Tapping Off Mechanism** - to apply changes to the GPF data that result from commands successfully processed by the GSME – e.g. Set Tariff and Price and Update Payment Configuration; and
- **Other data transfer flows** - that transfer remaining data from the GSME to the GPF where the data structures are created by the GPF and cannot be mirrored by native ZSE – e.g. Pricing and Calendar data.

The following diagram in Figure 4.3.5 shows these mechanisms in outline although the exact implementation is outside the scope of this document.

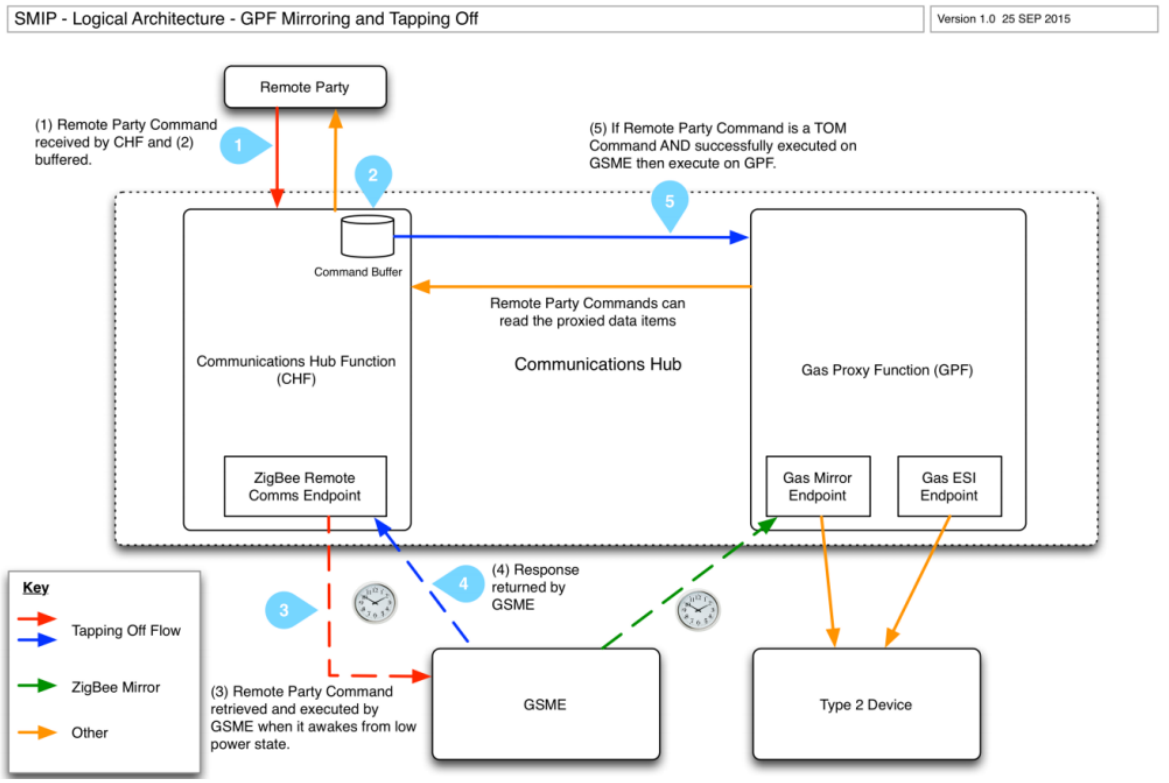

Figure 4.3.5: GPF Mirroring and Tapping Off Mechanism

4.3.5.1 Native ZSE Cluster Mirroring

Native ZigBee mirroring provides a mechanism to keep certain, but not all, GSME data in sync with the GPF copy. This flow is shown in green in Figure 4.3.5 and can only occur when the GSME is not in a low power 'sleep' state. The embedded spreadsheet in GBCS[5] Section 7.4 details the clusters, attributes and commands that are supported between devices on the SMHAN including data that is mirrored using native ZigBee cluster mirroring.

4.3.5.2 Tapping Off Mechanism

When a remote party command marked as "GPF required to tap off command" in the Mapping Table in section 20 of the GBCS[5] is sent to the GSME via the Communications Hub, the CHF or GPF within the Communications Hub takes a copy of the command and stores this until such time that the response to that command (or an alert in the case of future dated commands) is received from the GSME. Where the response indicates a successfully processed command the GPF then executes that command making changes to the GPF copy of the GSME data. Note the command can only be retrieved by the GSME from the Communications Hub when it is not in a low power state and the GSME's SMHAN radio is switched on (indicated by the dotted lines and clock icon). If the command was not executed successfully by the GSME or a timeout situation occurred the GPF data is not modified. In this way the GPF copy of the GSME data is kept in sync where native ZigBee mirroring is unable to do so (i.e. for remote party commands). The red (for inbound remote party command) and

blue (for successful application of that command to the GSME) flows in Figure 4.3.5 above show the sequence of events for a tapping off command.

GBCS[5] Section 10.3.4 lists the specific remote party commands that need to be handled using this Tapping Off mechanism.

4.3.5.3 Other Data Transfer Flows

Other data flows shown in Figure 4.3.5 for completeness (in amber) show firstly the flow of information from the GPF mirror to remote parties and also the flow of information from the GPF mirror to other devices on the SMHAN.

4.4 Information Model

The Information Model provides an illustration of the key entities, the relationships between them and the attributes, or key data items that comprise the entities. Since the purpose of this document is to provide a high level architecture view rather than act as a definitive design document, a complete model is not included here. Please see Section 6 for information on SMETS1.

4.4.1 Key Entities and Attributes

Figure 4.4.1 provides a high level view of the key entities and some of the attributes of those entities sufficient to illustrate, at a high level, the entity relationships in the SMIP end-to-end logical architecture[28]. Table 4.4.1 below provides a summary of the attributes listed here and references to the complete set of required attributes in SMETS2+[3] and CHTS[4].

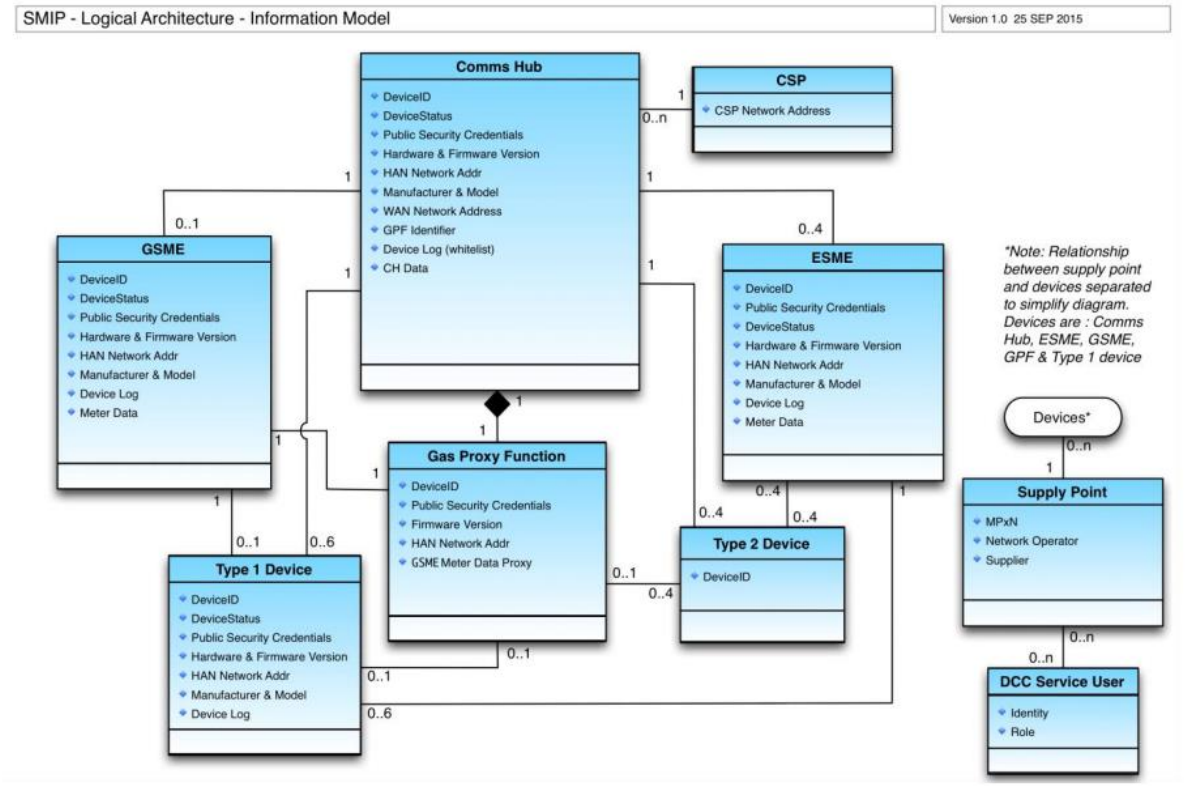

Figure 4.4.1: Key Entities and Attributes

Entity	Attribute	Description
Attributes Common to Comms Hub, ESME, GSME, GPF & Type 1 Devices		
	Device ID	Each device has a unique identifier based on the EUI-64 Institute of Electrical and Electronic Engineers standard.
	DeviceStatus	Held in the Smart Meter Inventory (see SEC[2] "SMI Status") to indicate whether a device is installed, commissioned, white-listed, decommissioned,

[28] The model is more infrastructure oriented than business data oriented. SMETS[3] and CHTS[4] provide a complete list of business data attributes.

Entity	Attribute	Description
		suspended or withdrawn.
	Public Security Credentials	Security credentials for the device and other parties authorised to communicate with it.
	Firmware Version	The version number for the active firmware of the device.
	HAN Network Address	Every device on the SMHAN becomes part of that network through a process of joining (See Section 4.3.4) and must be listed in the whitelist which is the Communications Hub Device Log. The SMHAN Network address uniquely identifies the device within the HAN.
	Device Log	A list of devices with which this device is able to communicate over the SMHAN.
	Make & Model	The manufacturer and model number (excl GPF)
Communications Hub		The Comms Hub provides routing of remote party messages between devices and the Access Control Broker via the Wide Area Network. In addition it hosts the Gas Proxy Function to allow real time access to data otherwise occasionally accessible on the GSME.
	WAN Network Address	The address of the Wide Area Network interface.
	GPF Identifier	The GPF which is hosted within the Communications Hub is an individually addressable device and therefore has its own EUI-64 ID.
	Device Log (whitelist)	As the trust centre for the Home Area Network (HAN), the Communications Hub's Device Log is the whitelist for all other devices on the HAN that may participate in communications.
	CH Data	The Communications Hub holds data to support communications and routing such as the Communications Store and Event Log Communications Hub Data is detailed in CHTS[4] Section 4.6.
ESME		The Electricity Smart Meter
	Meter Data	Meter data includes Constant, Internal, Configuration and Operational data stored on the device to support its purpose and functionality. A complete list of required data attributes can be found in the following sections of SMETS2+[3]: • Single Element Meter – 5.7 • Twin Element Meter (additional to Single Element) – 5.13 • Polyphase Meter (additional to Single Element) – 5.19
GSME		The Gas Smart Meter
	Meter Data	Meter data includes Constant, Internal, Configuration and Operational data stored on the device to support its purpose and functionality. A complete list of required data attributes can be found in SMETS2+[3] Section 4.6.
Gas Proxy Function		The Gas Proxy Function (GPF) provides a real time copy of GSME data to remote parties and other devices on the

Entity	Attribute	Description
		SMHAN as well as buffering commands pending wake up of the GSME.
	GSME Meter Data Proxy	In order to provide real-time access to GSME data, the Gas Proxy Function (GPF) maintains a copy of GSME data. CHTS[4] Section 4.6 provides a complete list of the attributes stored on the GPF.
Type 1 Device		A Type 1 Device is able to participate in two way communication with certain other devices in the SMHAN.
		See common attributes above
Type 2 Device		A Type 2 Device can only read data from other devices on the Home Area Network. It does not have a Device Log but does have a Device ID to identify it in the SMHAN.
	Device ID	The Device Identifier
Supply Point		The record of the current energy Supplier and Distribution Network Operator for a given premises supply point.
	MPxN	Unique identifier for every energy supply point in Great Britain being one of MPAN - Meter Point Administration Number for electricity or MPRN - Meter Point Reference Number for gas supply.
	Distribution Network Operator	The Distribution Network Operator to which the supply point is registered.
	Supplier	The current energy Supplier to which the supply point is registered
DCC Service User		A user of the DCC Services that access the Smart Meter system
	Identity	The identity related to a set of credentials such as User ID and password or other authentication mechanism.
	Role	The DCC Service User will have a role or role(s) which they have been granted and provide differing levels of access to DCC Services.
CSP		This entity provides a container for the attributes rating to a Communications Service Provider.
	CSP Network Address	The network and address details of the Communication Service Provider

Table 4.4.1: Key Entities and Attributes

4.5 Security Model

Smart metering in Great Britain is based on a series of distributed linked systems which provide services and communications between Smart Metering Equipment and the organisations which are responsible for, but remote from, the Smart Metering Equipment. The threats and risks this poses have informed the Security Architecture[9], which describes the security controls used to secure smart metering and how these controls are applied to the components within the end-to-end Technical Architecture. This section provides a high level view for the contextual framework of the security model employed for SMETS2+, together with the abstracted logical architecture upon which a trust modelling methodology was applied to derive the Security Architecture and some of its key controls.

SMETS1 benefits from the same security features with regards to the connection between the DCC Users and the DCC system; equally the communication from the DCC system to the HES is standardised and secured. The communication between the HES and SMHAN devices is secured individually for each HES since SMETS1 allows implementation specific the protocol selections. Please see Section 6 for SMETS1 information.

4.5.1 Contextual Framework

The controls surrounding smart metering ensure that the system is secure, that this security is proportionate to the risks, and that the system can be delivered to budget. Key to the success of smart metering is that:

- risks to critical national infrastructure, of which smart metering is a component, are minimised;
- reputational damage to smart metering, Government and the energy industry resulting from security vulnerabilities are minimised;
- trust (in terms of authenticity, integrity and non-repudiation) is placed with responsible parties; and
- risks relating to energy supply, financial fraud, data privacy and system availability are mitigated.

At the same time, the security architecture needs to be flexible to cope with future changes to business processes, and provide for additional security controls to be implemented as new threats emerge.

The Security Architecture has been designed with three principles in mind, namely:

- **Layered Security** - provide defence in depth through multi-layered controls within various components and entities;
- **Least Privilege** - support the principle of least privilege, whereby each component or entity involved in the end-to-end smart metering system has the minimum privileges required to carry out its defined function; and

- **Need to Know** - support the concept of each component or entity only being in receipt of information, or having access to information, if they have appropriate authorisation and require access to that information to conduct their duties. Access to information and systems should be denied by default.

4.5.2 Security Logical Architecture

The security requirements were developed using HMG IS1 Risk Assessment together with the security control categories in the ISO27001 control set. In order to ensure that trust within Smart Metering was implemented appropriately on each component part of the end- to-end architecture, a process of trust modelling was conducted with input from CESG[29].This was a five step exercise to:

1. develop a series of abstract business process models, assuming no solutions and no constraints;
2. identify the trust relationships, i.e. who originates and receives messages;
3. overlay a generic physical architecture covering the Smart Metering Equipment, the 'Actors' and any essential enabling functions, such as a Broker role;
4. develop 'derived' Trust Models that take solutions and constraints into consideration; and
5. identify security consequences (i.e. alignment and differences), and resolve any trade-offs.

In turn, this leads to a logical architecture (as shown in Figure 4.5.2) in which:

- trust is maintained between the point of origin and destination without reliance on intermediaries, such as the DCC. For example, meters must be able to determine whether a message has been changed by intermediaries and, should this occur, reject the associated message;
- intermediaries are unable to see personal data, so such data should be encrypted end-to-end;
- intermediaries are able to see other forms of data to implement certain security controls, specifically to provide early detection of potential systemic compromises;
- there should be no single point compromise for the smart metering infrastructure as a whole; and
- the number of points of potential attacks is minimised.

[29] Originally standing for the Communications Electronics Security Group although this expansion is no longer used. CESG has now be superseded and replaced by the National Cyber Security Centre (NCSC).

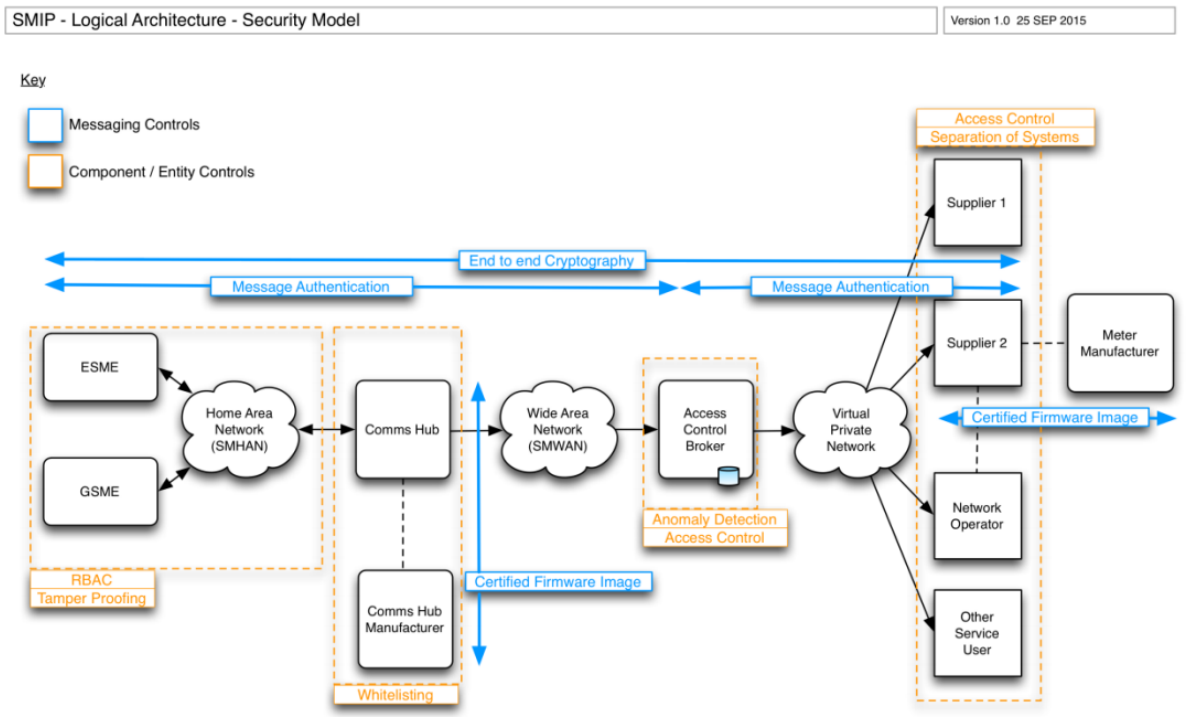

Figure 4.5.2: Key Security Controls

Physical constraints (not least meter processing power) mean that end-to-end authenticity, integrity and non-repudiation for all messages would give rise to disproportionate costs. Therefore, a hybrid model has been implemented whereby controls are applied only to Critical messages (see Section 4.1) which are potentially supply-effecting, relate to financial fraud or relate to the security of Smart Metering Equipment itself (e.g. updates to Firmware). Other *non-critical* messages are treated differently.

4.5.3 Components, Controls and Standards

In line with key principles of the Security Architecture, a series of layered security components, controls and standards have been derived. These are:

- end-to-end security based around a combination of asymmetric and symmetric cryptography, using recognised industry and protocol standards for security across the Home Area Network and Wide Area Network;
    - this cryptographic approach provides for:
    - Message Authentication;
    - Digital Signatures; and
    - Encryption.
- applied as appropriate to control risks and threats posed by critical, non-critical and sensitive transactions;
- Role based access control (RBAC) – system permissions determined by the role which a user, device or organisation has in relation to the system;

- Device-based access control (DBAC) and Whitelisting to manage access control between SMHAN devices at the level of a single SMHAN;
- anomaly detection – a set of services and tools to identify and respond to anomalous transactions or transaction patterns;
- physical, network and platform security considerations;
- ensuring that specific transactions (such as manual entry of prepayment credit top-ups) are specifically and appropriately secured;
- support for cryptographic key management to manage the creation, distribution and securing of cryptographic material, including a PKI Architecture to support the use of public certificates, and establish explicit trust between components;
- the PKI that supports end to end message security is referred to as Smart Metering Key Infrastructure (SMKI) and consists of:
    - PKI Governance structure, including operational management aspects;
    - Root Key and Root Certification Authority;
    - PKI hierarchy, defining Certification Authorities sub-ordinate to the Root and from which trust is derived; and
    - Key and Public Certificate management, including subscription, distribution, replacement, recovery and revocation.

Further detail can be found in the End to End Security Architecture[9] and the GBCS[5] sections 4, 8 and 12.

5 Architecture Considerations

This section further elaborates a number of specific architectural considerations. These are areas that are not immediately apparent from the Architecture Models presented so far and for which it is important to explain the approach / design adopted for SMETS2+; for information on SMETS1 please see Section 6. The following points are addressed:

- Criticality of message interactions;
- Role Based Access Control (RBAC);
- Routing of critical messages and Parse & Correlate;
- End to end time management;
- End to end error handling;
- Globally unique Entity Identifiers; and
- Message versioning.

5.1 Criticality of message interactions

A key architectural consideration which defines the integration architecture and security architecture is that of message criticality. In the SMIP, messages are sent between smart metering devices, Service Users and systems. Two kinds of message interaction (critical and non-critical) are defined and are treated differently from a security and message processing perspective. Different elements of security such as authenticity, integrity, confidentiality and non-repudiation (see Security Architecture[9]) may be applied and the routing of message interactions is different depending on criticality.

5.1.1 Critical Command

If a command is critical it means one or more of the following apply:

- it can potentially affect energy supply;
- it can potentially compromise the security of Smart Metering Equipment on consumer premises; or
- it can potentially lead to financial fraud.

For critical commands, end-to-end (i.e. between the smart metering device and the organisation originating an instruction for it) authenticity, integrity and non-repudiation is needed. For example, when a smart meter gets an instruction from its energy Supplier to disable supply, the smart meter needs to be sure that (a) the instruction really came from its Supplier and (b) the instruction originally issued by its Supplier was to disable supply.

The requirement for end-to-end authenticity, integrity and non-repudiation for critical commands is met by digital signing by the originator of the message (e.g. energy Supplier) and not by an intermediary (e.g. DSP). In addition to this a Message Authentication Code (MAC) is added to the digitally signed message by the DSP.

5.1.1 Non-critical Command

For non-critical commands, authenticity and integrity provides an adequate degree of protection. Non-repudiation would require the meter to check a digital signature requiring the meter to do relatively processor intensive cryptographic operations.

For example, if an energy Supplier wishes to display a Customer Identification Number on the consumer's smart meter or IHD:

1. The Supplier can send the request to the DCC. The DCC can check that the request came from the Supplier and that the request has not been altered in transit; and
2. The DCC can then send a request to the smart meter. The smart meter can check that request came from the DCC and has not been altered in transit (so is as the DCC sent it).

These requirements for non-critical commands are met by using digital signing for the interaction between the DCC and DCC Users, and by using a Message Authentication Code (MAC) for the interaction between the DCC and the smart meter rather than the end-to-end trust model described above for Critical Commands.

5.2 Role Based Access Control (RBAC)

Role Based Access Control is implemented both within the ACB and also within Devices. Each provides the following capabilities:

ACB RBAC	SME device RBAC
• determines valid DCC Users that can request consumer data, i.e. meter readings; • provides access control for pairing of devices including remote service for type 2 pairing requests • provides access control for valid DCC user requests for type 2 pairing and type 1 whitelisting (i.e. at Install & Commission); • provides access control at Change of Supply against registration data to validate pending/active registration; and • provides data level access control for transformation of noncritical DUIS service requests into 'HAN Ready' commands, e.g. import or export profile data.	• applies access control on every critical command received based upon known roles; Supplier, Distribution Network Operator, DSP, Recovery, Root.

Table 5.2: ACB and SME device Role Based Access Control

5.3 Routing of critical messages and Parse & Correlate

DCC Service Users interact with the Smart Metering Equipment via an interface called the DCC User Interface specified by DUIS[6]. This is a business level interface which abstracts the underlying encoded transmission format of messages to and from smart metering devices which Service Users do not necessarily need to understand. However, because the security requirements for Critical (only) messages mean that non-repudiation must be provided end-to-end (between the Service User and the Device), messages to the device must be digitally signed by the Service User and not by

some intermediate party. As such the encoded transmission (or HAN Ready) version of the message to the device must be made available to the Service User[30] and signed by them (rather than by the DCC's Access Control Broker) before being sent to the device.

This is achieved through a mechanism whereby the Service User makes a request via the DUIS to the Transform Service and the DCC returns to the user the encoded HAN Ready message which the Service User digitally signs and then sends back to the DCC via the DUIS for onward transmission to the Device.

However, because the Service User, or their systems, do not necessarily understand the encoded HAN Ready format of the returned HAN Ready message, a further capability is required to allow the Service User to verify that the encoded transmission format message returned by DCC is substantively equivalent to the original request content submitted in the DUIS request. This capability is provided to Service Users as an optional software component called Parse & Correlate which is physically deployed within their infrastructure. Once this software confirms the message is substantively equivalent the Service User can sign the message and send it via the DCC for onward delivery to the device.

So in summary the steps for a critical message are:

- Service User submits transform command DUIS Service Request to the DCC;
- DCC constructs and returns the encoded transmission format message;
- Service User verifies that the returned encoded message is substantively equivalent to the original Service Request using Parse & Correlate and then digitally signs the message;
- Service User submits the encoded message via a send command DUIS Service Request to DCC;
- DCC applies a Message Authentication Code (MAC) to the message; and
- DCC send the encoded, signed and MAC'd message to the Device.

In the case of non-critical messages, only authenticity and integrity but not end-to-end nonrepudiation is required so the process is simpler in that the DCC simply constructs and sends the encoded message directly on receipt of a DUIS Service Request.

There are two relevant interfaces to these services. Firstly DUIS[6] defines the interface to the DSP web services to transform and send messages. Secondly, the MMC[7] defines the interface to the locally deployed Parse & Correlate software (if used[31]).

If Parse & Correlate is not used, Service Users would need to understand the GBCS encoded transmission format of messages.

[30] Usually for abstracted interfaces, the underlying format would be encapsulated in the solution and not made visible to the user of the interface.

[31] The use of the Parse & Correlate component is optional but the message equivalency check is still a requirement.

5.4 Time Management on Devices

SMETS2+[3] states that each ESME / GSME must have a Clock of its own; see Section 6.7 for information about time management in SMETS1. Significant parts of the business functionality have a dependency on time and therefore the accuracy of the clock. Some of this functionality is 'critical' in that it:

- may affect load / supply (e.g. TOU prepay tariffs; Non Disablement calendars; HCALCS calendars);
- may have financial implications (e.g. application of standing charge); and
- the effectiveness of the cryptographic protections laid out in SMETS2+, and thus the security of the ESME / GSME is also partly dependent upon accurate time.

Therefore, the setting of ESME/GSME time is a 'critical' function that, in common with other ESME / GSME critical functions, needs to be under the control of the energy Supplier. The ESME/GSME functionality that relies on time has a range of 'real world' accuracy requirements (e.g. cryptographic protections do not require such accurate time as, say, TOU

tariffs). SMETS2+ requires accuracy of +-10 seconds of UTC32 under normal operating conditions.

Suppliers can send clock set remote party commands to the ESME and GSME but because the GSME is a sleepy device, it may not retrieve a clock set command from the Communications Hub command buffer until it next wakes up which could be up to 30 minutes after the clock set command was sent by the Supplier to the GSME (and therefore the Supplier's time specified in the command may be up to 30 minutes out of date).

However, the ESME and GSME devices do not set their clocks to the Supplier time value given in the command but rather set their clocks to the value of the Communications Hub time provided it lies within the tolerance specified in the remote party command. Therefore, when setting clock for the GSME, the tolerance specified in the command should account for the potential time delay between the command being sent and the GSME waking up to process the command.

This approach allows the Supplier to be in control of setting the clocks on the ESME and GSME while using the Communications Hub to provide accurate time (within CHTS[4] requirements of 10 seconds) to synchronise their clocks with.

Communications Hubs synchronise their clocks using the time provided over their SMWAN interface whenever time information is available.

ESME & GSME attempt to synchronise their clocks with the Communications Hub every 24 hours. It is expected that the DCC (via its CSPs) will secure its network time services appropriately and periodically monitor their accuracy against independent sources. GBCS[5] Section 9 provides detailed steps for time synchronisation and population of relevant time fields and status indicators and caters for situations where time is unobtainable or considered invalid.

5.5 End to End Error Handling

The majority of exceptions that may arise as part of the DCC service will be captured via specific device error responses, allowing standard incident management processes to manage the associated resolution outcomes.

However, the end-to-end system includes multi-party responsibility with multiple hops that lead to complexity when considering how to identify and handle error conditions arising from 'unfulfilled service requests', i.e. service requests that have had no response within the associated service level agreement (timeouts).

Integration constraints between all parties involved in Smart Metering require Service Requests to be managed end-to-end via the application layer, either to successful completion, failure or timeout. Whilst the DSP and CSP solution architectures allow for a greater degree of granularity with respect to root cause analysis and proactive identification of timeouts, the DSP must manage and report on timeouts for Future Dated & DSP Scheduled service requests. It is assumed that DCC User applications will manage interactions for On Demand service requests. (Note: Billing Reads are in SMETS2+ terms Alerts and so originate at the meter and therefore can only be tracked by the registered Suppliers).

5.6 Globally Unique Entity Identifiers

Within GB Smart Metering, the Entity Identifier is an item of data that uniquely identifies an Organisation or Device and thereby distinguishes it from all others. It may also be referred to as a Globally Unique Identifier (GUID). A key purpose of the Entity Identifier is to allow all messages to be correctly and reliably routed. To ensure end-to-end operations, device identity requirements and other areas of additional consideration:

- EUI-64 has been adopted for GUIDs for both Devices and Organisations;
- all organisations sending and receiving GBCS messages through the DCC, and all Device manufacturers, use an Organisationally Unique Identifier (OUI) issued by the IEEE[32] Registration Authority;
- the Device manufacturers are responsible for generating the GUID for each Device; and
- the manufacturer controlled part of the GUID will be an incrementing sequence number.

The GBCS uses the same field ('Entity Identifier') for Devices as for other Entities addressed within GB Smart Metering. The allocation of Identifiers (by the SEC Administrator) for all entities needs to be compatible to ensure uniqueness. The most effective way to ensure this alignment is to use the same allocation mechanism for all Entities within GB Smart Metering.

See GBCS[5] Section 4.3.1 for a full description of the requirements for Identifiers and Counters.

[32] Institute of Electrical and Electronics Engineers

5.7 Message Versioning

Over the lifetime of the Smart Metering solution, it may be necessary to modify existing messages to devices and/or introduce new messages. This section identifies the principles by which these changes will be supported in a controlled manner for the SMETS2+ system and, importantly, without change to the existing Technical Specifications[33].

Each message to a device is defined by a Use Case in the GBCS[5] and is uniquely identified by a MessageCode. In the release of GBCS current at the time of writing there are around 170 message codes in use.

Since there is no specific field defined to hold a version number, it has been proposed that the MessageCode field is used to distinguish between message versions. While it would be possible to structure the MessageCode field to have meaning (e.g. a reduced number of bits for the message identifier and other bits used to indicate version) the benefits of retaining a consistent mapping of message identifier to Use Case is outweighed by the fact that additional development changes may be required to distinguish and act on these sub fields. As such, no further meaning or structure is proposed at this stage to MessageCode and the field will simply distinguish between Use Cases and versions of Use Cases.

Robust configuration management is required to ensure the correct version of a Use Case is used with its respective unique MessageCode and over time different devices will support different versions. The GBCS[5] will provide the primary source of version information. Smart Metering components (e.g. Devices, DSP, Service User systems) will implement and use the required Use Case versions in the GBCS.

Given the need to achieve challenging implementation timescales for the commencement of roll out of the Smart Metering solution a simple and pragmatic approach to configuration management is required and as such there is no current intention to introduce new Use Cases to support Service Discovery[34] although this is not ruled out for future releases. The following principles summarise the approach to message versioning:

1. MessageCode[35] will be used to distinguish different versions of Use Cases by allocating a unique value for each version of the Use Case and its associated message;
2. existing Use Cases and their associated messages with given MessageCodes will not be changed during the life of the Smart Metering solution;
3. new Use Cases and new versions of Use Cases will each be allocated new MessageCodes;
4. new Use Cases and new versions of Use Cases will co-exist in the Smart Metering solution with previous versions of the Use Cases, therefore previous versions are still available unless explicitly withdrawn;

[33] Because the Smart Metering Implementation Programme is at an advanced stage and must meet challenging implementation timeframes. This does not rule out future change for future releases of the solution.
[34] Discovery would allow a Device to be queried for which MessageCodes are supported by it.
[35] Contained in the Grouping Header – see GBCS[5] Section 7.2.7

5. the relevant governance body will decide on a case by case basis whether multiple versions of Use Cases (with different message codes) are exposed through DUIS or whether DSP systems will present a single Service Request and call the appropriate version of Use Case based on certain rules;

6. existing Use Cases may be withdrawn from use (e.g. for Security reasons) in which case a change to GBCS will be issued stating this requirement and the Use Case and corresponding MessageCode of the newer version that should be used;

7. no structured subdivision of the MessageCode field is implied meaning that this field still has the same semantic meaning and no changes are required to its interpretation;

8. devices will be compliant with a given GBCS[5] version which will define the mapping of Use Case versions to MessageCodes;

9. energy suppliers are responsible for determining which version of the GBCS their equipment is aligned to; and

10. any party implementing a change to any device's firmware will, before doing so, have ensured that dependencies with versions of firmware in related devices is understood, that each possible combination of device firmware version has been tested and that distributing a firmware image will therefore not render the solution inoperable.

6 SMETS1 Enrolment

The SMETS2+ smart meter system described in the earlier sections of this document has been preceded by systems based on the SMETS1 specifications. These meters and their Head End system (HES) will be enrolled into the DCC systems to allow a seamless consumer experience and to facilitate standardised communications between Suppliers and SMETS1 meters. The key aspects of this enrolment are explained in the following sections.

6.1 SMETS1 Devices

SMETS1[16] defines three device functions:

- Gas Smart Metering System

  The Gas Smart Metering System (GSMS) is a gas meter with a HAN interface performing similar functions as the GSME defined in SMETS2+[3]. In addition, the GSMS is required to include a WAN interface for communications with the HES, see SMETS1[16] Section 4 for details.

- Electricity Smart Metering System

  The Electricity Smart Metering System (ESMS) is an electricity meter with a HAN interface performing similar functions as the ESME defined for SMETS2+[3]. In addition, the ESMS is required to include a WAN interface for communications with the HES, see SMETS1[16] Section 5 for details.

- In-Home Display

  The IHD is also defined in the SMETS1[16] specifications and is similar to the IHD defined in SMETS2+[3], see SMETS1[16] Section 6 for details.

It must be possible to change the WAN interfaces, which are part of the ESMS and the GSMS, without the need to replace the entire meter. Several SMETS1 ESMS and GSMS implementations use a cellular WAN radio module which can be easily exchanged.

The SMETS1 specifications do not describe or mandate other functions mandated by the SMETS2+ specifications; these functions and devices may be added to a SMETS1 Smart metering system:

- PPMID
- CH
- CHF
- GPF
- HCALCS
- ALCS
- HHT

Similar to the SMETS2+[3] specifications the Consumer Access Device is mentioned in SMETS1[16] but is not specified further.

In terms of communication with the SMETS1 devices via the DUIS interface S1SR[17] distinguishes the following devices and functions:

- SMETS1 CHF;
- SMETS1 ESME;
- SMETS1 GSME;
- SMETS1 GPF;
- SMETS1 PPMID;
- SMETS1 IHD; or
- any other device operating on a home area network created by a SMETS1 CHF.

As per SEC[2] - Section F2.1(b) SMETS1 devices are not required to have CPA certification. Following from SEC[2] – Sections G3.26, G327 and G3.28 the Responsible Supplier has to ensure that SMETS1 Smart Metering Systems are secured to an Appropriate Standard and that documentation is retained.

6.2 SMETS1 Communications and Architecture

The SMETS1 specifications mandate the use of a SMHAN based on open standards for the communication between devices but does not specify the actual technology and protocols.

Typical SMETS1 SMHANs use ZigBee ZSE communications in the 2.4 GHz radio frequency band.

Equally the protocol for the communication between the Supplier and the SMHAN is not governed by SMETS1[16], also the format of end-to-end messages between devices and the Supplier is not prescribed by the SMETS1[16] specification.

The typical SMETS1 system uses a cellular wide area network which connects the meters with the HES; the communication between the HES and the Supplier uses a WAN.

In the SMETS2+ system the Communications Service Provider (CSP) handles the communication between the DCC the and Smart Metering Network installed at the premises; the CSP services are assigned for defined geographic areas (as detailed in Section 3.4.2). The CSP functionality does not exist in SMETS1 systems and each HES uses its selected cellular communications service provider. This results in overlapping geographical footprints of the different HES systems.

The high level system architecture of a typical SMETS1 system is shown in Figure 6.2 below.

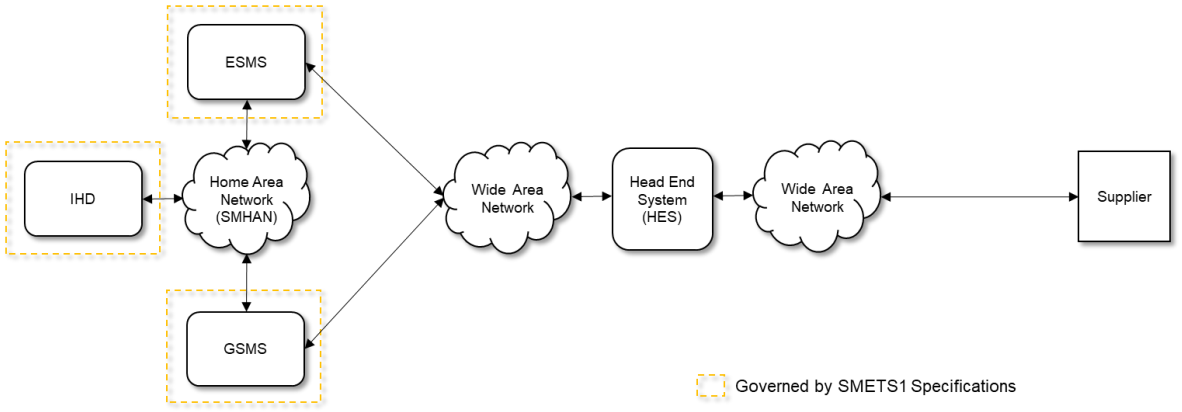

Figure 6.2: SMETS1 System Architecture

6.3 SMETS1 HES compatibility

The system architecture of the SMETS1 system described in Section 6.2 shows a single Supplier communicating with a single HES. It is also possible that the same HES provides communication services to several Suppliers.

Since the SMETS1[16] specifications do not define communications protocols and technologies, the actual HES implementations differ according to the solutions and protocols selected. This results in the connection to the HES and the functionality offered to Suppliers being specific to the actual HES implementation.

This may lead to possible incompatibilities in case of a CoS event: If the gaining and loosing Suppliers both use the same HES, then the communications with the meter may be possible following the CoS event; if the gaining and loosing Suppliers use two different HES, the communication with the meter may not be possible after the CoS event.

6.4 Enrolment of SMETS1 into the DCC Systems

As laid out in Section 6.3 above, the connection between the Supplier and a SMETS1 HES results in a number of challenges, in particular around CoS events:

- Bespoke Supplier connection to HES;
- Specific protocols used for a particular HES implementation; and
- Varying functionality for device commands, responses and alerts.

These challenges are mitigated by the enrolment of SMETS1 meters into the DCC systems and offer Suppliers a single interface for communications with SMETS1 and SMETS2+ devices. This ensures continuation of smart metering services for the consumer and the gaining Supplier after the CoS event.

This single interface is realised by updating DUIS[6] to version 3.1 and MMC[7] to version 3.1 introducing Service Requests targeted at SMETS1 devices; equally responses and alerts for SMETS1

devices have been defined. Details on the Alert Codes can be found in S1SR[17] Section 8. This preserves the communication interface between Suppliers and the DCC explained in Section 4.2.5.

Additional information relating to identifiers and counters used by the DUIS interface for SMETS1 related Commands and Responses can be found in S1SR[17] Section 6; the SMETS1 related Message Codes are documents in S1SR[17] Section 9.

Note that GBCS[5] is not supported for the communication with SMETS1 devices and therefore Section 4.2.5.1 Parse & Correlate and Section 4.2.5.4 Great Britain Companion Specification (GBCS) do not apply to SMETS1.

In the lower layers the communications protocol and the connection between the Supplier and the DCC have been maintained as depicted in Figure **Error! Reference source not found.** allowing simultaneous use for communications with SMETS1 and SMETS2+ devices. The DCC is connected to all enrolled SMETS1 HES and routes the messages for a particular metering device from the DCC Service User to the target HES associated with the metering device. The HES then is responsible for routing the message to the target metering device. Responses and alerts from the metering devices are routed to the HES, forwarded on to the DCC and then delivered to the target DCC User. The SMETS1 HES is also referred to as SMETS1 Service Provider (S1SP) in S1SR[17] and DUIS[6].

Figure 6.4 below shows the connectivity between multiple Suppliers and multiple SMETS1 HES via the DCC Systems:

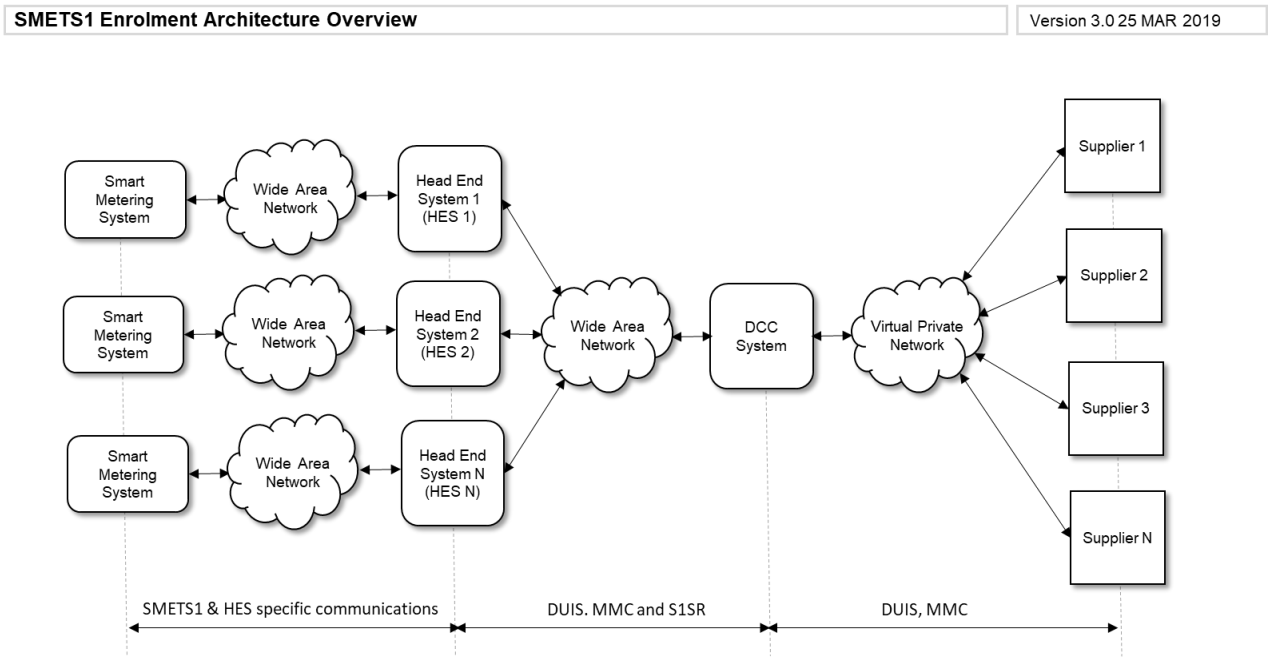

Figure 6.4: SMETS1 Enrolment Architecture

6.5 Globally Unique Entity Identifiers SMETS1

All organisations sending and receiving SMETS1 messages through the DCC are identified by their Organisationally Unique Identifier (OUI); see Section 5.6 for details.

SMETS1 devices enrolled into the DCC System are identified by their EUI64 address; this address is stored in the Smart Meter Inventory in the DCC System and is used for communications with the device when sending Service Requests, returning Responses and forwarding of device Alerts to the DCC user.

6.6 SMETS1 Business functions relating to Smart Metering Equipment

The enrolment of SMETS1 devices and HES into the DCC System makes most of the business functions listed in Table 4.1.3 available to DCC Users and consumers; the detailed requirements are contained in SMETS1[16], DUIS[6] and S1SR[17].

Suppliers are able to remotely join the PPMID with meters in SMETS1 using DUIS Service Requests which are forwarded to the targeted HES; see Ref. S08 in Table 6.6 below. The HES then converts this to the message format required for the target device; these formats and the joining methods are not defined in SMETS1[16] and are specific to the HES.

Table 6.6 below lists those business functions which are supported for SMETS1:

Ref	Name	Description
Consumer Functions		
C01	Information Display	The Consumer is able to read pricing and consumption data generated within the Smart Metering Equipment (SME).
C02	Enable Supply	The Consumer is able to enable the energy supply to the premises manually
C03	Pre-pay	The Consumer is able to add pre-pay credit and activate emergency credit to the SME.
Smart Metering Functions		
M01	Recording	The SME is able to record energy consumption and billing data in relation to time of use and block pricing tariffs. See SMETS1[16] Sections 4.3.7 & 4.3.8 and 5.3.7 & 5.3.8.
M02	Tariff	The SME is able to apply Time of Use (TOU) and Block pricing tariffs and switch between tariffs according to entries in the Tariff and measured consumption.
M03	Supply Control	The SME is able to Arm and Lock energy supply through remotely initiated commands and additionally according to defined rules when operating in pre-payment mode. See SMETS1[16] Sections 4.4.2.2 & 4.4.2.3 and 5.4.3.2 & 5.4.3.3.
M06	Event Recording & Alerting	The SME is able to record various events that occur during its operation in logs that are held on each device as well as sending Alerts for certain events across the SMHAN and SMWAN to authorised remote parties. See S1SR[17] Section 8 for a full table of Events and Alerts.
M07	Credit & Pre-payment	The SME is able to operate in both credit and pre-payment modes and maintain the current meter balance. When in pre-payment mode, the SME is able to accept prepayment credits from the Consumer. See SMETS1[16] Sections 4.3.6 and 5.3.6.
M08	Information Display and Provision	The SME is able to display information to the Consumer including energy consumption on the meters and In Home Display.
Service User Functions		

Ref	Name	Description
S01	Product Management	Functions in this category allow a DCC Service User to manage the mode of operation, price or tariff at a specified meter and for the meter to update its configuration to that effect. This service may be initiated by a variety of events, such as: • Change of Tenancy (CoT) • Change of Supplier (CoS) • New product offerings • Customer initiated • Supplier price changes Sub functions (see DUIS[6] version 3.0 for more detail) • Update Import Tariff • Update Price • Update Meter Balance • Update Payment Mode
S02	Prepay	Functions in this category enable a DCC Service User to manage their prepayment metering estate such that credit can be purchased, prepayment specific configurations can be amended, and debt can be managed. In managing their Prepayment metering estate, DCC Service Users may experience the following business events that initiate use of a Prepay service request: • following a business event (such as CoT or CoS) a DCC Service User wishes to amend one or more of Prepayment configuration (e.g. non-disconnection calendar), and / or debt register values; • a customer makes a prepayment credit purchase resulting in a request to send a prepayment top up to the device to apply the credit purchase to the device registers; or Sub functions (see DUIS[6] version 3.0 for more detail) • Update Prepay Configuration • Top Up Device • Update Debt • Activate Emergency Credit
S03	Customer Management	Functions in this category enable DCC Service Users to manage customer facing elements of a device at a specified meter. Sub functions (see DUIS[6] version 3.0 for more detail) • Restrict Access To Data For Change Of Tenancy • Clear Event Log
S04	Reading	Functions in this category enable a DCC Service User to retrieve an entry from various logs, counters, profile and configuration data on a specified device, or read the import or export register values at a point in time, of a specific device so that the DCC Service User can obtain

Ref	Name	Description
		Electricity or Gas Smart Metering Equipment consumption and usage details. Sub functions (see DUIS[6] version 3.0 for more detail) • Read Instantaneous Import / Export Registers • Read Instantaneous Prepayment Values • Retrieve Billing Data Log • Retrieve Import / Export Daily Read Log • Read Import / Export Profile Data • Read Network Data • Read Tariff • Read Prepayment Configuration • Read Prepayment Daily Read Log • Read Active Power Import • Read Meter Balance
S05	Scheduling	Functions in this category enable a DCC Service User to request that the DCC creates, maintains and operates a schedule of regular and repeating actions for a specified device. Billing data retrieval schedules are not part of this service. Sub-functions (see DUIS[6] version 3.0 for more detail) • Create Schedule • Read Schedule • Delete Schedule
S06	Device Management	Functions in this category allow a DCC Service User to manage the products/operating settings associated with a specific device. Sub-functions (see DUIS[6] version 3.0 for more detail) • Read Device Configuration (e.g. Voltage, Randomisation, Billing Calendar, Payment Mode, Event and Alert Behaviours, etc) • Update Device Configuration (e.g. Voltage, Load Limiting, Billing Calendar, Gas Flow, etc) • Synchronise Clock • Read Event or Security Logs • Issue or Update Security Credentials • Request Handover Of DCC Controlled Device • Read Device Log • Retrieve Device Security Credentials • Update Security Credentials (Change of Supplier) • Set Electricity Supply Tamper State

Ref	Name	Description
S07	Supply Management	Functions in this category enable an authorised DCC Service User to remotely manage the energy at a consumer premises without the need for local interaction. Sub-functions (see DUIS[6] version 3.0 for more detail) • Enable Supply (Electricity only) • Disable Supply • Arm Supply • Read Supply Status
S08	Device Estate Management	Functions in this category allow a DCC Service User to manage a device within the DCC estate such as commissioning, decommissioning, joining and un-joining devices moved in or out of the DCC estate or to confirm information held within the DCC for a specific device. Sub-functions (see DUIS[6] and S1SR[17] for more detail) • Commission / Decommission Device • Read / Update Inventory • Join / Unjoin Service • Read Device Log • Update Device Log(s)
S10	This row is intentionally blank	
S11	Firmware	Functions in the category enable a DCC Service User to upgrade the firmware on an ESME or GSME, e.g. following a firmware fix (or up-to-date version) being released by the meter manufacturer. Sub-functions (see DUIS[6] version 3.0 for more detail) • Update Firmware • Read Firmware Version • Activate Firmware
S12	Pre-Device Installation	Functions in the category enable a DCC Service User to provide device details to the Smart Metering Inventory to start the Smart Metering installation and commission process. Sub-functions (see DUIS[6] version 3.0 for more detail) • Device Pre-notification
S13	This row is intentionally blank	

Table 6.5: SMETS1 Business functions relating to Smart Metering Equipment

6.7 Time Management SMETS1

The time used for timestamps in SMETS1 for sending Responses and Alerts originates from the SMETS1 devices; where the time from a device is not available the SMETS1 Service Provider has to populate the timestamp with a UTC time value. The UTC time value must be within ten seconds of UTC.

7 Glossary

Access Control

Access control refers to exerting control over whom or what can interact with a specific resource.

Access Control Broker (ACB)

A system component that receives requests, encodes device specific messages, applies security controls to those messages and then routes those messages to the required device. Other functions such as command scheduling are also provided.

Alerts

A warning generated in response to a problem or the risk of a potential problem.

Anomaly Detection

The identification of either spurious transaction volumes or inappropriate command sequences based upon defined thresholds.

ASN/1

Abstract Syntax Notation One; ASN.1 is a standard notation for the definition of data types and values.

Certification Authority (CA)

A trusted entity which issues Public Key Certificates.

Consumer Identification Number (CIN)

A message that is sent to a consumer's device which can then be read off the device to aid identification.

Certificate Signing Request (CSR)

An electronic document sent to a Certification Authority to request the issue of a Public KeyCertificate.

Change of Supplier (CoS)

The process initiated by a consumer resulting in a change of ownership with respect to their Registered Energy Supplier.

Code of Connection

A mandatory set of requirements placed on a party connecting to a service provider (DCC Service User to DSP, DSP to CSP), to enable security, resilience and fairness of service to be maintained for all service users.

Communications Service Provider (CSP)

The service provider delivering and managing the SMWAN infrastructure and Communications Hubs to enable remote communication and management of SME across the whole of Great Britain.

Conceptual Architecture

A conceptual architecture is the highest level or most abstract model of a system. Its purpose is to allow early communication of key concepts of a solution to key stakeholders against which subsequently further design detail is aligned.

Confidentiality

Ensuring that information, in transit or at rest, is not accessible by unauthorised parties through either unintentional means or otherwise.

Consumer Premises Equipment (CPE)

All Smart Metering equipment installed and operated in relation to an individual consumers energy supply.

Consumer Access Device (CAD)

A device that provides consumers with access to consumption and pricing data.

CoS Party Private Key

The key in a Public-Private Key Pair which must be kept secure and used by the CoS Party.

CoS Party

The trusted party authorised on behalf of industry to change a Registered Supplier's credentials as part of the Change of Supplier.

CoS Transitional Service

The CoS Transitional Service will digitally sign all CoS service requests, once successfully authenticated, received from Registered Suppliers, using the CoS Party Private Key

Critical Alerts

Critical Alerts are alerts generated in response to Critical commands or initiated as a result of local events that may affect energy supply to Premises, the security of Devices or to lead to financial fraud.

Critical Commands

Commands that may affect energy supply to Premises, the security of Devices or to lead to financial fraud.

Data Communication Company (DCC)

The new entity that has been created and licensed to provide smart meter communication services. The DCC is responsible for the procurement and contract management of data and communications services, providing remote access to Smart Metering equipment.

Data Service Provider (DSP)

The company awarded the contract to provide central operational IT services to the Data Communications Company (DCC).

DCC User Interface

Used to connect the systems used by or on behalf of the DCC Service Users and/or operators of Other Energy Industry Systems (as opposed to Systems used by or on behalf of the DCC, any DCC Service Provider or any Contractor Person) to the DCC Services and/or relevant DCC & Contractor Systems.

DCC Service Users

Refers to the organisations that use the DCC to access metering equipment in consumers premises for energy related purposes.

DCC SMWAN Gateway Interface

This is an interface specification internal to DCC that provides a single set of services to the DSP for the transportation of DCC Service User requests, Responses and Alerts between the DSP and SME.

DCC User Network

The network connectivity utilised to connect DCC Service Users to the DCC.

Decryption

The process of converting encrypted information by an Authorised party to recover the original information.

Demand Side Management

Entails actions that influence the quantity or patterns of use of energy consumed by end users, such as actions targeting reduction of peak demand during periods when energy supply systems are constrained.

Device

A Device that is one of ESME, GSME, Gas Proxy Function, Communications Hub Function, Type 1 Device or a Type 2 Device which constitutes Smart Metering Equipment.

Digital Signature

A piece of information appended to a message which is created using the sender's Private Key, can be verified using the sender's Public Key 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.

Digital Signing Private Key

A private key used for digital signing.

Distribution Network Operator (DNO)

The term 'Distribution Network Operators' refers collectively to electricity distribution and gas transportation companies that are responsible for the gas and electricity networks that deliver energy to consumers' homes / business premises. Network Operators must hold a Licence issued by OFGEM and comply with all Licence Conditions for networks that they own and operate.

DLMS/COSEM

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

Dual Band Communications Hub (DBCH)

A Communications Hub capable of supporting a SMHAN at 2.4GHz and Sub-GHz frequencies simultaneously.

Encryption

The process of converting information in order to make it unintelligible other than to authorised parties.

Electricity Smart Metering Equipment (ESME)

Used for measuring Electricity consumption (SMETS2+ terminology).

Electricity Smart Metering System (ESMS)

Used for measuring Electricity consumption (SMETS1 terminology).

Firmware

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

Gas Proxy Function (GPF)

A logical Device hosted on the Communications Hub and connected to the SMHAN that holds replicated data provided to it by the GSME.

Gas Smart Metering Equipment (GSME)

Used for measuring gas consumption (SMETS2+ terminology).

Gas Smart Metering System (GSMS)

Used for measuring gas consumption (SMETS1 terminology).

Globally Unique Identifier (GUID)

A GUID is tightly bound to the Device that it identifies by physical means (for example, a barcode etched in the device casing) and by electronic means (for example, a 'write once' data item set at manufacture).

Head End System (HES)

The HES provides communication services between the smart meter infrastructure and the Supplier in SMETS1 systems. The HES is also referred to as SMETS1 Service Provider (S1SP) when enrolled into the SMETS2+ system.

Home Automation Controller

Connected to the SMHAN or to a Consumer Access Device, this device allows a consumer to control white goods within the home based upon consumption and/or pricing data made available via the SMHAN.

HSM

A type of secure cryptographic processor for the management of digital keys, accelerating cryptographic processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. These modules are normally separate physical devices that traditionally come in the form of a plug-in card.

In Home Display (IHD)

A device that provides consumers with access to consumption and pricing data.

Key Agreement

A Key Agreement is a means by which two parties can agree a shared Private Key for use in cryptographic algorithms, which is known to both parties but which is never sent between the two.

Logical Architecture

A logical architecture is business and technical model of a system where specific details of the physical implementation are avoided thus providing a higher level model which can be implemented in different ways or with different technologies but still satisfying the same business requirement.

Message Authentication

This provides the receiver with assurance that the sender is who they claim to be, and the message is as sent by the sender. This relies on a secret key known by the sender and the receiver of the message. A third party would not be able to tell which party created the message, since both sender and receiver know the secret key.

Message Authentication Code (MAC)

A piece of information calculated from a message and appended to it by the sender which allows Message Authentication by the receiver.

MPxN

Term used to refer to either:

- MPAN - Meter Point Administration Number (MPAN), each electricity supply point in Great Britain, such as that to a Consumer's home, is identified by a unique 21 digit MPAN; or
- MPRN - Meter Point Reference Number relates to gas supply.

Non Critical Commands

Any command not deemed to be a Critical Command.

On Demand Service Requests / Commands

An On Demand Service Request is a request which requires a real-time response since it is likely the business process using the service request is designed such that the end user waits for that response and the system they are prevents further interaction while waiting. In contrast to this, scheduled or future dated service requests will not result in a real time response and so the business process is likely to allow the end user to continue with the systems capturing responses or Alerts separately.

Other DCC Service Users

An organisation, other than a consumer's Registered Energy Supplier or Relevant Distribution Network Operator, which can use the DCC's energy related services.

OUI

Organisationally Unique Identifier. See also GUID

Physical Architecture

A physical architecture is the lowest level business and technical model of a system where specific products, technologies and specifications are defined that meet the requirements of the Logical Architecture.

Prepayment Metering Interface Device (PPMID)

Provides functionality to facilitate the use of prepayment services by consumers.

Private Key

The key in a Public-Private Key Pair which must be kept secure by its owner.

Public-Private Key Pairs

These are two numbers which are mathematically related and are for use in cryptographic algorithms. One of the numbers is designated the Private Key, and should never be circulated beyond the party owning it, while the other number is designated the Public Key and can be circulated to other parties.

Public Key

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

Public Key Certificate

An electronic document issued by a Certification Authority which confirms the ownership of a Public Key.

Recovery

The process of reassigning any of the Public Key Certificates on a device should a compromise occur of the corresponding Private Key.

Reference Architecture

A Reference Architecture provides a template architecture which can be applied to multiple domains.

Registered Supplier

The identity of the DCC Service User registered by the consumer as either their Import or Export supplier for whom the SME is managed.

Remote Party Message

Messages that are submitted by DCC Service Users who are remote from the smart metering equipment.

Role

Specifies a role played by a user or any other system that interacts with the subject/resource. A Role for a resource is the grouping of access rights to Commands with the access controls for each of the Roles defined through RBAC.

Role Based Access Control (RBAC)

A mechanism to define which Roles have what type of permissions to commands, services and messages associated with individual resources.

Security Credentials

Data used to identify and Authenticate an individual or system.

Sensitive Data

Data within a message which needs to be kept confidential during transit. Data can be kept confidential by using encryption.

Service User

A user of DCC services, for example an energy Supplier or Distribution Network Operator.

Single Band Communications Hub

A Communications Hub capable of supporting a SMHAN at 2.4GHz only.

Smart Metering Equipment (SME)

Smart Metering Equipment is equipment that meets SMETS2+ specifications.

Smart Metering Equipment Technical Specifications 1 (SMETS1)

Refers to the Smart Metering Equipment Technical Specifications Version 1.2 in SEC - Schedule 9.

Smart Meter Equipment Technical Specification 2+ (SMETS2+)

Refers to the Smart Metering Equipment Technical Specifications Version 2.0 or higher in SEC - Schedule 9.

Smart Meter Home Area Network (SMHAN)

A short range network that is present within the proximity of the consumer's premises and exists for the purposes of providing a defined set of message protocols and secure connectivity for SME to communicate with one another.

Smart Meter Wide Area Network (SMWAN)

A network infrastructure provided to enable the sending and retrieval of information between the DCC and SME installed and commissioned for operation through the DCC.

Smart Meter Implementation Programme (SMIP)

The programme responsible for working with industry to deliver the smart metering system.

Target Operating Model (TOM)

A high-level design of the future operating model for Smart Metering.

TOGAF

The Open Group Architecture Framework.

Trust Models

A method to identify the trust relationships that must be in place for the business process to operate effectively.

Trusted Source

A source whose identity is confidently and reliably validated.

Type 1 Device

A Device connected to the SMHAN that is allowed to issue or perform a range of SMHAN Interface Commands and can update the information stored in GSME, ESME or a GPF.

Type 2 Device

An IHD or any other Device connected to the SMHAN that enables a Consumer to read the information stored in ESME or a GPF.

Unique Transaction Reference Number (UTRN)

A cryptographic code used to convey prepayment top-up credit through human transfer to a GSME or ESME operating in prepayment mode.

Use Case

A list of steps, typically defining interactions between a role and a system, to achieve a goal. The term Use Case is used in GBCS to define a message interaction.

Zachman

The Zachman Framework of enterprise architecture developed by John Zachman.

ZigBee Smart Energy (ZSE)

A communications protocol for smart metering. See ZigBee Smart Energy Profile Specification [11].

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

secas@gemserv.com